



Aino Herranen

Building an Export Compliance Framework

Intangible Technology Transfer – Software offerings

Metropolia University of Applied Sciences

Master's Degree

Degree Programme in Business Informatics

Master's Thesis

16.04.2024

Abstract

Author: Aino Herranen
Title: Building an Export Compliance Framework
Intangible Technology Transfer – Software offerings
Number of Pages: 83 pages + 5 appendices
Date: 16 April 2024

Degree: Master of Business Administration
Degree Programme: Business Informatics

Instructor: Antti Hovi, Senior Lecturer

The objective of this thesis was to develop an export compliance framework to verify and monitor the export compliance of software offerings. After the tumultuous events at the beginning of the 2020s, economic sanctions have affected numerous exporting companies worldwide. Additionally, advancements in digital infrastructure are making export control restrictions increasingly complex. Non-compliance with foreign trade laws poses legal, financial, and reputational risks. The export compliance framework for software technologies has been incorporated into the sponsor company's 2023 Trade Compliance development plan.

This study commenced by reviewing relevant multilateral and national trade regulations related to the export control of software and technology. Using the existing knowledge, a conceptual framework was constructed to serve as a basis for supporting the co-creation process of the software export compliance framework. The co-creation process underwent multiple iterations and included several stages of data gathering. Subsequently, the current state analysis was conducted to examine the existing practices of Digital Services at the sponsor company. Drawing upon the conceptual framework and the results of the current state analysis, a proposal for the export compliance framework was formulated. Finally, the export compliance framework underwent refinement with input from key stakeholders of the sponsor company to produce the final outcome.

During the study, a clear need was identified to enhance risk mitigation in the export compliance process of software products within the organization. The framework was divided into two separate documents to address both, business conduct and the resource and responsibility matrix of software export compliance. The outcome is an export compliance framework that assists in mitigating the risks associated with the export control process of software offerings in the sponsor company.

Businesses operating in the software and technology sector should take proactive measures to adapt to emerging regulations, particularly in response to anticipated EU directives concerning the export of intangible technologies and the growing influence of geopolitically motivated protectionism. In this constantly evolving landscape, it is imperative to acknowledge that the regulations examined in this thesis reflect the state of affairs in 2023. It remains essential to verify current regulations whenever up-to-date information is needed.

Keywords Trade Compliance, Export Control, Intangible Technology

Contents

List of Figures

List of Tables

Glossary

1	Introduction	1
1.1	Business Context	1
1.2	Business Challenge, Objective and Outcome	2
1.3	Thesis Outline	2
2	Method and Material	4
2.1	Research Approach	4
2.2	Research Design	6
2.3	Data Collection and Analysis	8
3	Existing Knowledge and Regulations on Export Compliance for Software Technology Products	11
3.1	Background of export controls	11
3.2	The Wassenaar Arrangement	13
3.2.1	Software Technology Export Controls	14
3.2.2	Category 5 part 2 - Information Security	17
3.3	The United States Export Controls	19
3.3.1	Example of an export control classified software product	22
3.3.2	The Ten General Prohibitions	24
3.4	The European Union Export Controls	27
3.4.1	Export control of software and technology	28
3.5	Existing Compliance Frameworks and National Software and Technology Export controls	32
3.5.1	Information security	37
3.6	Conceptual Framework of This Thesis	40
4	Current State of Software Export Control in the Organization	42
4.1	Overview of the Current State Analysis	42
4.2	Description of Trade Compliance - Export Controls in Sponsor Company	43
4.3	Description of Digital Services	44
4.3.1	People - Organizational structure	44

4.3.2	Process - Software Supply	47
4.3.3	Product – Marine advisory system	49
4.4	Current State of Tangible Export Compliance - Strengths and Weaknesses	51
4.5	Key Findings based on PPP matrix	55
5	Initial Proposal for the Export Compliance Framework	58
5.1	Overview of the Proposal Building Stage	58
5.2	Findings from Data 2	60
5.3	Summary of the Initial Proposal	65
6	Validation of the Proposal	71
6.1	Overview of the Validation Stage	71
6.2	Validation by Subject Matter Experts	71
6.2.1	Developments to People, Process and Product elements of the Initial Proposal	72
6.3	Final Proposal	75
6.4	Recommendations for Next Steps	77
7	Conclusion	79
7.1	Executive Summary	79
7.2	Evaluation of the Thesis Objectives vs. Outcomes	82
	References	1

Appendices

Appendix 1. Project team interview frame

Appendix 2. Inquiry Regarding Export Control in Software Sales


Appendix 3. Preliminary Red-flag list

Appendix 4. Internal division interview frame

Appendix 5. The revised red-flag identification for Sales

Appendix 6. The WRITTEN STATEMENT on the use of AI-based tools in this thesis

List of Figures

- Figure 1. Research paradigm (adapted from: Patel 2015).
- Figure 2. Research design of the Thesis.
- Figure 3. The four main categories of export control.
- Figure 4. Categories of the List of Dual-Use Goods and Technologies.
- Figure 5. CCL Categories and Product Groups with an example of Category 3, Product Group D. "Software".
- Figure 6. Capture from the Commerce Control List Supplement No. 1 to Part 774 Category 4.
- Figure 7. Capture from the Official Journal of the European Union Category 4.
- Figure 8. Definition of 'technical assistance' in Regulation (EU) 2021/821 (2021, 7).
- Figure 9. PPT-Framework with ECP and ICP themes grouped under each element.
- Figure 10. Conceptual framework of this thesis.
- Figure 11. 
- Figure 12. Sales through internal sales unit. The black arrow represents the customer value creation and the green arrow the revenue stream. External entity marked with blue colour.
- Figure 13. Sales to external service provider without visibility to the end customer. The black arrow represents the customer value creation and the green arrow the revenue stream. External entity marked with blue colour.
- Figure 14. Software and Technology export delivery models in the organization.
- Figure 15. 3rd party software registry headlines.
- Figure 16. Initial Red-flag identification document.
- Figure 17. Initial export compliance matrix.
- Figure 18. Final export compliance matrix.

List of Tables

- Table 1. Details of Data collections 1 to 3
- Table 2. Internal documents used in the proposal building, Data 2.
- Table 3. Agencies responsible for enforcing Export Control Regulations in the United States
- Table 4. General Prohibitions (GP) 1 to 3 relate to the product classification based on CCL.
- Table 5. General Prohibitions (GP) 4 to 10 relate to End user, End-use and other controls.
- Table 6. Summary of export definitions and general export authorizations EU007, EU008 (Regulation (Eu) 2021/821, Annex II, 438-440.)
- Table 7. Key elements in US ECP and EU ICP.
- Table 8. Software export control regulation in the NL, UK and US.
- Table 9. People - Digital Service project team and Management.
- Table 10. Questionnaire on following internal Global Trade Instructions regarding export control (EC).
- Table 11. Current state of Export Control (EC), based on the results of Global Trade Risk Assessment.
- Table 12. Key findings from CSA for the current Export control of Intangible Technology Transfers.
- Table 13. Correlation of Data Collection 2 with Current State Analysis and Existing Knowledge
- Table 14. [REDACTED]
- Table 15. The project teams insights for Proposal building.
- Table 16. Insights and Pain Points from the Internal Division.
- Table 17. Expert suggestions (People) for the Initial proposal.
- Table 18. Expert suggestions (Process) for the Initial proposal.
- Table 19. Expert suggestions (Product) for the Initial proposal.

Glossary

BIS	Bureau of Industry and Security (US)
CCL	Commerce Control List (US)
CTCO	Country Trade Compliance Officer
Dual-use	Goods, software or technology that can be used for both civilian and military purposes
EAR	Export Administration Regulations (US)
ECCN	Export Control Classification Number (US)
ECP	Export Compliance Programme (US)
ECRA	Export Control Reform Act (US)
GP	General Prohibitions (US)
ICP	Internal Compliance Programme (EU)
MFA	Ministry for Foreign Affairs of Finland
PCE	Product Classification Engineer
PPT	People, Process, and Technology framework
PPP	People, Process, and Product matrix
TCO	Trade Compliance Officer
WA-list	The Wassenaar Arrangement list of dual-use goods & technologies and the munitions list.

1 Introduction

Throughout history, countries have implemented export controls as a strategic tool to achieve their foreign policy goals. These controls undergo continuous adjustments, aligning with changes in the security dynamics of a nation, its region, and the international context. Export controls are fundamentally characterized by their political nature, multilateral involvement, and responsiveness to global events (Aoi 2016, 1).

In the aftermath of the tumultuous events at the beginning of the 2020s, economic sanctions have affected many exporting companies worldwide. Simultaneously, revolutionary advancements in digital infrastructure, such as artificial intelligence and big data analytics, have propelled discussions on regulations governing software and technology export controls in many of the leading nations. The key objectives include safeguarding competitive advantages and protecting citizens from emerging threats like electronic surveillance by other nations. Considering the significant changes in this domain, export control restrictions are set to become increasingly complex. (Katterbauer 2023) Given the lack of maturity in multilateral processes and national regulations, companies involved in software and technology business should proactively prepare to adopt new restrictions and controls as they are introduced.

1.1 Business Context

The sponsor company of this thesis is a division of a leading technology corporation. The division in question concentrates on sustainable and intelligent shipping solutions. In Finland, the division employs around 500 maritime specialists. In intelligence shipping, automation is a growing trend, consequently the demand for more advanced software solutions will be expanding.

In the beginning of 2022, the sponsor company was involved in a group level workshop programme which dove into the export control classification of software offerings. The workshop programme included external consultants that were the experts in the US export control of software and cloud computing. This workshop programme was put on hold in March 2022 due to business effect of the Ukraine war. The local Trade Compliance organization was completely occupied with keeping up to date with all the different sanctions raised by different entities globally. This was a crash course to the different economic export control regulations laid out globally.

1.2 Business Challenge, Objective and Outcome

During the second quarter of 2022, distinct improvement areas were identified among the export control processes of the sponsor company. It was deemed necessary to establish a well-defined operational process that would be regularly maintained and updated as the different sanctions continue to be updated frequently.

The challenge for this thesis is to address the absence of export compliance process for software offerings amid the foreseeable EU regulations on intangible technology exports and increasing geopolitically driven protectionism. First, there is a clear demand to improve risk mitigation on the export compliance process of software products in the organization. Risks from non-compliance of foreign trade law regulations can be legal, financial and reputational. Second, the macroeconomic trends of the global economic shift with increased protectionism will continue to affect the organizations that engage in export activities. Most importantly, there is no longer a possibility to not pay attention to the exports that are intangible in nature. What the technology industry has learned from the aftermath of 2022 unprecedented economic sanctions, and the uncertainty of the global treaties, is that companies must be pro-active in their trade compliance efforts.

The Objective of this thesis is *to develop an export compliance framework to verify and monitor the export compliance of software offerings*. The Outcome is an export compliance framework which should assist the risk mitigation of the export control process of software offerings in the sponsor company.

The supervisor for the thesis will be the divisions Trade Compliance team and the local Trade Compliance Officer. The export compliance framework for the software technologies has been included to the division's trade compliance 2023 development plan. The Trade Compliance team is taking a lead role in the execution; however, the building phase will be a co-creation effort together with the divisions Digital Solution Experts.

1.3 Thesis Outline

To develop the export compliance framework, first, existing export control regulations will be explored to identify the applicable best practices. Second, data will be collected from internal experts from the division through interviews and data analysis. The study will include the investigation of the current state of digital service offering regime in the

division with interviews from relevant specialists. Based on the collected data, the current state analysis will be concluded from the Trade Compliance point of view.

Subsequently, the co-creation of the export compliance framework will commence. An action-based research method will be used including internal documents analysis and regular dialogues with internal and external stakeholders. At the end, the study will evaluate the program based on validation and feedback from the leading experts from the Country-level of the organization.

2 Method and Material

This section describes the research approach, research design, and data collection and analysis methods used in this Thesis.

2.1 Research Approach

A blueprint for traditional research can be considered to consist of the following steps as shown in Figure 1.

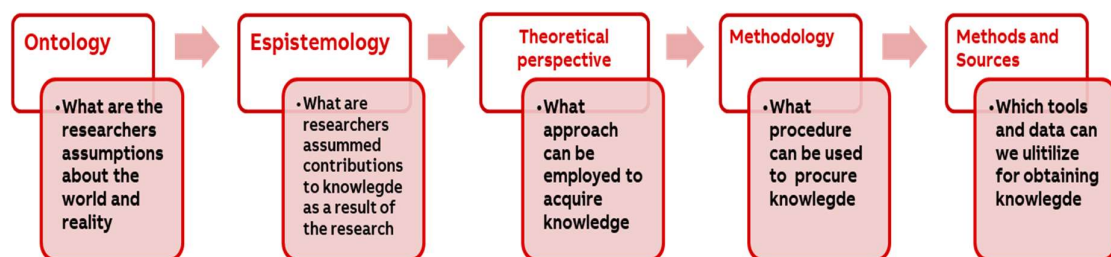


Figure 1. Research paradigm (adapted from: Patel 2015).

Research philosophy can be defined as a set of beliefs and assumptions about the development of knowledge. It encompasses the understanding of how knowledge is created, the nature of that knowledge, and how it relates to research. A well-thought-out and consistent set of assumptions forms a research philosophy that guides the methodological choice, research strategy, data collection and analysis procedures of a project. It requires the researcher to become aware of and actively shape the relationship between their philosophical position and the research they conduct. (Saunders et al. 2019, 159-160).

The theoretical approaches used in research are basic, applied and action research. The basic, or fundamental, research seeks to develop novel theories. Applied sciences aim to study current theories and assess their applicability. Action research is the utilization of the most effective approaches to actual application. This harsh divide between the approaches has conjured some criticism since it can be seen as a hindrance for today's dynamic innovation processes. According to Narayanamurti 2017, from Harvard University, the traditional dichotomy between fundamental and applied research is outdated and can be detrimental to scientific progress. We should instead come up with

a method of considering, organizing, and financing science as a cycle of discovery, then invention, and back again. This concept could remove the boundaries between fields and encourages collaboration. (Powell 2017.) Moreover, in the digital age, when quantitative data is easily accessible, some scientists believe that the value of collaborative field studies is at risk of being disregarded. Thus, more qualitative research is needed. (Berente & Recker 2021, 25:45).

One of these collaborative approaches is the Applied action research. Applied action research is a combination of research and development that is used to bring about change and improvement in organizations. It is a more focused type of Action research, with fewer iterations, and seeks to achieve tangible outcomes rather than simply researching the process of change. Its aims can include making improvements to processes, activities, products, services, and situations. Through the use of research techniques, data is accumulated, documented, and examined to obtain results that are both valid and innovative. The ultimate goal of Applied action research is to create a positive transformation. (Kananen 2013, 20-22.)

The most used methodologies used in Applied action research are qualitative and mixed research methods (Kananen 2013). Purely quantitative methods can be considered sub-optimal for this research approach due to the aim of producing an implementable and tangible change. However, through mixed methods, a combination of quantitative and qualitative methods such as register-based data or structured questionnaires, a methodological eclecticism could be reached where the research methods have been elected to best support the solving of the research question (Tuomi & Sarajärvi 2018, 78-79). Qualitative research methods have been described as “soft science” compared to the more strict quantitative methods. Qualitative methods focus on understanding the meanings, beliefs, experiences, and motivations behind people's behavior (Tuomi & Sarajärvi 2018, 73). They involve the use of more subjective methods to collect and analyze data, such as interviews, field notes, and observation. Qualitative methods are less structured and do not solely rely on predetermined variables or statistical analysis. Instead, researchers rely on open-ended exploration and analysis of the data to draw conclusions. (Ritala 2023, 20-21.)

This study will adopt pragmatist ontology and epistemology as it is concerned with changing the existing practice. Pragmatists employ a variety of methods to answer their research problems (Saunders et al. 2016, 151). Thus, an Applied action research choice

seems justified for improving the existing practices. Next, the study will rely on utilizing qualitative research methods. Qualitative research does not include explicit hypotheses building or their testing. This means that the theory does not limit the research but is used for support in developing and implementing change. Furthermore, the empirical data used is non-numeric, which also supports the choice of qualitative methods for this study.

This study is rooted in theoretical knowledge and best practices of official export control legislation. The data collection techniques will be multi-method, as more than one technique will be utilized to achieve an adequate saturation for the data collection. The data collection tools for this study are interviews, questionnaire and internal document reviews. This is also known as the between-method triangulation as it involves using multiple methods to collect data on a single research topic. (Tuomi & Sarajärvi 2018, 99, 168)

Finally, for the data analysis, a theory-driven content analysis will be used. It is a qualitative research method that is used to examine and analyze text-based content for the purpose of understanding how it relates to a particular conceptual framework. Theory-driven content analysis aims to uncover patterns and relationships between the data content and the existing knowledge (Tuomi & Sarajärvi 2018, 109-110). The analysis is based on abductive reasoning as the objective of this study is to identify a new solution by combining existing information in new ways.

2.2 Research Design

This subsection provides an overview of the research design applied in the study, explaining its key components. The research design is presented as a step-by-step process, as illustrated in Figure 1, outlining the distinct stages of data collection and the expected outcomes at each step.

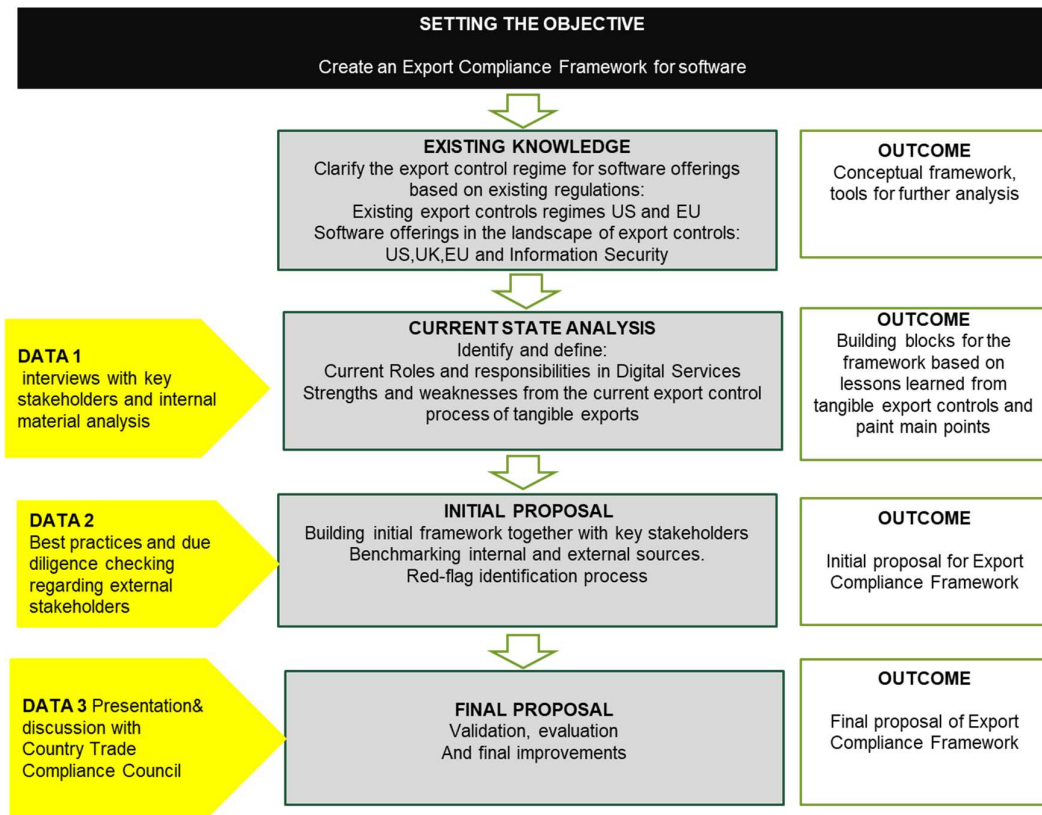


Figure 2. Research design of the Thesis

Once the objective of this study was established, the subsequent step in the research design process involved gaining familiarity with existing knowledge on the subject. Legislative and regulatory instructions were thoroughly investigated and compared. Drawing upon the identified similarities in the existing knowledge, a tool for further analysis was selected. The decision to delve into existing knowledge first was justified, as the author possessed prior knowledge in the field of export compliance but lacked specific insights into software-related export controls. This approach allowed for the development of a more comprehensive conceptual framework to underpin reflections on the company's current state in this area.

The Current State Analysis (CSA) was then conducted within the Digital Services Department of the sponsor company, generating Data 1. This department was chosen for inclusion in the co-creation process due to its exclusive focus on software sales. Data 1 comprised of interviews with experts and management from the Digital Service department, forming the project team. Additionally, country and local Trade Compliance representatives were involved in Data 1, providing the export compliance perspective

through project validation and a SWOT-analysis of existing practices in the sponsor company.

Building upon the conceptual framework and findings from the CSA, the initial proposal was crafted. The goal was to co-create this proposal through interviews, forming Data 2. These interviews involved external and internal stakeholders, exploring their best practices in the realm of software export controls. After implementing the findings from Data 2 into the proposal, the updated export compliance framework was presented to the main experts in export controls at the country and sponsor company level. This interactive interview process constituted Data 3. Following a constructive dialogue with subject matter experts, the final proposal was refined, and action points for future steps were identified.

2.3 Data Collection and Analysis

In this thesis, interviews constituted the primary method of data collection. The interviews were conducted in a semi-structured format, including both virtual and face-to-face interactions, with pre-established questions. Virtual interviews were recorded, and their main findings are detailed in the study. Prior permission was obtained from all interviewees to use the key findings in this study. However, in consideration of interviewees' privacy, no supplementary records of the interviews exist beyond the information presented in the main body of the thesis. The data collection process occurred over multiple rounds. Table 1 shows details of Data collections 1-3 used in this study. The questionnaires for 4 interviews (ID 4-7) can be found in Appendixes 1 to 4.

Table 1. Details of Data collections 1 to 3

ID	Participants / role	Data Type	Topic, description	Date, length	Documented as
Data 1, Current state analysis					
1	Head of Digital & Local Head of Sales for Digital Services	Teams Interview	Introductions to Export Control of Intangible Technology Resources needed from the digital solution teams	DEC 2022 / 60min	meeting memo
2	Trade Compliance Country level representation	Face-to-face meeting	Validation of Master Thesis project and schedule	JAN 2023 / 90min	meeting memo
3	Local Trade Compliance Officers EC &CC	Workshop	Global Risk Assessment 2023	MAY 2023/ 180min	SWOT
4	Digital Service(DS) Project team	Teams Interviews		MAR 2023	
	Product owners		<i>Product owner 1</i> , Domain Expert <i>Product owner 2</i> , Software Bill of Materials <i>Product owner 3</i> , 3rd party partnerships	50 min each	Recordings
	Global Sales Manager		Sales process for the onboard advisory product	50 min	Recordings
	Smart Asset Management Team Lead		Technical assistance	45 min	Recordings
	Local Head of sales for Digital Services		Organizational structure and responsibilities	50 min	Recordings
Data 2, Proposal Building					
5	Internal divisions PCE and TCO	Teams Interviews	Software export compliance best practises and product classification	NOV 2023 / 60min	Recordings
6	External partner	Teams Interviews	Software export compliance best practises and due diligence	NOV 2023 / 50min	Recordings (NDA)
7	DS Project teams Global Sales Manager	Questionnaire	Red-flag identification	NOV 2023 / 50min	Recordings
Data 3, from Validation					
8	Trade Compliance Country level representation & sponsor company TCO EC and CC	Teams Interview	Suitability from a regulatory perspective and next steps	DEC 2023/ 65min	Recordings

Data for this thesis was gathered through three distinct rounds, as presented in Table 1. The initial round, focused on acquiring Data 1, was undertaken for the analysis of the Current State. The commitment from the management level was initially confirmed through presentation-style discussions, aimed at validating the objective, expected outcome and the anticipated business impact. Subsequently, a project team was assembled from experts within the digital service department to gain a more comprehensive understanding of the software context. Additionally, the Trade Compliance team of the sponsor company conducted a workshop to formulate a risk review and a SWOT-analysis of best practices from the tangible export compliance experiences.

In the subsequent round, Data 2 was collected to identify best practices from both internal and external stakeholders for the formulation of the initial proposal. Data 2 also included a red-flag identification questionnaire with the project team global sales representative. Content analysis was employed to analyze the textual data, which was coded under specific interview themes to facilitate a comprehensive interpretation in connection with the thesis topic. The content analysis of internal division interviews led to the inclusion of certain internal documents in the initial proposal-building phase, and these documents are detailed in Table 2.

Table 2. Internal documents used in the proposal building, Data 2.

	Document name	Number of pages	Description
A	Software classification map	1 page	Process descriptions for software classification process
B	Product Classification Report (PCR)	4 pages	Product Classification information Template
C	Encryption Classification Form	11 pages	Encryption Classification information Template
D	End-User Certificate (EUC)	5 pages	Customer End-Use information Template

The main documents included four internal standard operating procedures (SOP). The documents underwent analysis and were subsequently incorporated into the initial proposal. This aligns with the study's objective, which is to identify a novel solution by combining existing data in innovative ways.

In the third round, Data 3 was gathered during the validation of the initial proposal. This dataset incorporated feedback on the proposal provided by Country-level Trade Compliance Experts. The feedback was categorized under the themes outlined in the initial proposal and subsequently integrated to shape the final proposal. Additionally, the study highlighted that certain key pain points remained resolved and further process development support is needed from Global Trade Compliance level.

In summary, the study draws from a variety of data sources. The base for the Current State Analysis was formed by getting acquainted with the thesis subject existing knowledge to better adhere with the theory-driven content analysis. Section 3 creates the conceptual framework to gain an overall understanding and develop initial impressions form software export compliance.

3 Existing Knowledge and Regulations on Export Compliance for Software Technology Products

This section of the thesis provides a comprehensive review of the existing knowledge in the domains of technology export controls, regulatory frameworks, and best practices established in both the United States (US) and the European Union (EU). The acquired information has been synthesized to construct a conceptual framework, which in turn serves as a foundation for co-creating the export control framework tailored to software offerings.

3.1 Background of export controls

The essence of the export controls lies not in the outright prohibition of global trade but rather focuses on preventing controlled exports from falling into the possession of undesirable entities. This relates to the responsibility of exporters to grant independent export authorities access to the relevant details of the transaction. (von Wittke, et al. 2016, 1:11:40) Consequently, due to apprehensions surrounding the proliferation of weapons of mass destruction and foreign policy goals, measures in the form of export controls have been introduced. Export controls serve as essential mechanisms to ensure that trade is directed solely towards entities and countries with whom the nations have established a sense of confidence and security in conducting business. (Deloitte 2019)

Historically, the primary target of export controls has been to control the advancement of weapons of mass destruction through the regulation of goods and technologies capable of supporting the creation of chemical, biological, or nuclear weaponry. Similarly, concerted efforts have been made to prevent the export of goods and technologies that might find utility in sensitive military applications, especially to nations subjected to arms embargoes. (IICS 2019) In more recent times, the scope of export controls has been expanded to address also human rights violations, such as technology and software utilized by governments to conduct surveillance on their citizens. (Foreign Ministry of Finland 2023)

Export controls are typically divided into four main categories: controls on products, controls on end-uses, controls on end-users, and controls on export destination. (Deloitte 2022). These four categories are illustrated in Figure 3.

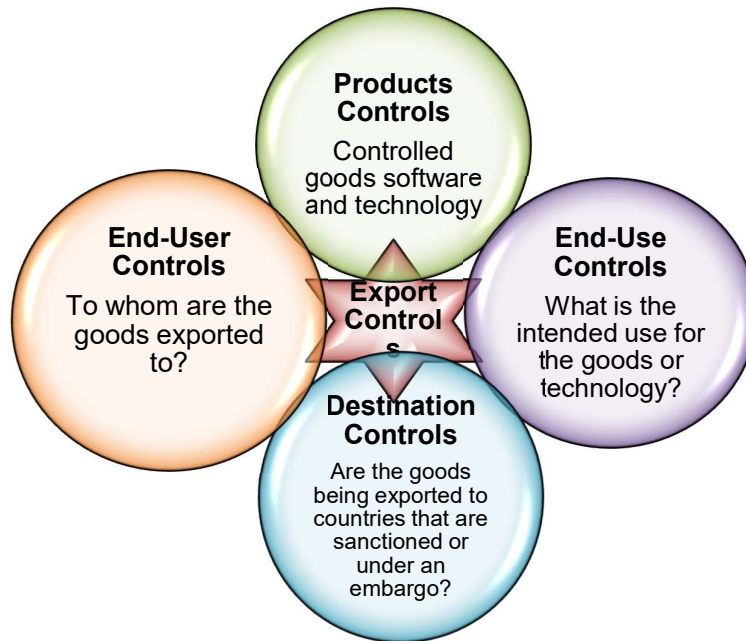


Figure 3. The four main categories of export control

The Product controls refer to the classification of goods or technology based on their specific technical details or attributes. Does the product have dual-use characteristics or is it suitable for military purposes? Under most regulations, military purpose refers to items that are specifically designed or modified for military applications. The key focus lies in the special design or alteration of an existing product to meet particular military specification. In contrast, Dual-use items are originally designed for civilian purposes but possess the potential for military application or weapons of mass destruction, due to their technical capabilities, if they end up for the wrong end-use or end-user. Thus, the classification of software and technology plays a significant role in determining the necessity for an export license. (Deloitte 2022)

The end-use refers to the purpose for which the technology will be deployed. Some end-uses, such as weapons proliferation, are prohibited regardless of the product being exported. The end-user refers to the institution and/or individual receiving the export. Are they allowed to receive it without a license? Are they listed as restricted parties? Finally, the destination control refers to the country to which the technology is being exported. Does the technology with a specific classification require an export license to that country? Is the final destination of the technology or software in a sanctioned country?

(Washington University 2019, 7) Each country has their own national regulations and competent authorities which decides which items are controlled and grants export authorizations for items that fall under the controlled export status. (Wassenaar Arrangement 2022)

Additionally, there are several international treaties which have been put in place to govern the export of commodities and technological advancements. These treaties consist of coalitions of nations that agree to comply with guidelines, with the goal of promoting trade while implementing stricter regulations for more sensitive items, such as materials related to nuclear or missile technology. (The Bureau of Industry and Security 2020)

3.2 The Wassenaar Arrangement

Wassenaar Arrangement established in July 1996 is the most significant export control related multilateral agreement. It sets the framework for the controls of dual-use goods and technologies as well as munitions. At the time of writing this thesis, there are 42 member nations including Argentina, Australia, Canada, India, Japan, Mexico, New Zealand, Norway, Russia, South Africa, South Korea, Switzerland, Turkey, Ukraine, the United States (US) and 27 European Union (EU) member states. (Wassenaar Arrangement 2022)

In order to promote transparency, the Wassenaar Arrangement encourages countries to voluntarily share information and notifications about their export activities related to weapons and items listed on the arrangement's two control lists: The Munitions List (Conventional Weapons) and the Dual-Use Goods and Technologies List. The latter list is divided into two tiers: Tier 1 for Basic Items and Tier 2 for Sensitive Items, with a subset of Very Sensitive Items. Through these information exchanges, Wassenaar aims to foster greater responsibility among its members in exporting weapons and dual-use goods, while also preventing the accumulation of destabilizing goods. (Wassenaar Arrangement 2022)

Thus, the Arrangement could be described as an international forum created to facilitate the exchange of views and information on international trade of conventional arms and dual-use goods and technologies. The Wassenaar Arrangement isn't a legally binding

agreement according to international law as the countries involved have neither ratified it nor was it ever intended to be ratifiable. The dialogues around the Wassenaar Agreement are usually between the member nations' government officials rather than high-level politicians. (Parviainen 2000, 11-12.) The countries that participate in this agreement typically have similar control lists, consequently the European Union (EU) has incorporated the Wassenaar Arrangement control lists into its legislative framework and operational practices. (EU 2015, 1.)

As the Wassenaar Arrangement operates based on consensus, a single country can block any proposal, and there is no veto authority for members over other members' proposed exports. Moreover, there is no unanimous agreement among the members on which countries should be considered "states of concern" or what defines a "destabilizing" transfer. While the Wassenaar Arrangement is not specifically focused on any particular region or group of states, as part of their efforts to prevent terrorist groups and individuals from acquiring sensitive goods and technologies, the members have agreed to exercise maximum restraint in exporting to the Great Lakes region of Africa. (Kimball 2022.)

3.2.1 Software Technology Export Controls

The latest publication of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies has been published in December of 2021 (Wassenaar Arrangement Secretariat, 2021). The document, also known as the WA-list, consists of the list of dual-use goods & technologies and the munitions list. The WA-list defines the term "Software" as follows:

A collection of one or more "programs" or "microprograms" fixed in any tangible medium of expression.

The Munitions List primarily encompasses items of a distinctly military nature and has designated certain software applications as subject to export restrictions. The ML21.a., ML21.b. and as concised by ML21.c.:

"Software", not specified by ML21.a. or ML21.b., specially designed or modified to enable equipment not specified by the Munitions List to perform the military functions of equipment specified by the Munitions List.

The list of Dual-Use Goods and Technologies consist of nine categories, as presented in Figure 3., in addition to the Sensitive List mentioned in section 3.2. Each of the list's categories comprises of several subsections designated alphabetically, which recur consistently within each respective category. The letter "D" designates the software subsection across all categories. The subsection "D" begins in all categories as follows:

"Software" specially designed or modified for the "development", "production" or "use" of equipment specified by (the Category in question)

Thus a more in depth analysis of the product characteristics is needed to determine whether the technology is subject to export controls. With regard to software being designated as the principal controlled item, a more comprehensive examination is needed within the Categories 4 and 5, as emphasized in Figure 4.

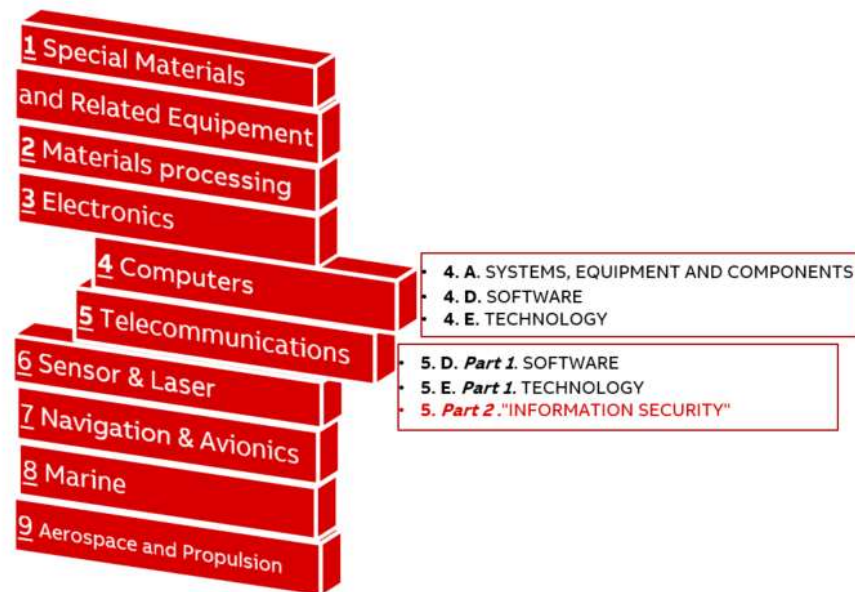


Figure 4. Categories of the List of Dual-Use Goods and Technologies (WA-LIST 2021)

Category 4, Computers, encompasses technological components relevant to hardware and their technical performance. Category 5 is divided into two parts, Part 1. Telecommunications and Part 2. Information Security. The International Telecommunication Union (2012, 7.) defines Telecommunication as the process of transmitting, receiving, or intercepting various forms of information, including signs,

signals, writings, images, and sounds, through the use of wire, radio, optical, or other electromagnetic systems. The WA-list Category 5. Part 1. considers the components, testing and manufacturing equipment, and corresponding software created specifically for telecommunications equipment or systems. Section 3.2.2 of this thesis will provide a more detailed examination of Category 5, Part 2, with a focus on the topic of Information Security controls.

The "technology" specified for the Dual-Use List is defined both in the General Technology Note and the Dual-Use List itself. It comprises specific information that's essential for the "development," "production," or "use" of a particular product. This information is presented in the form of 'technical data' or 'technical assistance'. As detailed in Technical Notes, 'Technical data' can manifest in various formats, including blueprints, plans, diagrams, models, formulae, tables, engineering designs, specifications, manuals, and instructions. These can be in written form or recorded on different media or devices like disks, tapes, or read-only memories. 'Technical assistance' encompasses the provision of guidance, skills, training, practical knowledge, and consulting services. It's worth noting that 'technical assistance' can involve the transfer of 'technical data. (WA-LIST 2021, 234)

The participating member states acknowledge the significance of implementing comprehensive regulations for designated "software" and "technology," including intangible exports. Therefore, national legislation related to export control should authorize the regulations to control transfers of listed "software" and "technology" regardless of how the export is done. This includes both physical transfers(tangible) and transfers done electronically via media, fax, or phone(intangible). Member Governments also see the value in sharing their experiences with implementing and enforcing these rules for intangible transfers. This way, they can adapt to novel developments and better address all associated risks related to this matter. (WA-LIST 2021, 241)

The WA-list (2021, 3) does not regulate software that meets the following criteria: readily available to the general public through unrestricted retail sales, including over-the-counter, mail order, electronic, or telephone transactions. Additionally, software that is designed for self-installation without significant supplier involvement, as well as software that is in the public domain or requires minimal "object code" for the installation, operation, maintenance, or repair of an export authorized item. However, in the latest update from December 2021, a regulation was introduced concerning Computer-

Assisted Design (CAD) software tools, which are specifically used in the development of sophisticated components and emerging classes of metallic and organic substrates. These regulations primarily relate to semiconductor items falling within Category 3, Electronics. (WA 2021, 1.)

In conclusion, the Wassenaar Arrangement establishes a foundational framework that outlines non-binding standards for regulating the export of Conventional Weapons and Dual-Use Goods & Technologies. Member states are expected to implement these standards nationally. In the following sections, the implementation of software technology export controls by the United States and the European Union is introduced in more detailed. In 2022, the US surpassed Sweden to become Finland's largest trade partner. This exceptional growth in goods exports can be attributed to higher export prices, forest-industry products, biofuels, and contributions from the cruise industry (Kostinainen, 2023.). Therefore, it is advisable for any Finnish company involved in export operations to be familiar with both United States trade regulations as well as the European Union legislation.

3.2.2 Category 5 part 2 - Information Security

According to the Wassenaar Arrangement, items or functions related to "Information Security" (IS) should be evaluated against the provisions in Category 5 - Part 2, even if they are components, "software," or functions of other items. This also applies to the information security components in software that is "readily available to the general public" and not subject to restrictions, as outlined in the previous section.

The WA defines IS as the methods and processes that secure information or communication accessibility, confidentiality, and integrity. Excluding measures against malfunctions. It involves elements like "cryptography" and its activation, which can be implemented as hardware, software, or technology. Additionally, there's 'Cryptanalysis', which involves analyzing cryptographic systems to extract confidential variables or sensitive data, even in plain text. "Cryptography" includes encryption and decryption (WA-LIST 2021, 221,225).

As an example, in the cryptographic information security in 5.A.2.a, including "cryptography for data confidentiality", the term "cryptography" pertains to digital techniques conducting cryptographic functions **excluding** authentication, digital

signatures, data integrity, non-repudiation, digital copyrights management, encryption/decryption for commercial entertainment, broadcasts, medical records, or private key management linked to prior functions. The restricted components, systems, and equipment must be designed or tailored to employ 'cryptography for data confidentiality' with a specified security algorithm. This cryptographic capability should be usable, activated, or activatable via means aside from secure cryptographic activation. This applies to:

1. Items with "information security" as a primary function.
2. Digital communication or networking systems, equipment, or components outside paragraph 1.
3. Computers, items focused on information storage/processing, and their components, beyond paragraphs 1 and 2.
4. Items not mentioned previously, where 'cryptography for data confidentiality' with a 'described security algorithm' supports a non-primary function of the item **and** is performed by incorporated "equipment" or "software" that, if it were a separate item, would be controlled under Category 5 - Part 2.

(WA-LIST 2021, 94.)

According to Cryptography Note 3 (WA-LIST 2021, 94.), exemptions do exist for 5.A.2 controls when the items fulfill **all** of these conditions:

1. Publicly available through retail points without restrictions
2. The item is of broad interest to individuals and businesses; and
3. The price and core functionality details are accessible pre-purchase without vendor consultation (simple price inquiries excluded)

Finally, the exemptions for hardware components or 'executable software', required for items described above in 5.A.2.a , which have been tailored for these existing items, and meet **all** of the following as stated in the WA-LIST 2021 (page 93):

1. *"Information security" is not the primary function or set of functions of the component or 'executable software'*
2. *The component or 'executable software' does not change any cryptographic functionality of the existing items, or add new cryptographic functionality to the existing items*

3. *The feature set of the component or 'executable software' is fixed and is not designed or modified to customer specification and*
4. *The appropriate authority in the exporter's country, can access component or 'executable software' details as needed to verify compliance with conditions described above*

In the context of the Cryptography Note 3, 'executable software' refers to "software" that can be run directly by a computer's hardware. This so called "main executable file", is excluded from the complementary full set of files and libraries required for running a software program often referred as the "binary image".

Moving on to Technology which is controlled under Category 5 part 2. The subsections 5.E.2, includes technical data resulting from procedures carried out to evaluate or determine the implementation of functions, features or techniques specified to be controlled in Category 5 – Part 2.

3.3 The United States Export Controls

Ensuring that exports adhere to regulations involves a coordinated effort from different US government departments. This is why several agencies responsible for enforcing export rules are collaborating. The export control related bodies include but are not limited to the agencies presented in the Table 3. These agencies are the key players responsible for implementing the Wassenaar Arrangement guidelines and other security measures within the USA.

Table 3. Agencies responsible for enforcing Export Control Regulations in the United States

The Directorate of Defense Trade Controls (DDTC)	Governs the International Traffic in Arms Regulations (ITAR) and the United States Munitions List (USML)
Office of Foreign Assets Control (OFAC)	Refers to the implementation of Sanctions programs against various individuals and entities.

The Commerce
Department's
Bureau of Industry
and Security
(BIS)

Governs a variety of exports regulated by the Export Administration Regulations (EAR)

The Directorate of Defense Trade Controls (DDTC) engages in matters concerning defense equipment and comparable items. DDTC aims to protect US national security and supports the goals of foreign policy guidelines. The ITAR regulates the production, export, and temporary import of defense items, provision of defense services, and brokering activities concerning USML-listed items. It undergoes consistent updates to align with technological advancements and shifts in US national security and foreign policy priorities. (DDTC 2023)

OFAC compiles a list of individuals and entities that are owned, controlled by, or working for targeted countries. This list also includes individuals, companies, and groups like terrorists and drug traffickers who are identified under programs that aren't tied to specific countries. All these individuals and companies are referred to as "Specially Designated Nationals" or "SDNs." Their assets are frozen, and under primary sanctions US persons are not allowed to do transactions with SDN listed entities. Together with the Non-SDN entities they form the OFAC's Sanctions List Search. The Non-SDN status refers to individuals who are under specific sanctions that don't involve freezing assets. The Non-SDN " Consolidated Sanctions List" provides details about the type of sanctions applied and the legal basis for them. Additionally, OFAC maintains a list called the "CAPTA List," which includes foreign financial institutions subject to sanctions related to international banking relationships and cross-border transactions. (OFAC 2023)

Dual-use items, which have predominantly commercial uses but may also have military applications, fall under the regulatory jurisdiction of the Bureau of Industry and Security (The BIS). The BIS oversees creation, application, and development of US export control policies for dual-use commodities, software, and technology. The objective of BIS is to provide guidelines regarding regulatory frameworks for distinct destinations, deemed exports (involving the transfer of US technology to foreign nationals), encryption, and other sensitive items. The comprehensive framework outlining the prerequisites and principles of export licensing is referred to as the Export Administration Regulations (EAR). (EAR 2021, part 730)

The EAR govern and impose limitations on exports containing scenarios where an individual intends to export goods from the United States, re-export US origin or US De minimis items from a foreign nation or facilitate transfers between parties within a foreign jurisdiction (deemed exports). In addition to tangible exports, the jurisdiction of EAR extends to also intangible exports like software and technical assistance (Alfano 2022, 34-35)

Commerce Control List (CCL) shown below in the Figure 5 is the point where the EAR intersect with the Wassenaar Arrangements Dual-Use Goods and Technology controls, as depicted in Figure 5.

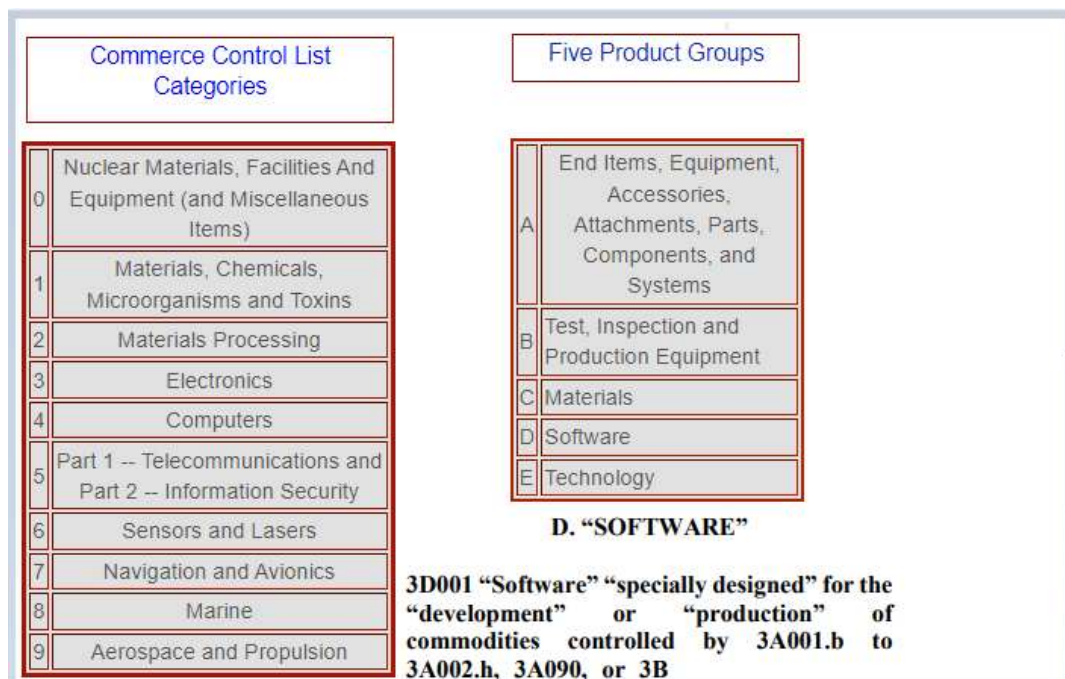


Figure 5. CCL Categories and Product Groups with an example of Category 3, Product Group D. "Software" (BIS, 2020.).

The CCL presents ten categories along with their respective technical parameters. To determine whether an item is controlled, it is necessary to analyze and compare the item's specifications with those outlined in the control list. This analytical process is commonly referred to as Product Classification which aims to identify whether the item falls under the EAR or not and further if the item is subject to the Export Control Classification Number (ECCN) based on its technical characteristics. (BIS, 2020.)

3.3.1 Example of an export control classified software product

Figure 6 presents an example of an export control classified software item with an ECCN 4D004.

4D004 “Software” “specially designed” or modified for the generation, command and control, or delivery of “intrusion software.”	
License Requirements	
1.) Reason for Control: NS, AT	
Control(s)	Country Chart (See Supp. No. 1 to part 738)
NS applies to entire entry	NS Column 1
AT applies to entire entry	AT Column 1
3.) List Based License Exceptions (See Part 740 for a description of all license exceptions)	
TSR:	N/A
APP:	N/A
ACE:	Yes, except to Country Group E:1 or E:2. See §740.22 of the EAR for eligibility criteria.
4.) Special Conditions for STA	
STA: License Exception STA may not be used to ship or transmit “software” specified by ECCN 4D004.	
5.) List of Items Controlled	
Related Controls: Software described in USML Category XI(b), and software directly related to a defense article, is “subject to the ITAR”; see § 120.10(a)(4).	
Related Definitions: N/A	
Items:	

Figure 6. Capture from the Commerce Control List Supplement No. 1 to Part 774 Category 4 (2023, 9.)

The initial numerical component designates the item's category, in this case, 4 signifies "Computers." The subsequent letter defines the relevant product group; the letter D denotes "Software." Following this, the next three digits indicate the regulatory foundation for the item control (Alfano 2022, 24.):

Ranging from **001 to 009**, the Wassenaar Arrangement (WA) is applied

100 to 199, the Missile Technology Control Regime is employed

200 to 299 relates to the Nuclear Suppliers Group

300 to 399 corresponds to the Australia Group (Chemical and Biological weapons)

500 to 599 refer to matters of National security or Foreign Policy

600 to 699 identify items from the WA Munition list or former US Munition list

The digits **900 to 999** are reserved for National Controls, which are built upon the baseline requirements set by the multilateral control arrangements.

Following the classification of an ECCN for a product, it is important to assess whether the item necessitates an export license application from the United States government. The Commerce Control List (CCL) outlines the reasons for control, in Figure 6 as:

- 1) Anti-Terrorism (AT) and National Security (NS) presented in two-letter abbreviations, which are expounded upon in Part 742 of the EAR (2023). In order to determine whether the intended export destination of the item mandates a license, reference must be made to:
- 2) The Country chart from Part 738 of the EAR (2021). Additionally, it is important to recognize the potential applicability of:
- 3) License exceptions, which have the potential to exempt the item from the requirement of an export license. Detailed information concerning these exceptions can be found from Part 740 of the EAR (2023). Technology and software under restriction (TSR) license exception permits exports and re-exports of technology and software when the recipient has provided the exporter with a signed written assurance before the export, stating that the goods will not be re-exported to specified countries. A license is required for the export of these technologies and software, if the written assurance is not obtained or if they are being exported to other than specified countries (Cornell Law School 20219).
- 4) For instance, as stipulated in License Exceptions, Part 740, on page 63, there is a provision for exceptions like the Strategic Trade Authorization (STA), although this particular ECCN code 4D004 is not applicable to such exemptions.
- 5) The final entry in the ECCN code listing is “List of Items Controlled”. This section offers a compilation of interconnected definitions, controls, and specific items associated with the given ECCN code. These specifications can be considered as a supplementary reference alongside the Commerce Control List (BIS 2018, 30.).

Items falling under the jurisdiction of US Department of Commerce but not listed on the Commerce Control List (CCL) are classified as EAR99. This alphanumeric code serves as a general category for items that do not fall under any specific CCL entry but can be found at the end of each Category on the CCL. (Part 732 of EAR 2022, 6.) "NLR," an acronym for "No License Required," is applicable to products categorized as EAR99 or items listed on the Commerce Control List (CCL) that, based on their intended destination, purpose, and recipients, do not demand a license. However, despite an EAR99 classification and the general absence of license requirements, certain scenarios may necessitate a license. This includes cases where the item is destined for an embargoed country, is intended for use by a restricted end user, or is designated for a prohibited end use. (BIS 2018, 6)

3.3.2 The Ten General Prohibitions

If an export, reexport, or in-country transfer falls under the jurisdiction of the Export Administration Regulations (EAR), it is necessary to conduct a comprehensive assessment of the License Exceptions outlined in Part 740, as well as a careful examination of the "Ten General Prohibitions" laid out in this section. The ten general restrictions include references to different parts of the EAR and, as such, help to explain the full range and extent of these overall restrictions. Table 4 and 5 provide a summary of all 10 restrictions, including summaries of their respective contents. (EAR Part 736 2023, 1-5):

Table 4. General Prohibitions (GP) 1 to 3 relate to the product classification based on CCL.

<p>GP 1. Export and re-export of controlled items to listed countries</p>	<p>It is prohibited to export or re-export any US-origin items to destinations that necessitate a license based on the control reason specified in the Country Chart of Part 738 of the EAR. However, if an exporter or re-exporter fulfills all the conditions outlined in any of the License Exceptions from Part 740 of the EAR, that particular License Exception overrides General Prohibition One.</p>
<p>GP 2. Re-export and export from abroad of foreign-made items incorporating more than a de minimis amount</p>	<p>Re-exporting foreign-made products from abroad that incorporate controlled US-origin goods, software or technology. Thus, making the non-US made end-product subject to the EAR if incorporating or mixing with more than the "<i>De minimis rule</i>" amount of controlled US content, as defined in Part 734.4 of the EAR (2023):</p> <ul style="list-style-type: none"> • <u>Exceeds 0 % of total value</u> of the non-US item in special situations (semiconductors, high speed interconnect devices, hot section technology, certain encryption or cryptanalytic items and military commodities)

of controlled U.S. content	<ul style="list-style-type: none"> • <u>Exceeds 10% of the total value</u> of the non-US item, when exporting to embargoed countries CU, IR, SD, SY or KP • <u>Exceeds 25% of the total value</u> of the non-US item, when exporting outside of CU, IR, SD, SY or KP
GP 3. Foreign-direct product (FDP) rules	Items produced outside the US can be subject to the EAR if they are manufactured using specific technology or software, specified in Part 734.9 of the EAR (2023), or if they are made in a plant or with a major component of a plant that is itself operating using specific US technology or software.

Table 5. General Prohibitions (GP) 4 to 10 relate to End user, End-use and other controls.

GP 4. Engaging in actions prohibited by a Denial Orders	<p>The exporter is responsible for ensuring that any transactions, involving a person or entity that has been denied export privileges, do not violate the terms of the denial orders issued under part 766 of the EAR. To check for orders denying export privileges, the exporter should refer to the OFAC’s Sanctions Lists and the BIS list of “Denied Persons,” which includes foreign governments, corporations, groups, and individuals.</p> <p>NOTE. There are <u>NO</u> License Exceptions described in Part 740 of the EAR that authorize conduct prohibited by GP4.</p>
GP 5. Export, re-export, or transfer (in-country) to prohibited end-uses or end-users (End-Use End-User).	It is forbidden to knowingly export, re-export, or transfer (in-country) any item subject to the EAR to an end-user or end-use that is prohibited by Part 744 of the EAR, unless authorized by BIS. Restrictions vary from Maritime nuclear propulsion end-uses to Restrictions on specific activities of “US persons”.
GP 6. Export, re-export, and transfer (in-country) to embargoed destinations (Embargo)	<p>It is forbidden, without a license or license exception, to export, re-export, or transfer (in-country) any item subject to the EAR to a country or region that is embargoed by the US or otherwise made subject to controls under Part 746 of the EAR.</p> <p>Unless a license exception or other authorization is applicable based on part 746 of the EAR, the license exceptions described in Part 740 of the EAR are <u>NOT</u> available to overcome GP6.</p>
GP 7. Support of proliferation activities and certain military intelligence end uses and end users (“U.S. person” activities)	Restriction on providing support for any activities related to the spread of weapons of mass destruction or technology and specific military or intelligence purposes prohibited by Part 744.6(b) or (c) of the EAR. This rule applies to US individuals or entities engaging in such activities without a license from BIS.

<p><u>GP 8.</u> In transit shipments and items to be unladen from vessels or aircraft (Intransit)</p>	<p>Shippers and operators of vessels or aircraft are not allowed to export or reexport an item subject to EAR through, or ship certain items in-transit a country listed in paragraph (b)(8)(ii); Armenia, Azerbaijan, Belarus, Cambodia, Cuba, Georgia, Kazakhstan, Kyrgyzstan, Laos, Mongolia, North Korea, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, Vietnam. Unless, there is a license exception or authorization permitting the direct export or reexport to a specific transit country, or unless the export or reexport qualifies for transit through that country without needing a license.</p>
<p><u>GP 9.</u> Violation of any order, terms, and conditions (Orders, Terms and Condit.)</p>	<p>This rule is designed to prevent the use of indirect methods to bypass export controls and trade restrictions presented in the Ten General Prohibitions or License Exception issued in part 740 Of the EAR</p>
<p><u>GP 10.</u> Proceeding with transactions with knowledge that a violation has occurred or is about to occur (Knowledge Violation to Occur)</p>	<p>The rule covers activities such as financing and servicing that are typically not addressed by the EAR. If a violation occurs, subsequent actions related to the exported item are also restricted e.g. warranty services. This means that US item exporters, foreign re-exporters, and resellers need to avoid activities involving items linked to regulatory violations and be cautious of changes in the export control status of the end user or destination they're dealing with to prevent potential breaches of GP 10 in the future.</p>

Breaching these rules, including the authorizations granted within them, can result in administrative penalties and other legal consequences as imposed by the United States court. These include but are not limited to civil monetary penalties, denial of export privileges and exclusion from practice. The enforcements, protective measures and penalties from non-compliance to these US Export Control Regimes are outlined in Part 746 of the EAR. Entities and individuals are prohibited from participating in activities that are against or oppose the Export Administration Regulations (EAR), any other licenses, or the Export Control Reform Act (ECRA). (EAR, Part 746 2020, 1-3.)

The ECRA, introduced in 2018 as bipartisan legislation, strengthens controls over "emerging and foundational technologies critical to US national security." It specifically targets new digital technologies that bypass customs checks at physical borders. These technologies are notable for their "omni-use," providing a diverse range of simultaneous functions, and their "omnipresence," as they are frequently integrated across various sectors of society. Section 1758 of ECRA authorizes BIS to establish appropriate controls on the export, reexport or transfer of these emerging and foundational

technologies. ECRA serves as an extension of the EAR, subjecting emerging or foundational technologies under its control to the same regulations as other items presently on the CCL. Consequently, ECRA is relevant not only to US-based companies but also to any company worldwide engaged in re-exporting US made goods or technology, integrating previously exported US technology, or falling under the jurisdiction of the United States. In November 2018, the Department of Commerce's Bureau of Industry and Security (BIS) released an initial list of 14 emerging technologies to be restricted, including robotics, additive manufacturing (e.g. 3D printing), and advanced surveillance technologies. (Lazarou & Lokker 2019, 1-2)

3.4 The European Union Export Controls

In the European Union (EU), the export of dual-use items and technologies is regulated by Regulation (EU) 2021/821 of the European Parliament and the European Council. The item lists integrated into the European Union's legislation correspond to the catalogues agreed upon in the international export control regimes listed below. In some control procedures, EU has gone further in its harmonization efforts than what is internationally required. These International export control regimes include the Wassenaar Arrangement (WA), the Australia Group (AG), the Missile Technology Control Regime (MTCR), and the Nuclear Suppliers Group (NSG). (Foreign Ministry of Finland 2023)

The European union export controls reinforce EU's foreign and security policy goals, like conflict resolution, counterterrorism, preventing weapon proliferation, and upholding democracy and human rights. These interventions are manifested through the restrictive measures or 'sanctions'. The implementation of financial sanctions, specifically asset freezes, are a binding obligation for both the public and private sectors. Initiated by Credit Sector Federations, an initial database was established, containing a consolidated list of individuals, groups, and entities subjected to financial sanctions, primarily asset freezes. The European Commission assumed responsibility for its upkeep and the regular updating of the Consolidated List of Financial Sanctions. In 2017, the European Commission introduced a web-based consolidated list of financial sanctions, featuring asset freezes in various formats. (DG FISMA 2020)

The Commission develops secure systems for cooperation, issues guidelines, submits annual reports, amends control lists via simplified procedures, and conducts the regulation evaluations for the European Parliament. The Dual-Use Coordination Group, led by the Commission, addresses regulatory issues, consults stakeholders, and forms expert groups. The Commission and Member States promote global convergence on export controls through information exchange, capacity building, and outreach. (Publications Office of the European Union 2023)

These all impose legal duties on EU citizens, operators, and businesses within the EU. The Council of the EU establishes the export controls, but it is the task of the 27 Member States to enforce them. Penalties for breaches over EU sanction applications and enforcement across the Member States is being monitored by the European Commission. (European Commission 2023)

3.4.1 Export control of software and technology

Annex I of the Regulation (EU) 2021/821; Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items, includes the same approach of 0 to 9 Categories like the US Commerce Control List (CCL) shown in Figure 5. Furthermore, the five product groups from A to E remain identical. Consequently, the alphanumeric codes identifying specific items exhibit notable similarities across both regulatory systems. However, it's **essential to observe** that the term "ECCN" (Export Control Classification Number), which is employed in the United States, is not utilized within the Regulation (EU) 2021/821. Rather, the term "Control list No" is used (Annex III 2021, 444.). Figure 7, below, presents the same control list number in EU context, as the US example in Figure 6 in page 22.

4D004	"Software" specially designed or modified for the generation, command and control, or delivery of "intrusion software".
<p><u>Note:</u> 4D004 does not control "software" specially designed and limited to provide "software" updates or upgrades meeting all the following:</p> <p>a. The update or upgrade operates only with the authorisation of the owner or administrator of the system receiving it; <u>and</u></p> <p>b. After the update or upgrade, the "software" updated or upgraded is not any of the following:</p> <ol style="list-style-type: none"> 1. "Software" specified in 4D004; <u>or</u> 2. "Intrusion software". 	

Figure 7. Capture from the Official Journal of the European Union Category 4 (2021, 266.)

Similarly to the US license exemptions where single export licenses can be avoided, the EU has general export authorizations. These authorizations are valid throughout the customs territory of the Union for exports to specified destinations (EUR-Lex 2023.). To fully understand their application within the context of software, it's essential to first familiarize with how the European Union defines the export of software and technology. To facilitate this understanding, Table 6 below provides both the definitions and the relevant general export authorizations that are applicable in the field of software and technology.

Table 6. Summary of export definitions and general export authorizations EU007, EU008 (Regulation (Eu) 2021/821, Annex II, 438-440.)

REGULATION (EU) 2021/821 2021, page 7.	EXPORT; <i>Transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the customs territory of the Union; it includes making available in an electronic form such software and technology to natural or legal persons or to partnerships outside the customs territory of the Union; it also includes the oral transmission of technology when the technology is described over a voice transmission medium;</i>
REGULATION (EU) 2021/821 2021, page 7.	EXPORTER; <i>Any natural or legal person or any partnership that decides to transmit software or technology by electronic media, including by fax, telephone, electronic mail or by any other electronic means to a destination outside the customs territory of the Union or to make available in an electronic form such software and technology to natural or legal persons or to partnerships outside the customs territory of the Union.</i>
UNION GENERAL EXPORT AUTHORISATION No EU008	ENCRYPTION. The authorization shall be valid only when the items use only published or commercial cryptographic standards, do not use cryptographic standards specially designed for government use and any cryptographic functionality used by the items cannot be easily changed by the user.
UNION GENERAL EXPORT AUTHORISATION No EU007	INTRA-GROUP EXPORT OF SOFTWARE AND TECHNOLOGY. The authorization covers all technology and software specified in Annex I, except technology and software related to items under 4A005, 4D004, 4E001.c, 5A001.f and 5A001.j.

Other types of export authorizations available in the Member state level, as per EUR-Lex Summary of the Dual-use export controls (2023), are:

- **National general export authorizations.** Applicable for destinations beyond the specifications of the EU general export authorizations.
- **Individual.** Issued for up to 2 years to one exporter for the export of one or more dual-use items to one end-user in a non-EU country.

- **Global.** Issued for up to 2 years to one exporter for the export of multiple items, countries and end-users.
- **Large project authorizations.** Issued to one specific exporter, in respect of a type or category of dual-use items which may be valid for exports to one or more specified end-users in one or more specified non-EU countries for the purpose of a specified large-scale project.

Finland effectively enforces the European Dual Use Export Control Annex I in its regulatory framework. The Finnish export licensing authority responsible for dual-use items is the Ministry for Foreign Affairs (MFA). Furthermore, the Ministry of Defence holds the specified responsibility of being the designated export licensing authority for defense articles. (BIS 2020)

When applying these export authorizations the exporter must report to the MFA the end-user, the intended country of destination and end-use of the item exported. Regarding the exported item itself, the dual-use classification, the description of the software and technology and if applicable, the quantity and the value of the software and technology need to be included in the application. To acquire this necessary information, the MFA offers guidance through documents known as *End User Statement*, based on the Wassenaar Arrangement Export Controls for Conventional Arms and Dual-Use Goods & Technologies, and *Know Your Customer questions* aligning with the guidance provided by the European Union on the Internal Compliance Programme (ICP) for Dual-Use Trade Controls. (MFA 2023)

3.4.1.1 Technical assistance

Regulation (EU) 2021/821 Article 8 takes a stance on technical assistance related to export-controlled items outlined in Annex I. The WA definition for 'technical assistance', as outlined in Section 3.2.1 is the export of guidance, expertise, training, advisory services and may include the sharing of 'technical data'. In the context of the Annex 1 controlled items under regulation (EU) 2021/821, the Article 8 of the regulation defines the 'technical assistance' as shown in the below Figure 8.

- (9) 'technical assistance' means any technical support related to repairs, development, manufacture, assembly, testing, maintenance, or any other technical service, and may take forms such as instruction, advice, training, transmission of working knowledge or skills or consulting services, including by electronic means as well as by telephone or any other verbal forms of assistance;
- (10) 'provider of technical assistance' means:
- (a) any natural or legal person or any partnership that provides technical assistance from the customs territory of the Union into the territory of a third country;
 - (b) any natural or legal person or any partnership resident or established in a Member State that provides technical assistance within the territory of a third country; or
 - (c) any natural or legal person or any partnership resident or established in a Member State that provides technical assistance to a resident of a third country temporarily present in the customs territory of the Union;

Figure 8. Definition of 'technical assistance' in Regulation (EU) 2021/821 (2021, 7).

Under the EU dual-use Regulation, technology encompasses various forms of technical support, including verbal instruction, training, the sharing of technical knowledge and skills, as well as advisory services, whether delivered through telephone or electronic means. To be considered technical assistance, these activities must meet the specific technology criteria outlined in Annex I of the dual-use Regulation. Therefore, providing guidance to a colleague working at a research institute in a third country could trigger a license requirement for technical assistance. Export authorization is mandatory when offering technical assistance for purposes outlined in Article 4(1). Article 4 (2021, 9) refers to dual-use items connected to the creation, production, operation, or management of weapons of mass destruction, or intended for countries under an arms embargo seeking these items for military end-use. When the provider of technical assistance knows that the items are meant, even partially, for such uses defined in Article 4(1), they must inform the competent authority of the member state. This authority then determines whether the technical assistance should be subject to authorization or not. Some authorization exemptions apply when exporting technical assistance to specific countries listed in Annex II, part 2 (2021, 425) or for end-use purposes of EU Member States official tasks. Furthermore, Article 8(f) (2021, 12) includes a provision of somewhat ambiguous nature, applicable in cases where:

[The technical assistance] *is the minimum necessary for the installation, operation, maintenance (checking) or repair of those items for which an export authorisation has been issued.*

When planning to apply the exception under Article 8(f) it is best to consult the competent authorities which granted the preliminary export authorizations for the Annex I dual-use item. If an application process for an export license is required the provider of technical assistance must supply the competent Member State authority with details of the dual-use items location, a comprehensive item description, the quantity involved, details of third parties involved in the transaction, the destination country, and precise information about the end-user and its location within that country (Article 13. 2021, 15.).

The Providers of technical assistance are required to maintain registers of records related to services performed for Annex I items. These records should serve as evidence, upon request, containing information about the dual-use items that underwent technical assistance, the timeframe during which the items received these services, their intended destination, and the countries associated with the services. These records must be retained for a minimum of five years following the conclusion of the calendar year when the technical assistance was rendered. Additionally, these records must be presented to the competent authority if requested. (Article 27. 2021, 24.) In conclusion, even if the technical assistance itself is exempt from export authorization the assistance services performed for a dual-use software or technology need to be recorded properly.

3.5 Existing Compliance Frameworks and National Software and Technology Export controls

Both the United States and the European Union have established their own programs for best practices for the guidance of dual-use trade controls in their respective jurisdictions. In the US it is called the Export Compliance Program (ECP) and is based on the Export Administration Regulations (EAR) (BIS 2017). The EU version is called the Internal Compliance Programme (ICP) and is based on the multilateral agreements and the Regulation (EU) 2021/821 of the Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. (European Commission 2019)

Each set of guidelines encompasses in total of seven fundamental elements. These elements are established as foundational pillars for tailoring a compliance program suited to a company's unique requirements. Their purpose is to aid companies in contemplating the most suitable strategies and processes to ensure compliance with both national and international dual-use trade control regulations. A key aspect of crafting a compliance program is to maintain its relevance to the company's structure and operations. This involves ensuring that the internal procedures are simple and standardized, effectively capturing the day-to-day activities and processes. The specifics of these compliance programs will depend on many factors such as the company's size, organizational structure, business scope, the strategic significance of its products, potential end-uses or end-users, customer distribution across geographic regions, and the maturity of their internal export procedures. (BIS 2017, 1) Tables 7 present the key elements of both compliance programs summarized.

Table 7. Key elements in US ECP and EU ICP.

US ECP	EU ICP	Summary
BIS 2017, Export Compliance Guidelines	Commission Recommendation (EU) 2019/1318	
Management Commitment	Top-level management commitment to compliance	Senior Management's written commitment shapes the foundation of an effective Export Compliance Program, creating a culture of compliance top-down throughout the organization.
Risk Assessment	Organisation structure, responsibilities and resources	Initiating a risk assessment to establish a tailored dual-use trade risk profile, covering relevant aspects of the company's operations. This assessment should evaluate product range, stakeholders, and business operations affected by dual-use trade controls, prompting necessary adjustments to corporate policies and the organization structure. The outcomes of this risk assessment will shape the necessary actions and suitable approaches for developing or implementing the company's specific compliance procedures.

Export Authorization	Transaction screening process and procedures	To ensure regulatory compliance, evaluating transaction-related risks requires the implementation of transaction screening measures, commonly referred to as the due diligence principle. These procedures involve gathering and analyzing relevant data concerning item classification, transaction risk assessment, license determination and application, and post-licensing controls. They enable the establishment and maintenance of a standardized approach to handling suspicious inquiries or orders, and they encompass internal measures within the company to prevent transactions from occurring without the requisite licenses or in violation of applicable trade restrictions or prohibitions.
Recordkeeping	Recordkeeping and documentation	Recordkeeping system is essential for conducting performance evaluations, meeting national documentation retention mandates, and supporting collaboration with authorities during dual-use trade control investigations. Recordkeeping encompasses procedures for lawful document storage, record management, and tracking of dual-use trade control activities, including maintaining records of interactions with competent authorities and end-use(r) controls for non-listed dual-use items, as well as technical classification advice.
Training	Training and awareness raising	Mandatory, regular training for all dual-use trade control staff is essential for compliance with regulations. Ensure that all employees are informed about relevant dual-use trade control laws, policies, and control lists through awareness programs and consider customized training. Additionally, incorporate lessons learned from performance reviews, audits, and corrective actions into training and export awareness initiatives when applicable.
Audits	Performance review, audits, reporting and corrective actions	Compliance programs must be dynamic and subject to regular review, testing, and revision as needed to ensure ongoing compliance. Audits assess transaction execution in relation to established procedures and offer recommendations for procedure revisions or corrective actions, subject to management approval. Incorporate these lessons into training and export awareness programs.
Handling export violations and taking corrective actions	Physical and information security	To safeguard sensitive dual-use items, it's crucial to implement security measures. These measures should be tailored based on the company's risk assessment to prevent unauthorized access to sensitive items. This may involve physical safeguards, restricted access areas, and personnel access controls.

		Swift detection and response to noncompliance are essential to minimize organizational risk.
Build and maintain your ECP	N/A for EU	In the United States, alongside the Export Control Plan (ECP), organizations involved with controlled intangible technology and foreign nationals should place extra emphasis on technical information exchanges. As part of their compliance program, these entities should implement a comprehensive Technology Control Plan (TCP), which should cover elements of physical and information security, personnel screening, corporate commitment, training, and self-assessment.

The two programs have notable similarities. Any exporting company is expected to possess a variety of established policies and standard operating procedures that align with the particular compliance program. For such companies, the framework of core elements could potentially serve as a valuable benchmarking tool on their compliance approach (Commission Recommendation (EU) 2019/1318, 17.).

The EU recognizes the need for controlling the transmission of dual-use software and technology to destinations outside the Union's customs area in the Regulation (EU) 2021/821 (11) (2021, 11). To streamline processes for exporters and the competent authorities of Member States, it is recommended to introduce general or global licenses and establish standardized interpretations of regulations. This approach aims to reduce administrative burdens. Additionally, the ICP (2019, 26) suggests that exporters should consider information security measures when dealing with; *uploading software or technology to the 'Cloud', storing it in the 'Cloud' or transmitting it via the 'Cloud'*. This approach has drawn criticism for placing significant responsibility on Member States. For example, both the trade association Digitaleurope (2021) and the American Chamber of Commerce to the European Union (2021, 2) have expressed concerns about the lack of clarity, which results in varying interpretations and regulatory requirements for intangible transfers within the Union's customs area and between the EU and its global partners.

The Netherlands (NL) is one of the EU Member States with a national regulatory framework for controlled software and technology. In 2018, the Dutch Ministry of Foreign Affairs issued an updated advisory document known as the 'Guidance Note.' This document outlines the Dutch perspective on when an intangible transfer qualifies as an export, who is considered the exporter, the relevance of consignee nationality, and the vital role of information security measures in facilitating the transfer of controlled software or technology without the need for an export license. The most significant security

measures are the different encryption standards. The encryption enables the controlled technology from getting into to wrong hands by limiting the access to the data to those whom the exporter provides the encryption key. (Bennink 2019)

The need for `end-to-end encryption` when exporting controlled software or technology is also acknowledged in the regulatory frameworks of both the former EU Member State United Kingdom (UK) and the United States (US). End-to-end encryption refers to safeguarding data using encryption so that it remains unreadable during transmission from the sender to the receiver, and the decryption keys are not shared with anyone else. This can apply even if the sender and receiver are the same person (EAR Part 734.18 2023, 20.). Other similarities between the established software and technology export control regulation of the NL, UK and US and be found from the Table 8.

Table 8. Software export control regulation in the NL, UK and US.

No-license required (NLR)	United States (EAR Part 734.18 2023)	United Kingdom (Bond 2021)	Netherlands (Bennink 2019)
Intangible export	Occurs when a controlled software or technology exits the US or when technology or source code is made available to a foreign individual, making it an deemed export to the foreign individual's most recent country of citizenship or permanent residence	Occurs when the controlled software or technology is made available for an entity or in a destination outside of the UK borders	Occurs when the controlled software of technology is made available to individuals physically located outside the Netherlands
Information Security	As a minimum requirement, utilizing security measures conforming to industry standards and employing end-to-end encryption	As a minimum requirement, utilizing security measures conforming to industry standards and employing end-to-end encryption	As a minimum requirement, utilizing security measures conforming to industry standards and employing end-to-end encryption
Server Location in third countries	NLR, if data is unclassified, controlled item is securely transmitted utilizing end-to-end encryption or not intentionally stored in a country under a US Arms Embargo or in Russia.	NLR, if the server is used for storage purposes only, controlled item is secured with end-to-end encryption and thus not made available for access to an entity outside of UK	NLR, if it adheres to industry-standard security measures, employs a private server, and ensures transactions are protected with at least end-to-end encryption.
Nationality of the consignee	The foreign national's latest country of citizenship or permanent residency is one where exporting the	Requires a license only when the controlled software of technology is	The recipient's nationality matters if they are considered a sanctioned party. NLR,

	controlled technology or source code from the US would be allowed by the EAR either through a license exception or in cases where no license is required	accessed outside the UK borders	if controlled technology is shared with individuals inside the NL. Often an EU general license suffices for exporting controlled technology and there's no need for an additional Dutch license
--	--	---------------------------------	---

3.5.1 Information security

In 2013, the Wassenaar Arrangement(WA) incorporated the human security perspective as part of its efforts to mitigate human rights violations highlighted during the Arab Spring pro-democracy uprisings. The WA introduced two categories of cybersurveillance tools: surveillance technologies and intrusion software. (von Wittke, et al. 2016, 13:50) Despite successfully overcoming numerous prior challenges, the WA encountered substantial criticism, notably concerning disagreements among participating states regarding the incorporation of regulations related to information security into their respective national export control legislation.

In May 2015, the US Department of Commerce (DOC) introduced a national proposal on surveillance and intrusion tools. This proposal brought changes to the definition of intrusion software, specifically including network penetration testing products using intrusion software to identify vulnerabilities. Google was among the opponents, expressing concerns about the broad and vague rules, which could financially burden companies involved in vulnerability detecting efforts. By July 2015, a coalition of cybersecurity companies opposed the proposal due to its ambiguity, perceived disregard for the interests of US based companies, and its adverse impact on global research and development. Notably, academic and research institutions faced unique export control challenges, given their commitment to the free exchange of ideas, engagement in cutting-edge technologies, organizational structures, and the international nature of their scientific collaborations (von Wittke, et al. 2016, 39:00.). Following intense lobbying efforts, the DOC proposal was withdrawn, leading to the US renegotiating the 2013 amendments at the December 2016 Wassenaar plenary session. The concept of intrusion software remains part of the Wassenaar Arrangement, with the aim of restricting the export of "hacking tools" that could potentially be used for cybercrime and illegal surveillance. (Ruohonen & Kimppa 2019, 10-11.)

Security researchers, hackers, and academics play a crucial role as the system's "whistleblowers." Companies, governments, and malicious actors are not inclined to expose vulnerabilities in their own software or technology. Consequently, these researchers and academics are the primary source for discovering the facts and ground truth regarding security issues. When these entities are restricted, it raises questions about where accurate information and insights about security vulnerabilities will originate. (von Wittke, et al. 2016, 39:50).

When viewed within the context of the Wassenaar Arrangement, Ruohonen & Kimppa (2019, 14) imply that it does seem unlikely that the arrangement can effectively curb the spread of surveillance technologies and intrusion software, regardless of the scope and their precise definitions. As argued by Bruce Schneier (2019), a fundamental question arises regarding whether the future will prioritize security or surveillance. It's a choice between allowing everyone to conduct surveillance or ensuring that no one can.

The Information security and Privacy expert Bruce Schneier introduced, in the 1999, the People, Process and Technology framework, which became a foundational concept in cybersecurity. This framework emphasizes that when one element changes, the other two must also adapt for a balanced and effective response to change. Over the decades since, the business and technology landscape has undergone profound transformations, driven by the rapid advancement of digital technologies. These changes have revolutionized how we work, learn, and engage with the world. Additionally, new challenges, including information security threats, pandemics, disruptive competition, and geopolitical conflicts, have arisen. Yet, the People, Process and Technology framework remains a widely utilized model and can be considered even more valuable today due to these significant shifts. To thrive, businesses must accelerate innovation, enhance risk management, and meet increasingly demanding expectations. Effectively designing and managing their people, processes, and technologies in times of change can provide the necessary insight and understanding to achieve these goals. (Karlson, 2022) Figure 9 illustrates the practical application of the People, Process, and Technology (PPT) framework by integrating it with the key themes found in the compliance programs of both the United States and the European Union.

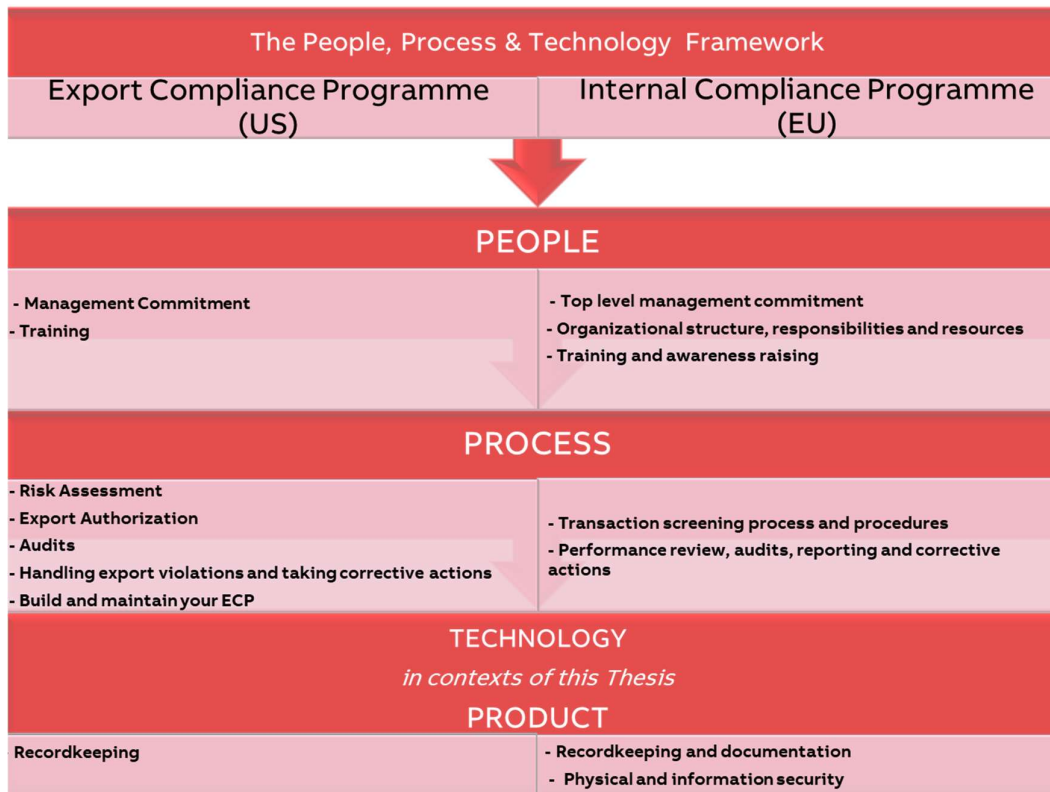


Figure 9. PPT-Framework with ECP and ICP themes grouped under each element.

With this framework Schneider (2013) emphasizes that security should not solely rely on technology; it should also incorporate people and processes into a comprehensive security system. Human intelligence is sometimes necessary to comprehend and respond appropriately to cyberattacks. While technology operates at computer timescales, people and processes function on human timescales. They play essential roles at the strategic and, occasionally, tactical levels. However, the more we can automate these aspects, the more effective our security measures become.

Same can be said from the export control landscape. The four main categories of export control, presented earlier in Figure 3, could be said to present the *people* and *technology* elements. The process element comes into play through how trade compliance units apply this information in accordance with multilateral guidelines and national legislation, as detailed in this existing knowledge section. As a result, the People, Process, and Technology framework provides a solid foundation for a novel export control tool tailored to software and technology exports. This thesis serves as the initial export compliance tool for software products within the sponsor company. Thus, at this stage, the original context of the technology element, pertaining to the tools utilized in the cybersecurity

operations, is not applicable. Furthermore, to prevent confusion regarding technology terminology in export control regulations, the Technology element will represent the actual end-product. This transformation turns the framework in this study into the People, Process, and Product (PPP) matrix."

3.6 Conceptual Framework of This Thesis

The Wassenaar Arrangement <i>(Wassenaar Arrangement (WA), 2021)</i>		
People, Process & Technology framework <i>(Schneier 2013)</i>	US Software export control regulations	EU Software export control regulations
People	<ul style="list-style-type: none"> • Bureau of Industry and Security, 2023: • Export Administration Regulations (EAR) • Commerce Control List (CCL), Product groups D and E • SDN-list & Consolidated non-SDN-list <i>(Office of Foreign Assets Control 2022)</i> 	<ul style="list-style-type: none"> • The European Parliament And The Council, 2021: • Regulation (EU) 2021/821 on on dual-use items • Annex I, subcategories D and E • Consolidated List of Financial Sanctions
Process	<ul style="list-style-type: none"> ✓ Export Compliance Programme (ECP) ✓ Technology Control Plan (TCP) <i>(BIS 2017)</i> ✓ General Prohibitions 4 to 10 (EAR Part 736) 	<ul style="list-style-type: none"> ✓ Internal Compliance Programme (ICP) <i>(European Commission 2019)</i>
Technology <i>and software</i> Product classification	<ul style="list-style-type: none"> ❖ EAR § 734 (EAR Part 734.18 2023) ❖ General Prohibitions 1 to 3 (EAR Part 736 2023) 	<ul style="list-style-type: none"> ❖ Member State specific legislation: Dutch Ministry of Foreign Affairs advisory document 'Guidance Note.' <i>(Bennink 2019)</i>
Information security (WA 2021, Part 5.2) & (EAR Category 5 Part 2) & (Regulation (EU) 2021/821 Annex I, PART VII Category 5 part 2)		

Figure 10. Conceptual framework of this thesis.

The Wassenaar Arrangement serves as an overarching organization without governing authority, where recommendations outlined in the Wassenaar Arrangement WA-List are to be incorporated into the legislative framework of participating states. This thesis primarily focuses on these two participating entities: the United States (US) and the European Union (EU).

A common element across the Wassenaar Arrangement, the US, and the EU, concerning software and technology, is the inclusion of information security within their respective national regulations. Specifically, the US incorporates information security into the Commerce Control List under Category 5 Part Two, while the EU addresses it in Regulation (EU) 2021/821, Annex I, PART VII, Category 5 Part 2. Thus, a tool for further content analysis was derived from the realm of information security. The content from the software export control compliance efforts of both participating states was structured according to the categories outlined in the Bruce Schneier (2013) *People, Process, Technology* – framework.

Both participating states have their own national entities, *People*, to govern the export compliance matters. Further, the *Processes* to reinforce the export compliance regulations include respective compliance programs. In the US, these programs are mandatory for exporting companies, while in the EU, they are merely recommendations. The third theme involves identifying whether the exported software product is indeed a dual-use controlled item. Under the *Technology* category, a distinct disparity becomes evident between the participating states. The US has more comprehensive legislation regarding product-related controls, while the EU has delegated the responsibility for software-specific regulations to its member states.

To conclude, the US is ahead of the EU in terms of software export compliance controls. However, this does not exempt EU companies from the responsibility of staying informed about the export control status of their software offerings. As identified in the General Prohibitions 1 to 3 (EAR Part 736 2023), the US also controls the re-export of technology and software manufactured in the US.

4 Current State of Software Export Control in the Organization

This section takes a closer look at the current state of the case company in terms of its software end-product and export compliance practices. To begin with, an overview of the current state analysis process will be presented, and the information gathered from this analysis will form Data 1. By examining this data, the study will gain a better understanding of the company's strengths and weaknesses and identify the needed features for building the framework for software export control.

4.1 Overview of the Current State Analysis

The goal of the current state analysis was to determine how the existing export control practices support software end-product compliance at the case company. This analysis was conducted on the assumption that current practices within the company provide a basis for those practices discussed in Section 3 of this Thesis. The CSA was conducted in 3 steps.

In Step 1, the conceptual framework was applied for conducting the current state analysis. As stated in Section 1.2, the sponsor organization has yet to implement a process for ensuring compliance with software export controls. To determine how the already established tangible export control practices can be incorporated into a newly built software export compliance framework, a People, Process & Product (PPP) matrix was adopted. This theory-based structure was developed in Section 3 as a basis for conducting the current state analysis and then for developing the proposal later in Section 5. The current state analysis examined how these categories can be applied within the context of the case organizations Software Export Compliance processes. The aim was to determine those areas where knowledge is lacking and to discover potential synergies.

Data for this analysis was obtained through discussions with Management in both Digital Services and Country Trade Compliance, interviews with subject matter experts in Digital Service operations, and an internal workshop to gather data on local units' trade compliance processes and resources. When collecting the data, first, *the management commitment* was confirmed, second, internal company instructions were reviewed, and third, subject matter expert interviews were conducted.

In Step 2, the results for the People, Process & Product (PPP) matrix were pulled together in the context of Export Control practices at the sponsor company. The analysis categories were adopted from the PPT-framework. However, in the scope of this thesis, the 'Technology' category will refer to the actual end-product (Product), further specified as the software offerings of the sponsor company.

In Step 3, the PPP matrix categories served *to identify the key building blocks for the software export control processes* in combination with the tangible export control best practices currently utilized in the sponsor company. A SWOT analysis was conducted to gain a deeper understanding of the current strengths and weaknesses of the tangible export control process. This analysis aimed to identify aspects that could be applied or adapted to enhance the intangible export control framework.

In summary, the current state analysis assesses the suitability of tangible export compliance processes for intangible products and aims to identify gaps that need to be addressed in the software context. This analysis provides a foundation for developing the initial software export compliance framework in Section 5.

4.2 Description of Trade Compliance - Export Controls in Sponsor Company

The focus of this thesis is on software export control as part of the Group's initiative to improve Trade Compliance processes in local divisions. In addition to the national and global trade laws and regulations discussed in Section 3, the sponsor company has developed several internal guidelines, such as the Global Trade Program and Code of Conduct. These documents form the basis for Global Trade Compliance Procedures which aim to ensure that the local divisions have right tools and guidance available in order to comply with applicable Trade Laws and Regulations.

Trade Compliance encompasses the entire order-delivery process, from the initial quoting phase to the delivery of equipment and services, and ultimately invoicing the customer. The trade compliance responsibilities in the sponsor company are divided into Export Control (EC) and Customs Compliance (CC). This Thesis will concentrate on the Export Control Compliance matters.

Each local division has their own Trade Compliance team. The sponsor company's, Trade Compliance organization consists of: Vice President Finance&Controlling, Trade Compliance Officers (EC&CC) and Product Classification Engineers (EC&CC).

The demand for this thesis emerged within the organization as the tangible export control process took center stage in 2022. It marked a substantial learning curve for the entire Trade Compliance team, offering firsthand insights into addressing all four pillars of Trade Compliance, as presented in Figure 3, with regards to tangible exports.

Several areas for improvement were identified and addressed over the course of the year 2022. Consequently, it was identified that technology-related export controls are not limited to tangible exports alone but also extend to intangible transfers.

During a Country Trade Compliance visit to the sponsor company unit, a meeting was arranged which included units' business management representatives and the Local Trade Compliance team. When asked about the next themes the unit should be prepared to address regarding export control, the Country Trade Compliance Officers response was clear: A similar export compliance framework should be established for the unit's software offerings as for its tangible exports.

4.3 Description of Digital Services

The sponsor company offers a wide portfolio of marine software and optimization systems to the maritime market. The Digital Service Product Portfolio consists of a broad range of advisory and fleet management reporting solutions, integrated automation, vessel management and control systems.

4.3.1 People - Organizational structure

At the outset of the initiative, a kick-off meeting was arranged with The Head of Digital and the Head of local Digital Service to clearly denounce the risks associated with non-compliance. These risks included legal, financial, and reputational consequences that could impact the business and its updated strategy from November 2022. To demonstrate their commitment, Management was tasked with assembling a project team

from the Digital Service operations. This team would serve as the counterpart to the Trade Compliance project lead in developing the Export Compliance Framework.

Ultimately, the project team was composed of several Digital Service experts with specialized knowledge and expertise in their respective fields. The project team, interviewee IDs and working location can be seen in Table 11 below.

Table 9. People - Digital Service project team and Management.

Function - <i>CONFIDENTIAL</i>	Interview ID	Location
	P1	Finland
	P2	Netherlands
	P3	Netherlands
	S1	Netherlands
	SAM1	Finland
	Interviewee 1	Global (Finland)
	Interviewee 2	Finland
	Interviewee 3	Finland

When defining the `People` and their responsibilities, the geographic distribution of the project team members posed a challenge, as most of the operations-level team members were located abroad. This raised questions about whether the sales attributed by the Dutch team members should be considered as part of the Finnish office's sales or of Netherlands' entity. Management confirmed that all Digital Service sales performed by the project team are conducted under the sponsor company unit, thereby establishing that all software sales transactions performed by the interviewees fall under the jurisdiction of the Finnish Trade Compliance organization.

The initiative received further validation when Interviewee 2 emphasized to the project team that it is important to Digital Services on a global scale:

I think this exercise is important [...] We need to have these controls in place now that this is trending, stay on top of this one and check the software channels. (Interviewee 2)

A consensus was reached, that this systematic approach to the initiative will also benefit Digital Service by providing an overview of deliverables and helping to improve internal processes in areas such as product management.

4.3.1.1 Customers

Confidential.



4.3.2 Process - Software Supply

This category was divided into two process models: the Sales Process and the Export Delivery Process. The Export Delivery process refers to the method by which products or services are delivered to the end customer (Figure 14).

In addition to direct sales to end customers by the sponsor company, two other sales process models were identified: sales through other intra-company sales units (Figure 12) and sales to external service providers without visibility to the end customer (Figure 13).



Figure 12. Sales through internal sales unit. The black arrow represents the customer value creation and the green arrow the revenue stream. External entity marked with blue color.



Figure 13. Sales to external service provider without visibility to the end customer. The black arrow represents the customer value creation and the green arrow the revenue stream. External entity marked with blue color.

When selling products to end-customers through internal sales units, the responsibility for conducting due diligence on the end-customer lies with the allocated fronting unit. To support local units in gathering the necessary information from customers to verify their compliance, the group-level trade compliance unit has published the End-User Certificate (EUC). This internal document covers all four pillars of trade compliance introduced in Section 4.2. During the Digital Service project teams interviews, it was noted that the stakeholders were not familiar with this document or the red-flag identification email that was distributed last year during the height of EU sanction regimes related to the 2022 geopolitical crisis. However, Interviewee P3 identified that the end-user controls extend beyond the potential geopolitical crisis:

What if any country might be added for whatever reason. So how quick can we then identify that? I assume, that in the process, you are also developing focus more on documentation and linking it to that? (P3)

Regarding the sales via external service providers (Figure 13) a valid concern was raised by Interviewee 2:

What I'm more concerned now is that we utilize sales channels where we provide software as part of this sales channel's product. [...] do we have enough adequate controls in place that we ensure that this third-party entity doesn't sell our products to countries that are sanctioned. (Interviewee 2)

The delivery models were identified as: tangible exports, where the software product is configured into hardware and shipped to the customer, and intangible exports, where the software or service is delivered via cloud or as technical assistance and maintenance.

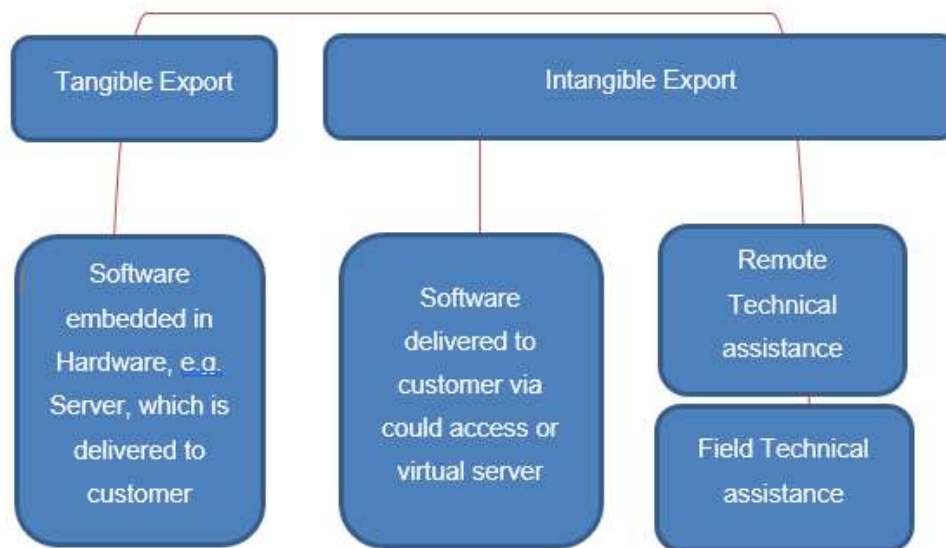


Figure 14. Software and Technology export delivery models in the organization.

In accordance with the Wassenaar Arrangement, intangible technology transfers include the delivery of blueprints and other technical data. In the sponsor company, this falls under the category of technical assistance. In an interview with the Interviewee SAM1, it was highlighted that the SAM technical assistance team has the ability to remotely optimize customers' operational parameters through intangible technology transfer. This aspect may raise export control-related requests from end-customers and will need to be addressed outside the scope of this thesis project.

4.3.3 Product – Marine advisory system

The Marine Advisory System is a modular product family designed for performance management in marine operations. The installation process is straightforward, allowing for immediate reductions in fuel consumption and emissions. The system facilitates real-time monitoring of ships' availability and safety via secure data transmission. Users have access to a variety of information, such as vessel trim data, bunker transfers, fuel consumption rates, power plant optimization, electricity usage, speed recommendations, propulsion power analysis, and hull cleanliness status.

The software is client-server based and can be connected to multiple computers on a vessel. Displays can be configured to show location-specific information and data is automatically recorded. The integration to customers systems was clarified by Interviewee P1 as follows:

Depending on the modules, the preliminary hardware configuration is done at the office and once it is completed the server is shipped to the vessel. The configuration is finalized remotely, during which the firewall settings are checked, and signals testing is performed. (P1)

The software supports different sailing modes and configurable dashboards based on installed licenses and signals. Regarding the user control, one of the benefits of the advisory system is that it is license controlled and needs to be engineered by the supplier as emphasized by the Interviewee S1 in his interview:

Normally, the licenses are annual [...] It is not possible (for the customer) to transfer the system from one vessel to another and we can let the licenses expire in addition to stopping all services, like support. (S1)

Consequently, the only re-selling is done through the external third-party partnership as presented previously in Figure 13. This module of the advisory system is a full integration feature in the third-party partners end-product which is considered to be a sub-product of the advisory system. The basic version includes a sensor and with a more advanced version a 3D module is available for more accurate results. The sponsor company is responsible for supplying the licensing site and the external third-party can control the activation of customer license entries and renewals which are the indicators of actual orders of the module. Thus, the end-user data should be accessible to the sponsor organization if requested from the third-party provider. However, Interviewee P3

mentioned that actual direct end-customer contacts are very rare in the partnership model and are mostly based on customer feedback on technical questions.

4.3.3.1 Classification characteristics

The Software Bill of Materials (SBOM) ties together the cyber security and export control classification in software development. The cyber security requirements related to products intended for use in the industrial automation and control systems environment

Name of software	Contract type/license	Date of contract	Date of supplier compliance	Type of supplier compliance (imp)	Version 21.03.1210	Version 21.06.1228	Responsible technical person
------------------	-----------------------	------------------	-----------------------------	-----------------------------------	--------------------	--------------------	------------------------------

includes standard IEC 62443 4-1 which has multiple requirements related to third-party patch management. For patch management purposes the organization is building a third-party software registry based on the Advisory systems SBOM. Figure 15 shows the organizations 3rd party software registry from the headline level.

Figure 15. 3rd party software registry headlines

Interviewee P2 is responsible for the Cybersecurity of the Advisory systems and is therefore the person monitoring the third-party software database. The registry is divided according to the three applications of the advisory system: server, client, and configurator. During his interview, when discussing the addition of export control related product details to this registry, he mentioned that keeping the register up-to-date is not a significant task in its current state. However, for the future, roles and responsibilities (RACI) would need to be better defined:

In our current way of working [checking the registry] it is always in the end. Everybody needs to check what was the update and do we still need to update things. So it's not part of the process and if that [RACI] would be part of the working process, it would be much easier. (P2)

Furthermore, Interviewee P2 raised an important point regarding the potential synergy benefits of centralizing the third-party software registry rather than maintaining it at the individual product level:

If every product has their third-party software on this list, and also the version of it, it is something that the organization could save money with because we can have a license sharing. (P2)

Regarding the possibility for obtaining the export classification info from the third-party software providers, Interviewee P2 expressed some skepticism, considering that in software development, some of the utilized products operate on a free license basis and thus does not create any obligatory responsibilities towards the software supplier to deliver such information.

Regarding the classification status of the actual Advisory system, Interviewee P2 was not familiar with the classification of software products. However, based on general knowledge of dual-use and military end-use, P2 estimated that the Advisory systems would not fall under any product-related controls. Similarly, the Interviewee S1 estimated that due to the advisory nature of the product, the risk of it being used for unwanted activities would be low:

The software is functional only when it's engineered from our side and it has license control [...] our software is advisory software and not a critical part of the operation. If you disable it the vessel can still sail and we are not controlling anything in the engine room what so ever. (S1)

Overall, the general consensus was that the Advisory system would not be classified as a controlled product. However, given the incomplete SBOM of third-party software, this form of generalization indicates the extent to which product owners and software sales personnel comprehend the significance of the export control landscape.

4.4 Current State of Tangible Export Compliance - Strengths and Weaknesses

As previously mentioned, intangible technology transfers represent an emerging area of export control for the unit. Therefore, the following strengths and weaknesses matrix is based on experiences gathered from the tangible export control side. However, the pillars of export control remain consistent, irrespective of the specific technology being evaluated for compliance with international trade laws and regulations.

This export compliance strengths and weaknesses matrix was a summary gathered during the Global Trade Risk Assessment Workshop in May 2023 (Table 1, ID 3). The workshop was held to respond to a group-level Risk Assessment Panel questionnaire

regarding the current state of Trade Compliance, both EC and CC, in each division globally.

Regarding export control (EC), the questionnaire was used to inquire how each unit implemented the following internal Global Trade Instructions, presented in Table 9, across their value chain.

Table 10. Questionnaire on following internal Global Trade Instructions regarding export control (EC).

Areas of internal Global Trade Instructions
<ol style="list-style-type: none"> 1. Critical Assessment process 2. Sensitive <i>Internal</i> Protocol 3. Who oversees and manages the Global Trade Program 4. How to review and resolve Sanctioned Party List (SPL) screening hits 5. Integrity List and other Screening Lists 6. How to identify if you need an export authorization 7. How to obtain an End Use Certificate 8. How to classify products, software & technology 9. How to create a Technology Control Plan 10. How to manage global trade recordkeeping

The results of the questionnaire were categorized into strengths and weaknesses, providing insights into the current state of the export control processes, as shown in Table 10 below. Due to the business sensitivity of the Global Trade Risk Assessment, the details of how the results were obtained are exclusively accessible through the Global Trade Compliance portal and could not be reported in this study.

In the SWOT analysis the four pillars of export control are themed under the categories of People, Process and Product.

Table 11. Current state of Export Control (EC), based on the results of Global Trade Risk Assessment.

The 4 Pillars of Trade Compliance, Export control	Product related controls	End Controls	User	Destination Controls	End Use Controls
Strengths and Weaknesses					
PEOPLE	<p>TCO team's members have received dedicated time for their compliance related tasks</p> <p>Not enough Product classification resources</p>	<p>Adequate amount of trained personnel to check the sanction databases</p> <p>Fronting sales unit awareness regarding export control "red flags"</p>		<p>Adequate amount of trained personnel to check the sanction databases</p> <p>Fronting sales unit awareness regarding export control "red flags"</p>	<p>Standardized statement (EUC) for allowing more detailed end-customer screening</p> <p>End-customer communication regarding trade compliance due diligence</p>
PROCESS	<p>Classification synergies from other business divisions utilized adequately</p> <p>Obtaining the technical knowledge of the products and classification process</p>	<p>FI organizations understanding of compliance roles and responsibilities is adequate</p> <p>Fronting sales unit awareness regarding compliance roles and responsibilities</p>		<p>Adequate number of databases and internal recourses to adequately stay on top of controls</p> <p>Fronting sales unit awareness regarding compliance roles and responsibilities</p>	<p>FI organizations understanding of compliance roles and responsibilities is adequate</p> <p>Process for end-customer communication to be established</p>
PRODUCT	<p>Own production end-products can be considered originating from the European union.</p> <p>How to obtain and upkeep the third-party component classification data</p>	<p>Deemend export mostly related to US, CN and RU</p> <p>Process for 3rd party spare parts sales to be established</p>		<p>Deemend export mostly related to US, CN and RU</p> <p>Process for 3rd party spare parts sales to be established</p>	<p>Own production tangible dual-use items have been identified</p> <p>Additional technical understanding needed to objectively make end-use risk assessments</p>

When analyzing these results with the sponsor company Trade Compliance Officer (LTCO), the key insights that came up as significant for building the framework for the intangible product export control were as follows.

First, regarding the 'People' aspect, it was identified that the local unit has a good understanding on the tangible export control regulations and an adequate training plan

for local stakeholders. Secondly, a question was raised should there be a 'Process' to verify whether the intra-company customers (e.g. other sales unit) comply with these Global materials locally. Consequently, the LTCO wanted to highlight the importance of identifying the correct Responsible, Accountable, Consulted, and Informed (RACI) entities:

It is important to note that the 'People' category encompasses various departments within the organization, ranging from R&D to Sales, Procurement and Logistics. The primary responsibility of the Trade Compliance Team is to educate these departments on the global trade compliance laws and regulations for which they are accountable for in their daily tasks locally.

Other intra-company sales units may seek consultancy regarding the direct deliveries of products and services from the Finnish organization. However, the responsibility of the end-customer due diligence lies with the fronting sales unit.

Regarding the 'Product' category, it was identified that technical expertise is a notable weakness within the local Trade Compliance team. Especially, the sponsor company's own production is in urgent need of additional resources for the role of Product Classification Engineer (PCE). Furthermore, it will be necessary to place greater emphasis on the handling of Export Control master data of third-party components. As an example, when third-party components are resold as spare parts, the responsibility for ensuring the accuracy of their product classification status is transferred to the reseller organization.

4.5 Key Findings based on PPP matrix

The goal of the Current State Analysis(CSA) was to identify the key building blocks for the current software export control process, based on tangible export control best practices in the sponsor company. Table 12 present the key insights gained in each category of the PPP matrix.

Table 12. Key findings from CSA for the current Export control of Intangible Technology Transfers.

Product, End-User, Destination, End-Use	The Four Pillars of Export Control
PEOPLE	Establish the way-of -working regarding export compliance with external service providers <i>The sales via license are different to tangible deliveries defined by delivery terms.</i>
PROCESS	Red-flag identification for Intangible technology transfer <i>Awareness raising throughout the value chain</i>
PRODUCT	Determine the data required for export classification process <i>Identify, and assist to obtain, the info that should be combined to the SBOM third-party registry</i>

Regarding the *People*, for the Trade Compliance Team, the primary responsibility is to provide internal stakeholders with up-to-date information regarding applicable trade laws and regulations and assist in daily operations. In the context of software offerings, controlled exports can be embedded into a hardware component, making them a tangible export or they can fall under the intangible transfer category presented on the export delivery models in Figure 14 on page 52.

As previously stressed, the sponsor company has several internal guidelines that should be implemented by each sales unit respectively. While the responsibilities may require some internal review, a greater challenge could be identified with the external service providers. Again, each external service provider should comply with applicable global trade laws and regulations. It is important to engage with existing service providers to confirm and potentially learn from their implementation of relevant legislation, such as US software export controls.

As for the *Process*, the need for a “Red-Flag” identification was a recurring theme all the way from the unit’s business management to the different project team members. The

awareness-raising could be achieved through Trade Compliance training, which should be taken into account when planning the next training cycle in the sponsor company unit. The complexity of marine vessel ownership structures, combined with the introduction of a new customer segment (purely software customers), necessitates a review of the red-flags identified with the tangible exports. The overall attitude towards compliance issues within the sponsor organization appeared to be evolving. Similar to the field of information sciences in general, the subject of export control compliance involves both social and technical elements. A culture of compliance is necessary to fully understand and adhere to current laws and regulations.

Finally, the *Product*, the Advisory system is primarily delivered through intangible means. Irrespective of the specific technology being exported, the transaction must always be evaluated against the four pillars of export control.

While the actual classification of the sponsor company's software end-products is ultimately the responsibility of the Product Classification Engineer (PCE), general understanding and the data gathering required for classification purposes can be initiated through the export compliance framework project. The third-party software registry serves as a valuable foundation and has the potential to benefit both the Trade Compliance team and the Digital Service operations. From the perspective of Trade Compliance, the key tasks include identifying the export control-related data, facilitating communication with third parties regarding subject matter requirements, and emphasizing the importance of roles and responsibilities in maintaining an up-to-date registry.

5 Initial Proposal for the Export Compliance Framework

This section integrates the outcomes of the Current State Analysis(CSA) and the conceptual framework, leading to the development of the initial proposal through internal co-creation and external partner interview, which form the basis for Data Collection 2.

5.1 Overview of the Proposal Building Stage

This section presents the steps in the Proposal building for this study. The aim is to develop solutions to the key findings identified in the Current State Analysis, Table 13. The foundation for constructing the proposal is established upon the existing knowledge from Section 3, which will be supplemented by the interview discussions conducted in Data Collection 2.

Table 13. Correlation of Data Collection 2 with Current State Analysis and Existing Knowledge

Existing Knowledge	Product	End-user	Destination	End-use
PEOPLE	CSA: Establish the way-of -working regarding export compliance with external service providers			
	Data 2	Interviewee II: External Partner, Commercial Leader, Shipping (US) Interviewee I: External partner, Product Director, Shipping (NL)		
PROCESS	CSA: Red-flag identification for Intangible technology transfer			
	Data 2	Interviewee III: Project team member, Global Sales Manager(2)		
PRODUCT	CSA: Determine the data required for product classification process			
	Data 2	Interviewee IV: Trade Compliance Officer, Other Internal Division Interviewee V: Product Classification Teams leader, Other Internal Division		

Under the *People, Process and Product* themes, the proposal should take into account all the pillars of export control identified in Figure 3 of the existing knowledge. To better

support the sponsor company specific approach to the proposal, the co-creating entities were chosen based on the key finding identified in the CSA.

Under the *People* theme, the focus was on understanding how external partnerships manage their export due-diligence. Consequently, interviewees were selected from an external software sales provider of the Advisory systems product. To organize this interview, a set of questions was compiled and sent to the interviewees in advance to allow them to prepare. These questions were formulated based on the topics identified in the existing knowledge. They tackle elements pivotal for due diligence screenings and explore areas that could offer the sponsor company valuable perspectives on how other organizations implement these procedures. The questionnaire template can be found in Appendix 2. Due to a Non-Disclosure Agreement between the sponsor company and the external service provider, this section of the proposal will be excluded from the publicly available study.

In the *Process* theme, it was crucial to involve a member from the Project team, established in the CSA in Section 4. The interviewee was chosen from the direct customer interphase, specifically from the sales department. As highlighted in the key findings of the CSA, the identification of red flags in the delivery process was not clear enough for the project team to independently recognize potential due-diligence risks. Therefore, an initial red-flag identification document was established as the foundation for this interview. The document was developed based on existing knowledge best practices related to red-flags in export processes, combining both regulatory sources and already established red-flags from the tangible products of the sponsor company. The document can be found from the Appendix 3.

The *Product* theme encompassed the most technical information. As indicated in the CSA, the Software classification process had not yet been established within the sponsor company. However, other divisions under the company group were already engaged in ongoing processes related to software classification. Consequently, an interview with a knowledgeable internal division was deemed necessary. Additionally, as highlighted in the CSA, there are several internal guidelines in connection to export controls that all divisions should be implementing. Therefore, a similar baseline had already been established among the internal divisions. The interview with the export control- and product classification specialists from the other division primarily focused broadly on the themes of software classification and export control in general, aiming to extract the most

valuable best practices from their experiences. The layout of the interview framework can be found in Appendix 4.

5.2 Findings from Data 2

The selection of the external service provider for the co-creation proposal development phase was based on their presence in both the Netherlands and the United States. These locations are governed by comprehensive legislation concerning intangible export controls, as outlined in the existing knowledge Section 3. The results from this interview will not be published due to the Non-Disclosure Agreement.



<i>Key focus areas from CSA</i>	<i>Inputs from existing knowledge</i>	<i>Possible additions from Data 2 for the Proposal</i>	<i>Descriptions of Interviewee input (in detail)</i>
CONFIDENTIAL			

CONFIDENTIAL		

The initiation of the red-flag identification process within the sponsor company involved the formulation of a comprehensive red-flag identification document. This document was developed by integrating red flags identified by the Trade Compliance Officer in relation to tangible products and aligning them with the parameters outlined in the European Union Internal Compliance Programme (ICP) (European Commission 2019, 30). The Global Sales Manager from the project team quickly showed a strong understanding of the co-creation process, recognizing early on that they had discussed delivering products to sensitive countries before. However, these prior conversations primarily centered on financial compliance, with no training resources dedicated to this specific area. The Global Sales Manager also acknowledged that the Local Sales Units (LSU) identified in the CSA bear the primary responsibility for due-diligence matters, given their direct interface with end-customers. One concern raised by the Global Sales Manager was his perception that expertise in product-related controls represents a gray area for him, necessitating further clarification. Table 15 summarizes the key findings collaboratively generated with the Global Sales Manager.

Table 15. The project teams insights for Proposal building.

<i>Key focus areas from CSA</i>	<i>Inputs from existing knowledge</i>	<i>Possible additions from Data 2 for the Proposal</i>	<i>Descriptions of Interviewee input (in detail)</i>
Awareness raising on red-flag identification	1) 'Red flags' relating to suspicious enquiries (ICP 2019, 30)	1a) Checklist of red-flags before contract signing	The Sales Manager recalled the existence of a sales checklist outlining key considerations for contracts with new customers. Unfortunately, the tangible document of the checklist was no longer accessible, having become obsolete over time.
		1b) Product related controls need to be more specific and tangible	The Sales Manager expressed a lack of current information regarding the extent to which the software products could have dual-use applications. He emphasized the importance of verifying this aspect.

Upon analyzing the key findings, it was determined that a distinct checklist for red flags (1a) was necessary. The implementation of separate documents for Customer and Product controls could enhance precision in guiding users of the export compliance framework(1b). Additionally, introducing a specialized Red-flag checklist could explicitly outline European Union (EU) regulations that the LSU might inadvertently overlook during their due-diligence checks on end-customers.

The concluding segment of Data 2 collections for proposal building focused on best practices for the software export control classification process. The interviewed internal division doesn't directly sell dual-use classified software as the final output. Instead, it develops software products that, when integrated with hardware and accompanied by the appropriate license, transform the end-product into a dual-use item. This internal division, and the sponsor company, are actively working in the global compliance environment. Given that this study will be validated at the Country level compliance, it was justifiable to gather the primary challenges the division encountered in its software export control process. This approach aims to bring these challenges to light at the country level, fostering synergies. This facilitates co-creation in both directions, addressing the internal division's challenges and, ultimately, benefiting all divisions if global compliance takes action based on the suggestions proposed in this Thesis. Thus, Table 16 presents the key findings and the main pain points identified by the internal division.

Table 16. Insights and Pain Points from the Internal Division.

<i>Key focus areas from CSA</i>	<i>Inputs from existing knowledge</i>	<i>Possible additions from Data 2 for the Proposal</i>	<i>Descriptions of Interviewee input (in detail)</i>
Determine the data required for product classification process	1) People 2) Process 3) Product	1 a) Registry of third-party software's with designated owners for each component and embedding 1 b) Team of product classification engineers(PCE)	The PCE team leader presented a thorough database guiding to the third-party registry that outlines roles and responsibilities for each member named in the registry. Prior to the software classification by the PCE team, all pertinent information for the related components must be submitted. The PCE team currently consists of four engineers, none of whom specialize in software. Therefore, accurate information from the third-party registry is essential for proper classifications.
		2 c) Utilizing existing internal guidelines like the Software Classification Map and the Product Classification report(PCR)	The PCE team leader explained that they utilize the software classification map supplied by the Country Trade Compliance Officer (CTCO). This document involves creating another internal report, the Product Classification Report, which the division's TCO can then proceed with to assess the potential requirement for an export license application

		<p>3 e) Identifying embedded US content in the software, along with component's value share in the final product and ultimately the ECCN</p> <p>3 f) Software classified by the EU dual-use regulation based on capabilities and characteristic</p>	<p>The PCE team leader mentioned that the initial step involves identifying US content associated with the software under consideration. The subsequent step involves the US ECCN classification, if applicable. After that, they proceed with the EU classification process, with emphasis on the software's properties and potential cryptographic elements. As of now, no defense-related classification has been conducted.</p>
Main Pain points	<ul style="list-style-type: none"> • Third-party component export control details, how the information is inquired and validated. According to the PCE team leader, <i>"In 90% of the cases, when asking the supplier for export control classification, they did not recognize what was being asked."</i> • The management of batch upgrades, with regard to export control considerations, is facilitated through the license model, enabling the utilization of software as outlined by the PCE team leader. Is this a sufficient method for managing updates on classified software products? • PCE team leader and the TCO both agreed that the support offered by global-level compliance was insufficient concerning software export control matters. This includes support for software expertise in PCE roles and tools for leveraging emerging technologies while still adhering to company regulations and legislation. 		

The software classification process within the division is based on a third-party software registry (1a). The PCE team (1b) utilizes information from this registry to perform the export control classification process. Throughout the classification process, the PCE team makes use of internal compliance tools, such as the software classification map and Product Classification Report (2c). When classifying a software product, the initial step involves calculating the US content and share value, followed by identifying ECCN codes at both the component and end-product levels (3e). Subsequently, the software undergoes evaluation against the EU dual-use regulation to determine the EU classification code. Following this stage, the Trade Compliance Officer (TCO) undertakes a pivotal role in the compliance process, conducting a comprehensive due-diligence examination across all four pillars of export control.

The PCE team faced significant challenges primarily centered around maintaining and ensuring the cleanliness of the third-party registry. Obtaining export control data from suppliers proved to be a complex task, demanding additional actions to facilitate the

classification process. This difficulty was compounded by the fact that the PCE team lacked the necessary software expertise, despite a year-long recruitment effort. Concerning emerging technologies, the absence of clear company-level guidelines was recognized as a risk both commercially and reputationally. The rapid pace of digital transformation requires swift evolution of the compliance tools; failure to keep up could expose companies to potential commercial losses or reputational risks if export control is not executed properly or hinders product development.

5.3 Summary of the Initial Proposal

The initial proposal was organized into a matrix, with the People, Process, and Product elements structured under the four pillars of export control. The substance for the framework matrix is based on a combination of findings from co-creation Data 2 and regulations studied in existing knowledge. Additionally, in line with best practices from the external service provider and previous compliance processes recalled by the project team, a separate document for identifying red flags was created to better support the initial customer interactions. The Red-flag identification document is presented in Figure 16.

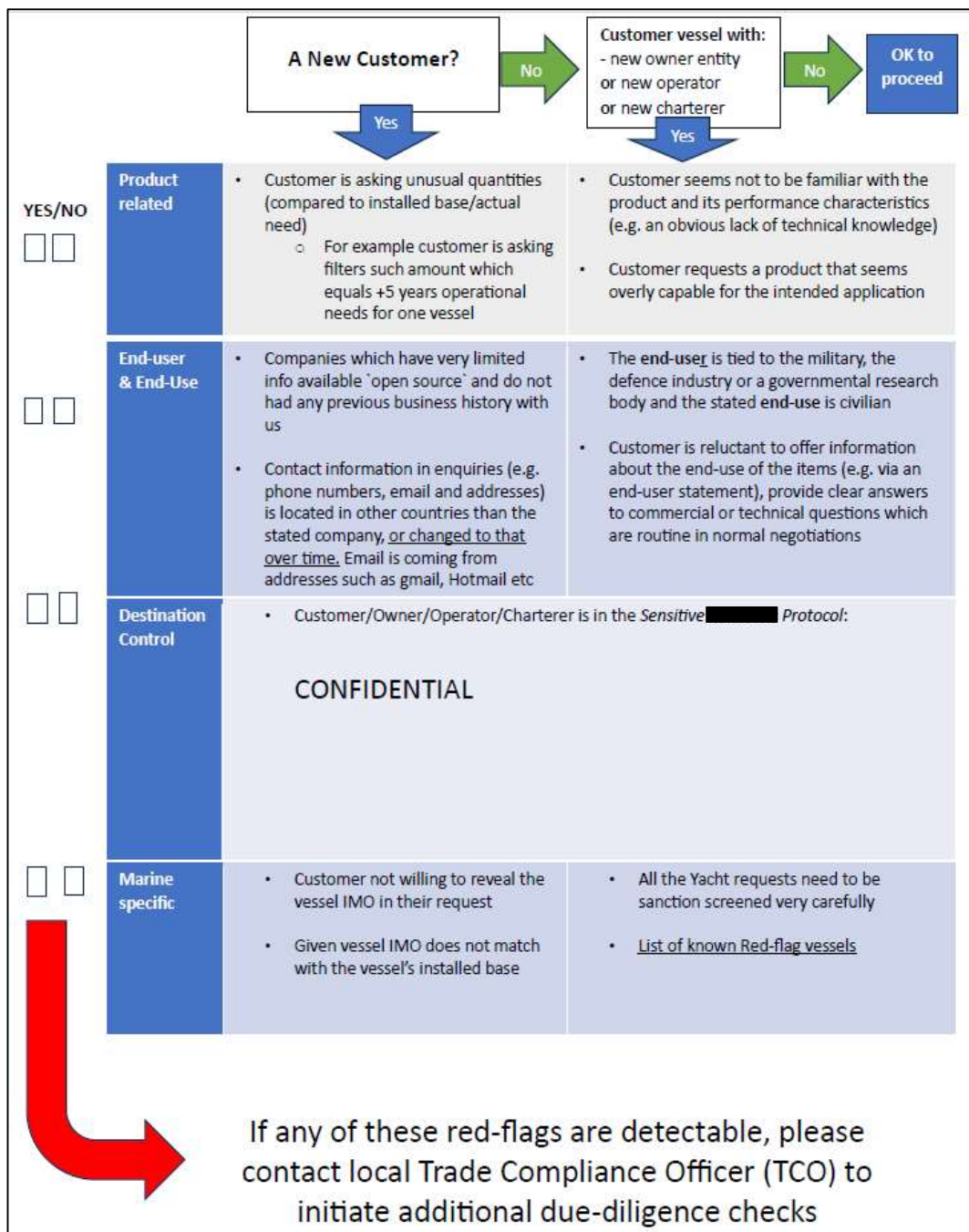


Figure 16. Initial Red-flag identification document.

The document instructs users to contemplate the two main scenarios that could prompt a due diligence check: one involving a completely new customer and another involving an existing customer whose vessel has undergone changes in its organizational entities. If one of these scenarios is identified, the documents will guide the user through export control-related scenarios. The user must check if any of them apply to the specific case.

The document's closing statement directs the user to contact the local Trade Compliance Officer (TCO) if any of these statements are marked as "YES." This format allocates the responsibility for the initial due-diligence check to the user and helps the TCO understand the nature of the case in question and paves the way towards the more in-depth export compliance matrix presented in Table 17, below.

Software Export controls (US and EU)	Product related controls	End-user Controls	Destination Control (Country of destination)	End-use Controls
PEOPLE	<ol style="list-style-type: none"> 1) Trade compliance officer (TCO) 2) Product classification engineer (PCE) 3) Software owner <ul style="list-style-type: none"> ➤ provide BOM with export control details** 	<ol style="list-style-type: none"> 1) Fronting sales unit <ul style="list-style-type: none"> ➤ Provide full information 2) Trade Compliance Officer <ul style="list-style-type: none"> ➤ for due diligence screening ➤ LINK EUC 	<ol style="list-style-type: none"> 1) Fronting sales unit <ul style="list-style-type: none"> ➤ Provide full information 2) Trade compliance officer <ul style="list-style-type: none"> ➤ for due diligence screening ➤ LINK EUC 	<ol style="list-style-type: none"> 1) Fronting sales unit <ul style="list-style-type: none"> ➤ Provide full information 2) Trade compliance officer <ul style="list-style-type: none"> ➤ for due diligence screening ➤ LINK EUC
PROCESS	<ul style="list-style-type: none"> • Software Classification Map LINK • Product Classification report(PCR) LINK <ul style="list-style-type: none"> ➤ Product classification in Master database 	<ul style="list-style-type: none"> • SDN-list & Consolidated non-SDN list (GTS) • EU Consolidated List of Financial Sanctions (GTS) <ul style="list-style-type: none"> ➤ TCO to perform screening from databases (Orbis, MKdenial, web search) 	<ul style="list-style-type: none"> • Red-Flag Country list, <i>Internal</i> • EAR Part 736: <i>General Prohibitions 4 to 10, External</i> <ul style="list-style-type: none"> ➤ BIS Commerce Country Chart 	<ul style="list-style-type: none"> • Is the end-use military, intelligence or navy? Please contact TCO.
PRODUCT	<ul style="list-style-type: none"> • **US content calculation and value share • **US ECCN classification <ul style="list-style-type: none"> ➤ Component level • US ECCN classification <ul style="list-style-type: none"> ➤ End-product level • EU dual-use classification 	<ul style="list-style-type: none"> • User login trail: <ul style="list-style-type: none"> ➤ license key based ➤ other 	<ul style="list-style-type: none"> • Data storage location not in the Red-Flag Country list <ul style="list-style-type: none"> ➤ GDPR rules for data storing • EAR Part 736: <i>General Prohibitions 1 to 3</i> 	<ul style="list-style-type: none"> • EU Official Journal C 72/2023 • US Munition list: eCFR 22 CFR Part 121 ❖ <i>ECRA; Section 1758 technologies</i>

Figure 17. Initial Export Compliance matrix.

The color coding in the matrix indicates who is responsible to provide each information. Green marks for responsibilities of the user and light blue the responsibilities of the Trade Compliance Officer (TCO) and Product Classification Engineer (PCE). The color again allocates the responsibility of information gathering and speeds up the due-diligence process creating a more efficient export control process.

The People element is quite consistent across all four pillars. As established in the current state analysis, the primary sales unit serves as the initial point of contact for customer due diligence information. The TCO can only initiate the due diligence checks once this information is provided by the leading sales unit. In the Product related controls pillar, an addition of PCE and the Software owner was deemed necessary. This is because the classification process requires a subject matter expert to carry out the software classification. Moreover, it is essential that all information from the bill-of-materials level be accessible through the cooperation of the software product owner. Alternatively, the third-party registry could serve as an alternative source for providing the needed information.

The Process element primarily comprises internal guidelines or tools identified during interviews with the other division. Additionally, certain EU and US regulations related to the export control process have been included, some of which are integrated into the sponsor company's ERP system (GTS), while others were identified in the existing knowledge section. In the End-use Controls pillar, special attention was given to the potential for military end-use.

Within the Product element, the monitoring of US content within final products is a pivotal element in the product classification procedure. As presented in the existing knowledge, the United States actively oversees the re-exportation of goods originating from its territory. Moreover, findings from interviews conducted with both the External Service Provider and the Internal Division in Data 2 underscore that US based companies are obligated to adhere to US regulations. The ongoing capability of End-user Control was considered feasible for the Marine Advisory System through the license key-based registry. However, scaling this functionality to non-license-based software products may present challenges. When establishing Destination Control for data location, it is essential to account for the internal guideline limitations, GDPR regulations, and US restrictions. Additionally, End-Use Controls could make the software fall under the consideration of US or EU military lists. Finally, emerging technologies were incorporated

into the End-Use Control to serve as a reminder for TCO and PCE, anticipating potential future developments in software and technology controls.

In conclusion, the framework matrix aims to clarify the roles and responsibilities of all business functions related to export control due diligence. The initial proposal incorporates many best practices established in Data 2. Additional key regulations were included as supplements to assist the Trade Compliance team in their due diligence and product classification tasks. However, some details, such as End-user tracking, were left open in the initial proposal. Therefore, the validation process could play a crucial role in making the final proposal more impermeable. Furthermore, there should be discussions around the main pain points identified in data 2.

6 Validation of the Proposal

In this section, the validation process and the ultimate result of the thesis are presented. It discusses the completed tasks and outlines the forthcoming steps.

6.1 Overview of the Validation Stage

This section outlines the validation outcomes for the proposal detailed in Section 5. The validation process comprised three sequential steps. First, the initial proposal was presented to the organization's country-level Trade Compliance experts possessing extensive knowledge in export compliance. Second, the comments provided by these experts were collected and analyzed, as illustrated in Table 18, 19 and 20 formed by each element. Lastly, in the third step, the feedback from the experts was incorporated into the final proposal.

6.2 Validation by Subject Matter Experts

The organizations subject matter experts were invited into a meeting for the preview of the proposal created in Section 5. This meeting creates the Data Collection 3. The subject matter experts consisted of the Country Trade Compliance Managers in export control and customs control. The Sponsor company Trade Compliance officers were also present. In the meeting the red-flag identification and the framework matrix were presented, and ongoing dialog was advised to the listeners. Furthermore, the main focus points identified within the other divisions during the proposal-building stage were brought up for discussion.

The red-flag identification received only minimal feedback as it was mainly based on the EU official Internal Compliance Programme (ICP) materials. A suggestion was put forward to modify the layout, suggesting that it would be more effective to initially address the various themes of red-flags before determining the customer's status as new or existing. This would enhance the awareness of the reader as defined by the sponsor company Trade Compliance Officer:

When the reader/user first goes through all the red flags related to the business conduct, it provides more context to their awareness than just settling for the lowest hanging fruit of a new customer.

The revised red-flag identification document can be found from Appendix 5. The revisions to the framework matrix will be gone through in more detail in the next sub-section.

6.2.1 Developments to People, Process and Product elements of the Initial Proposal

The People element within the framework matrix was emphasized as a resource-related concern. The focus was placed on the necessity for a Product Classification Engineer (PCE) with expertise in software products. Additionally, attention was drawn to the due diligence responsibilities of Local Sales Units (LSU), underscoring the importance of expertise in export compliance across various country units. Detailed remarks from the Country-level Compliance Officer concerning the People element can be referenced in Table 16.

Table 17. Expert suggestions (People) for the Initial proposal.

<i>Element from the Initial proposal matrix</i>	<i>Pillar commented in Validation</i>	<i>Description of the remarks from experts</i>	<i>Implementation to the Initial proposal</i>
People	a) Product related controls	a.1) Securing a proficient PCE with the requisite expertise is currently proving to be a considerable challenge. If urgent needs occur, assistance for software classification activities can be sought from other divisions.	The role of the PCE will be removed from the current matrix due to the unavailability of resources at present and in the foreseeable future

The need for a skilled software classification engineer triggered a lot of discussion among the *People* element. As emphasized, the issue isn't confined to the sponsoring company but was one of the main pain points identified with the other internal division. Consensus was reached that there is no swift solution to address this issue. Considering the rarity of an expert possessing both software characteristics and export control knowledge – a combination likened to finding a unicorn. (a.1) However, the CTCO emphasized that

initiating the process with a software professional who shows an interest in export controls could serve as a viable starting point:

The initial factor is the genuine interest in the topic. By immersing themselves in the knowledge, expertise is cultivated. The crucial aspect is that this growth occurs authentically through interest, not through coercion.

In addition, addressing the challenge of acquiring such expertise should be escalated to the global division-level trade compliance discussions. The objective could be to cultivate a global-level expert capable of aiding local divisions with mandatory level classifications, while allowing the definition of division-specific characteristics to be handled locally.

Table 18. Expert suggestions (Process) for the Initial proposal.

<i>Element from the Initial proposal matrix</i>	<i>Pillar commented in Validation</i>	<i>Description of the remarks from experts</i>	<i>Implementation to the Initial proposal</i>
Process	a) Product related controls	a.1) A revised Code of Conduct (CoC) for suppliers is scheduled to be introduced next year, and the training sessions could serve as an excellent platform for educating suppliers on the export control requirements	The CoC for Suppliers link to be added to the matrix to emphasize the responsibility of the suppliers
		a.2) Work instructions are required for the US content calculation process to ensure its standardization	A reference to the US content calculation instructions will be include, upon completion

The inputs to the Process element once again centered on controls related to the product. Firstly, to underscore the supplier's responsibility in providing component-level export control information, it was suggested to incorporate the revised Code of Conduct into the Process element level. Additionally, there was a proposal to organize training sessions for suppliers as part of the revised Code of Conduct info-sessions. Finally, the CTCO emphasized the importance of standardizing the US content calculation process to ensure consistency in calculations during potential auditing sessions.

In conclusion, especially for the sponsor company that works in the project business and has to perform the due-diligence, such as sanction screenings, mostly manually the need

for verified standardized operating procedures is enhanced as highlighted by the sponsor company Trade Compliance Officer:

We have various sales channels, and merely understanding how each of them operates is a task in itself and the complexity is compounded by the unique characteristics of vessel ownership structures.

Table 19. Expert suggestions (Product) for the Initial proposal.

<i>Element from the Initial proposal matrix</i>	<i>Pillar commented in Validation</i>	<i>Description of the remarks from experts</i>	<i>Implementation to the Initial proposal</i>
Product	a) Product related controls	a.1) Access to component-level product classification data from suppliers should be improved, and clear requirements should be communicated to suppliers.	Updating the responsibility for component-level classification data to green indicating that the primary responsibility does not lie with the TCO team
		a.2) The removal of the sponsor company's main product from the EU dual-use classification list does not absolve the responsibility of identifying the US content of software at the bill-of-material level	Mention of the third-party COMPONENT registry to be added to the Matrix

The discussion concerning supplier responsibility continued in the People element. This dialogue emphasized the importance of providing comprehensive instructions that can be sent to suppliers, guiding them on the necessary export control-related data and the process to obtain it. Recognizing that the challenge of component-level export classification data extended beyond the sponsor company, as acknowledged during the initial proposal building stage, it was deliberated to escalate this matter for consideration at the global level of trade compliance.

On the day of the Validation interview, the EU published a revised list of dual-use items subject to export controls, outlined in the Export Control Regulation (EU) 2021/821 as Annex I. This updated list resulted in the removal of the sponsor company's main product from its dual-use status, thereby exempting the software's operating the unit from

potential dual-use classification. However, discussions persisted regarding software sold as the main product, such as in the digital services department, introduced in the Current State Analysis Section. The Country Trade Compliance Officer (CTCO) emphasized the need for the product classification process to be applicable to all independent software, with a particular focus on the US content aspect:

The US content review cannot be bypassed. It is necessary to separate all third-party software and acquire the product classification information from each of them. This data must be codified into the content calculation method to demonstrate the justification for the approach.

This notion, given by the CTCO, highlighted the significance of the third-party component registry as a tool for the software classification process. Going forward, it should be integrated into all software across the sponsor company.

6.3 Final Proposal

The final export compliance matrix, presented in Figure 18, incorporated the valuable feedback and insights gathered from the key stakeholders. After analyzing and incorporating the comments and suggestions provided, the framework was enhanced to ensure its effectiveness and alignment with the organization's goals and requirements. This collaborative refinement process finalized the development of a comprehensive export compliance framework that aims to meet the needs of the organization and effectively mitigate risks associated with export control compliance.

Software Export controls (US and EU)	Product related controls	End-user Controls	Destination Control (Country of destination)	End-use Controls
PEOPLE	<ol style="list-style-type: none"> 1) Software owner <ul style="list-style-type: none"> ➢ provide BOM with export control details** 2) Trade compliance officer (TCO/PCE) 	<ol style="list-style-type: none"> 1) Fronting sales unit <ul style="list-style-type: none"> ➢ Provide full information 2) Trade Compliance Officer <ul style="list-style-type: none"> ➢ for due diligence screening ➢ End User Certificate LINK 	<ol style="list-style-type: none"> 1) Fronting sales unit <ul style="list-style-type: none"> ➢ Provide full information 2) Trade compliance officer <ul style="list-style-type: none"> ➢ for due diligence screening ➢ End User Certificate LINK 	<ol style="list-style-type: none"> 1) Fronting sales unit <ul style="list-style-type: none"> ➢ Provide full information 2) Trade compliance officer <ul style="list-style-type: none"> ➢ for due diligence screening ➢ End User Certificate LINK
PROCESS	<ul style="list-style-type: none"> • Supplier Code of Conduct LINK • Software Classification Map LINK • Product Classification report(PCR) LINK • Encryption Classification Form LINK 	<ul style="list-style-type: none"> • SDN-list & Consolidated non-SDN list (GTS) • EU Consolidated List of Financial Sanctions (GTS) <ul style="list-style-type: none"> ➢ TCO to perform screening from databases (Orbis, MKdenial, web search) 	<ul style="list-style-type: none"> • Red-flag Country list, LINK • EAR Part 736: <i>General Prohibitions 4 to 10, External</i> <ul style="list-style-type: none"> ➢ BIS Commerce Country Chart 	<ul style="list-style-type: none"> • Is the end-use military, intelligence or navy? Please contact TCO.
PRODUCT	<p>**3rd party components:</p> <ul style="list-style-type: none"> • US content and ECCN classification • EU dual-use classification <p>End-product level:</p> <ul style="list-style-type: none"> • US ECCN classification • EU dual-use classification 	<ul style="list-style-type: none"> • User login trail: <ul style="list-style-type: none"> ➢ license key based ➢ other 	<ul style="list-style-type: none"> • Data storage location not in the <u>Red-flag Country list</u> <ul style="list-style-type: none"> ➢ GDPR rules for data storing • EAR Part 736: <i>General Prohibitions 1 to 3</i> 	<ul style="list-style-type: none"> • EU Official Journal C 72/2023 • US Munition list: eCFR 22 CFR Part 121 ❖ <i>ECRA; Section 1758 technologies</i>

Figure 18. Final Export Compliance matrix.

6.4 Recommendations for Next Steps

A recurring theme during the validation of the proposal revolved around *Product*-related controls. There is a substantial amount of work required, beginning with the identification of third-party software's and followed by obtaining the necessary classification data from them. Of utmost importance is the need to ensure the third-party software registry is kept up to date, with a designated individual responsible for its maintenance. By successfully completing this step, the software classification process would have functional and robust foundation. In the meantime, software product owners should assess whether their end-products utilize encryption or are predominantly developed with U.S.-based software. This approach would initiate the product classification process in a tangible manner.

The *Process*, on how to obtain the export classification data from suppliers requires clear instructions. These instructions should be provided to personnel operating within the supplier interface as well as directly to the suppliers. Implementing both training sessions and standard operating procedures (SOP) would represent an optimal approach. It is crucial to acknowledge that, despite not being novel, these requirements are not widely known among many suppliers and personnel. As a globally sourcing company, involving global-level trade compliance is essential to instigate this proper business conduct. The findings from this thesis can serve as justification to Global Trade Compliance for the importance of this initiative. At the local level, the export compliance matrix developed in this thesis can function as the initial operational model. The subsequent step involves finalizing the SOP for US content calculation and presenting the matrix to Digital Service Operations.

As mentioned, the topic of software export controls remains unfamiliar to most stakeholders within the sponsor company. This not only poses challenges with suppliers but also impacts the resourcing of the Trade Compliance Team, a dilemma shared by other divisions. Despite an ongoing search for a Software Product Classification Engineer (PCE), suitable candidates for the position have not been identified. Given that this has evolved into a widespread challenge, it is imperative to inform Global Trade Compliance, anticipating their readiness to offer necessary support to different divisions. While software may not constitute the core business of the sponsor company or the Group at large, the ongoing digital transformation mandates that all technology

companies adhere to these regulations. Proactively acquiring this knowledge internally is preferable. With the digital landscape evolving, relying on external experts when new EU or other regulations are enforced could prove costly and challenging given the potential high demand for such services. Having competent *People* internally can mitigate this risk.

7 Conclusion

This section offers a concise overview of the key finding from this study. Subsequently, it conducts an evaluation of the thesis, summarizing the work from its objectives to outcomes, and assessing it from both research and author's perspective.

7.1 Executive Summary

The challenge addressed in this thesis involved establishing an export compliance process for software offerings within the sponsor organization. With the anticipated EU regulations on intangible technology exports and the rise of geopolitically driven protectionism, export control restrictions are expected to become multifaceted. Consequently, companies engaged in the software and technology business should proactively prepare to adopt new restrictions and controls as they are introduced. As a result, the objective of this thesis was to develop an export compliance framework for verifying and monitoring the export compliance of software offerings. The outcome is a framework designed to assist in risk mitigation within the export control process for software offerings at the sponsor organization.

This thesis is grounded in contemporary theoretical knowledge and the latest best practices in export control legislation. Employing a multi-method approach, various techniques were utilized to ensure comprehensive data collection. The primary tools for data collection included interviews, questionnaire, and reviews of internal documents. Subsequently, the data was analyzed using theory-driven content analysis, guided by abductive reasoning to uncover a novel solution by consolidating existing information in innovative ways.

To develop the export compliance framework, first, existing US and EU export control regulations were explored to identify the applicable best practices. Recognizing similarities between these regulatory landscapes, a tool was selected for further analysis from the information security realm—the People, Process, and Technology (PPT) framework. The study then investigated the current state of the digital service offering regime through interviews with relevant specialists, collecting data and conducting a Trade Compliance-focused analysis. Following this, the initial export compliance framework was formed using an action-based research method involving co-creation

with internal and external stakeholders. Finally, the framework is evaluated based on validation and feedback from leading experts at the Country level Trade Compliance.

Export controls can be divided into four main categories: product controls, end-use controls, end-user controls and export destination controls. Both the US and the EU are members of the multilateral Wassenaar Arrangement, each governed by their respective national entities in the realm of export compliance. The enforcement of export compliance regulations involves compliance programs, which are mandatory in the US but merely recommendations in the EU. The third aspect revolves around identifying whether the exported software qualifies as a dual-use controlled item. There, a noticeable discrepancy emerges between the US and the EU. The US has more comprehensive legislation on product-related controls, while the EU entrusts software-specific regulations to its member states. In conclusion, the US leads the EU in terms of software export compliance controls. Nevertheless, EU companies are still obligated to stay informed about the export control status of their software offerings, as the US also regulates the re-export of technology and software manufactured in the US.

Building on the insights gained from existing knowledge and the PPT-Framework, a more in-depth analysis was conducted into the current state of the digital service department and its advisory system. The key findings from the CSA were organized under the PPT-framework categories, with the adaptation of the Technology-category being reframed as the Product-category to avoid misinterpretation and to clarify that the category would concern product classification matters. In the People category, the main concern raised was the due-diligence process in the reselling process, where an external service provider was the main contact for the end-user. Each external service providers should comply with global trade laws and regulations. Next, the Process-category highlighted the need for a Red-Flag identification process to raise awareness of compliance risks throughout the value chain. A culture of compliance is necessary in the organization to fully understand and adhere to current laws and regulations. Finally, the revised Product category brought forth the need to better understand the software offerings at the bill-of-material level to identify the export control-related data. Thus, an up-to-date third-party component registry was deemed necessary.

The initial proposal was built in a co-creation manner. Firstly, an external service provider was interviewed to better understand their due-diligence process and the best practices they had regarding export controls. The external service provider in question did not have

any dual-use classified software but had continuous screening available for the entities that use the sponsor organization's product. Further, they were particularly aware of the geo-location of their data storages by utilizing a US-based cloud provider and complying with the GDPR regulation for their EU data.

Secondly, a sales representative from the global sales of digital services was presented with a questionnaire on predetermined red-flags. During this interview, it was discovered that some kind of red-flag identification document had existed earlier, but it was mostly concentrated on financial compliance matters. It was agreed that the red-flag identification checklist would be an ideal addition to the sales process for early compliance issue detection.

Finally, an internal division that had prior experience with software product classification was interviewed. The Trade Compliance team of the division guided us through their product classification process, including US content calculations, and provided advice on some internal guidelines that could be implemented into the initial proposal. Further discussion revealed similar challenges as in the sponsor organization in finding software-qualified product classification engineers and the difficulty in obtaining export control-related data of third-party components, culminating in a bottleneck on how to solve these issues at the division level. This message was agreed to be taken into the validation phase with the Country-level Trade Compliance team.

The final proposal of the export control framework developed into two documents: the red-flag identification checklist and the software export compliance matrix. The red-flag identification checklist was designed to assist the sales teams in identifying possible compliance risks. If any risks were identified, they were instructed to contact the local Trade Compliance team for further due-diligence analysis. The export compliance matrix allocated responsibilities related to People, Process, and Product categories between the user of the document and the Trade Compliance team. The four pillars of export control were grouped under these categories, and each box of the matrix contained information on whom to contact or the process to be performed regarding export control measures.

The validation with the Country-level Trade Compliance introduced these two documents and received positive feedback for capturing a complex matter in such comprehensible form. However, more emphasis was requested on the US content calculations and

supplier responsibility in delivering the export control-related data from their components. Furthermore, the joint concerns identified with the other divisions in the initial proposal building stage were brought forward. The conclusion was to present the findings from this thesis to the Global Trade Compliance organization to shed light on the issues the divisions are facing.

The implementation of the export compliance framework will take place after the operating procedures, identified as missing in the validation phase, have been completed. By implementing the framework, the sponsor organization will have better tools for mitigating the legal, financial, and reputational risks arising from non-compliance with foreign trade law regulations.

7.2 Evaluation of the Thesis Objectives vs. Outcomes

This thesis addresses the challenge of the absence of an export compliance process for software offerings in the sponsor organization. The main objective was to develop an export compliance framework to improve risk mitigation in the export compliance process for software products and to proactively adapt to the changing global economic controls. The development of the framework involved collaboration with the division's digital solutions experts and external and internal stakeholders. The ultimate outcome is to establish a well-defined operational process that is regularly maintained and updated to address evolving sanctions and regulations. The anticipated practical implications were included in the sponsor organizations Trade Compliance 2023 development plan.

The study proceeded to develop an export compliance framework through a multi-step process. Initially, existing export control regulations were examined to identify relevant best practices. The material was gathered from present export compliance regulations, mainly in the United States (US) and the European Union (EU), and for better credibility, some individual national regulations were added for comparison. The existing knowledge delved deep into to product classification regulations. The section is intended to serve as a valuable resource in the training of future product classification engineers, thereby enhancing the practical implications of the study. The primary challenge in constructing the theoretical framework was handling legislation-based data and summarizing official regulations without compromising their integrity. Thus, citations for direct quotes were essential to avoid plagiarism concerns.

In the current state analysis and the proposal building phase the data collection techniques used were multi-method to achieve triangulation on the thesis topic. The data collection tools in the co-creation process included interviews, questionnaire and internal document reviews. The co-creation process also offered the author valuable information on the software product characteristics, which was lacking in the beginning of this study.

The content analysis utilized with the datasets was grounded in the People, Process, and Product (PPP) matrix, which assisted in uncovering patterns and relationships between the data content and the thesis topic. The PPP matrix was adopted from the original People, Process, and Technology framework with a minor change to better support the thesis topic. This change aimed to avoid confusion regarding technology terminology and added emphasis on the product classification topic in the analysis. This approach also supports abductive reasoning, as its objective is to form a new solution by combining existing information in new ways.

The final proposal was validated by the country-level subject matter experts of the organization. Unfortunately, due to the updates suggested by the subject matter experts, the export compliance framework was not ready for implementation. The needed revisions require expertise beyond the scope of this thesis. This leaves room for reflection on whether the objective of having a ready-made export compliance framework was too ambitious to start with. Nevertheless, the final output consists of two documents that address red-flag awareness throughout the value chain and the export compliance matrix. Even in its current state, the matrix can assist stakeholders in understanding the responsibilities and steps needed for efficient export compliance risk management.

References

- Alfano, Peter C. 2022. Introduction to the US Export Administration Regulations. Squire Patton Boggs. Training Materials. Published 14.06.2022. Retrieved 05/08/2023. <https://www.tradepractitioner.com/wp-content/uploads/sites/25/2022/06/Introduction-to-the-US-Export-Administration-Regulations-Slides.pdf>
- Aoi,Tamotsu. 2016. Historical Background of Export Control Development in Selected Countries and Regions. International Security Trade Control Department. Whitepaper. Published April 2016. Retrieved 28.1.2024. https://www.cistec.or.jp/english/service/report/1605historical_background_export_control_development.pdf
- Bennink, Sebastiaan. 2019. Netherlands introduces updated guidance on cloud exports. Published 30/01/2019. Retrieved 29.08.2023. https://batradelaw.com/wp-content/uploads/2019/12/Netherlands_introduces_updated_Guidance_on_cloud_experts.pdf
- Berente, Nick & Recker. 2021. METHOD-ISM, this IS research. Podcast. Spotify. Published 17/03/2021. Retrieved 12.02.2023. <https://open.spotify.com/episode/6n0EtXrHAoOVIXt1PLALzK?si=ba76d93b0ef54748>
- The Bureau of Industry and Security (BIS). 2017. Export Compliance Guidelines: The Elements of an Effective Compliance Program. Published 01.01.2017. Retrieved 27.08.2023. <https://www.bis.doc.gov/index.php/documents/pdfs/1641-ecp/file>
- The Bureau of Industry and Security (BIS). 2020. FINLAND EXPORT CONTROL INFORMATION. Retrieved 26.08.2023. <https://www.bis.doc.gov/index.php/all-articles/220-eco-country-pages/1044-finland-export-control-information>
- The Bureau of Industry and Security (BIS). 2018. Frequently Asked Questions to Export Licensing Requirements. Published November 2018. Retrieved 13/08/2023. <https://www.bis.doc.gov/index.php/documents/pdfs/286-licensing-faq/file>
- The Bureau of Industry and Security (BIS). 2020. Multilateral Export Control Regimes. Policy Guidance. Retrieved 05/08/2023. <https://www.bis.doc.gov/index.php/policy-guidance/multilateral-export-control-regimes>
- The Bureau of Industry and Security (BIS). 2023. Index. Export Administration Regulations(EAR). Retrieved 05/08/2023. <https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>

- The Bureau of Industry and Security (BIS). 2023. Commerce Control List (CCL). Supplement No. 1 to Part 774 Category 4. Published 16/03/2023. Retrieved 05/08/2023. <https://www.bis.doc.gov/index.php/documents/regulations-docs/2335-ccl4-5/file>
- The Bureau of Industry and Security (BIS). 2020. Commerce Control List (CCL). Retrieved 05/08/2023. <https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl>
- Cornell Law School. 2021. 15 CFR § 740.6 - Technology and software under restriction (TSR). Electronic Code of Federal Regulations (e-CFR). Published 19/01/2021. Retrieved 13/08/2023 <https://www.law.cornell.edu/cfr/text/15/740.6>
- Deloitte. 2019. Customs & Global Trade Overview. Article. Global Trade Advisory. Retrieved 05/08/2023 <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/Tax/us-tax-customs-global-trade-overview-brochure-guide-updated-061219.pdf>
- Deloitte. 2022. ABB Export Control Classification Workshop. Not published.
- The Directorate of Defense Trade Controls (DDTC). 2023. ITAR & Export Controls. Web-page. Retrieved 14/08/2023. https://www.pmdtc.state.gov/ddtc_public/ddtc_public?id=ddtc_public_portal_itar_landing
- The Directorate of Defense Trade Controls (DDTC). 2023. Overview. Web-page. Retrieved 13/08/2023. <https://www.state.gov/bureau-offices/under-secretary-for-arms-control-and-international-security-affairs/bureau-of-political-military-affairs/directorate-of-defense-trade-controls-pm-ddtc/>
- Directorate-General for Financial Stability, Financial Services and Capital Markets Union (DG FISMA). 2020. The European Commissions. Dataset. Published 23.12.2020. Retrieved 26.08.2023. http://ec.europa.eu/dgs/finance/contact/index_en.htm
- EUR-Lex. 2023. Dual-use export controls. Summaries of EU Legislation. Published 12.01.2023. Retrieved 26.8.2023. <https://eur-lex.europa.eu/EN/legal-content/summary/dual-use-export-controls.html>
- European Commission. 2023. Welcome to the EU Sanctions Whistleblower Tool. EQS Group AG. Webpage. Retrieved 14/08/2023. <https://eusanctions.integrityline.com/frontpage>
- European Commission. 2023. Consolidated list of persons, groups and entities subject to EU financial sanctions. PDF-document. Retrieved 14/08/2023. <https://data.europa.eu/data/datasets/consolidated-list-of-persons-groups-and-entities-subject-to-eu-financial-sanctions?locale=en>
- European Commission. 2019. COMMISSION RECOMMENDATION (EU) 2019/1318 on internal compliance programmes for dual-use trade controls under Council Regulation (EC) No 428/2009. Document 32019H1318. Official Journal of the European Union. Published 30.07.2019. Retrieved

27.8.2023. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318>

The European Union. Regulation (Eu) 2021/821 Of The European Parliament And Of The Council. Official Journal. Published 20.05.2021:

Annex I, Retrieved 26.08.2023.

Annex III, Retrieved 26.08.2023.

Union General Export Authorisation No EU008, Retrieved 26.08.2023.

Union General Export Authorisation No EU007, Retrieved 26.08.2023.

Annex II, Retrieved 26.08.2023.

Article 8, 8(f) Retrieved 26.08.2023.

Article 4(1), Retrieved 26.08.2023.

Article 13, Retrieved 26.08.2023.

Article 27, Retrieved 26.08.2023.

EU Statement on Wassenaar Arrangement. OSCE Forum for Security Co-operation Nr 778 Vienna 02/04/2015. FSC.DEL/19/15. Retrieved 02/08/2023.

<https://www.osce.org/files/f/documents/9/5/139606.pdf>

Foreign Ministry of Finland. 2023. Services and guidelines for export control. Retrieved 13/08/2023. <https://um.fi/services-and-guidelines-for-export-control>

Foreign Ministry of Finland. 2023. Verkkoalvontatuotteiden vientivalvontaohjeistuksen julkinen kuuleminen. Vientivalvontautiset 03/04/2023. Retrieved 13/08/2023.

https://um.fi/vientivalvontautiset/-/asset_publisher/ygyQWQ1LWoQP/content/verkkoalvontatuotteiden-vientivalvontaohjeistuksen-julkinen-kuuleminen/385035%20

The International Institute for Cyber Stability (IICS). 2019. 2016 Lunch Panel: The Wassenaar Arrangement: What it Means for the Future of Global Cybersecurity. Retrieved 06/08/2023.

<https://www.youtube.com/watch?v=xiE-Vqs3flw>

The International Telecommunication Union. 2012. Radio Regulations. Volume I – Articles. Retrieved 06/08/2023.

https://web.archive.org/web/20150319031957/https://www.itu.int/dms_pub/tu-s/oth/02/02/S02020000244501PDFE.PDF

Kananen, Jorma. 2013. Design research (Applied action research) as thesis research: A practical guide for thesis research. Jyväskylä: Jyväskylä University of Applied Sciences.

Karlson, Peter. 2022. Is The 60-Year-Old 'People Process Technology' Framework Still Useful?. Forbes Technology Council Post. Published 29/12/2022. Retrieved 03/09/2023.

<https://www.forbes.com/sites/forbestechcouncil/2022/12/29/is-the-60-year-old-people-process-technology-framework-still-useful/>

Katterbauer, Klemens. 2023. AI and its impact on EU Export Control Restrictions. LikedIn. Article. Published 05.08.2023. Retrieved 28.01.2024.

<https://www.linkedin.com/pulse/ai-its-impact-eu-export-control-restrictions-dr-klemens-katterbauer>

- Kimball, Daryll. 2022. The Wassenaar Arrangement at a Glance. The Arms Control Association. Fact sheets & briefs 01.02.2022. Retrieved 02.08.2023. <https://www.armscontrol.org/factsheets/wassenaar>
- Kostiainen, Juho. 2022. FINLAND-U.S. ECONOMIC DEEP DIVE 2023. The transatlantic investment and trade relationship: stronger and more important than ever. Article. <https://amcham.fi/wp-content/uploads/2023/04/230411-Finland-U.S.-Economic-Deep-Dive-FINAL-WEB.pdf>
- Lazarou, Elena & Lokker, Nicholas. 2019. United States: Export Control Reform Act (ECRA). PE 644.187. European Parliamentary Research Service. Published 01.11.2019. Retrieved 08.10.2023. [https://www.europarl.europa.eu/cmsdata/210523/EPRS_BRI\(2019\)644187_EN.pdf](https://www.europarl.europa.eu/cmsdata/210523/EPRS_BRI(2019)644187_EN.pdf)
- Lee, Betty et al. 2022. Emerging Technology Controls. Conference materials. The Bureau of Industry and Security (BIS). Published 30.06.2022. Retrieved 08.10.2023. <https://www.bis.doc.gov/index.php/documents/2022-update-conference/3073-rev3-emerging-tech-update-2022-section-1758-controls-tongele/file>
- The Ministry for Foreign Affairs. Export authorizations for dual-use items. Export control forms. Retrieved 27.08.2023 https://um.fi/documents/35732/48132/end_user_statements/71f63148-57ae-dce9-32dd-5d40cd1db902?t=1525689029033
- Office of Foreign Assets Control (OFAC). 2023. Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists. Sanctions Lists. Published 11/08/2023. Retrieved 11/08/2023. <https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>
- Parviainen, Simo-Pekka. 2000. Cryptographic Software Export Controls in the EU. Faculty of Law. University of Helsinki. Thesis (master's). Retrieved 05/08/2023. <http://urn.fi/URN:NBN:fi-fe20001230>.
- Patel, Salma. 2015. The research paradigm – methodology, epistemology and ontology – explained in simple language. Web-page. Retrieved 12/02/2023. <https://salmapatel.co.uk/academia/the-research-paradigm-methodology-epistemology-and-ontology-explained-in-simple-language/>
- Powell, Alwin. 2017. The false choice of basic vs. applied research. Harvard College: President and Fellows of Harvard College. Published 3/01/ 2017. Retrieved 12/02/2023. <https://seas.harvard.edu/news/2017/01/false-choice-basic-vs-applied-research>
- Publications Office of the European Union. 2023. Dual-use export controls. Summaries of EU legislation. EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legisum:4532505>
- Ritala, Paavo. Johdatus tutkimusmetodologiaan. LUT University. Retrieved 12/02/2023. <https://docplayer.fi/67751641-Johdatus-tutkimusmetodologiaan.html>

- Ruohonen, Jukka & Kai K. Kimppa. 2019. Updating the Wassenaar debate once again: Surveillance, intrusion software, and ambiguity, *Journal of Information Technology & Politics*, 16:2, Retrieved 03/09/2023. DOI: 10.1080/19331681.2019.1616646
- Saunders, Mark; Lewis, Phillip & Thornhill, Adrian. 2019. *Research methods for business students*. (Eighth edition). Pearson.
- Schneier, Bruce. 2019. China Spying on Undersea Internet Cables. *Schneier on Security Blog*. Pulished 15/04/2019. Retrieved 03/09/2023. https://www.schneier.com/blog/archives/2019/04/china_spying_on.html
- Schneier, Bruce. 2013. "People, Process, and Technology". *Blog*. Pulished 30/01/2013. Retrieved 05/09/2023. https://www.schneier.com/blog/archives/2013/01/people_process.html
- Tuomi, Jouni., & Sarajärvi, Anneli. 2018. *Laadullinen tutkimus ja sisällönanalyysi (Uudistettu laitos)*. Helsinki: Tammi.
- von Witke, Albrecht & Korzak, Elaine & Mayer, Robert & McGuire, Cheri & Moss, Jeff & Szemerényi, Reka. 2016. Lunch Panel: The Wassenaar Arrangement: What it Means for the Future of Global Cybersecurity. Youtube-video. Published 22/10/2019. Retrieved 3/9/2023 <https://www.youtube.com/watch?v=xiE-Vqs3flw>
- Washington University. 2019. Export Management and Compliance Program. Internal policy and procedures 15/05/2023. Retrieved 06/08/2023. <https://research.wustl.edu/wp-content/uploads/2017/07/Export-Management-Compliance-Program-PDF.pdf>
- Wassenaar Arrangement(1). 2021. List of Dual-Use Goods and Technologies and Munitions List (WA-LIST). Compiled by the Wassenaar Arrangement Secretariat 22/12/2021. Retrieved 06/08/2023. <https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-II-2021-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-2021.pdf>
- Wassenaar Arrangement(2). 2021. List of Dual-Use Goods and Technologies and Munitions List (WA-LIST). Summary of changes 22/12/2021. Retrieved 13/08/2023. <https://www.wassenaar.org/app/uploads/2021/12/Summary-of-Changes-to-the-2019-2020-Lists.pdf>
- Wassenaar Arrangement(3). 2021. List of Dual-Use Goods and Technologies and Munitions List (WA-LIST). Definitions. Retrieved 20/08/2023. <https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-II-2021-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-2021.pdf>
- Wassenaar Arrangement. 2022. What is the Wassenaar Arrangement? Video. Retrieved 06/08/2023. <https://www.wassenaar.org/what-is-the-wassenaar-arrangement/>

Project team interview frame

Interview frame

Name and date	
General info:	
Business partner/customer sanctioned party status?	
Data storage location?	
Are Users located in EU/US restricted countries (Geo-location)	
User management, login and registration for downloadable elements?	
Does the application contain controlled items?	

Inquiry Regarding Export Control in Software Sales

Date: 15th of NOV 2023

Present: CONFIDENTIAL

- (1) What are the "redflags" for your end-user due-diligence checks?
- (2) What kind of a control procedure the company has in place for monitoring user management, login, and registration with respect to downloadable elements?
- (3) What kind of monitoring is in place regarding the geographical location of data storage, for instance, compliance with US EAR Country Group D:5 countries?
- (4) What is the established protocol for the classification of software within your organization?
- (5) How is the oversight and control process managed concerning third-party suppliers of end-product Bill of Materials (BOM) components/software?
- (6) Do you possess experience in exporting "emerging technologies," as defined by ECRA; Section 1758 technologies?

Appendix 3

Preliminary Red-flag list

Product related	<ul style="list-style-type: none"> Customer is asking unusual quantities (compared to installed base/actual need) <ul style="list-style-type: none"> For example customer is asking filters such amount which equals +5 years operational needs for one vessel 	<ul style="list-style-type: none"> Customer seems not to be familiar with the product and its performance characteristics (e.g. an obvious lack of technical knowledge); Customer requests a product that seems overly capable for the intended application
End-user & End-Use	<ul style="list-style-type: none"> Companies which have very limited info available `open source` and have not had any previous business history with ABB Contact information in enquiries (e.g. phone numbers, email and addresses) is located in other countries than the stated company, <u>or changed to that over time</u>. Email is coming from addresses such as gmail, Hotmail etc 	<ul style="list-style-type: none"> The end-user is tied to the military, the defence industry or a governmental research body and the stated end-use is civilian Customer is reluctant to offer information about the end-use of the items (e.g. via an end-user statement), provide clear answers to commercial or technical questions which are routine in normal negotiations or to provide an end user statement.
Destination Control	<ul style="list-style-type: none"> Customer/Owner/Operator/Charterer is in the <i>Sensitive Countries Protocol</i>: <p style="text-align: center;">CONFIDENTIAL</p>	
Marine specific	<ul style="list-style-type: none"> Customer not willing to reveal the vessel name in their request Given vessel name does not match with the vessel's installed base 	<ul style="list-style-type: none"> All the Yacht requests need to be sanction screened very carefully List of red-flag vessels

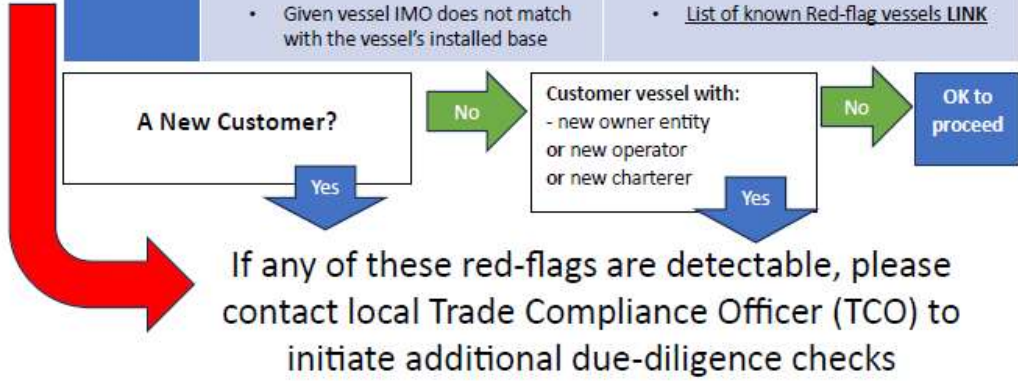
Appendix 4

Internal division interview frame

Software Export controls (US and EU)	Product related controls	End-user Controls	Destination Control (Country of destination)	End-use Controls
PEOPLE				
PROCESS				
PRODUCT				

Red-Flag identification for Sales

<p>YES/NO</p> <p><input type="checkbox"/> <input type="checkbox"/></p>	<p>Product related</p>	<ul style="list-style-type: none"> Customer is asking unusual quantities (compared to installed base/actual need) <ul style="list-style-type: none"> For example customer is asking filters such amount which equals +5 years operational needs for one vessel 	<ul style="list-style-type: none"> Customer seems not to be familiar with the product and its performance characteristics (e.g. an obvious lack of technical knowledge) Customer requests a product that seems overly capable for the intended application
<p><input type="checkbox"/> <input type="checkbox"/></p>	<p>End-user & End-Use</p>	<ul style="list-style-type: none"> Companies which have very limited info available 'open source' and have not had any previous business history with us Contact information in enquiries (e.g. phone numbers, email and addresses) is located in other countries than the stated company, or changed to that <u>over time</u>. Email is coming from addresses such as gmail, Hotmail etc. 	<ul style="list-style-type: none"> The end-user is tied to the military, the defence industry or a governmental research body and the stated end-use is civilian Customer is reluctant to offer information about the end-use of the items (e.g. via an end-user statement), provide clear answers to commercial or technical questions which are routine in normal negotiations
<p><input type="checkbox"/> <input type="checkbox"/></p>	<p>Destination Control</p>	<ul style="list-style-type: none"> Customer/Owner/Operator/Charterer is in the <i>Sensitive</i> ██████████ Protocol: <p style="text-align: center;">CONFIDENTIAL</p> <p><i>Act:</i> Countries/regions Afghanistan, Bahrain/Arabian Gulf, Iraq, Libya, Mali, Myanmar (Burma), Niger/Darfur, Somalia, South Sudan, Sudan, Venezuela, Yemen.</p> <ul style="list-style-type: none"> Business in or with Act countries is subject to case-by-case approval. Exceptions from Act country conditions require CEO approval 	
<p><input type="checkbox"/> <input type="checkbox"/></p>	<p>Marine specific</p>	<ul style="list-style-type: none"> Customer not willing to reveal the vessel IMO in their request Given vessel IMO does not match with the vessel's installed base 	<ul style="list-style-type: none"> All Yacht requests need to be sanction screened very carefully List of known Red-flag vessels LINK



**WRITTEN STATEMENT
on the use of AI-based tools in this thesis**

by Aino Herranen , the student of BI Master's Degree Programme

Thesis title: Building an Export Compliance Framework, Intangible Technology Transfer – Software offerings

According to the “*Guidance for addressing the use of AI-based tools in studies at Metropolia Business School (for written submissions)*” from August 2023, I make this statement on the use of AI-based tools in my submitted Master's thesis.

1) Which AI-based large language models or other AI-based tools I used

Chat GPT

2) In which parts of the thesis which tools were used, and for which tasks (*please make a list*)

7.1 Executive Summary, page 79 onwards.

3) What portion of the text was helped with these tools, for each use

Sentences

4) Which prompts were asked, exactly (*please indicate the page number in the text where used*)

“Please check grammar:”

5) Here, I describe what continues an ethical and reliable use of AI-based tools that I used

As per documents from MBS Guidance

6) Here, I describe how ethically and reliably I used the AI-based tools in my thesis submission

Use of AI tools was minimal for English language grammar checks.

This written statement makes part of my thesis and is done to help in evaluation and assessment.

 06.05.2024
(Data and place)

(Signature) Aino Herranen