jamk

EU Cybersecurity Regulation

Cyber Resilience Act

Ari Huttunen

Master’s thesis
March 2025
Master's Degree Programme in Information Technology, Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Huttunen, Ari

EU Cybersecurity Regulation: Cyber Resilience Act

Jyväskylä: Jamk University of Applied Sciences, March 2025, 116 (90+26) pages.

Master's Degree Programme in Information Technology, Cyber Security. Master's thesis.

Permission for open access publication: Yes

Language of publication: English

Abstract

The number of Internet-connected devices has risen rapidly, and cybercrimes follow the same curve. European Union has battled against cybercrime by regulation. Cyber Resilience Act (CRA) is a novel EU cybersecurity regulation, that entered into force in December 2024. The CRA sets strict cybersecurity requirements for the manufacturers of products with digital elements.

The CRA proposal came out in September 2022, and the final version of the CRA legal text was published in November 2024. As the existing literature was referring to the CRA proposal text the research aimed to clarify the final version of the CRA legal text, thus helping the product manufacturers in the compliance process and fulfilling the CRA requirements.

Pragmatism research philosophy was applied and qualitative research approach used, combining exploratory research and applied research, to answer the following three research questions: What is the CRA? What are the cybersecurity requirements in the CRA? What kind of tool could be developed to help manufacturers in the CRA compliance process?

To understand the history and the reasons behind the new regulation, the existing cybersecurity legislation was researched. The new regulation was researched and a clear overview of the CRA was presented to give readers an overall understanding on the regulation. Requirements of the CRA were brought together and each of them were explained for clarity. A tool was developed to help the product manufacturers in the compliance process.

The tool was developed with Microsoft Excel. The tool makes collaborating possible in the compliance process, offers an easy monitoring of the progress, and enables storing the results of the process in a single location. The tool was developed to guide users in using the tool and following the logical path of the CRA compliance by comprehensive instructions.

Keywords/tags (subjects)

Cybersecurity, Cyber Resilience Act, CRA, Regulation, Legislation

Miscellaneous (Confidential information)

-

jamk

Kuvailulehti

Huttunen, Ari

EU:n kyberturvallisuussääntely: Kyberkestävyyssäädös

Jyväskylä: Jyväskylän ammattikorkeakoulu. Maaliskuu 2025, 116 (90+26) sivua.

Master's Degree Programme in Information Technology, Cyber Security. Master's thesis.

Julkaisun kieli: englanti

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Internetiin kytkettyjen laitteiden määrä on kasvanut voimakkaasti, ja kyberrikollisuuden määrä kasvaa samassa suhteessa. Kyberkestävyyssäädös on uusi EU:n kyberturvallisuusasetus, joka astui voimaan joulukuussa 2024. Säädös asettaa tiukkoja tietoturvavaatimuksia yrityksille, jotka valmistavat digitaalisia elementtejä sisältäviä tuotteita.

Säädösehdotus julkaistiin syyskuussa 2022, ja lopullinen versio marraskuussa 2024. Koska olemassa oleva kirjallisuus käsittelee säädösehdotusta, tutkimus pyrki selventämään säädöksen lopullista versiota, ja siten auttamaan tuotteiden valmistajia vaatimustenmukaisuusprosessissa sekä säädöksen vaatimusten täyttämisessä.

Seuraaviin tutkimuskysymyksiin vastattiin soveltamalla pragmatistista tutkimusfilosofiaa ja kvalitatiivista tutkimusta, yhdistäen eksploratiivista ja soveltavaa tutkimusta: Mikä kyberkestävyyssäädös on? Mitä kyberturvavaatimuksia kyberkestävyyssäädöksessä on? Minkälaisen työkalun voisi kehittää auttaakseen valmistajia kyberkestävyyssäädöksen vaatimustenmukaisuusprosessissa?

Uuden asetuksen historian ja sen taustalla olevien syiden ymmärtämiseksi tutkittiin voimassa olevaa kyberturvalainsäädäntöä. Uutta asetusta tutkittiin ja siitä esitettiin selkeä katsaus, jotta lukijat saisivat yleiskäsityksen asetuksesta. Kyberkestävyyssäädöksen vaatimukset koottiin yhteen ja selvennettiin. Tuotteiden valmistajien avuksi vaatimustenmukaisuusprosessissa kehitettiin työkalu.

Työkalu kehitettiin Microsoft Excelillä. Työkalu mahdollistaa yhteistyön vaatimustenmukaisuusprosessissa, tarjoaa helpon prosessin edistymisen seurannan ja mahdollistaa prosessin tulosten tallentamisen yhteen paikkaan. Työkalu kehitettiin siten, että se opastaa käyttäjiä työkalun käytössä ja kyberkestävyyssäädöksen vaatimustenmukaisuuden loogisen järjestyksen seuraamisessa kattavien ohjeiden avulla.

Avainsanat (asiasanat)

Kyberturvallisuus, kyberkestävyyssäädös, CRA, sääntely, lainsäädäntö

Muut tiedot (salassa pidettävät liitteet)

-

Contents

Figures

1 Introduction

"If everything is connected, everything can be hacked" – Ursula von der Leyen (European Commission, 2021).

The European Union new cybersecurity regulation Cyber Resilience Act (CRA) will require digital product manufacturers to fulfil strict cybersecurity requirements for the products with digital elements placed on the market from December 11th, 2027, onwards. As legal texts often are hard to understand, also the CRA and its requirements will need clarification. This research aims to clarify the final version of the CRA text and to help the manufacturers of the products with digital elements in complying with the new regulation. This chapter provides an introduction for the study giving background for it and presenting the research problem and questions.

Our society, the businesses and citizens, is highly dependent on the ICT (information and communications technology) systems and networks. The number of Internet-connected devices is growing exponentially, especially due to the fast growth of the IoT (Internet of Things) market. The rise of the cybercrime follows the same curve. Legislation can be used as a weapon in the fight against the cybercrime. European Union proposed a new regulation, the CRA, in September 2022 to respond the emerging threats. The regulation was entered into force December 10th, 2024. The manufacturers will have three years transition before applied and will need to fulfil the CRA requirements for the products that will be made available on the market from December 11th, 2027, onwards.

New legislation may bring challenges to whom it may concern if the legal text is not clear. As the CRA regulation is novel and may be hard to interpret, it will require familiarisation. The aim of my thesis is to clarify the adopted version of the regulation and to help manufacturers in the compliance process. The first research question *What is the CRA?* will explain the background of the regulation, its purpose and whom it concerns. As a part of the first research question, the existing EU cybersecurity related legislation and decisions is represented to show the relation of new regulation to the past ones. The second research question *What are the cybersecurity requirements in the CRA?* gathers and explains the requirements set by the CRA. The third question *What kind of*

tool could be developed to help manufacturers in the CRA compliance process? research on the need of and possibility to create a tool to help manufacturers in the CRA compliance process.

This research aims to help recognise the existing cybersecurity related legislation, understand the manufacturers' requirements that the new European Union's regulation Cyber Resilience Act presents and study what kind of tool could be designed and developed to help manufacturers on their journey to be compliant with the regulation.

2 Research

This chapter explains what the rationale for this thesis is, what is the research problem and what are the research questions derived from the research problem. It also describes the research methodology used in the thesis and the ethics of the work including the use of artificial intelligence.

2.1 Rationale

Cybercrime is a global issue that does not recognise geographical limits. It requires collective effort to tackle the problem but there is no magic bullet to clear the universal problem. The European Union has been responding to challenging situation on security of the ICT field by legislation and has now pulled bigger guns for the fight. The Network and Information Systems directive (NIS2) already laid down strict cybersecurity rules for the operators and providers of essential services, and now the new EU CRA regulation orders manufacturers of "products with digital elements" (for the convenience of the reader, "products with digital elements" will be referred to as "products" and "manufacturers of products with digital elements" will be referred to as "manufacturers" throughout this paper) to ensure their products are cybersecure for their entire lifecycle. The CRA, once in force, is expected to have a tremendous positive impact on the cybersecurity of not only in the European Union area, but also across borders globally (Geiger & Botting, 2024; Kazakova, 2023).

The CRA aims to reduce cybersecurity risks for businesses and consumers by requiring manufacturers to take responsibility for bringing only cybersecure products to market, and to provide security updates that ensure the cybersecurity of the products from the earliest stages of design till the end of the product's life. The regulation harmonises the cybersecurity requirements of products facilitating the trade of the products within European Union. Through the regulation, the consumers can be confident that the products they buy are secure.

The CRA adopts a risk-based approach to cybersecurity. The manufacturers must carry out a risk assessment for their products. Based on the identified risks, they must comply with the relevant essential requirements on cybersecurity and vulnerability management. The regulation requires manufacturers inter alia, to report security incidents and exploited vulnerabilities, set up a Coordinated Vulnerability Disclosure policy, and provide a set of documentation to market surveillance authorities and to the users of the products. A failure to comply with the requirements may be penalised, with up to 15 M€ or 2,5% of company's annual worldwide turnover, whichever is higher.

Complying with the CRA requirements requires involvement of many functions of companies and needs to be managed carefully. Achieving compliance with the regulation is a complex task but is mandatory to all manufacturers that are active within the European Union market. The CRA requirements place a significant burden on companies to understand and comply with the regulation. New regulation is often based on the existing regulation but requires updates as the world changes. It needs to be studied to understand which kind of requirements the regulation brings, and to make it more comprehensible for individuals needing to work with the subject.

2.2 The Research Problem and Research Questions

The European Union's new cybersecurity regulation CRA will require all manufacturers, importers, distributors, and re-sellers that places products on the European Union market to comply with the requirements of the regulation three years after the adoption of the law. The regulation text doesn't take a stand on how the requirements can be fulfilled. Even if the essential cybersecurity requirements are listed in the Annex I (appendix 1) it is not feasible to comply the requirements of the regulation only by studying the list. As the requirements are mandatory, and the non-compliance of the requirements can be heavily penalised, the willingness of complying the requirements

should be guaranteed. Studying the CRA document started in the summer of 2023, and it became evident it would require deep attention. The commissioning company agreed it would be a suitable topic for a master's thesis.

To start with very general level on the novel regulation, the first research question is ***What is the CRA?*** It will delve what is the reasons behind the new regulation, its history and purpose, and whom does it concern.

As the CRA is a regulation, it is a legal text and not a technical specification. To clarify the ambiguity of the requirements the regulation sets, my second research question is ***What are the cybersecurity requirements in the CRA?*** It will help assimilating and explaining the different requirements of the CRA. It will give answers for example on how the various products are categorised, which kind of technical requirements there are, and what is required from the processes point-of-view.

It is vital to have a clear view on the requirements of the regulation, but that is far from being compliant. ENISA (The European Union Agency for Cybersecurity) and JRC (European Commission's Joint Research Centre) published a document that did the mapping between the CRA requirements and the related existing standards that will help especially the European Standardisation Organisations (ESOs) when drafting the required EU harmonised standards. (European Union Agency for Cybersecurity et al., 2024). As the CRA has many kinds of requirements and achieving compliance is a complicated the process, a tool to help the manufacturers in the process would be useful. The third research question is ***What kind of tool could be developed to help manufacturers in the CRA compliance process?*** Research will be made for what kind of tool would be useful for the CRA compliance process and could be produced as a part of this thesis. In the core of the question is what kind of tool would be valuable for the manufacturers.

2.3 Research Methodology

This thesis is based on a pragmatism research philosophy. The thesis is a combination of theoretical understanding and practical solution. Pragmatism is a problem solving by nature, aims to find practical solutions and considers that truth is rather functional or instrumental than a definite final

fact (The Ethics Centre, 2022). Also, in pragmatism the truth is not regarded as fixed or pre-established, but is rather an instrumental view, that will be found in practical ways (Leavy, 2014). For example, due to the dynamic nature of cybersecurity, in making a product cybersecure, there isn't any perfect solution that will apply now and forever, but there can be a solution, that on the current best knowledge is covering a product from known threats. Pragmatism considers that the research philosophy should be chosen based on the research problem and the results count to be important (Žukauskas et al., 2018). In this thesis combining theory and practice is a driving theme, and pragmatism serves the current research problem well. Pragmatism also gives flexibility for the researcher, which may be needed during the research, as the author has neither earlier experience on the EU legislation, their composition, and dependencies, nor creation of any kind of tool.

Qualitative research approach can be used in various fields of study on a wide range of topics. It is used as an umbrella term for different research practices. Research methods are means for data collection. Several different research methods are used in qualitative research, including document analysis and content analysis. Best tools to gather data for the certain study should be utilised when selecting the research method. Qualitative research is practical and gives leeway for researcher, and considers limitations, like time, funding, researcher's previous experience and pre-existing information sources. (Leavy, 2014)

The research approach is purely qualitative for analysing the evolution of the cybersecurity legislation and understanding or explicating the content of the CRA. For the third research question, that relates to the tool to be developed, a mixed methods approach might be needed, depending on the outcome of what kind of tool will be developed.

Basic research is advancing knowledge and supporting applied research. It is helping to improve existing theories and advancing new theories. Exploratory research is a sub-category of basic research, that concentrates on novel and less comprehended phenomena. (Hassan, 2024) Exploratory research is essential to develop understanding on the existing important EU cybersecurity related legislation and to carefully study the new CRA regulation.

The present thesis is largely relying on primary sources (American Psychological Association, n.d.). A review is done to clarify the past EU cybersecurity legislation from EU legal documents and proposals. The information will be mainly collected from the official sources in European Union to minimise possible bias from any citing quarter. Document analysis will be conducted for the relevant important cybersecurity legislation with a special focus for the CRA to get a clear vision on the regulation.

Due to the novelty of the topic, the number of scholarly articles available for the CRA, at least in the early stages of the thesis process, will be low. Data collection time horizon for the study is somewhat longitudinal, as it's clear that the law-making process goes ahead, and changes in the CRA are inevitable (Caruana et al., 2015). During the thesis process new literature on the topic will arise, and a review of new literature will be made to search for newly published articles or theses on the CRA. It is evident that the CRA being an extremely important piece of legislation in the ICT field, during the course of writing this thesis a substantial number of articles, discussions, overviews and guides will be published by different parties and authors, and within the time constraints, not all of them can be reviewed and even some significant and valuable sources may escape the authors attention.

Applied research will be used to collate the need for and applicability of the tool to support in the CRA compliance process (OECD, 2015). Here, the requirements from the commissioner of the thesis will be also considered. Relevance and type of sampling strategy will depend on the decision on what kind of tool will be created. For the regulatory text as a source in the theoretical part of the study no sampling strategy is required.

The most significant limitation of this thesis arises from the novelty of the CRA and the background of the author. The regulation, at the time of start of the thesis work, is on the level of proposal, and will most likely face adjustments during the legislation process. Also due to the alterations in the progress of the CRA, many of the sources citing or referring to the regulation will become at least partly obsolete after the law draft development, and before final version is confirmed. This is also one reason the EU official sources will mainly be used as the information source. The CRA will require technical changes when applied, but the aspect of this thesis is also considering the legal requirements of the regulation. The reliability of this thesis is enhanced by using the EU official

sources for information. Still, there is always the possibility of error in research. Given the technical background of the author, tackling the challenge of the chosen topic is an identified risk and a calculated step into the realm of discomfort. Bearing this in mind, even with a thorough study of the regulation, it is still possible for the author to make mistakes in interpreting the legal text.

2.4 Research Ethics and the Use of Artificial Intelligence

The research is conducted with integrity and follows the ethical principles of Jyväskylä University of Applied Sciences (JAMK University of Applied Sciences, 2018) and the Arene's (2019) ethical recommendations for thesis writing at universities of applied sciences. The aim of the thesis is to bring value by researching a novel EU regulation and helping manufacturers in their obligations of compliance. Reliable primary sources will be prioritised, and the reference information is acknowledged when citing or referencing other authors, being them individuals or organisations.

Even if when starting the study, it was not considered to use of any artificial intelligence tools at all, to learn more on its capabilities, I went back on my words. The risks in using artificial intelligence in the thesis were acknowledged, but decision was made to experiment if it could be facilitated in the task.

Artificial intelligence, ChatGPT specifically, has been used as a discussion companion and to ask for "another opinion" in this thesis. As an example, after listing and summarising the existing EU cybersecurity related legislation in person, ChatGPT was asked to list the ten most relevant legislations, to see if something had been missed. Also, ChatGPT has been used to summarise the content of some regulation, but only after summarising it myself. Few corrections were done after reviewing the legal text again, based on the points raised by ChatGPT.

Another example of using AI, specifically as a discussion companion, was when I struggled to form my opinion for the CRA requirement of vulnerability disclosure. I was not sure if I had misunderstood the requirement, and I was turning over my interpretations with ChatGPT, until I had confidence what the legal text meant. The discussion with the AI helped in confirming what the legal text really meant.

Artificial intelligence is really powerful tool when used correctly. Incorrect or careless use may pose risks. Especially in the thesis concerning a novel regulation, when the CRA was developing, I came across with the fact that ChatGPT was answering based on the outdated information. I also noticed how inaccurate AI tool answers can be, and how important it is to define the prompt well, and especially to confirm its answer from a trusted source to make sure the AI is not hallucinating.

3 Literature Review

This chapter provides background information for the purposes of the CRA by looking into the rise in the quantity of the connected devices, explaining cybersecurity and cyberattacks, and the associated costs. It will also shortly explain the EU legislation before looking into existing literature on the CRA.

3.1 The Number of the Connected Devices Is Surging

While the global population is a bit above eight billion, around two thirds of the population are using the Internet. At the beginning of 2024, there were 5,35 billion Internet users and the number is steadily growing. Still the number of Internet users is a minority of the total number of connected devices. (Kemp, 2024)

Due to the IoT boom the number of Internet-connected devices is exploding. In 2019 there were ten billion IoT and non-IoT devices each (Lueth, 2020). While the number of non-IoT devices is expected increase with few hundred million by 2027, IoT Analytics predicts the number of IoT devices to grow to nearly 30 billion in same time frame (Satyajit, 2023). This huge growth means also escalating needs for better cybersecurity to prevent threats snowballing.

3.2 Cybersecurity

In today's digital and ever more interconnected world businesses and citizens are constantly faced by cybersecurity threats and the situation is expected to worsen. The importance of cybersecurity is without doubt getting higher when all the functions of the society are, or at least will soon be, in digital format, and the number of interconnected devices is surging. More and more knowledge and competence are needed to properly address the cybersecurity, and the choice for a secure

product is cumbersome. The world is full of different definitions for cybersecurity and even the cybersecurity experts don't have a coherent definition for the term (van Dijk, n.d.). As cybersecurity threats are shapeshifting rapidly and cybercriminals are persistently evolving their ways of executing new cybercrimes, a loose definition might be more functional than a very accurate one. The way International Organization for Standardization (ISO) has condensed cybersecurity, "safeguarding of people, society, organisations and nations from cyber risks" sounds great in all its simplicity; especially with their elaboration "safeguarding means to keep cyber risk at a tolerable level" (International Organization for Standardization, 2023a). As many definitions for cybersecurity seem to focus on organisations or enterprises, ISO remembers to include us, the people in the subject of the protection needs. Their specification for safeguarding emphasizes the often-repeated fact that there is no bullet-proof cybersecurity, but the level of protection needs to be assessed case-by-case based on the risk tolerance. CISA's denotation on cybersecurity in their blog post takes more technological approach: "Cybersecurity is the art of protecting networks, devices, and data from unauthorised access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information" (America's Cyber Defence Agency, 2021). According to Tunggal (2023), some important ways to enhance cyber security are:

- encrypting the sensitive data
- installing the latest software updates and security patches
- deploying cybersecurity devices
- implementing security policies

3.3 Cyberattack

Despite the disparity in stance for defining cybersecurity between different operators, the unanimous goal is to defend against cyberattacks. Similar kind of ambiguity pertain in the definition of cyberattack. NIST glossary has four different interpretations on cyberattack, depending on the context of the document it has been defined in (National Institute of Standards and Technology, n.d.). A dictionary definition for cyberattack, "an attempt to gain illegal access to a computer or computer system for the purpose of causing damage or harm" (Merriam-Webster, n.d.) is again a broad definition, that gives room to include a failed attempt as cyberattack and 'harm' includes everything from a severe data breach to a pesky pop-up that might be all that the attack causes. On the other hand, the definition only talks about computers or computer systems, which leaves a

question mark whether e.g., IoT devices like smartwatches are included. Another definition for cyberattack from Cisco is “a malicious and deliberate attempt by an individual or organisation to breach the information system of another individual or organisation. Usually, the attacker seeks some type of benefit from disrupting the victim’s network.” (Cisco, n.d.). Here a noteworthy detail is that cyberattacks are intentional acts to do harm. Even if human errors or natural disasters are a great danger to security of information systems, they don’t fall under the definition of cyberattack. With this, it’s important to realise that cybersecurity aims to defend against deliberate malicious acts. Crowdstrike lists the most common cybersecurity attacks of 2024 (Baker, 2024):

1. Malware, which is a malicious software, code or program designed to harm information systems.
2. Denial-of-Service attacks, that creates surge on the network traffic aiming to hinder the accessibility of information system resources.
3. Phishing, that uses different techniques to trick the victim to hand over any sensitive information to the attacker.
4. Spoofing, where the attacker impersonates a trusted party to gain access to victim’s information system.
5. Identity-based attacks, where an attacker tries to gain victims user credentials with different techniques to be later used to compromise the information system.
6. Code infection attacks, where malicious code is injected into a vulnerable device.
7. Supply chain attacks, where target company’s trusted supplier is attacked to eventually compromise the target company
8. Social engineering attacks, where the target person is manipulated to take the actions, that the attacker wants.

It is necessary to highlight that the most common cyberattack, malware, is an umbrella term, that includes several distinct kinds of malicious software, like ransomware, trojans, worms, exploits and botnets.

3.4 Cyberattacks’ Number and Cost

Cyberattacks have become so incredibly frequent that it’s hard, if not impossible to even keep up with the total number. SonicWall Capture Labs reported to have detected over six billion malware attacks in 2023 worldwide (SonicWall, 2024). 47,5 million adults were estimated to have been victims of an identity theft in 2022 (Gen Digital, 2023). In addition to increase in the number of cyberattacks also the scale has expanded. By January 2024 there were public information on four

data breaches against different companies exposing more than a billion user records each, with CAM4, an adult live-cam website having more than ten billion user records exposed (Tunggal, 2024).

At the same time the cost of the cybercrime is skyrocketing. Based on the IBM 2024 report the average cost of a data breach increased 10% from the year before (IBM, 2024). Microsoft confirms the emerging situation in their yearly Digital Defence Report. They emphasise as well that the cybercrime is these days close to the maturity level of nation-state sponsored attacks (Microsoft, 2024). Some implication of the severity of cybercrime can also be drawn from that the International Monetary Fund (IMF) has devoted one entire chapter out of three chapters in their first 2024 Global Financial Stability Report for cyber risks and emphasizing the consequences of cyberattacks (International Monetary Fund, 2024). As listed by Greenberg (2018), by far the most expensive cyberattack has been NotPetya. This malware spread to computers all over the world in 2017 and caused damages with estimated costs of $10 billion. The pharmaceutical giant Merc is alone estimated to have suffered $870 million damages. Total costs of cybercrime are far beyond these figures. According to Statista the global cost of cybercrime in 2024 will be more than $9 trillion and has estimated it to soar to nearly $14 trillion by 2028. (Fleck, 2024)

3.5 EU Legislative Composition

The terminology of the EU is versatile, and the basics of EU legislation system are required to better understand this thesis. The composition of the EU legal system has changed and will change over time, and the explanation below describes the situation during the time of authoring the thesis.

The rules of the EU are set in the *Treaties*. The European Union was initially found in 1951 by six countries when the *Paris Treaty* was signed. Though, the EU as it is known today was established in 1992 by *Maastricht Treaty* and currently consists of 27 *Members States*. The EU is operating as *a single market*, which means, amongst other things, that people are free to live, study and work in any of the EU country, and products or services are guaranteed free movement without trade barriers within the EU single market. (European Union, n.d.-d; European Union, 2023; Barnard & Peers, 2023, pp. 11-12; Gayubas, 2024)

The EU legal set-up consists of several European institutions, EU bodies and EU agencies. The EU administration is led by the following four main decision-making institutions (European Union, n.d.-e):

- The European Council,
- The Council of the European Union,
- The European Commission, and
- The European Parliament.

There is the “Council of Europe”, the “European Council” and the “Council of the European Union”, which are all different things, and care should be taken not to mix them up. The Council of Europe is not a part of the European Union, but a distinct European organisation. **The European Council** is the Union’s top decision-maker and is the highest-level representative of the Member States. It is responsible of the European Union development and defines the common political guidelines and priorities. The members include the President of the European Council, the President of the Commission and the heads of government or state of each Union country, like the President or Prime Minister. (Hartley, 2014, pp. 21-22)

The European Commission (often referred as the Commission or EC) is the EU’s politically independent institute that can propose or adopt EU laws and implements the Council and the Parliament decisions. The Commission uses specialists and the public consultation in the law proposals to have the technical details correctly. Directorate-General are departments that handle the daily tasks, each of them having the experts of the specific policy area. The Commission consists of a Commissioner from each Member State, one of being the Commission President, currently Ursula von der Leyen. (Barnard & Peers, 2023, pp. 44-45; European Union, n.d.-a)

The Council of the European Union (often referred as the Council) comprises of the elected members, that are ministers of the Member States. The members of the Council are not fixed but is depending on the policy area in question. The Councils has several tasks, but in the context of this thesis the most important task is to negotiate and adopt the EU laws in cooperation with the European Parliament based on the European Commission’s proposal, as seen in the Figure 1. (Hartley, 2014, pp. 21-22; European Union, n.d.-b)

The European Parliament represents the citizens of the European Union through Members of the European Parliament (MEPs), who are selected for five-year term by the elections. The number of the MEPs can't exceed 750, and the current number of the MEPs is 720. The Parliament has the right to request proposals of the Union acts from the Commission. Citizens of the Union have a right to send a petition to the Parliament on a matter related to the Union that affects the citizen. The parliament also has a right to set up a committee of inquiry if they see necessary to the Union law is not followed properly. (Hartley, 2014, pp.13-18; European Council, 2023)

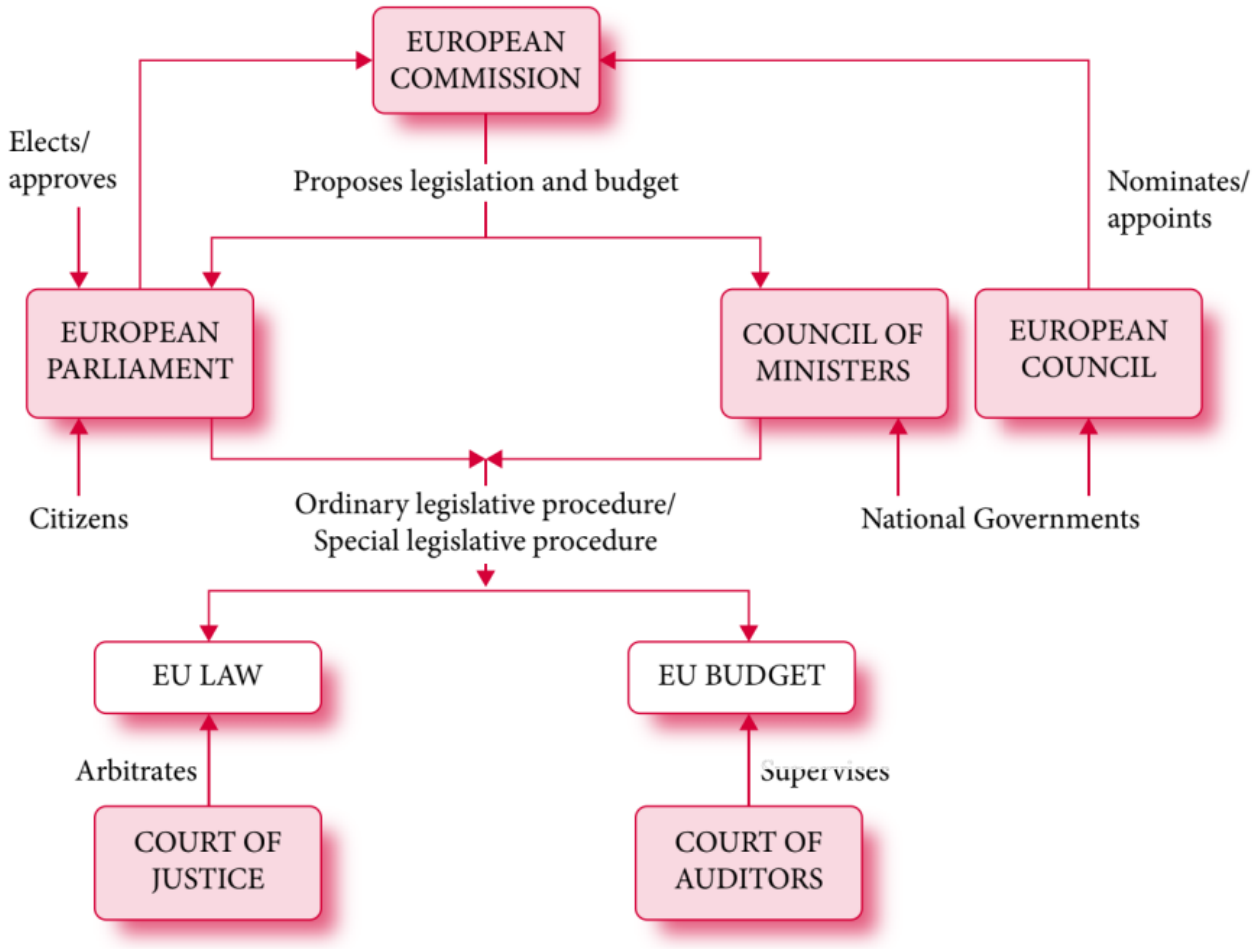


Figure 1. A breakdown of how the different EU institutions relate to each other (Barnard & Peers, 2023)

In the EU decision-making the three last mentioned are involved. The Parliament is representing the citizens, the Council represents the governments, and the Commission represents the EU over-all interests. In the *ordinary legislative procedure*, as shown in Figure 2, after the Commission has

assessed the impact a new law would have, they can make a proposal for it, and the Parliament and the Council will review the proposal. Based on their review they can adopt the law at *the first reading*, or both can come up with corrections, or *amendments*. In such case, the three bodies can have an informal *trilogue* meeting to agree on the amendments. If no agreement on the final text is made, *a second reading* will take place. *A third reading* is also possible if needed, and it will involve a *conciliation committee*. The proposal can finally be rejected if no agreement is found. If the bodies agree with the final text in one of the readings, the proposal is approved and the law adopted after it has been published in the *EU's Official Journal*. (European Council, n.d.; European Parliament, n.d.-a; European Union, n.d.-c)

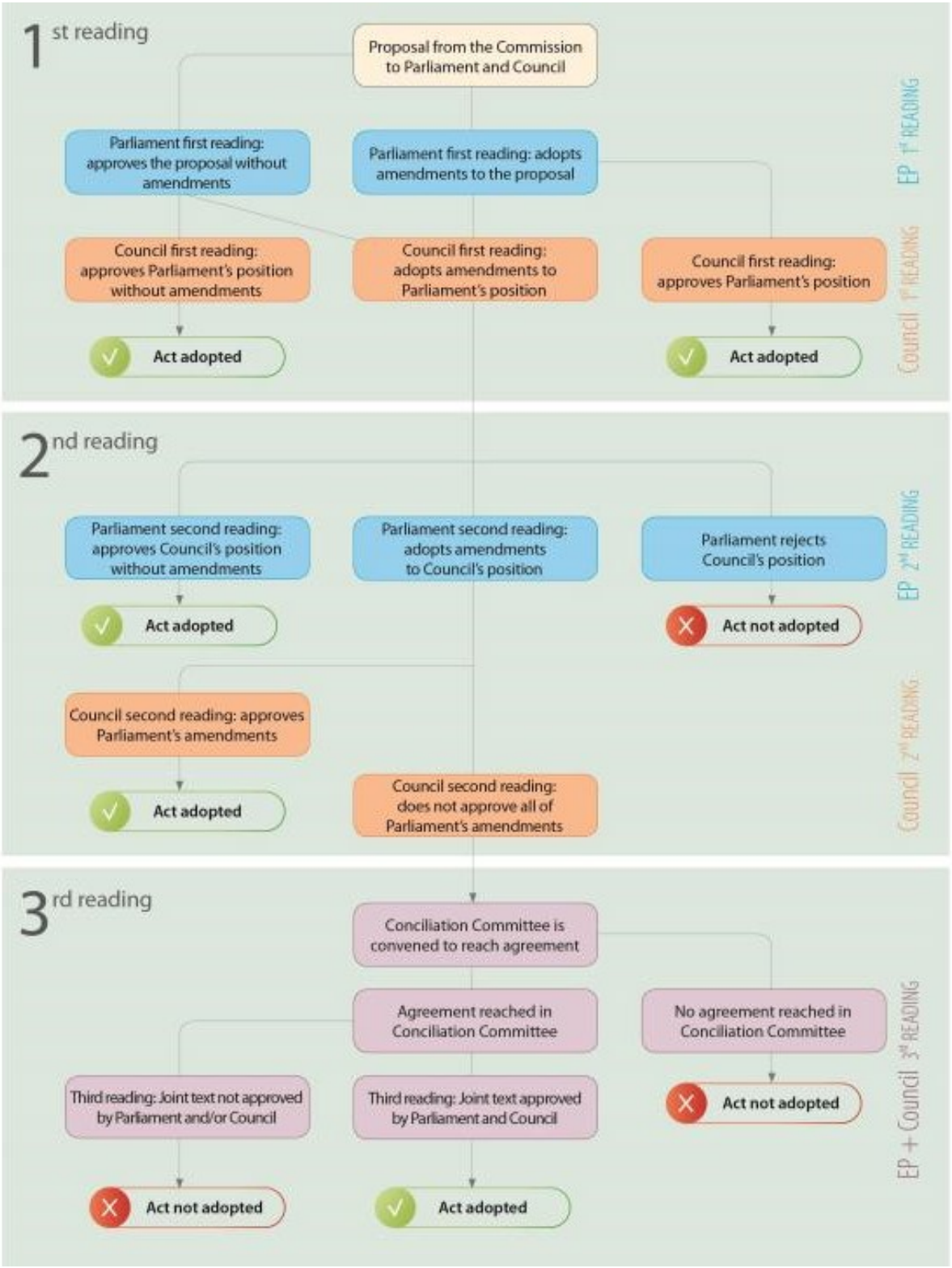


Figure 2. The EU Ordinary Legislative Procedure explained (European Parliament, n.d.-b)

The European Union legislation includes many types of legal acts. In the context of this thesis, from regulations, directives, decisions, recommendations and opinions, the two first mentioned

are the most relevant. The EU, while making the legislations, sets its goals. A *directive* is a type of legislation that leaves the Member States some leeway by *transposing* the directive to device their own law. While the freedom in transposing the law may sometimes be necessary due to difference of each Member State, it can also bring some issues due to the fragmentation of the legislation across the internal market, as it was seen e.g., with the NIS directive (Contreras, 2023, pp. 332-333). A *regulation* avoids this kind of issues, being a legislative act that is binding and must be applied in its entirety in each Member State. (European Union, n.d.-f)

3.6 The Proposed CRA Regulation

During the literature review the access for and availability of articles related to the CRA was quite scarce even if it was mentioned in several. It is expected that the literature proliferates during the development of the regulation and the closer to the adoption of the law. Furthermore, there were no theses found written on the subject from the thesis databases available.

As Chiara (2022) explains in his article, the past EU cybersecurity regulation has followed vertical approach, but the new CRA will set the rules for cybersecurity of the products horizontally. He emphasises that the connected products increase the attack surface and needs to be better protected. Harmonised rules for cybersecurity are the most powerful way in increasing the cyber resilience.

Burri and Zihlmann (2023) state that the lack of cybersecurity in the products available on the market originate from the competition of the markets with price and early access. The motivation for producing cybersecure products is missing. European manufacturers are suffering in the competition when non-EU manufacturers bring cheap products to market on the expense of security. Authors see that the new law being a regulation rather than a directive is reducing the regulatory fragmentation but are highlighting the importance of the current regulation's clarity. For example, the criteria on products belonging to a list of higher importance is not clear and they question whether the list of the products can follow the rapid evolution of the development of the technology. Furthermore, the regulatory requirements in the CRA are spread through the regulation text and annexes making it imperative to analyse the CRA text holistically.

Mueck et al. (2023), in the IEEE article, bring up the importance of the EU harmonised standards (HSs). The regulation includes presumption of conformity i.e., the conformity with the essential requirements of the regulation can be supported by following the HSs, but the HSs are yet to be drafted by the ESOs.

This thesis aims to contribute the academia by considering the most recent version of the CRA. The law proposal was reviewed by the Horizontal Working Party on Cyber Issues (HWPCI), and it met some significant changes on topics like its scope, the product categories and reporting obligations, before the Council reached agreement with the text in July 2023 (Council of the European Union, 2023). As the available literature is based on the CRA proposal rather than the final text, there is a gap that this thesis will aim to fill. It will investigate the existing cybersecurity regulation as to explain the evolution that has led to the CRA. Thesis will explain the basics of the new regulation, and the goal is to help the manufacturers of the products with digital elements in complying with the new regulation. The analysis of the CRA in this thesis has been updated to use the final, adopted version of the regulation, that can be found from European Union official website (Regulation 2847/2024).

4 History of the EU Cybersecurity Regulation

Even though the Network and Information Security (NIS) directive from 2016 is mentioned to be the first *cybersecurity* legislation covering the entire European Union, it is not the first time the EU is working on securing and protecting the European population in the cyber space (European Commission, 2022a). The cybersecurity and information security laws recently published, and the ones in the making, are a result of a lengthy process, and as the technology evolves the legislators need to keep up the pace.

There's a plethora of Regulations, Directives, proposals, opinions, reports and such, related to security in information technology from different European institutions. In the following chapter I will shortly go through significant legislation and decisions related to cybersecurity in chronological order (Figure 3). The list is not meant to be exhaustive but rather replay important decisions and observations as a path to the most recent legislation.

Figure 3. Timeline of EU decisions

Data Protection Directive, DPD, 1995

Data protection is a subclass of cybersecurity and plays a vital role in securing personal data in the computer systems. Since the end of World War II there has been legislative means protecting the right for personal data, but the first law in Europe dedicated to personal data protection was introduced as far as back in 1970 in Germany (European Parliament, 2020). Council of Europe's Convention 108 from 1981 was the first internationally binding legal instrument on protecting personal data on automatic data processing (Wilhelm, 2016). On the EU level the first legal implementation saw daylight in October 1995, when the Data Protection Directive (DPD), set down the rules for protecting the processed personal data (Directive 95/46/EC).

Telecommunications Data Protection Directive, 1997

The development of new digital telecommunications technologies, like digital mobile networks and ISDN was fast and legislators soon needed to complement and specify the privacy laws with the Telecommunications Data Protection Directive. Unlike the previous, this directive specifically applied to publicly available telecommunications service. In addition to the privacy requirements, the new directive stated that electronic communications service and network providers needed to ensure the technical security level based on the risk and confirm the confidentiality of the communications service. (Directive 97/66)

eEurope, 1999

In 1999 the Council started an initiative called eEurope, which aimed to foster the EU's footprint in the digital economy e.g., by bringing access to cheaper and faster Internet connections, enhancing digital services in health care and transportation and providing risk capital funding for high-tech companies (European Commission, 1999). In the subsequent eEurope Action Plan (Commission of the European Communities, 2001a) there was seen a need for strong emphasis on the network security and the battle against cybercriminals.

Budapest Convention on Cybercrime, 2001

Even if in the beginning of the new millennium the cyber regulation was not yet flourishing, in regards of combating cybercrime EU achieved something that could be called revolutionary; agreement on the first international convention with sole focus on cybercrime. In 2001 the Council of Europe adopted the Budapest Convention on Cybercrime, which aiming to harmonise national laws, defined cybercrime and authorities' rights to prevent, investigate and prosecute cybercrime, and pursued advancing international co-operation in the fight against cybercrime. (Council of Europe, 2001)

Strategy on the Network and Information Security, 2001

Although the theme of the European Council's meeting in Stockholm in March 2001 was economic and social questions, it touched also the security of digital networks. In the meeting they concluded that the Council should develop with the Commission a strategy on the security of the electronic networks (European Council, 2001). As a response to this, the Commission communicated in mid-2001 with "Network and Information Security: Proposal for A European Policy Approach". The commission's outlining for the strategy complemented the policies for cybercrime, data protection and telecommunications. It has a review of the prevailing security threat landscape and gives practical ways of improving the network and information security. They highlighted the need for evolution for any related policies in the light of the dynamic nature of network and information security; the technology development is fast, and the society and critical infrastructure is increasingly dependent on working and reliable networks. In their recommendations, amongst others, they proposed increasing the awareness and international co-operation, and supporting new technology development and new standardisation. (Commission of the European Communities, 2001b)

Telecoms Package and ePrivacy Directive, 2002

In 2002 EU decided about its larger regulatory Framework for Electronic Communications called 'Telecoms Package'. For the most part it dealt with boosting the competition in the sector of electronic communications and enhancing consumer position by lower rates and freedom of choice, but parts of it concerned security matters. As a part of 'Telecoms Package', the Directive on privacy and electronic communications replaced the former Telecommunications Data Protection Di-

rective. Better known as ePrivacy Directive (ePD), or with its mocking name “Cookie Law”, required the websites to inform the user about the use of cookies and to allow the user to refuse cookies. As an important change in the directive, it broadened the scope of the communications the legislation applies from traditional telecommunications to any electronic communications. Also, meta data, or traffic data, as the directive says, was now included in the privacy requirements. (Directive 2002/58/EC; Kavya, 2024)

The EU Telecoms Package also included the Framework Directive, where Member states were obliged to supervise that the tasks assigned to the national regulatory authorities by the Directive were taken care of by a proficient player. The tasks assigned included making sure of the public communications networks maintained the security and integrity, and that privacy and protection of personal data were well taken care of. (Directive 2002/21/EC)

eEurope, 2002

In 2002 eEurope initiative had given satisfactory results and was continued with eEurope 2005 action plan to further bolster the information society. Boosting the digitalisation and technical development with new services and communications networks the security was still heavily involved in the equation. It was clear that when devices are increasingly interconnected and online services are increasing, it is necessary to ensure the communications are secure. A practice chosen was to adjust the legislation to support the intended development, initiate projects to help in following the best practices, monitor the progress of the set objectives and coordinate with the existing policies. A decision was made to establishing a cyber security task force (CSTF) as a focal point on security matters. (European Commission, 2002)

Establishment of ENISA, 2004

Network and information security had long been a topic with high focus on EU legislators. To avoid the requirements being implemented in diverse ways, to raise awareness and to provide training and guidance, a central body to was to be established. ENISA (the European Union Agency for Cybersecurity) was found in 2004 with a mandate for a limited period of five years with the following purpose:

> "*For the purpose of ensuring a high and effective level of network and information security within the Community and in order to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, thus contributing to the smooth functioning of the internal market, a European Network and Information Security Agency is hereby established*"

From the start ENISA had an advisory role in information security. By providing information and assistance all the way from European Parliament, the Commission and Member states to universities, public and private sector businesses and EU citizens, ENISA will help to foster collectively Europe's security posture. On top of the consulting ENISA was tasked with keeping an eye for the network and information security associated standards development. (Regulation 460/2004)

Revised Strategy on the Network and Information Security, 2006

As the Internet use had significantly increased and related threats were more sophisticated, the EU saw a need to invigorate the Network and Information Security (NIS) strategy from 2001. In May 2006 EU published a preparatory document "A strategy for a Secure Information Society – Dialogue, partnership and empowerment". In the new strategy the EU states that the entire ICT sector is absolutely important for European economy and society, but there are challenges in the security of the network and information systems. The document stresses that the risks are underestimated, the enterprises see security as a cost due to lack of distinct return on investment and individual users don't understand their significance in the puzzle of overall security. It also recognises the difficulty the policy makers have, to deal with large amount of stakeholder groups in setting the regulation and public policies to enhance NIS. As per its name, the strategy aims to harness dialogue, partnership and empowerment as tools in achieving its ambition. (Commission of the European Communities, 2006)

Critical Information Infrastructure Protection, 2008

In 2008 the Council Directive concerning the need of the identification and protection of European critical infrastructures (ECI), specifically focused on the energy and transport sectors and left the ICT sector as a priority to be discussed in the future (Directive 2008/114/EC). The Communication

from the Commission in 2009 instead had a full focus on ICT sector, its critical information infrastructures (IIC) and urge on enhancing EU's NIS policy. Dependency of other industries increases the importance of IIC even higher. With this Communication the Commission started the preparations for identifying the European critical ICT infrastructures, enhancing the resilience and preparedness on large scale security incidents and further advancing the co-operation both between Member States and on international level. (Commission of the European Communities, 2009)

Amended ePrivacy Directive, 2009

The ePrivacy Directive was amended in 2009. It is really the one that brought the cookie consent banners to our Internet browsing sessions by strictly requiring the websites to ask for consent from the user to use the cookies. Amendment obliged service providers to guarantee authorisation and integrity of the personal data in transit and at rest and implement a policy on processing it. One of the biggest changes by the new Directive was, that when earlier the service provider was obliged only to state users on the possible risks of a breach of a network, now for the first time there was a requirement to notify the national authority on the breach of personal data. Moreover, if the breached data could cause harm to the individual whose personal data was breached, the notification was required also to the individual itself. (Directive 2009/136/EC)

Establishment of the European Cybercrime Centre, 2013

To help in fight against the increasing cybercrime, in 2012 the European Cybercrime Centre (EC3) was decided to be established. EC3 focus is the cybercrimes committed by the organised criminal groups, ones that will cause grave harm to its victims, or target to critical infrastructure or information systems in the European Union. EC3 is to support the Member States in operational tasks and act as a cybercrime information focal point with expertise to help EU countries in building their own capacity by providing training especially to the different police units. The EC3 was established as a part of Europol in 2013. (European Commission, 2012)

The First EU Cybersecurity Strategy, 2013

In the European Union's first cybersecurity strategy (EUCSS), that dates back from 2013, EU shares their vision on cybersecurity, defines the roles and responsibilities of different stakeholders, and

lists the required actions to make European information systems safe and well protected. EU wants to keep the same values, principles and norms in the web that apply in real life, and it requires collaboration of governments and the private sector to protect the cyberspace from any threats endangering its reliability and openness. The priorities in the strategy are set for reaching cyber resilience; minimising cybercrime; generating policy and skills for cyber defence; ensuring the European cybersecurity technological and industrial resources; and forming an international cyberspace policy leaning on EU core values. The main goal of the EU's cybersecurity strategy is to make the European networks the safest in the world. (European Commission, 2013)

NIS1, 2016

In July 2016 the first EU-wide cybersecurity legislation saw daylight, when the Directive on Security of Network and Information Systems (NIS) was adopted by the European Parliament. Member States were required to transpose the directive into their national law by May 2018. The directive obliges Member States to create a national strategy to ensure the security of network and information systems. Every Member State is required to appoint a Computer Security Incident Response Team (CSIRT) which has duties inter alia to follow and respond on national level the security incidents, arrange notifying and alerting of the risks and incidents, and engage in the cooperation of CSIRTs network. Also, a Cooperation Group consisting of ENISA, the Commission and representatives of the Member States must be established to enhance the Union and international liaison to achieve required minimum level of security in the networks and information systems. (Directive 2016/1148)

To tackle the unequal level of cybersecurity in the Union, the directive imposes minimum requirements for operators of essential services (ESP) and digital service providers (DSP) within each Member State on a common level of protection of network and information systems' users. Both ESPs and DSPs are required to ensure appropriate and proportional security measures on technical and organisational level based on the risks posed on their systems to prevent and mitigate the impact of possible security incident. Moreover, they both have an obligation to report security incidents having significant impact on their services to the competent authority or CSIRT. The directive itself doesn't specify any measures to be compliant but directs ENISA to draw up advice

and guidelines for this. The NIS directive categorises critical infrastructure, like energy, transportation, banking and health sector to be included in ESP. DSP includes online marketplaces, online search engines and cloud computing systems. (Directive 2016/1148)

GDPR, 2016

Perhaps the most well-known privacy or IT related regulation of the European Union was adopted in 2016 to protect online privacy rights of personal data: the General Data Protection Regulation, better known on its acronym GDPR. Since May 2018, when GDPR rules took effect, any organisation in the world handling personal data of an EU citizen had to comply with this law. (Regulation 679/2016)

GDPR is considered to be the most stringent law related to privacy and security with hefty fines for violating it. (Wolford, n.d.) Many countries outside the Europe quickly followed EU's example using GDPR as a benchmark (European Data Protection Supervisor, n.d.).

Second Cybersecurity Strategy, 2017

The revised EU cybersecurity strategy in 2017 drove to boost the cyber resilience by fully implementing the NIS Directive. Information sharing and cooperation between public and private sector was seen to have room to improve. An initiative was proposed to encourage for security-by-design principles and reducing of product vulnerabilities. The importance of awareness and training was acknowledged, especially to the public administration. ENISA's mandate was seen constraining its operation and was proposed to be regularised. The strategy highlighted the importance of cyber preparedness, responding to cyberattacks and building a deterrence for those considering cyberattack. (European Commission, 2017)

CSA and Permanent Mandate for ENISA, 2019

The temporary mandate for ENISA was extended several times until 2019 the mandate was made permanent and expanded its role from a pure advisory to an operational one. At the same time EU regulators adopted the Cyber Security Act to build up a harmonised cybersecurity certification framework of ICT products, services and processes. By harmonising, the Union aimed to avoid the

fragmentation of the Single Market which facilitates the trade within the EU. The certification was set to be voluntary and empowering the Commission to assess where the certification should be made mandatory. (Regulation 881/2019)

New Cybersecurity Strategy, Dec 2020

European Commission (2020a) published in July 2020 their Joint Research Centre's cybersecurity report that estimated the cost of cybercrime to more than double from €2,7 trillion figures of 2015 to €5,5 trillion in 2020. Cybersecurity was seen to need to change from a choice to a necessity. The outcome of the report was a recommendation to implement an EU-wide unified cybersecurity strategy.

In December 2020 European Commission lined up their new Cyber Security Strategy (2020b). The intention of the strategy is to develop the cybersecurity posture, increase the tolerance against cyberattacks, and assist in ensuring the EU citizens and organisations can use reliable and secure connected devices and digital services. This will require upgrading the operational cybersecurity capabilities. Cybersecurity should be enhanced in all parts of the supply chain and improve the collaboration both between the EU and its international partners and across the EU four cybersecurity communities – internal market, law enforcement, diplomacy and defence. In the heart of the strategy were NIS2 and CER directives that both addresses the resilience of the critical entities and networks but from different angle.

DGA, 2022

Data Governance Act was set to ease the sharing of data within EU to use the potential of the vast amount of data. It provides for example rules and safeguards to reuse the publicly held data on a secure manner ensuring the privacy of the data, or the data shared on an altruistic basis for use of general interest. The means to reuse also protected data with certain limitations is created. The Act introduces the data intermediaries that will work as neutral third parties facilitating the data exchange between the parties. (Regulation 868/2022)

NIS2, 2022

The limitations of the NIS1 were evident quite quickly, and NIS2 directive was introduced to fix the inconsistencies. It broadened the scope to cover more sectors and entities, included more specific and stringent rules for incident reporting and emphasised the importance of the supply chain risk management. NIS2 divided the affected sectors to essential and important entities based on their criticality both having different level of obligations. The new directive increased the power of national authorities, expressed heavier penalties for non-compliance and introduced a Coordinated Vulnerability Disclosure (CVD) framework with EU Vulnerability Database (EUVD). (Directive 2022/2555; European Commission, 2023a)

CER, 2022

Even if not purely a cybersecurity law, the Critical Entities Resilience Directive, that repealed its predecessor [Directive 2008/114/EC], has a strong link with NIS2 in building up the strong defence and resilience of the European Union critical entities. It covers the physical security and allow for the risk of hybrid threats to increase the overall security of the critical entities. (Directive 2022/2557)

DORA, 2023

The Digital Operations Resilience Act [Regulation (EU) 2022/2554] was adopted in November 2022, entered into force in January 2023, and will apply two years later. It targets to harmonise the cybersecurity rules and enhance the overall cybersecurity of financial sector, like banks and investment companies. DORA requires for example ICT risk management, reporting of ICT incidents and concrete digital operational resilience testing. (Council of the EU, 2022; European Insurance and Occupational Pensions Authority, n.d.)

AI Act, 2024

The European Union Artificial Intelligence Act is the first legal framework on Artificial Intelligence in the world (European Commission, 2024b). It aims to reduce the risks and ensure trust in the AI systems, make sure the protection of health, safety and fundamental rights is on high level and enhance the free movement of AI-based goods and services. The Act has risk-based approach with

four risk categories for AI systems all having different level of obligations. The non-compliance can be punished with hefty fines of up to 35 million euros or 7% of company's annual worldwide turnover. (Regulation 1689/2024)

Analysis

An analysis of cybersecurity legislation over the past three decades shows that it has had to change in line with the technological development. While the law-making is a slow process, the legislation sometimes struggles to keep up with the technology evolution. Although it is usually only possible to start drafting legislation once the relevance of a technology has been recognised, by which time it is often already in widespread use, the European Union has shifted from reactive measures towards proactive frameworks trying to anticipate the technological evolution. The early legislation was often targeted in nature, whereas more recent law-making has taken a more systemic approach and entails rather an entire ecosystem.

In the 90s and 2000s when the number and speed of data connections was in a rapid growth the legislation was much focused in the security of the information networks. The combat against cybercrime started already on previous decade but had more weight on 2000s. ENISA was established to build up competencies in cybersecurity and act as a central advisor in the subject.

In 2010s the focus moved towards resilience of the networks and services and the significance of incident response and reporting was emphasised. The EU worked for harmonising the cybersecurity rules. The need for international cooperation was increased and collaboration between different stakeholders bolstered. Privacy matters saw a huge improvement with the GDPR. ENISA's role was seen as mandatory, and its mandate was made permanent and role expanded.

Accountability has increased on 2020s, shifting the responsibility for cybersecurity towards operators and manufacturers. The interplay between different regulations has always been there but seems to have taken a leap forward. EU jurisdiction has more extraterritorial features, and since the GDPR, the high penalties for legislation non-compliance are more common.

It is clear that the CRA is a continuum and an expansion on the existing cybersecurity legislation and follows the cybersecurity strategies set by the EU. Even if the CRA is "just a next step", it is expected to have a great positive impact on cybersecurity both within the EU and globally. The next chapter will take a closer look at the CRA.

5 Cyber Resilience Act

This chapter is explaining first what the CRA is, who does it concern and why it is important, before taking a deep dive in defining the requirements the new regulation sets. Information in this chapter and its subchapters is analysed from the CRA document by the author unless otherwise referenced. References to the CRA document are left out avoiding excessive repetition for reader's convenience.

5.1 Overview of the CRA

"If everything is connected, everything can be hacked" declaimed Ursula von der Leyen, the President of The European Commission, in her State of the Union speech in September 2021, when announcing the new European Union regulation, the CRA (European Commission, 2021). One year later the European Commission published the first proposal for the EU CRA (European Commission, 2022c). The proposed law raised strong resistance especially in the open-source community and the proposal saw a plethora of amendments before it saw several changes and was agreed in the third trilogue in the end of November 2023, adopted by the parliament in March 2024, and finally adopted by The Council in October 2024 (Polona, 2024). The CRA was published in the European Union Official Journal on November 20th, 2024, and entered into force December 10th, 2024. The regulation will apply i.e., requirements need to be fulfilled, from December 11th, 2027, except the reporting obligation, which starts already in September 2026.

Cybercrime is extremely expensive for companies, organisations, communities and individuals. Poor cybersecurity level of products makes networks and telecommunications systems prone to cyberthreats, and lack of security updates makes the fight against cybercrime difficult. Choosing secure products is cumbersome without a thorough investigation, and is often a mission impossible for an ordinary consumer. For cybersecurity professionals the new law is a godsend. Far too

often, I've heard from the cybersecurity community that cybersecurity is still seen as a burden rather than an enabler for many organisations. Just as insurance payments are seen as a pointless expense before accident occurs, cybersecurity is often seen as expensive before a security incident or breach occurs. Whether it's a smart doorbell for a consumer, or a router for a business, it could be a device connected to your network that is the culprit that exposes all your data to a malicious actor. And for sure the cybersecurity professionals are not the biggest part of population that are having the benefits: most of the consumers – or even organisations - may not have the sufficient knowhow or skillset to evaluate or achieve the level cybersecurity to be safe from cybersecurity threats. The CRA is an answer from EU for the ever growing cyberattacks. The regulation pushes the responsibility of cybersecurity back to the manufacturers by laying ground strict rules for adequate level of cybersecure products. (European Commission, 2023b)

The CRA will be the first EU wide law that lays binding rules for product manufacturers on their products' cybersecurity. The CRA has requirements also for importers and distributors of products, but as the technical requirements are similar as the requirements for manufacturers, the thesis focuses on manufacturers. Apart from above-mentioned, the CRA has requirements also for open-source software stewards, market surveillance authorities and assessment bodies, but they are out of scope of this thesis. Being a regulation rather than a directive, it brings harmonisation in the cybersecurity rules: each of the 27 EU Member States will follow exactly the same law. Harmonised rules make it easier for the free movement and supplying products anywhere in the European market.

The CRA applies with some exception for any product, either hardware or software, that has possibility for a remote data processing. The CRA has four different categories for products based on how big of a risk an adverse effect could pose. All categories have the same cybersecurity requirements, but products in higher risk categories have stricter requirements for the conformity assessment procedure. Products need to be assessed for the risks their intended use and usage environment expose them for. Horizontal cybersecurity requirements for manufacturers apply the wide range of products for the whole lifecycle from planning, design and development to their production, delivery and maintenance until the end of the product's life. Manufacturers need to exercise due diligence when they are utilising any components sourced from third-party suppliers, meaning that the manufacturer needs to make sure the third-party components, that are integrated to

their product, need to be safe and not endanger the security of the product. The manufacturer needs to provide instructions to users, and craft a technical documentation on the product for availability of market surveillance authorities. Products need to be placed on the market with no known exploitable vulnerabilities, with secure by default configuration, and the security of the product needs to be maintained throughout the entire expected lifespan of the product with proper vulnerability management. Before placing the product on the market, a conformity assessment needs to be conducted, and CE marking affixed to the product.

Rules seldom work without an incentive. If having secure products, that can avoid costly and disruptive security breaches is not big enough stimulus, the regulation lays penalties for non-compliance. Administrative fines of up to 15 MEUR or 2,5 % of the company's worldwide annual turnover for non-compliance of the essential cybersecurity requirements should be heavy enough penalty to encourage every company to make their best in fulfilling the obligations set by this regulation.

The CRA document, like any EU legislation, starts with a part called the preamble, which contains recitals. It is a part that explains the background and reasons for the act and the aim or objective, using more like common language rather than normative language. (Practical Law, n.d.) The latter part of the CRA, that is divided in eight chapters and eight Annexes, is the part where the legal requirements are. Chapters include Articles with a running number throughout the document. Chapters and Annexes of the CRA have the following titles:

I. General provisions
II. Obligations of economic operators and provisions in relation to free an open-source software
III. Conformity of the product with digital elements
IV. Notification of conformity assessment bodies
V. Market surveillance and enforcement
VI. Delegated powers and committee procedure
VII. Confidentiality and penalties
VIII. Transitional and final provisions

Annex I ESSENTIAL CYBERSECURITY REQUIREMENTS
Annex II INFORMATION AND INSTRUCTIONS TO THE USER
Annex III IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS
Annex IV CRITICAL PRODUCTS WITH DIGITAL ELEMENTS
Annex V EU DECLARATION OF CONFORMITY
Annex VI SIMPLIFIED EU DECLARATION OF CONFORMITY
Annex VII CONTENT OF THE TECHNICAL DOCUMENTATION
Annex VIII CONFORMITY ASSESSMENT PROCEDURES

This study is meant to help the manufacturers in understanding the requirements of the regulation and what needs to be done for the compliance. In the following subchapters I will guide through the requirements the CRA sets.

5.2 Reporting Obligations

There is a liability set in the CRA Article 14 for manufacturers, that must be met already from September 2026: reporting of actively exploited vulnerabilities in their products and any severe incidents that impact the security of the product. The report needs to be sent simultaneously to ENISA and the designated Computer Security Incident Response Team (CSIRT) of the Member State where the manufacturer has its main establishment. If the manufacturer is active in more than one Member State, the reporting is done for the CSIRT of the Member State where the manufacturer makes the cybersecurity related decisions. ENISA is responsible on establishing a single reporting platform to ease the reporting obligation of manufacturers. Manufacturers need to inform also the impacted users, or depending on the case, all the users of the product on exploited vulnerability or severe incident and the related corrective or mitigation actions.

5.2.1 Actively Exploited Vulnerability

Whenever a manufacturer becomes aware of any actively exploited vulnerability, it needs to send an early warning notification as soon as possible, but within 24 hours. If applicable, the notification should have information in which of the Member States the product is used in.

A vulnerability notification needs to be sent also as soon as possible, but within 72 hours from becoming aware of the vulnerability exploitation. The notification should include the general information on the product, on the exploit and on the vulnerability. Apart from these, also the information on the mitigation actions already taken, the mitigation actions the user may take and the sensitivity of the notification information if seen relevant.

After a correction or mitigation measures information is delivered, manufacturers have 14 days to deliver a final report. It needs to include a vulnerability description along with severity and impact;

information on the malicious actor exploiting the vulnerability in case the actor is known; and detailed information on the security update or any mitigation instructions to remedy the vulnerability.

5.2.2 Severe Incidents Impacting the Security of the Product

For a severe incident that hampers the security of the product, an early warning notification needs to be sent within 24 hours. The notification needs to describe if the incident is suspected to be a malicious or unlawful act. If applicable, the notification should have information in which of the Member States the product is used in.

An incident notification needs to be sent also without delay, but latest within 72 hours from becoming aware of the incident. The notification should include the general information on the product, on the nature of the incident, and a first assessment of the incident. Apart from these, also the information on the corrective actions already taken, the mitigation measures the user may take and the sensitivity of the notification if applicable.

Within one month from the incident notification, manufacturer needs to provide a final report including at the very least a detailed explanation of the incident combined with the incident severity and impact information; the root cause of the incident or the threat causing the incident; and the mitigation actions already done and being prepared.

5.3 Categorisation of the Products

The first thing to clarify about the CRA requirements is which products the CRA applies to and to which category the applicable products belong. By the CRA Article 2, the requirements apply to "*products with digital elements made available on the market, the intended purpose or reasonably foreseeable use of which includes a direct or indirect logical or physical data connection to a device or network*". A "*product with digital elements*" has been defined in Article 3 and includes basically any hardware or software products and their related components that has remote data processing functionality.

The CRA Article 3 has definitions of different terms used in the regulation, and the European Commission's (2022b) reference document 'Blue Guide' has a more thorough definitions for the terms "Placing on the market" and "making available on the market". "Placing on the market" means when a manufacturer for the first time makes the product available on the EU market, and it can only be done once per product. "*Making available on the market*" instead is any further supplying of that product. The applicability of the CRA requirements for the products placed on the market before the CRA applies can be interpreted in more than one way. The Article 13, "Obligations for manufacturers", mentions that the requirements apply when "placing a product on the market", whereas the Article 6 mentions that the products can be "made available on the market" only when they fulfil the requirements of the Annex I.

The Article 2 lists products that are excluded from the CRA, for a reason that they are already covered by other Union legislation. The list contains medical devices that are covered in the regulations (EU) 2017/745 and (EU) 2017/746, motor vehicles and trailers regulated in (EU) 2019/2144. The CRA applies neither for civil aviation nor marine equipment covered by (EU) 2018/1139 and 2014/90/EU. Also, the products that are exclusively for national security or defence purposes, are not in the scope of this regulation.

The CRA uses a risk-based approach on dividing the applicable products into four different categories, which all employ different methods to conduct the conformity assessment, which is explained more detailed in a later chapter. While the CRA doesn't mention "a default category", it's convenient to address that all applicable products belong either to the default category or one of the higher categories. The CRA Annex III (appendix 3) lists "important products with digital elements" dividing them to class I and class II, for the latter to have more stringent requirements for conformity assessment. The most demanding conformity assessment requirement is for the category of critical products which are listed in the Annex IV (appendix 4) of the regulation. Article 7 of the CRA states the Commission's responsibility to specify the technical details related to the product categorisation by an implementing act latest in December 2025.

One important reminder in Article 7 is that categorising a product is done by the core functionality of the product, and integrating a product from another category doesn't necessarily mean the product should belong to the higher category where the integrated part belongs to. As a concrete

example, firewalls belong to Important Class II, but integrating firewall functionality to a default category product doesn't mean the product would automatically fall under the Important Class II.

5.4 Cybersecurity Risk Assessment

Manufacturers need to conduct a cybersecurity risk assessment for their products, as mentioned in the Article 13. The risk assessment gives a good insight on the cybersecurity risk level in a product enabling necessary risk treatment. Knowing where the soft spots are is a key to make the product more resistant to cyberthreats and this way prioritising and managing the risks. The CRA requires the assessment to include explanation on how the cybersecurity and vulnerability handling requirements in the Annex I apply to the product and how they are taken care of. As a bare minimum the risk assessment must contain an analysis of the risks based on intended and reasonably predictable use; the conditions of using the product, like the intended environment, taking into consideration also the expected lifespan of the product. The cybersecurity risk assessment needs to be documented and updated during the product's support period as the threat landscape is constantly changing and new vulnerabilities are found. The documented cybersecurity risk assessment needs to be included in the provided technical documentation provided, which in turn needs to be available to notified bodies performing conformity assessment and market surveillance authorities upon request.

The cybersecurity risk assessment is not something light and trivial, but needs competent resources and involvement and commitment of all stakeholders (Cobb, 2024). As the companies and organisations differ from each other there is no one-size-fits-all rule for conducting a cybersecurity risk assessment. There is a lot of instructions on the Internet on how to conduct a cybersecurity risk assessment and there's of course an option to outsource this work for professionals if there are no internal resources for the task. The CRA doesn't take a position on the risk assessment methodology to be used, neither does lawmakers yet - at the time of conducting this study - provide a harmonised standard that would reliably meet the requirement for the cybersecurity risk assessment. ETSI has also raised this anomaly in their document (ETSI Technical Committee Cyber Security, 2023). Without further instructions from the legislation, the best approach would be to use a widely recognised sources to conduct the assessment, like standards or frameworks from

ISO/IEC 27000-series, ISO/IEC 31000-series or NIST Cybersecurity Framework. In short, by Finio and Downie (2024) the cybersecurity risk assessment for a product consists of:

- analysing the asset being assessed;
- identifying the product related threats and vulnerabilities;
- estimating the probability of the threats;
- measuring the impact of threat realisation;
- calculating the risk from the probability and impact;
- mapping security controls to each risk;
- implementing the controls based on the risk analysis; and
- monitoring and documenting the outcome of the assessment.

The cybersecurity risk assessment document will help the management in decision making by evaluating the risk level and mapping findings to available controls to treat the risks. The document should be understandable for broad audience, as readers often do not have the same cybersecurity expertise as the one conducting the assessment.

5.5 Conformity Assessment

Even if the conformity assessment needs to be done in a later phase, it is worthwhile to explain its specificities as it will impact in how meeting the essential cybersecurity requirements is evaluated. In conformity assessment a manufacturer of a product needs to demonstrate that their processes meet the vulnerability handling requirements set in the part II of the Annex I and the product meets the essential cybersecurity requirements set in the part I of the Annex I. It will be a long way from the categorisation of a product before the conformity assessment will be done, but for the preparation it is important to know that depending on under which category the product falls, the procedure of conformity assessment differs. Article 32 and Annex VIII (appendix 8) explain the different procedures of the assessment.

The CRA sets the minimum requirement for the conformity assessment procedure but gives manufacturers freedom to choose more stringent procedure for the assessment. The difference between the assessment procedures is explained later in this chapter. The lack of any guidelines for conducting the conformity assessment will make the task hard and hinder the comparability of results between two identical products (European Cyber Security Organisation, 2024).

The products that fall under the default category are non-critical and can be assessed with internal control using Module A, even if the manufacturer has not applied any harmonised standards, common specifications or EU cybersecurity certification scheme (Figure 4). As the CRA Article 32 states, important Class I products can be assessed also with internal control, but in that case, they need to apply harmonised standards, common specifications or EU cybersecurity certificate. This is important to note if the manufacturer for a reason or another wish to avoid third party assessment. The other option for Important Class I product is procedure using Modules A and B, meaning both, the EU-type examination of the product by a third party and internal production control. Important Class II products will always need third party conformity assessment for the product, meaning assessment with Modules A and B. Default and Important Class products can also be assessed using Module H, which is based on full quality assurance.

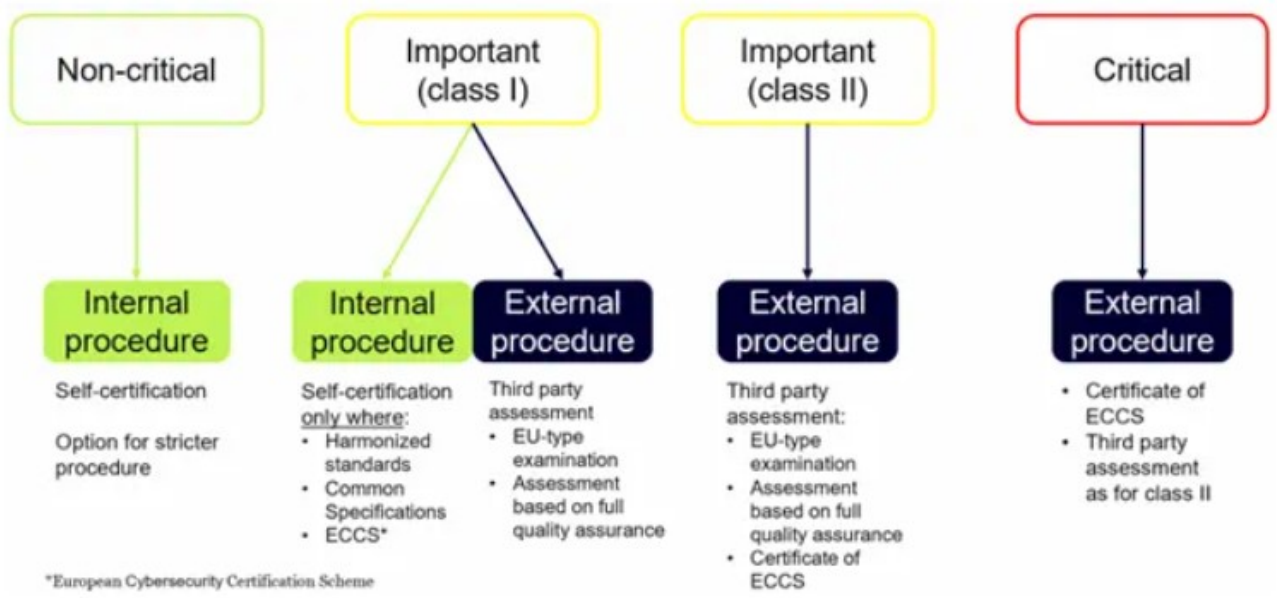


Figure 4. Conformity assessment procedure options for different category products (Hanssen & Vogel, 2024)

Article 8 refers to the conformity assessment of critical products. It is a decision to be made by a separate delegated act from the Commission, on which of critical products will need to apply for the European cybersecurity certificate, at a minimum assurance level ‘substantial’. Before such delegated acts are adopted, the conformity assessment for critical class products will be done the same way as for Important Class II products.

It's fair to say that manufacturers should follow the evolving regulatory framework, as for the time being the harmonised standards and common specifications are a work in progress. The European Commission provides an updated list of harmonised standards published in the Official Journal of the European Union on their website (European Commission, n.d.).

The different procedures used for conformity assessment in the CRA were established originally in The European Parliament and The Council Decision No 768/2008/EC, and are based on the most appropriate modules for assessment selected for the CRA. All of the procedures have somewhat similar rules for affixing the CE marking, all of them require manufacturer to include the technical documentation described in Annex VII for the products being assessed, draw up an EU declaration of conformity in writing and keep it together with technical documentation available for national authorities for 10 years or longer if the support period exceeds 10 years. The procedure to demonstrate the conformity for the cybersecurity requirements instead has great differences between the modules. Regardless of the chosen assessment process, the result of a passed conformity assessment is affixing the CE marking to the product and a written EU declaration of conformity.

Module A, Internal Control

In internal control the manufacturer takes the full responsibility that the product meets the cybersecurity requirements set in Part I of Annex I and the manufacturer meets the vulnerability handling requirements set in Part II of Annex I. This is the only module that does not require a third-party assessment. The manufacturer needs to ensure that their processes from design and development phases to vulnerability handling and the supervision of the processes are compliant with the requirements in Annex I.

Module B, EU-type Examination

EU-type examination focuses on the technical design and development phases of the product being assessed. Manufacturer needs to provide the technical documentation which proves that the product assessed has been designed and developed according to the cybersecurity requirements in Part I of Annex I, and the manufacturer's processes of vulnerability handling meet the requirements in Part II of Annex I. It should clearly state the used design and development method for the

parts it's not done according to harmonised standards or technical specification. Additional supporting evidence including relevant conducted tests and their results need to be provided especially covering the parts that do not follow relevant harmonised standards or technical specification. By inspecting the technical documentation and the provided evidence, including the risk assessment, the notified body will assess the conformity of the product. Notified body will audit one or more critical sections of the product that it has been developed or manufactured according to the provided technical documentation and that it fulfils the cybersecurity requirements.

Module C, Internal Production Control

In internal production control the manufacturer must assure that the production and its supervision ensure conformity with the product that has certified in the EU-type examination. Manufacturer needs to make sure the production complies with the cybersecurity requirements set in Part I of Annex I and the manufacturer meets the vulnerability handling requirements set in Part II of Annex I.

Module H, Full Quality Assurance

The full quality assurance requires manufacturers to operate an approved quality system for its design and development phases, that secures they are in compliance with both parts of Annex I. All the policies, procedures and instructions should be written down systematically for a third-party assessment. The quality system needs to be maintained, and it will be monitored by the third party. It should also involve the final inspection of the product and testing of the products.

5.6 Essential Cybersecurity Requirements

Perhaps the most important content of the CRA is condensed into Annex I as "essential cybersecurity requirements". Manufacturers are obliged to cover the essential cybersecurity requirements based on the risks that have been identified in the cybersecurity risk assessment. The Annex I is divided into two parts, the first setting the requirements for the products and the second focusing on more process related duties. It goes without saying that seeing these two pages of essential cybersecurity requirements is not sufficient to understand the entirety of the regulation, let alone to be able to achieve compliance with the requirements.

In the absence of harmonised standards, manufacturers can find some help in the document "Cyber Resilience Act Requirements Standards Mapping", recently published by the European Commission's Joint Research Centre in collaboration with ENISA to support European standardisation bodies (ESOs) in their obligation to develop EU harmonised standards. It is to be noted, that the final version of the CRA had some revisions, like a different order of requirements and some amendments or additions, and the Standards Mapping document is based on a former, draft version of the CRA. The document identifies in which of the existing major standards the requirements are already covered, and which kind of gaps there still exists. As soon as the harmonised standards are published, the manufacturers can use them to facilitate their objective of achieving compliance with the essential cybersecurity requirements.

This chapter summarises the main practices from the standards recommended in the Standards Mapping document. The aim is not to provide a thorough guide, as this would require in-depth analysis and would more work than the Master's thesis is intended to provide.

5.6.1 Product Cybersecurity Requirements

In this chapter the indented ***bolded italic*** texts are a direct quotation from the legal text of the requirements in Annex I Part I. It's notable, that the requirements need to be applied based on the risks identified in the cybersecurity risk assessment. Keeping this in mind, the summarised practices below may not be necessary, if the related risks are absent.

> ***(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.***

In the first requirement the manufacturer needs to make sure their manufacturing processes are in shape. This includes conducting the cybersecurity risk assessment and keeping it up to date during the product's lifetime. It is mandatory to plan, execute and document cybersecurity in all phases of the production: design, development and manufacturing. This is probably the most labour-intensive requirement as it concerns the entire production cycle.

Principles like secure by design, secure coding and defence in depth can be used to increase the level of cybersecurity. A proper security management needs to be specified for the entire production cycle. Results of risk assessment and threat modelling can be used to help specifying the security requirements. Secure design should apply in all stages of design process taking into consideration among all, any interface, being it logical or physical and accessible externally or internally, users, privileges and roles. Security should be implemented in all layers to make sure the product is protected despite if one or even multiple layers are compromised. Design secure best practices should be applied and secure coding standards used. It should be reviewed that the product was developed and implemented using the secure design and verified by testing. For the integrated third-party components, the manufacturer should apply due diligence to make sure the supply chain doesn't pose risk in the product. Vulnerabilities need to be assessed along the development phase and managed accordingly. The software to be delivered needs to be digitally signed and file hashes of software components provided to ensure file integrity. All this needs to be documented and processes reviewed and updated accordingly if security-related issues are found. (International Electrotechnical Commission, 2018)

> ***(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:***
>
> ***(a) be made available on the market without known exploitable vulnerabilities;***

Manufacturers should consult European Vulnerability Database in detecting the exploitable vulnerabilities. At the time of conducting this study the database was not yet available. Different techniques are required for effective vulnerability detection. Known and published vulnerabilities have been recorded in public vulnerability databases including the signature of the vulnerability. An automated vulnerability scanning tools with an updated vulnerability database can be used to detect such vulnerabilities. Finding zero-day vulnerabilities, those that have not been published, require more advanced and versatile methods. In penetration testing the vulnerabilities of the system are tried to be exploited with authorisation. Different automated or manual tools and technologies are used to evaluate the cybersecurity of the assessed product. Fuzzing technique can be used by giving the tested system or software unexpected input, and monitoring if the system can

handle it, or if due the malfunction the cybersecurity is compromised. Where source code is available, a review for the code can be done. Commonly the source code is so large, an automated solution needs to be used, but often it is practical to include also manual checks. If the source code is not available, the binary analysis tools can be used to found vulnerabilities also from the third-party components or libraries. (International Telecommunication Union, 2018) It is meaningful to automate and integrate the vulnerability detection from applicable parts to the CI/CD (Continuous Integration / Continuous Delivery) pipeline to decrease manual work and to be able to find the vulnerabilities in the early phase of the development chain.

After finding vulnerabilities it is vital to have proper processes for security updates. Applicable software patches need to be evaluated, product needs to be tested after applying the patches, and the product security updates documented in suitable manner. Security updates need to be delivered to customers in timely manner, including appropriate instructions on applying the security patches. (International Electrotechnical Commission, 2018)

> ***(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;***

Range of different possible configurations is wide, thus challenging to cover by any general document or standard. There are many common configurations that will still cover majority of the products concerned. It is more purposeful to deliver products with secure configuration accompanying instructions to loosen certain security configuration as per customer's needs, than delivering insecure products alongside with hardening instructions.

Access rights of the users should follow principle of least privileges and usage of privileged access rights should be managed and kept minimal. Authentication should be made on secure manners depending on the level of security required, taking advantage of digital certificates, smart cards or security tokens over passwords. Where passwords are seen as appropriate authentication means, the password policy should follow current best practices and no universal default passwords shall be used. Logging and monitoring should be preconfigured and secure protocols, algorithms and

crypto suites used by default. Access to networks, ports and used protocols should be limited to only the strictly required ones. (International Organization for Standardization, 2022)

> ***(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;***

Patch management best practices should be followed when issuing corrections for security vulnerabilities. The updates should be automated where technically feasible. Exceptions can be for example air-gapped equipment or sites, or toys that can connect to a mobile app but not to Internet. In this case the security fixes still must be made available even if automatic installation is not an option.

> ***(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;***

Users of the product need to be identified to correctly handle authorisation, being the user a human, software process or a device. Anonymous users or unknown processes or devices must not be granted access or be allowed to exchange any data. Authentication can be done depending on the risk level with passwords, security tokens, digital certificates, biometrics or a mix of these. If password-based authentication is provided, the password policy rules need to be configurable to enforce strong passwords and strict security rules. Unsuccessful login attempts and unauthorised usage attempts should be logged and on the former, a login delay should be applied to hinder brute-force login attempts. When using a key-based or a certificate-based authentication, the strength of the algorithms needs to be assessed based on the risk level. After successful identification and authentication, the system needs to limit the access of the authenticated user only to the resources the user has authorisation. Authorisation can be made either on the level of users, groups or roles and it should always be made with principle of least privileges. All of the previous

should be extended to involve also the physical access. (International Electrotechnical Commission, 2019)

> ***(e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;***

Data confidentiality means protecting the data from unauthorised access. Not all data is confidential, but it's not always possible to define the confidential data in the design or development phase. Confidentiality of data-at-rest can be protected by file permissions, access control lists or data encryption. (International Telecommunication Union, 2003)

In encryption the used encryption algorithm is applied to the plaintext data resulting ciphertext that can't be read without further decrypting the data with the key used for encryption. A choice of encryption system and the key management system must be decided on-need basis. (International Organization for Standardization, 2021)

Backups are often easily forgotten as important data to be protected. Depending on the data backed up, they may contain all the same data as the running system, including possible cryptographic keys, but often with less security controls (International Electrotechnical Commission, 2019). The data-in-transit can be sent as an encrypted payload or through a secure channel, like VPN or TLS (ETSI, 2020). When utilising cryptographic means, it's essential to use strong encryption and hash algorithms that are proven to be secure. Databases should also facilitate encryption for both, the data-at-rest and in data-in-transit.

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

Integrity can be compromised by many ways and be provided by several different mechanisms. Integrity can be compromised e.g., intentionally, by accident, by hardware failure or by error in transmission. Data integrity can be protected by prevention, detection, through context or by

cryptography. Example of preventing is by denying access to a file using file permissions or using access control. Detection mechanism include for example digital signatures, message sequence numbers or data replication. Calculating a hash with an algorithm can be used to detect changes in files, configuration or software. (International Telecommunication Union, 1995)

Secure boot is a mechanism relying on hardware root of trust, that can be used to verify the integrity of the software (ETSI, 2020). A Message Authentication Code (MAC) can be used to verify that data has not been altered illicitly (International Organization for Standardization, 2011).

> ***(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);***

For the data minimisation and data retention the GDPR best practices can be followed. GDPR concerns the personal identifiable information (PII), but some of the practices can be applied also to other data. The more data is stored and processed, the more can be exposed in case of data breach. For data, especially PII, only the data that is absolutely necessary for the specified purpose should be stored and processed. When the data is not needed anymore it should be securely destroyed or anonymised. (International Organization for Standardization, 2020a)

> ***(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;***

Safeguarding availability requires a holistic approach. It can be roughly divided in securing the data, securing adequate resources and preparing for recovery. A cyberattack can hinder the functionality of a product with diverse ways. Availability alone is disturbed in denial of service (DoS) or distributed denial of service (DDoS) attack, but plethora of other incidents effect on the availability too. If for example in ransomware attack data is encrypted or it is deleted by a wiper malware, the data and the function it relies on is not available anymore.

Proper capacity management enhances availability when enough resources for data processing, memory and storage is secured. The adequacy of the transmission devices needs to be guaranteed too. Load balancing and rate limiting helps in restricting the saturation of the network. Availability can be enhanced with redundancy solutions. For example, high availability and redundancy of a product cover from losing one node, and if georedundant or backup site is used, it covers from losing an entire site. Being prepared is a key for a bad day. If data is lost, but there is a backup and the data recovery has been planned and tested, the issue can be resolved easily. Same applies in bigger scale, if a piece of hardware or an entire site is lost. (International Organization for Standardization, 2022)

(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

The product should keep from unnecessary flooding of the network. During a failure situation, like being disconnected from the network, the reconnection should be done gracefully. Methods like incremental back-off or a random delay before attempting to reconnect lowers the burden of a connecting device in case there are a substantial number of other products simultaneously recovering from the outage. (ETSI, 2020)

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

The very basics of limiting the attack surface includes disabling all the unused interfaces and ports, physical or logical. Only the necessary software services should be installed and enabled, and the access, especially external one, to these should be limited to minimum. Applications, services, processes or daemons should be running with least privileges, and where feasible, running with a user dedicated for the service. The unauthenticated disclosure of information via any interface needs to be minimised, including via the physical interface of a hardware product, like charging or debug connector. (ETSI, 2020)

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

Using the design and development best practices like defence in depth and principle of least privileges help to reduce the impact of an incident. All users need to be identified and authenticated. Sensitive or confidential data should be encrypted at-rest and in transit. Only required software needs to be installed, and relevant services be enabled. Universal or hard-coded passwords should not be used. (ETSI, 2020)

> ***(l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;***

Logging for relevant security needs to be enabled on a large scale by default. All logs should include identification of the user, timestamp, activity done, identification of the device and system where activity was done, and the network address and protocol used. This is vital information that needs to be available to really identify who did what and when. (International Organization for Standardization, 2022)

Depending on the product and system, and the identified risks in the risk assessment, the requirement for logged events vary. Inter alia, successful and failed login attempts, changes made to the configuration, audit log events and events related to backup and restore should be included. (International Electrotechnical Commission, 2019)

An important aspect to consider is for logs to be usable and trustworthy, is that they need to be immutable, and they should be stored externally from the product whenever possible. In case of an incident the product's data may be deleted or encrypted, and usually an attacker would try to hide the trails by destroying or altering the logs.

> ***(m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.***

This requirement serves especially the purpose of the late phases of the product life cycle: phase-out, retire, recycle and disposal. To prevent any compromise of information, there needs to be an

easy way to remove any data that resides in the product. A common way used for confidential data is to physically destroy the storage media on secure manner. Other means are deleting and overwriting the media on a certain technique that makes retrieving the data impossible. In case the product is being replaced with another one, there should be a procedure and instructions on how to securely transfer the data from old product to the new product. (International Organization for Standardization, 2022)

5.6.2 Vulnerability Handling Requirements

In this chapter the indented ***bolded italic*** texts are a direct quotation from the legal text of the requirements in Annex I Part II.

> ***Manufacturers of products with digital elements shall:***
>
> ***(1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;***

To effectively detect and treat vulnerabilities it is vital to know all the software components and their versions the product contains. In ICT supply chain it is challenging to know which software component are used upstream, meaning by the suppliers or their suppliers. (International Organization for Standardization, 2023b)

A Software Bill of Materials (SBOM) is an inventory of the software components including inter alia their versions and dependencies in a machine-readable format (Jump et al., 2019). Manufacturer needs to compile SBOM and based on that identify and document vulnerabilities in used software components utilising a well-known vulnerability database. As new vulnerabilities spawn daily, the document needs to be regularly updated. Common machine-readable formats include SPDX, CycloneDX and SWID (Clarc et al., 2019).

(2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

Manufacturer needs to, taking advantage of the compiled SBOM, identify the vulnerabilities and evaluate on the base of identified risks in the risk assessment the need for vulnerability treatment. Vulnerability reports can be received from internal or external sources. Manufacturer can get vulnerability updates from appropriate information resources like CERTs, cybersecurity organisations, public vulnerability databases or product vendors. For relevant vulnerabilities there needs to be a security patch created and provided to the users of the product. Proper vulnerability management processes are valuable in treating the vulnerabilities respectably. (International Organization for Standardization, 2022) Security updates should not be delivered as a part of functionality update. Though, in a complex system where many interdependencies between software components exists it may not always be feasible to separate the security updates from the functional ones.

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

Security testing needs to be made as an integral part of the software development process. Testing should include the security configurations, security functions and secure coding. Testing should be conducted in a planned way and reflect to the required security level of the product and its functionalities. Automated tools like vulnerability scanners, code analysis and binary analysis tools can be integrated to the CI/CD environment to enable continuous testing in each phase of development. Manual activities like code review, fuzzing and penetration testing can be made to complement the automated testing. (International Organization for Standardization, 2022)

(4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where

> ***manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;***

Vulnerability handling process and vulnerability disclosure are parallel processes as seen in the Figure 5. One of the last steps of the vulnerability disclosure process is sharing a public advisory. Clear and concise communication to users is vital to be able to know whether their product is vulnerable and how they can remediate. Information is important for users of the product, administrator or maintenance persons responsible for the product and managers to make decisions of updating their products. Depending on the audience, the information may need to be very technical and detailed for an administrator to know all the details, or very straightforward and unambiguous for a basic user to be told about the need to update and having clear instructions to follow. Advisory should have basic information, like identifiers for the advisory itself, for the product and for a possible CVE. Date, descriptive title and summarising overview are a must. There should also be a more detailed but not too revealing description, representation of the severity and impact of possible exploitation of the vulnerability. The remediation part should distinctly explain the steps of the corrective actions needed, being it upgrading, patching, documenting or making a configuration change. Possible workarounds should also be stated in case the final solution can't be performed for a reason or another. Advisory may contain appropriate or required references and references for the reporter or founder of the vulnerability can be expressed if practical. (International Organization for Standardization, 2020b)

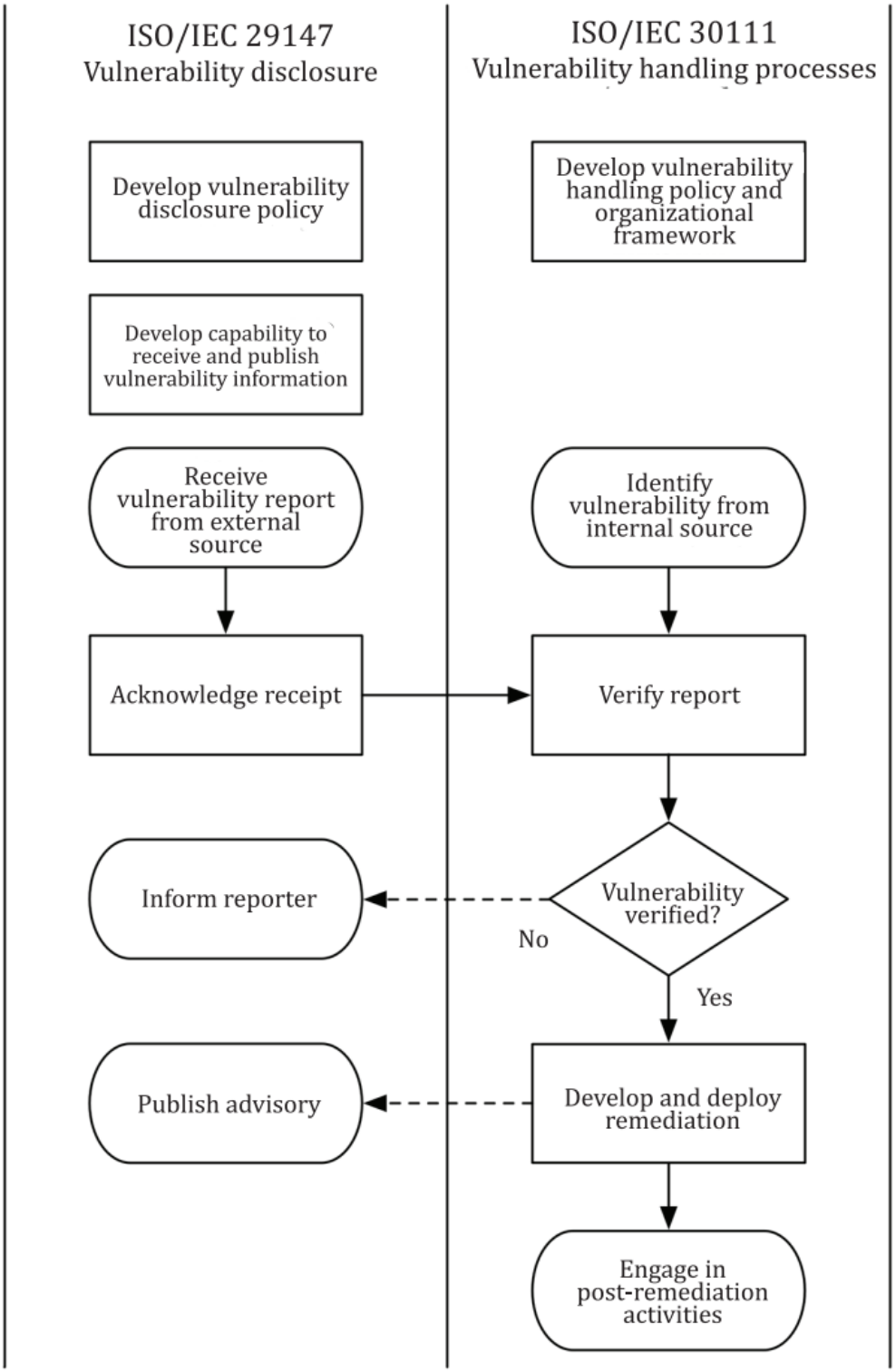


Figure 5. A diagram illustrates the relationship between vulnerability disclosure and vulnerability handling process. (International Organization for Standardization, 2020c)

(5) put in place and enforce a policy on coordinated vulnerability disclosure;

Vulnerability Disclosure (Figure 5) consists of being notified of a vulnerability and providing information for remediation. It aims for minimising risk, cost and harm caused. By getting notified of the vulnerabilities by the users of a product the manufacturer can reduce the risk fallen on users. Cost and harm are reduced when the manufacturer is able to remediate the vulnerability before it is being exploited. Manufacturer needs to set up a Coordinated Vulnerability Disclosure (CVD) policy. It is a model where the manufacturer provides a contact mechanism for users to report the vulnerabilities. It can be via a web form, e-mail, dedicated phone number or via customer service. Due to the nature of the policy, a secure communications path is a must. The policy should include instructions to reporters about the scope the policy applies, how the outcome i.e., advisory or remediation is published, and how the reporters are acclaimed. The information exchange in vulnerability disclosure may take many different forms depending on the case (Figure 6), but the main ones are the potential vulnerability report to the manufacturer and advisory from the manufacturer to users. (International Organization for Standardization, 2020b)

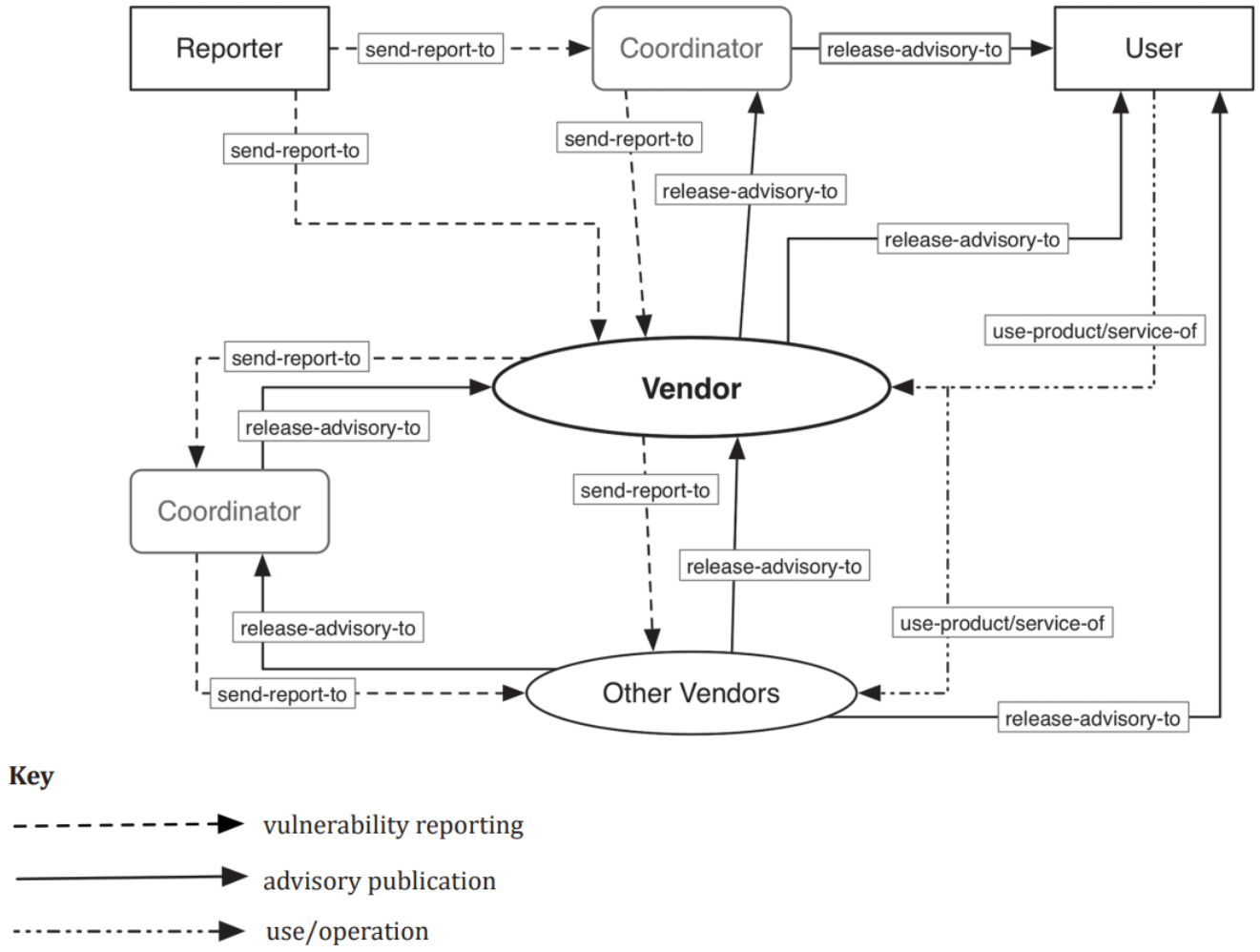


Figure 6. Depending on the case the information exchange during vulnerability disclosure process may consist of multiple parties and different steps (International Organization for Standardization, 2020b)

> ***(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;***

This requirement emphasizes the need of sharing the information of detected vulnerabilities and highlights that also third-party components fall within the requirement. As the upstream supply

chain software dependencies may contain vulnerabilities, it should get same attention as the software built in-house. The upstream software provider should provide vulnerability information and remediation instructions for their software. (International Organization for Standardization, 2020c) Requirement also specifies the need for providing a contact address for vulnerability reporting. The vulnerability requirement 5, on the CVD policy, properly implemented and applied covers also this requirement.

> ***(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;***

When the vulnerabilities are corrected the software should go through a testing process. The updates should be packaged and deployed securely. Code signing or file hashes can be used to verify the integrity and authenticity of the update. Users of the product needs to be informed about the available update.

The update needs to be made available and delivered secure manner through an official repository, update server or similar distribution channel together with instructions to apply the update. Authenticity and integrity checks and version checking can be utilised to prevent a malicious actor infringing the update system. (ETSI, 2020)

> ***(8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.***

Users of the product needs to be informed according to CVD policy through advisory. Communication can happen e.g., via company website, mailing list or where available, through an automated update system. In case of a high-risk vulnerability or already actively exploited vulnerability all required mitigation actions or workarounds need to be informed to customers before remediation is available. Manufacturer can also, depending on the nature and criticality of found vulnerability,

send an advisory before remediation is available as a warning for users to be prepared for immediate actions when the remediation is published. (International Organization for Standardization, 2020b)

A remediation can be inter alia, a security patch, configuration change or an upgrade. Releasing security updates needs to be done according to vulnerability handling process. (International Organization for Standardization, 2020c)

5.7 Documentation Requirements

Apart from the technical requirements, the CRA induces also quite a burden for documentation. The security risk assessment and conformity assessment were already handled in the chapter 5.4 and chapter 5.5 respectively, but there's more. In addition, the manufacturer needs to provide information and instructions to users, draw up the technical documentation and the EU declaration of conformity. The documentation requirements are somewhat interconnected and simultaneous e.g., the information and instructions to users, the risk assessment and a copy of the EU declaration of conformity needs to be included in the technical documentation. The requirements for documenting are pretty straightforward, and they are included in the appendices of this thesis.

5.7.1 Information and Instructions to Users

The CRA Annex II defines the bare minimum of the information and instructions the manufacturer needs to provide to the users. Either on paper or electronic format, on "language which can be easily understood", the manufacturer needs to instruct how to securely install, operate and use the product. The instructions need to be available at least 10 years from placing the product on the market. The information part includes e.g., the information of the manufacturer itself including a single point of contact for coordinated vulnerability disclosure policy, identification information on the product and its intended use. The CRA Annex II can be found from the appendix 2.

5.7.2 Technical Documentation

The technical documentation is the largest required document in the CRA and is a sort of collection of all the required documents. The cybersecurity risk assessment, the information and instructions to users, and a copy of the EU declaration of conformity do need to be included in the technical documentation. It needs to include all of the relevant documents, details and data, that ensures the compliance with the CRA requirements. In addition, if there are essential cybersecurity requirements that the manufacturer sees as not applicable for the product, it needs to be clearly justified in the technical documentation. The CRA Annex VII, in appendix 7, sets the minimum requirements for the technical documentation. The manufacturer needs to describe the product in question, including its intended purpose and the software version. It also requires describing the processes of the entire manufacturing cycle added with the vulnerability handling process. The CRA Article 13 rules that the technical documentation (as well as the EU declaration of conformity) has to be available for the market surveillance authorities for 10 years after placing the product on the market, or more, if the support period is longer.

5.7.3 EU Declaration of Conformity and Affixing the CE Marking

When all the CRA requirements are carried out, the manufacturer needs to draw up the EU declaration of conformity, where the manufacturer states that it fulfils all the applicable cybersecurity requirements and takes the responsibility of compliance with the CRA. The structure of the EU declaration of conformity is expressed in the CRA Annex V (appendix 5) and needs to contain the elements according to the conformity assessment procedure used requires. A manufacturer can also choose a simplified EU declaration of conformity, which can be found from the CRA Annex VI (appendix 6). It is required to have an Internet address for the actual EU declaration of conformity. Drawing up the EU declaration of conformity is the last step before the manufacturer can obtain the CE marking and affix it to its product.

6 The CRA Tool

The third research question of this thesis is *What kind of tool could be developed to help manufacturers in the CRA compliance process?* The tool development was encouraged by the commissioner

of the thesis, and it's planned to be used in the compliance process of the commissioning company. This chapter will introduce the CRA tool that has been developed as a part of this thesis. The chapter starts with the planning phase and continues with explaining the design of the tool before summarising the tool and its development process.

6.1 Planning of the CRA Tool

The third research question of this thesis is to investigate what kind of tool would be beneficial to manufacturers in the CRA compliance process, and that could be developed within boundaries of the thesis work. The tool creation was also suggested by the commissioner of the thesis. As the EU harmonised standards are being developed by the ESO's, it wasn't seen worthwhile to provide any best estimation of means to achieve compliance with the CRA, because it can't be reliably done before the standards are ready. Instead, the focus was on the compliance process itself. The planning of the tool started by investigating of some pain points in such processes generally, and four main issues were discovered to be taken into account when developing the tool: not everybody is familiar with the CRA; big tasks need collaboration of several stakeholders; the status of the process needs to be easily followed; and the information is often fragmented in different places.

During the process of absorbing the theoretical basis for this study it became very evident that legal documents are not self-explanatory and that reading them may prove to be a tedious task for people used to technical documents. The tool should be developed to be intuitive and have instructions to user on how the tool should be used and what is required from the CRA point of view. The CRA compliance process is expected to involve many stakeholders from distinct functions, like architects, product owners, project managers, quality team, documentation department, product compliance department, etc. In that sense, the tool should be able to be used in collaboration with all the required stakeholders. The demanding task of meeting all the requirements of the CRA will most likely take a great amount of time, and the process needs to be monitored carefully. Since time spent in reporting the status is often taken away from the task at hand, the tool should provide an easy way for anyone to check the current status. Companies often have a plethora of tools and different file sharing or storing systems, and the information easily gets fragmented between these. Finding the needed information is frustrating and wastes time, so the tool should ensure the resulted information is stored centrally or can be easily located.

6.2 Design and Development of the CRA Tool

Inspired by the Finnish Traficom's Kybermittari (National Cyber Security Centre Finland, 2023), it was decided to develop the tool on top of Microsoft Excel. Excel can be used in collaboration if using Microsoft 365, but without it, the collaboration is difficult. This is why the development of the tool was striving to be compatible also with Google Sheets.

As to stay within the indicative workload of the thesis, there was a need to carefully consider what will be included in the version that will be a part of the thesis, and how the tool would be implemented. The usability and ease of use were seen imperative, but the appearance can be improved later if seen necessary. The development of the tool will continue based on the feedback from the users, and for example the publishing of the EU harmonised standards will trigger a need for further development of the tool.

6.2.1 Structure

The tool is divided between different sheets, each requirement area of the CRA having its own sheet. The sheets are in sequence they are logical to be implemented, but for example the vulnerability handling requirements may be taken care of before cybersecurity requirements. The order in the tool is the following:

- Categorisation of the product
- Cybersecurity risk assessment
- Cybersecurity requirements
- Vulnerability handling requirements
- Information and instructions to users
- Technical documentation
- Conformity Assessment
- Declaration of conformity
- Affixing the CE marking

The selections of the compliance status of requirements are made from the drop-down menus. The selection will update the table on the status sheet. Each sheet has a field for the assessment responsibility to facilitate the manufacturer internal communication. It is easier to know whom to

contact if there is unclarity or any questions regarding the selections made in the tool. The responsibility of the task is also updated on the status page.

Following the Status

For any project the status follow-up is a vital task. On the opening sheet of the tool, there is a simple table showing the status of the tasks (Figure 7). It shows the specific product under assessment, gathers the selections from other sheets, and summarises which tasks have been done and who is the responsible person for the particular assessment. To increase the clarity of the status, the completed tasks will appear in green background and tasks that still need to be done are on red background. The status colour is implemented with the conditional formatting.

CRA-tool v0.4

This tool is created to help manufacturers in achieving compliancy with the Cyber Resilience Act, CRA.
The tool can be used to track the status of the CRA compliance process.
Please check the instructions for the tool from the "Instructions" tab.

The reporting obligation (not included in the tool) applies from **11.9.2026**.
The rest of the requirements in this tool apply from **11.12.2027**.

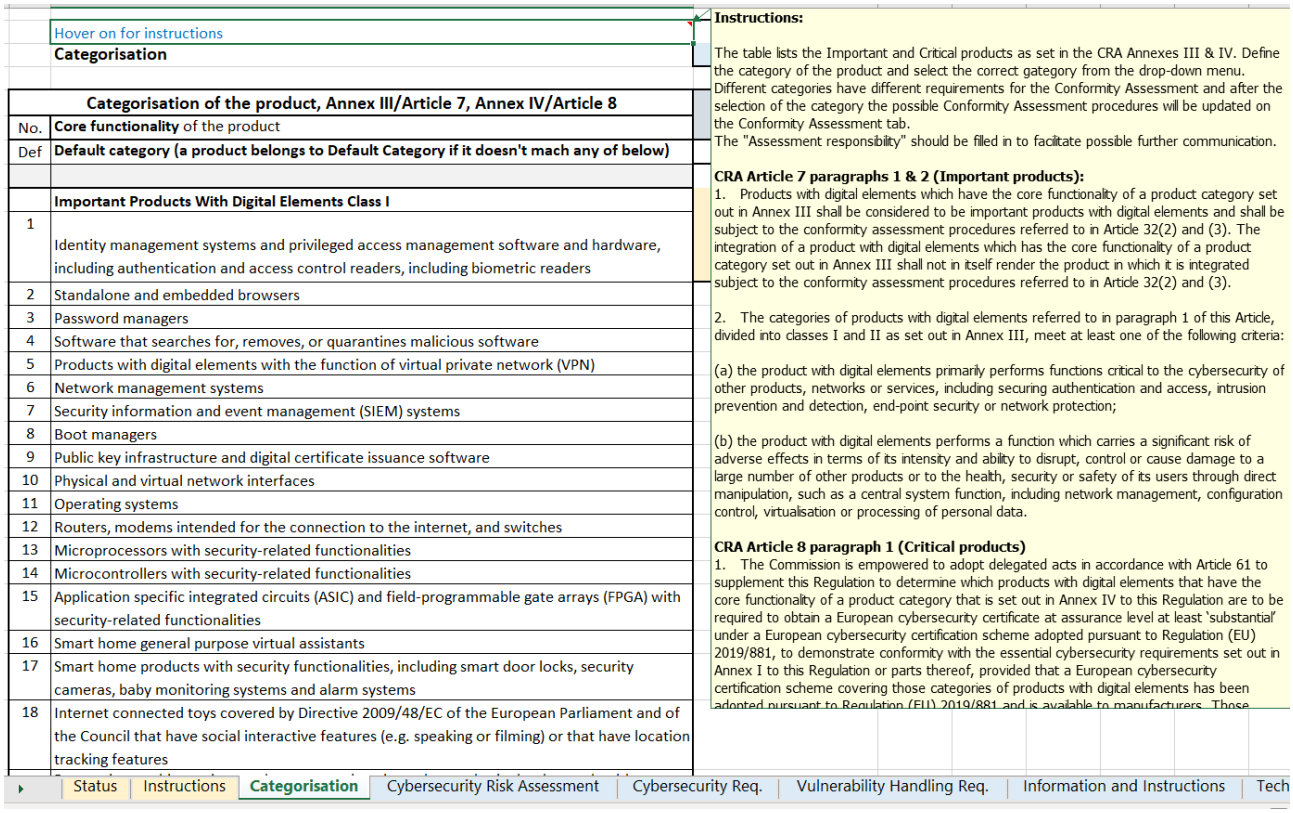
Name or identifier of the product (for internal use):		**PasswordSmith v2.8**			
	Assessment responsibility				
Status of readiness		Fully	Partially	No	N/A
Categorisation	John Smith	On Categorisation tab you have selected the product belonging to Important Class I category.			
Cybersecurity Risk Assessment	Jane Smith	Cybersecurity Risk Assessment has been done and link to report is provided			
Cybersecurity Req.	John Smith	11/14	1/14	1/14	1/14
Vulnerability Handling Req.	Jane Smith	8/8	0/8	0/8	0/8
Information and Instructions	not defined	0/14	0/14	14/14	0/14
Technical Documentation	not defined	0/13	0/13	13/13	0/13
Conformity Assessment	not defined	No Conformity Assessment done			
Declaration of Conformity	not defined	0/8	0/8	8/8	0/8
CE marking	not defined	No CE marking affixed			

Figure 7. The progress can be quickly seen from the status sheet. An artificial product is used in the example.

Instructions

For the ease of use of the tool and to avoid the need of users of the tool to constantly go back to the CRA legal text, the tool includes instructions. Instructions-sheet provides general instructions for the tool, and on each sheet, there's a separate "Hover on for instructions" cell, that provides guidance on the current sheet (Figure 8). It provides instructions for the use of the tool and includes the parts of the CRA text related to the requirement in question. To avoid filling the sheets

too much, the instructions are implemented by adding them as a comment and will appear only when hovered on the cell or toggling “Show/Hide Comments” setting.



Hover on for instructions

Categorisation

	Categorisation of the product, Annex III/Article 7, Annex IV/Article 8
No.	**Core functionality** of the product
Def	**Default category (a product belongs to Default Category if it doesn't mach any of below)**
	Important Products With Digital Elements Class I
1	Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers
2	Standalone and embedded browsers
3	Password managers
4	Software that searches for, removes, or quarantines malicious software
5	Products with digital elements with the function of virtual private network (VPN)
6	Network management systems
7	Security information and event management (SIEM) systems
8	Boot managers
9	Public key infrastructure and digital certificate issuance software
10	Physical and virtual network interfaces
11	Operating systems
12	Routers, modems intended for the connection to the internet, and switches
13	Microprocessors with security-related functionalities
14	Microcontrollers with security-related functionalities
15	Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities
16	Smart home general purpose virtual assistants
17	Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems
18	Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council that have social interactive features (e.g. speaking or filming) or that have location tracking features

Instructions:

The table lists the Important and Critical products as set in the CRA Annexes III & IV. Define the category of the product and select the correct gategory from the drop-down menu. Different categories have different requirements for the Conformity Assessment and after the selection of the category the possible Conformity Assessment procedures will be updated on the Conformity Assessment tab.
The "Assessment responsibility" should be filled in to facilitate possible further communication.

CRA Article 7 paragraphs 1 & 2 (Important products):
1. Products with digital elements which have the core functionality of a product category set out in Annex III shall be considered to be important products with digital elements and shall be subject to the conformity assessment procedures referred to in Article 32(2) and (3). The integration of a product with digital elements which has the core functionality of a product category set out in Annex III shall not in itself render the product in which it is integrated subject to the conformity assessment procedures referred to in Article 32(2) and (3).

2. The categories of products with digital elements referred to in paragraph 1 of this Article, divided into classes I and II as set out in Annex III, meet at least one of the following criteria:

(a) the product with digital elements primarily performs functions critical to the cybersecurity of other products, networks or services, including securing authentication and access, intrusion prevention and detection, end-point security or network protection;

(b) the product with digital elements performs a function which carries a significant risk of adverse effects in terms of its intensity and ability to disrupt, control or cause damage to a large number of other products or to the health, security or safety of its users through direct manipulation, such as a central system function, including network management, configuration control, virtualisation or processing of personal data.

CRA Article 8 paragraph 1 (Critical products)
1. The Commission is empowered to adopt delegated acts in accordance with Article 61 to supplement this Regulation to determine which products with digital elements that have the core functionality of a product category that is set out in Annex IV to this Regulation are to be required to obtain a European cybersecurity certificate at assurance level at least 'substantial' under a European cybersecurity certification scheme adopted pursuant to Regulation (EU) 2019/881, to demonstrate conformity with the essential cybersecurity requirements set out in Annex I to this Regulation or parts thereof, provided that a European cybersecurity certification scheme covering those categories of products with digital elements has been adopted pursuant to Regulation (EU) 2019/881 and is available to manufacturers. Those

Status | Instructions | Categorisation | Cybersecurity Risk Assessment | Cybersecurity Req. | Vulnerability Handling Req. | Information and Instructions | Tech

Figure 8. Each sheet provides instructions related to the requirements and the use of the tool.

The CRA Requirements

As the possible conformity assessment depends on the selected category (Figure 9), the conformity assessment option changes when the category is changed (Figure 10).

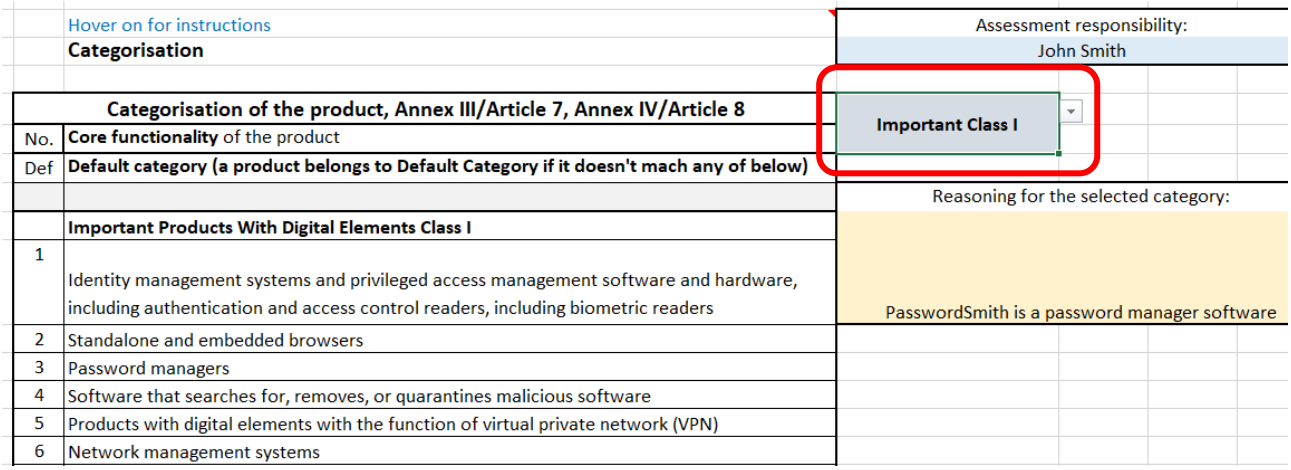


Figure 9. Categories are in the tool as a table and correct category is selected from the drop-down menu.

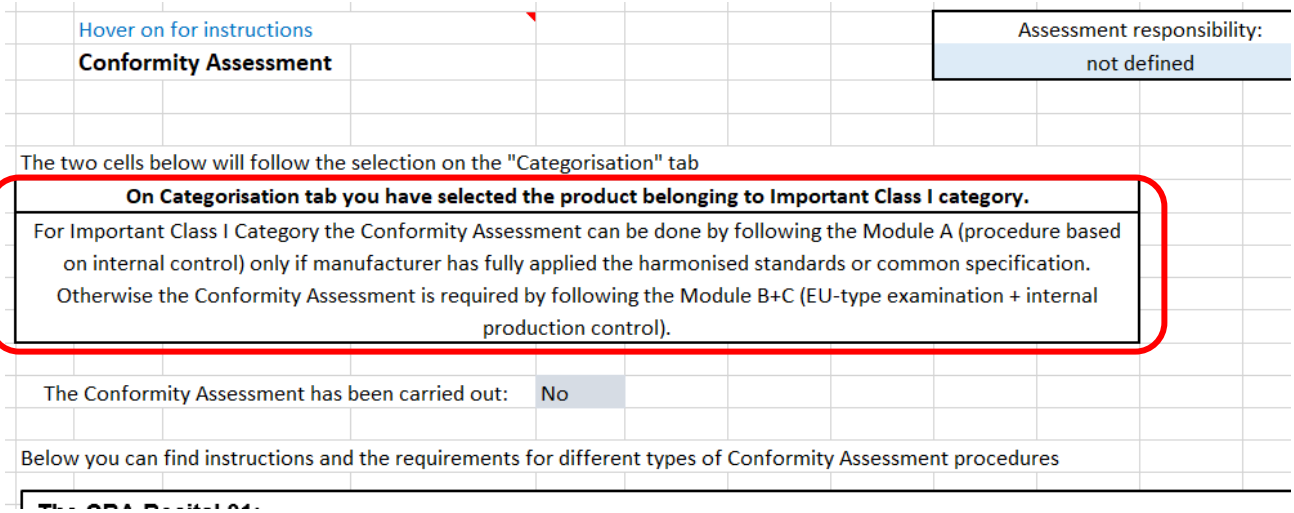


Figure 10. The conformity assessment sheet will show the minimum applicable procedure corresponding with the selected product category.

The cybersecurity risk assessment is a significant part of the CRA. There is a great deal of different means to conduct the risk assessment, and each company can follow their selected methodology and tools in conducting the assessment. The CRA tool doesn't take a stand on the way the risk assessment is done. The Cybersecurity Risk Assessment sheet has the CRA requirements, instructions for the tool and links to well-known resources of different means to conduct the assessment (Figure 11). The user can select whether the assessment has been done, and if the assessment report is inserted into or linked in the tool.

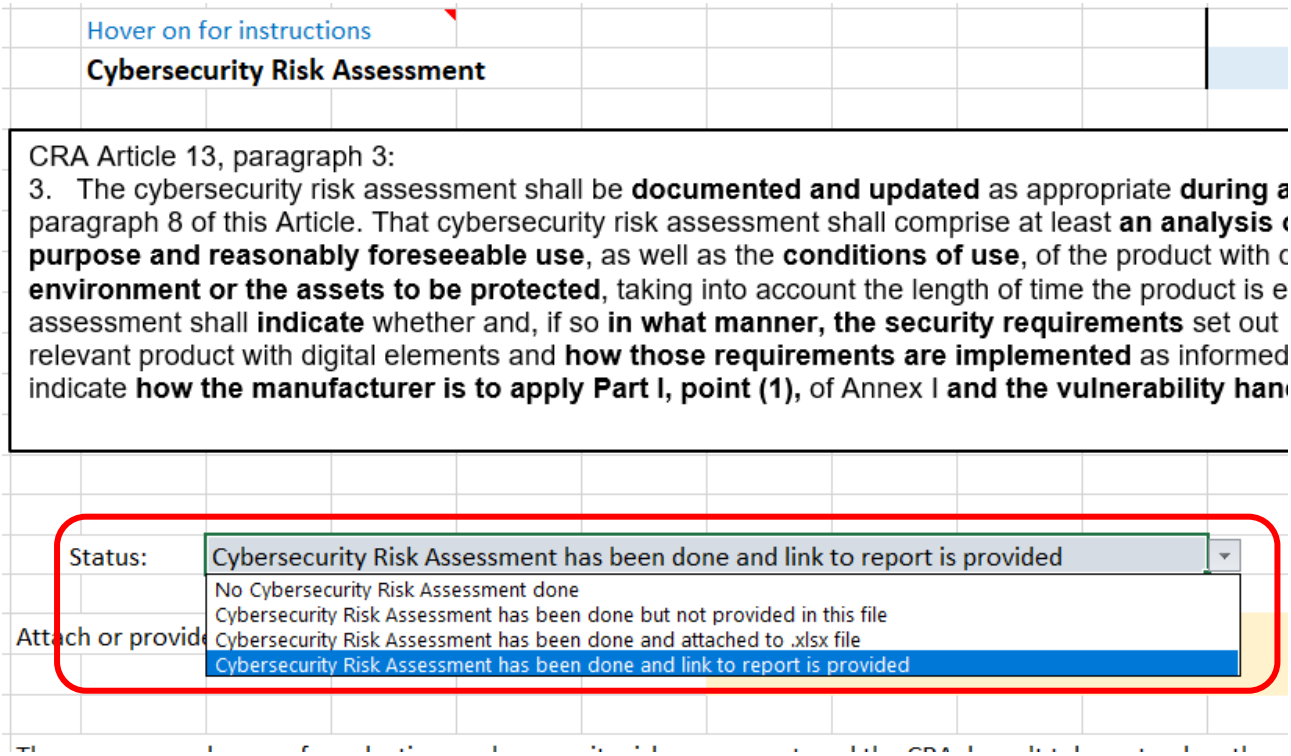
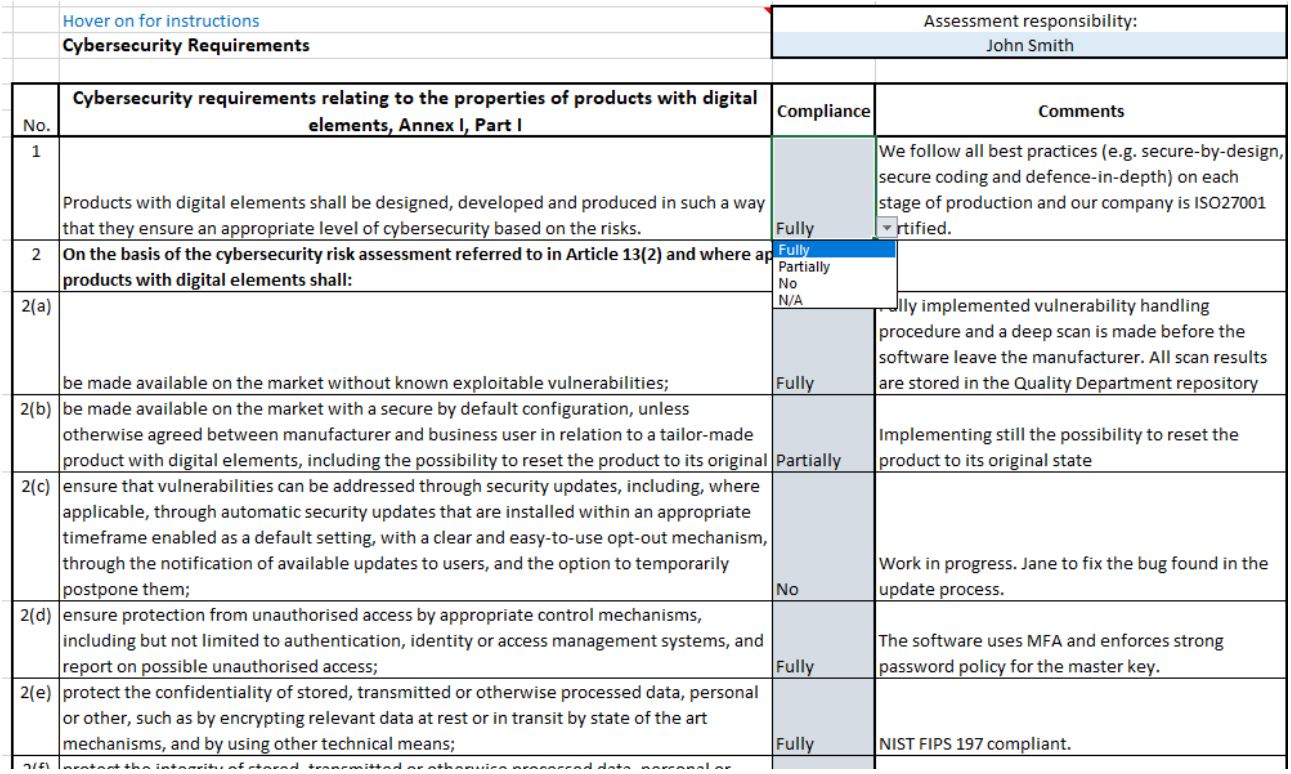


Figure 11. The way the cybersecurity risk assessment is conducted is not relevant in the tool. It only tracks if it has been conducted and whether the assessment report is attached or linked in the tool.

Requirements of the CRA for cybersecurity, vulnerability handling, information & instructions to the users, technical documentation and declaration of conformity are presented in tables on separate sheets, where the compliance status of each requirement is selected from the drop-down menus (Figure 12) on the respective sheet. As the CRA will require supporting evidence when assessing the sufficiency of the solutions for technical design and development or for vulnerability handling processes, the tool has a comments field where evidence, or link to evidence, can be provided. Reasoning for “not applicable” can be expressed also in the comments field.



	Hover on for instructions	Assessment responsibility:
	Cybersecurity Requirements	John Smith

No.	Cybersecurity requirements relating to the properties of products with digital elements, Annex I, Part I	Compliance	Comments
1	Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.	Fully	We follow all best practices (e.g. secure-by-design, secure coding and defence-in-depth) on each stage of production and our company is ISO27001 rtified.
2	**On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where ap products with digital elements shall:**	Fully Partially No N/A	
2(a)	be made available on the market without known exploitable vulnerabilities;	Fully	lly implemented vulnerability handling procedure and a deep scan is made before the software leave the manufacturer. All scan results are stored in the Quality Department repository
2(b)	be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original	Partially	Implementing still the possibility to reset the product to its original state
2(c)	ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;	No	Work in progress. Jane to fix the bug found in the update process.
2(d)	ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;	Fully	The software uses MFA and enforces strong password policy for the master key.
2(e)	protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;	Fully	NIST FIPS 197 compliant.
2(f)	protect the integrity of stored, transmitted or otherwise processed data, personal or		

Figure 12. The compliance status of the requirement is selected individually and comments field can be used to note the evidence or reasoning.

The tool has instructions for the conformity assessment and affixing the CE marking. As with other sheets, the current status is selected from the drop-down menu, and it updates to the status sheet.

6.3 Summary of the CRA Tool

The tool was presented to stakeholders of the commissioner, and it received a warm welcome. The functionality of the tool has been tested both with Microsoft Excel and Google Sheets. As not all functions of Excel are supported by Google Sheets, it was needed to adjust some of them. For example, the categorisation of the product was originally implemented with radio buttons, but they did not work in Sheets, and thus it was changed to a drop-down menu. The text box functionality is neither fully compatible with the two spreadsheet applications, and the format of the text box shown in Sheets may sometimes appear different than in Excel. Some annoyance may be caused also as the comments in Google Sheets appear differently than in Excel. Where in Excel the

size and position of the comments field can be adjusted, in Sheets it appears as quite a small window, where the size and location can't be controlled. Only seen drawback of Excel compared to Google Sheets is that in Sheets the small arrow in drop-down menus is always visible, when in Excel it only appears when the cell is selected. Visibility of the small arrow should make it obvious for anyone using the tool that the cell contains a selection by a drop-down menu.

The planned objectives of the tool were all well met. As the status page updates automatically based on the selections in the other sheets, it makes the progress follow-up is easy and clear. The instructions for the tool and for the CRA facilitate the use of the tool and the overall compliance process. The tool can be used in collaboration either through Google Sheets or Microsoft 365, but the latter has not been tested. The users have freedom either to attach any external documents to the Excel document or link them in the tool. As the documentation required by the CRA is not static by nature, but e.g., the cybersecurity risk assessment needs to be updated as appropriate, it is expected that the users will link any evidence documentation rather than insert the files directly. Although, both ways are supported.

The tool is not combat proven yet. It has been agreed with the commissioner, that the development of the tool continues, based on the feedback when the tool will be taken into use. Also, the development of the EU harmonised standards may bring a need for further development of the tool. The tool is planned to be shared in the commissioning company's GitHub (Airbus CyberSecurity, 2025).

7 Reflections on the CRA

The CRA is a great piece of legislation. It is my honest opinion, that forcing the cybersecurity through the regulation is a must. There has been cybercrime for so long already, and have the manufacturers made their best to protect users from it? Some for sure have, but definitely there's a huge part that has not. It saves costs when you don't have to invest in developing a secure product, and that distorts the competition between the companies. I think complying with the CRA requirements will not be a massive task for companies who have tried their best within the cybersecurity already before the coercive regulation. But hopefully this regulation eliminates the

manufacturers who have totally neglected the cybersecurity and only concentrated on quick wins by quick release of products.

7.1 More Precise Definitions Required

Even if the idea behind the CRA is brilliant, there are some needs of honing it. Working on this thesis it became clear that the law is complex. Part of the complexity becomes from the ambiguity of the legal text, like the contradiction of Articles 6 and 13, as explained earlier in the chapter 5.3. It might be that a legally trained people would find the text less ambiguous than an engineer with technical background, and for this reason the text requires explaining from an EU body, like the Commission or ENISA.

ECSO (European Cyber Security Organisation, 2024) conducted a survey in autumn of 2023, mapping the potential challenges that companies see in implementing the CRA requirements. Even if the survey is based on the older CRA proposal text, the results speak for themselves. Due to lack of clear product taxonomy organisations struggle on identifying in which of the categories their products belong to. Similarly, clarification is needed in conducting the cybersecurity risk assessment or the conformity assessment. Without clear and unified approach, the results of different assessors might be very dissimilar.

Conducting a cybersecurity risk analysis is a prerequisite for meeting the other CRA requirements. The CRA applies a risk-based approach, but in the regulation, there is no pointer on the acceptable risk appetite. The Annex I, listing the essential cybersecurity requirements, says "*ensure an appropriate level of cybersecurity based on the risks*". Who is to define what is "*appropriate level*"? What is the risk level that can be tolerated? Is it the manufacturer or the end user who should define the accepted risk level? Without further directions from the lawmakers, it might eventually be a court of justice that decides it.

7.2 EU Harmonised Standards

The ECSO survey lists several concerns about lack of supporting documentation, like guidelines or checklists. One important concern, that I've stressed out in my work, the lack of harmonised

standards, was also raised by the survey respondents. The date when the EU harmonised standards for the CRA is still unclear, but the signs from the draft CRA standardisation request are alarming (European Commission, 2024a). DIGITALEUROPE demands realistic timelines for the harmonised standards be finished. In the current draft standardisation request the deadline for part of the harmonised standards is set to end of October 2027, which is around 40 days before manufacturers should be compliant with the regulation requirements. Without the EU harmonised standards all products belonging to Important Class I needs to involve a third-party assessor in the conformity assessment, which for sure will jam the notified bodies making the EU-type examinations. (DIGITALEUROPE, 2024)

The standards to come may not be the only thing that will change in the near future. As the CRA text depicts, the Commission has reserved right to make some changes or amendments in the CRA, and it's possible that some changes will be inherited from the Radio Equipment Directive (Sahm, 2024).

7.3 Time Constraints

The CRA Annex I states: "*On the basis of the cybersecurity risk assessment … and where applicable, products … shall be made available on the market without known exploitable vulnerabilities*", which might be challenging task for some manufacturers. Developing a new software for a big IT system, especially for critical systems, is often time-consuming task, and requires versatile and thorough testing that may take weeks or even months. With the speed of new vulnerabilities are published, there will likely be new vulnerabilities found also during the time range of testing, and in the worst case the found vulnerabilities are exploitable. Fixing them would require another testing round, and so we have a vicious circle that may never end.

If a manufacturer has planned a software release cycle, how critical the vulnerability needs to be so that the manufacturer needs to steer development resources from its original release plan to produce a separate fix for the found vulnerability? What if there is a low severity vulnerability with a known exploitation, and few critical vulnerabilities, where there are no known exploits available? Wouldn't it be better to direct all the resources in fixing the critical bugs before exploit is made? I certainly hope the rules wouldn't be carved into stone, and manufacturers could use common

sense in directing the resources to holistically improve the security of the products instead of only concentrating in complying with each requirement of the CRA. Actions for cybersecurity should be done to secure the product rather than to comply with the regulation on tick-a-box basis.

There's ambiguity also in the terms "without delay" and "without undue delay". For example, the Annex I states, "*address and remediate vulnerabilities without delay*". What kind of time frame is accepted if something needs to be done "*without delay"*? If we're talking about fixing vulnerabilities, it requires proper screening of the vulnerability, implementing the fix and testing it. How thorough testing can, or should be conducted, if the remediation needs to be done "*without delay"*?

7.4 Will It Work?

Kazakova (2024) brings up an interesting aspect in her article. The CRA has great intentions, and if everything goes as it has been designed, the outcome will have a great positive effect on the global cybersecurity. What about if it doesn't work as planned? What if other nations are not willing to obey the rules set by the EU? The CRA has a *requirement* to report on the vulnerabilities to ENISA and national authorities, but it's not said that non-EU countries will obey this rule. And despite of good will of the CRA, some less friendly state may set up their own extraterritorial laws with less good intentions. It remains to be seen how well the anticipated outcomes will realise in practice when the requirements fully step in force in December 2027. I will remain positive that cybersecurity globally will be enhanced by the CRA, but I'm not expecting it to be a magic bullet to solve all the problems.

8 Conclusion

The number of Internet-connected devices has been rising rapidly mainly due to upsurge of IoT-devices. In the same proportion the cybercrime has increased and causes globally losses of several trillion U.S. dollars yearly. The European Union has been fighting against cybercrime by legislation. Adaptation to laws is required when the technology evolves.

The Cyber Resilience Act (CRA) is a new European Union regulation, first proposed in 2021, and entered into force in December 2024. It aims to improve the cybersecurity of the products placed on the market in EU area and thus reducing cybercrime. Product manufacturers of any software or hardware product with remote data processing capabilities need to comply with the CRA requirements if they are providing their products within EU markets.

This thesis aimed in helping the product manufacturers in their CRA compliance process. It first provides the general information on the CRA, then researches the requirements the CRA sets and investigates what kind of tool would benefit manufacturers in the CRA compliance process and could be developed as a part of the thesis.

8.1 Cybersecurity Requirements in the CRA

The CRA has a risk-based approach, and the products are categorised in four different categories (default, Important Class I & II, Critical) based on the risk they may pose. Depending on the category the product falls in, the EU conformity assessment procedure may need a third-party assessment. Manufacturers need to conduct a cybersecurity risk assessment on their products, and based on the risks observed, treat the risks to fulfil the requirements. The CRA has requirements related to manufacturers' processes, product technical properties, vulnerability handling and documentation.

The EU harmonised standards are in the making by the European Standardisation Organisations. The harmonised standards will eventually indicate which means are adequate to comply with the requirements, and following those standards eliminates the need for third-party conformity assessment for Important Class I products. The exact schedule for standards to be finished is uncertain, but there are signs that it might be very close to application date of the CRA requirements.

The CRA requires products to be designed, developed and produced according to the requirements set in Part I of Annex I. The requirements range from products to be exploitable vulnerability free to protecting unauthorised access and limiting the attack surface. Manufacturers need to build up a Software Bill of Materials (SBOM) and set up vulnerability management process to ef-

fectively detect and correct any vulnerabilities in their products. The requirements of the documentation, like information and instructions to users, technical documentation and EU declaration of conformity are clearly defined in the CRA annexes.

8.2 Tool for Manufacturers

Research was conducted to find out what kind of tool would help the manufacturers in the compliance process and be created as a part of the thesis. Four key issues were identified in similar processes and projected in the tool creation goals: general lack of understanding the CRA, need of collaboration in the process, possibility to easily follow the process status, and concentrating all required information in one place.

The tool was created with Microsoft Excel, keeping in mind the compatibility with Google Sheets to facilitate collaboration if Microsoft 365 was not available for the users. The progress of the compliance process can be followed from the tool's intuitive status sheet that updates automatically based on the progress on other sheets of the tool. The tool has instructions for the use of the tool and for the specific part of the CRA in each sheet. The requirement compliance level is selected from drop-down menus on each sheet, and assessment responsibility filled in to simplify the internal communication for any parts of the assessment. The tool has a field for comments to further clarify the justification of selected compliance level and the related documents, like the cybersecurity risk assessment, can be inserted as a file to the Excel document or a link to supporting document can be provided. The tool is planned to be shared in the commissioning company's GitHub (Airbus CyberSecurity, 2025).

9 Discussion

The aim of the thesis was to clarify the final version of the CRA document and to help the product manufacturers in the CRA compliance process. The first research question was ***What is the CRA?*** It gives general idea on what the new regulation is, what's its purpose and whom does it concern. The second research question was ***What are the cybersecurity requirements in the CRA?*** It gathered and explained the requirements the regulation sets for the manufacturers. The third research question was ***What kind of tool could be developed to help manufacturers in the CRA compliance***

process? It researched what kind of a tool would benefit the manufacturers in the CRA compliance process, and that could be developed within the thesis.

9.1 What is the CRA?

The review of existing EU cybersecurity related regulation shows that the legislation has had to evolve along with the technical development. Many of the new legislation is based on the existing laws but adapting to a changed situation. The CRA is the first ever EU-wide regulation of the kind and contains new parts, but the foundation of the regulation lays on the existing legislation and EU cybersecurity strategy. The fight against the cybercrime has required to place the responsibility of security upstream to the product manufacturers. CRA will greatly append the NIS2 directive that already dictates cybersecurity rules for operators and service providers by involving manufacturers in the same security bee. Chapter 4.1 answers to the first research question, ***What is the CRA?*** It gives a good overview on what the CRA is: a new EU-wide cybersecurity regulation for product manufacturers, that sets a plethora of different requirements both from technical and documentation aspect, and is aimed to combat against cybercrime by making the products more secure by default. Non-compliance may be heavily penalised if the requirements are not met. The thesis differs from majority of the analyses made about the CRA by analysing the final version of the CRA regulation instead of earlier drafts.

9.2 What are the cybersecurity requirements in the CRA?

The difficulty in the CRA is its ambiguity. The rules are binding, they concern vast number of manufacturers globally and non-compliance with the requirements is heavily sanctioned, but the clear instructions how to be fully compliant are missing. The CRA legal text structure doesn't gather all the requirements in a concise manner or in logical order, but the requirements are spread in different chapters and annexes. The lack of the EU harmonised standards makes it still impossible to know whether following market de facto standards is a golden ticket to compliance, but at least it can be recommended; with or without need to the CRA compliance. The sub-chapters of chapter 5 answers for the second research question, ***What are the cybersecurity requirements in the CRA?*** It gathers all the requirements the CRA sets, be they technical, documentational or process related. Essential cybersecurity requirements under the chapter 5.6 are sorted out on a high level, but a comprehensive analysis and solution is necessary for each specific product separately. The

EU harmonised standards and the related application guides are expected to help, but the current schedule for them to be finished seems to be too late.

From the documentation requirements the cybersecurity risk assessment is expected to cause the worst headache. The assessment needs to be conducted to each product and updated as the vulnerability landscape or other factors in the assessment changes. There is not much help for the risk assessment from the regulation. Without further guidance on the risk assessment, it can't be expected that the results of the assessment between assessors would be coherent, which is normally expected in any risk assessment.

9.3 What kind of tool could be developed to help manufacturers in the CRA compliance process?

The CRA tool developed as a part of this thesis can help manufacturers in the CRA compliance process. Chapter 5 presents the developed tool.to answer the third research question, ***What kind of tool could be developed to help manufacturers in the CRA compliance process?*** The CRA tool will help users in perceiving the entire process, and guide in proceeding with the task. It will also help in following the status of the progress and to better plan the use of resources. It is a light and intuitive tool with good instructions, so it should be easy to start using the tool. The tool can be used simultaneously by several individual facilitating the collaboration in the compliance process, and the results of the assessment are gathered in the tool itself or linked to within the tool. Development of the tool needs to be continued after the thesis based on the feedback from the users and according to the changes or amendments to the regulation.

9.4 Research goals and results

The research goals were met as explained above. Reader should get quite clear view of the CRA and its requirements for product manufacturers. The CRA tool is planned to be used in the CRA compliance process of the commissioning company. There are also plans to present the tool in a certain Centre of Excellence (CoE) in Cybersecurity and propose its wider use and further development in cooperation with the CoE. The tool is planned to be shared in the commissioning company's GitHub (Airbus CyberSecurity, 2025).

The results of the thesis are expected to be reliable. Reputable sources were preferred for the information gathering and legal texts are directly from the European Union sources. It is always possible that the research has some errors. Reliability could have been enhanced by involving a person who is familiar with the law. Other enhancement would have been to collaborate with someone familiar with the CRA itself to discuss and ponder the legal text. The outcome of the tool could have been improved by having a test group using the tool. It was not possible during the research, but the development of the tool will continue after the thesis. One development area of the tool would be the translation of the tool, as it seems that certain countries prefer local language instead of English. Further development could include helping manufacturers in their task of conducting the cybersecurity risk assessment and conformity assessment for the CRA, which both are substantial tasks. Either clear instructions or a tool could benefit manufacturers in the assessments.

9.5 Author's recommendation

The author recommends starting preparations of the compliance process immediately. As the reporting obligation of actively exploited vulnerabilities and severe incidents starts already in September 2026, it would be logically the first task to take care of. At the same time the assets, i.e., the manufactured products, should be collected to make sure each product will go through the process. The categorisation of the products in an early phase will indicate whether the manufacturer needs to involve a third-party assessor for the conformity assessment or if that task can be handled in-house. If the manufacturer doesn't yet have vulnerability handling process in place, the ISO/IEC 30111 (International Organization for Standardization, 2020c) will be helpful in setting it up. As for Coordinated Vulnerability Disclosure process, the ISO/IEC 29147 (International Organization for Standardization, 2020b) standard can be utilised. As stated by ETSI (2020), there is not yet an approach that would reliably give consistent results between different assessors conducting the cybersecurity risk assessment. Thus, the recommendation is either to continue with the method the manufacturer has been using, or lean on ISO/IEC 27000-series, ISO/IEC 31000-series or NIST Cybersecurity Framework. ETSI document can also be used for looking for alternatives. Even if the harmonised standards are not ready, manufacturers are recommended to start to enhance their security posture by taking security by design principles in use in their manufacturing processes and make sure secure coding practices are followed in the software development.

References

Airbus CyberSecurity. (2025). *Airbus CyberSecurity*. GitHub. https://github.com/airbus-cyber

American Psychological Association. (n.d.). *Secondary Sources*. https://apastyle.apa.org/style-grammar-guidelines/citations/secondary-sources

America's Cyber Defence Agency. (2021, February 21). *What is cybersecurity?* https://www.cisa.gov/news-events/news/what-cybersecurity

Arene. (2019, September 12). *Ethical recommendations for thesis writing at universities of applied sciences*. https://www.arene.fi/wp-content/uploads/Rapor-tit/2020/ETHICAL%20RECOMMENDATIONS%20FOR%20THESIS%20WRITING%20AT%20UNIVERSITIES%20OF%20APPLIED%20SCIENCES_2020.pdf?_t=1578480382

Baker, K. (2024, March 20). *10 Most Common Types of Cyber Attacks*. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

Barnard, C., & Peers, S. (2023). *European Union Law* (4th ed.). Oxford University Press.

Burri, M., & Zihlmann, Z. (2023, February 17). *The EU Cyber Resilience Act – An Appraisal and Contextualization*. Ssrn.com. https://ssrn.com/abstract=4375552

Caruana, E., Roman, M., Hernández-Sánchez, J., & Solli, P. (2015). Longitudinal studies. *Journal of Thoracic Disease*, *7*, E537-40. https://doi.org/10.3978/j.issn.2072-1439.2015.10.63

Chiara, P. G. (2022). The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. *International Cybersecurity Law Review*, *3*(2), 255–272. https://www.doi.org/10.3978/j.issn.2072-1439.2015.10.63

Cisco. (n.d.). *What Is a Cyberattack?* https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

Clarc, C., Gandhi, R., Gates, C., Manion, A., Martin, B., Nandakumarajah, C., O'Conner, B., Stewart, K., Herz, J., Walsh, T., Waltermire, D., & Springett, S. (2019). *Survey of Existing SBOM Formats and Standards*. https://www.ntia.gov/files/ntia/publications/ntia_sbom_formats_and_standards_whitepaper_-_version_20191025.pdf

Cobb, M. (2024, January 18). *How to Perform a Cybersecurity Risk Assessment in 5 Steps*. TechTarget. https://www.techtarget.com/searchsecurity/tip/How-to-perform-a-cybersecurity-risk-assessment-step-by-step

Commission of the European Communities. (2001a, January 26). *Communication from the Commission to the Council, the European parliament, the economic and social committee and the Committee of the regions: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*. (Report COM/2000/0890). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF

Commission of the European Communities. (2001b, June 6). *Communication from the Commission to the Council, the European parliament, the economic and social committee and the Committee of the regions: Network and Information Security: Proposal for A European Policy Approach*. (Report COM/2001/0298). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298

Commission of the European Communities. (2006, May 31). *Communication from the Commission to the Council, the European Parliament, the European Economic and Social committee and the Committee of the Regions - A strategy for a Secure Information Society - "Dialogue, partnership and empowerment" {SEC(2006) 656}*. (Report COM/2006/0251). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52006DC0251

Commission of the European Communities. (2009, March 30). *Communication from the Commission to the European parliament, the Council, the economic and social committee and the Committee of the regions: on Critical Information Infrastructure Protection "Protecting Europe from large*

scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". (Report COM/2009/0149). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0149

Contreras, P. (2023). *The transnational dimension of cybersecurity: The NIS directive and its jurisdictional challenges* (C. Onwubiko, P. Rosati, A. Rege, A. Erola, X. Bellekens, H. Hindy, & M. G. Jaatun, Eds.; pp. 327–341). Springer Nature Singapore.

Council of the European Union. (2023). *Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/102 - Mandate for negotiations with the European Parliament*. https://data.consilium.europa.eu/doc/document/ST-11726-2023-INIT/en/pdf

Council of Europe. (2001). *Convention on Cybercrime*. https://rm.coe.int/1680081561

Council of the EU. (2022, November 28). *Digital finance: Council adopts Digital Operational Resilience Act*. [Press release]. https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/

DIGITALEUROPE. (2024). *Recommendations on updated draft CRA standardisation request*. https://cdn.digitaleurope.org/uploads/2024/12/Recommendations-on-updated-draft-CRA-standardisation-request_DIGITALEUROPE.pdf

Directive - 97/66. *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector*. https://eur-lex.europa.eu/eli/dir/1997/66/oj

Directive 95/46/EC. *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. http://data.europa.eu/eli/dir/1995/46/oj

Directive 2002/21/EC. *Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive)*. https://eur-lex.europa.eu/eli/dir/2002/21/oj

Directive 2002/58/EC. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*. https://eur-lex.europa.eu/eli/dir/2002/58/oj

Directive 2008/114/EC. *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/dir/2008/114/oj

Directive 2009/136/EC. *Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/dir/2009/136/oj

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

Directive 2022/2555. *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Directive 2022/2557. *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

ETSI. (2020). *CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements* (ETSI

EN 303 645 V2.1.1 (2020-06)). https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

ETSI Technical Committee Cyber Security. (2023). *Cyber Security (CYBER); Assessment of cyber risk based on products' properties to support market placement*. (ETSI TR 103 935 V1.1.1). https://www.etsi.org/deliver/etsi_tr/103900_103999/103935/01.01.01_60/tr_103935v010101p.pdf

European Commission. (n.d.). *Harmonised Standards*. https://single-market-economy.ec.europa.eu/single-market/european-standards/harmonised-standards_en

European Commission. (1999). *eEurope - An information society for all*. https://eur-lex.europa.eu/EN/legal-content/summary/eeurope-an-information-society-for-all.html

European Commission. (2002, May 28). *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - eEurope 2005: An information society for all - An Action Plan to be presented in view of the Sevilla European Council, 21/22 June 2002*. (Report COM/2002/0263). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52002DC0263

European Commission. (2012, March 28). *Communication from the Commission to the Council and the European parliament: Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre* . (Report COM/2012/0140). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF

European Commission. (2013, February 7). *Joint communication to the European parliament, the Council, the European economic and social committee and the Committee of the regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. (Report JOIN/2013/01). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013JC0001

European Commission. (2017, June 13). *EUR-Lex - 52017JC0450 - EN - EUR-Lex*. (Report JOIN/2017/0450). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52017JC0450

European Commission. (2020b, December 16). *New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

European Commission. (2022a). *Commission welcomes political agreement on new rules on cybersecurity of network and information systems* [Press release]. https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_22_2985/IP_22_2985_EN.pdf

European Commission. (2022b, June 29). *Commission notice: The "Blue Guide" on the implementation of EU product rules 2022 (Text with EEA relevance) 2022/C 247/01*. (Report C/2022/3637). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2022.247.01.0001.01.ENG

European Commission. (2022c, September 15). *New EU cybersecurity rules ensure more secure hardware and software products* [Press release]. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/news/new-eu-cybersecurity-rules-ensure-more-secure-hardware-and-software-products

European Commission. (2023a, June 29). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) - FAQs*. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs

European Commission. (2023b, December 1). *Cyber Resilience Act - Questions and Answers*. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_5375

European Commission. (2024a, April 17). *Draft standardisation request to European Standards Organisations in support of Union policy on cybersecurity requirements for products with digital elements*. Europa.eu. https://ec.europa.eu/docsroom/documents/58974

European Commission. (2024b, October 14). *Regulatory framework on AI*. Shaping Europe's Digital Future. https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

European Commission, Joint Research Centre, Baldini, G., Barrero, J., Draper, G. (2020a). *Cybersecurity, our digital anchor: a European perspective*, (M.Dewar,editor,I.Coisel,editor,S.Chaudron,editor,I.Nai Fovino,editor,G.Kambourakis,editor,G.Barry,editor,B.Mortara,editor,J.Sanchez,editor,J.Nordvik,editor,H.Junklewitz,editor,I.Kounelis,editor) Publications Office. https://data.europa.eu/doi/10.2760/352218

European Council. (n.d.). *The ordinary legislative procedure*. Europa.eu. Retrieved January 2, 2025, from https://www.consilium.europa.eu/en/council-eu/decision-making/ordinary-legislative-procedure/

European Council. (2001). *Precidency Conclusions: Stockholm European Council*. https://www.consilium.europa.eu/media/20994/stockholm-european-council-presidency-conclusions.pdf

European Council. (2023, September 22). *The European Council establishes the composition of the European Parliament*. Consilium. https://www.consilium.europa.eu/en/press/press-releases/2023/09/22/the-european-council-establishes-the-composition-of-the-european-parliament/

European Cyber Security Organisation. (2024). *Challenges of the industry to implement the CRA WG1 -Trusted supply chains*. https://ecs-org.eu/ecso-uploads/2024/03/ECSO_Survey_CRA_2024.pdf

European Data Protection Supervisor. (n.d.). *Data Protection*. Retrieved June 11, 2024, from https://www.edps.europa.eu/data-protection/data-protection_en

European Insurance and Occupational Pensions Authority. (n.d.). *Digital Operational Resilience Act (DORA)*. Retrieved November 6, 2024, from https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

European Parliament. (n.d.-a). *Legislative powers*. Retrieved January 2, 2025, from https://www.europarl.europa.eu/about-parliament/en/powers-and-procedures/legislative-powers

European Parliament. (n.d.-b). *Overview*. Retrieved January 4, 2025, from https://www.europarl.europa.eu/olp/en/ordinary-legislative-procedure/overview

European Parliament. (2020). *EU policies - Insights: Understanding EU data protection policy*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651923/EPRS_BRI(2020)651923_EN.pdf

European Union. (n.d.-a). *European Commission*. Retrieved January 2, 2025, from https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-commission_en

European Union. (n.d.-b). *European Council*. Retrieved January 2, 2025, from https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-council_en

European Union. (n.d.-c). *How EU policy is decided*. Retrieved January 2, 2025, from https://european-union.europa.eu/institutions-law-budget/law/how-eu-policy-decided_en

European Union. (n.d.-d). *Internal market - EUR-Lex*. Europa.eu. Retrieved January 2, 2025, from https://eur-lex.europa.eu/summary/chapter/internal_market.html?root_default=SUM_1_CODED%3D24&locale=en

European Union. (n.d.-e). *Types of institutions and bodies*. Retrieved January 2, 2025, from https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/types-institutions-and-bodies_en

European Union. (n.d.-f). *Types of legislation*. Retrieved January 2, 2025, from https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en

European Union. (2023). *Facts and figures on the European Union*. https://european-union.europa.eu/principles-countries-history/facts-and-figures-european-union_en

European Union Agency for Cybersecurity, Joint Research Centre, Hernandez Ramos, J. L., Karopoulos, G., Nai Fovino, I., Spigolon, R., Steri, G., Gorniak, S., Magnabosco, P., Atoui, R., Crippa Martinez, C., & Sportiello, L. (2024). Cyber resilience act requirements standards mapping. In *Publications Office of the EU*. https://data.europa.eu/doi/10.2760/905934

Finio, M., & Downie, A. (2024, August 9). *What is a Cybersecurity Risk Assessment?* IBM. https://www.ibm.com/think/topics/cybersecurity-risk-assessment

Fleck, A. (2024, February 22). *Cybercrime Expected To Skyrocket in Coming Years [Digital image]*. Retrieved May 12, 2024, from https://www-statista-com.ezproxy.jamk.fi:2443/chart/28878/expected-cost-of-cybercrime-until-2027/

Gayubas, A. (2024, January 22). *History of the European Union*. Encyclopedia of Humanities. https://humanidades.com/en/history-of-the-european-union/

Geiger, H., & Botting, A. (2024, January 31). *Vulnerability Management Under The Cyber Resilience Act*. Center for Cybersecurity Policy and Law. https://www.centerforcybersecuritypolicy.org/insights-and-research/vulnerability-management-under-the-cyber-resilience-act

Gen Digital. (2023, February). *2023 Norton Cyber Safety Insights Report*. https://www.gendigital.com/media/aq2bu5io/2023-ncsir-us-global-report_final.pdf

Greenberg, A. (2018, August 28). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hanssen, H., & Vogel, A. T. (2024, November 21). *The EU Cyber Resilience Act: Implications for Companies*. Hogan Lovells. https://www.hoganlovells.com/en/publications/the-eu-cyber-resilience-act-implications-for-companies-

Hassan, M. (2024, March 25). *Basic Research - Types, Methods and Examples*. Research Method. https://researchmethod.net/basic-research

Hartley, T. C. (2014). *The foundations of European Union law: an introduction to the constitutional and administrative law of the European Union*. Oxford University Press.

IBM. (2024). *Cost of a Data Breach Report 2024*. https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec

International Electrotechnical Commission. (2018). *Security for industrial automation and control systems. Part 4-1: Secure product development lifecycle requirements* (EN IEC 62443-4-1:2018).

International Electrotechnical Commission. (2019). *Security for industrial automation and control systems. Part 4-2: Secure product development lifecycle requirements* (EN IEC 62443-4-2:2019).

International Monetary Fund. (2024, April). *Global Financial Stability Report: The Last Mile: Financial Vulnerabilities and Risks*. Accessed from, https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024?cid=bl-com-SM2024-GFSREA2024001#Overview

International Organization for Standardization. (2011). *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher.* (EN ISO/IEC 9797-1:2011).

International Organization for Standardization. (2020a). *Information technology - Security techniques - Privacy framework* (EN ISO/IEC 29100:2020).

International Organization for Standardization. (2020b). *Information technology. Security techniques. Vulnerability disclosure* (EN ISO/IEC 29147:2020).

International Organization for Standardization. (2020c). *Information technology. Security techniques. Vulnerability handling processes* (EN ISO/IEC 30111:2020).

International Organization for Standardization. (2021). *Information security — Encryption algorithms — Part 1: General* (ISO/IEC 18033-1:2021).

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security controls* (EN ISO/IEC 27002:2022).

International Organization for Standardization. (2023a). *Cybersecurity–Guidelines for Internet security* (ISO/IEC Standard No. 27032:2023).

International Organization for Standardization. (2023b). *Cybersecurity — Supplier relationships — Part 1: Overview and concepts* (ISO/IEC 27036-1:2023).

International Telecommunication Union. (1995). *Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems: Integrity Frameworks* (ITU-T X.815 (11/95)).

International Telecommunication Union. (2003). *Security architecture for systems providing end-to-end communications* (ITU-T X.805 (10/2003)).

International Telecommunication Union. (2018). *Cyberspace security – Cybersecurity: Security assessment techniques in telecommunication/information and communication technology networks* (ITU-T X.1214 (03/2018)). https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1214-201803-I!!PDF-E&type=items

JAMK University of Applied Sciences. (2018). *Ethical Principles for JAMK University of Applied Sciences: Approved by the Student Affairs Board on 11 December 2018*. https://www.jamk.fi/sites/default/files/2021-12/Ethical%20Principles%2011122018.pdf

Jump, M., Manion, A., Corman, J., Dillard, D., Gates, C., Gray, L., Hart, C., Hatch, A., Heierman, E., Hertz, J., Landfield, K., Lear, E., Lowenthal, B., Ma, C., Martin, B., Nandakumarajah, C., Sarvepalli, V., Sparrel, D., Stewart, K., & Friedman, A. (2019). *Framing Software Component Transparency: Establishing a Common Software Bill of Material (SBOM)*. https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf

Kavya. (2024, October 21). *A Guide to Cookie Law*. CookieYes. https://www.cookieyes.com/blog/cookie-law/

Kazakova, A. (2024, April 4). *EU Cyber Resilience Act: Enforcing cyber norms far beyond Europe - Diplo*. Diplo. https://www.diplomacy.edu/blog/eu-cyber-resilience-act-enforcing-cyber-norms-far-beyond-europe/

Kemp, S. (2024, January 31). *Digital 2024: Global Overview Report - DataReportal – Global Digital Insights*. DataReportal. https://datareportal.com/reports/digital-2024-global-overview-report?utm_source=Global_Digital_Reports&utm_medium=Partner_Article&utm_campaign=Digital_2024

Leavy, P. (Ed.). (2014). *The Oxford Handbook of Qualitative Research*. Oxford University Press.

Lueth, K. L. (2020, November 19). *State of the IoT 2020: 12 billion IoT connections, surpassing non-IoT for the first time*. IoT Analytics. https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time/

Merriam-Webster. (n.d.). *Cyberattack*. In Merriam-Webster.com dictionary. Retrieved May 11, 2024, from https://www.merriam-webster.com/dictionary/cyberattack

Microsoft. (2024). *Microsoft Digital Defense Report 2024*. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

Mueck, M. D., On, B., & Du Boispean, S. (2023). Upcoming European Regulations on Artificial Intelligence and Cybersecurity. *IEEE Communications Magazine*, *61*(7), 98–102. https://doi.org/10.1109/MCOM.004.2200612

National Cyber Security Centre Finland. (2023, January 10). *Materials for securing critical infrastructure*. Finnish Transport and Communications Agency Traficom. https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/instructions-and-guides/materials-securing-critical-infrastructure

National Institute of Standards and Technology. (n.d.) *Glossary – Cyber Attack*. Retrieved May 11, 2024, from https://csrc.nist.gov/glossary/term/cyber_attack

OECD. (2015). Frascati Manual 2015. In *The Measurement of Scientific, Technological and Innovation Activities*. OECD. https://doi.org/10.1787/9789264239012-en

Polona, C. (2024, November 20). *Horizontal cybersecurity requirements for products with digital elements: In "A Europe Fit for the Digital Age."* Legislative Train Schedule. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act

Practical Law. (n.d.). Recital (EU). In *Practical Law glossary*. Retrieved December 7, 2024, from https://uk.practicallaw.thomsonreuters.com/w-009-6368?contextData=%28sc.Default%29&transitionType=Default

Regulation 460/2004. *Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/reg/2004/460/oj

Regulation 679/2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Regulation 868/2022. *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

Regulation 881/2019. *Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC

Regulation 1689/2024. *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

Regulation 2847/2024. *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) (Text with EEA relevance)*. https://data.europa.eu/eli/reg/2024/2847/oj

Sahm, T. (2024, December 3). *Cybersecurity standards EN 18031 series and ETSI cybersecurity standards*. Globalnorm.de. Retreived February 3, 2025, from https://www.global-norm.de/en/news-product-compliance/details/cybersecurity-standards-en-18031-series-and-etsi-cybersecurity-standards/

Satyajit, S. (2023, May 24.). *State of IoT 2023: Number of connected IoT devices growing 16% to 16.7 billion globally*. IoT Analytics. https://iot-analytics.com/number-connected-iot-devices/

SonicWall. (2024). *2024 SonicWall Cyber Threat Report*. https://www.sonicwall.com/medialibrary/en/white-paper/2024-cyber-threat-report.pdf

The Ethics Centre. (2022, January 10). *What is pragmatism? - Ethics Explainer by The Ethics Centre*. https://ethics.org.au/ethics-explainer-pragmatism/

Tunggal, A. T. (2023, June 15). *What is Cybersecurity Risk? A Thorough Definition*. https://www.upguard.com/blog/cybersecurity-risk

Tunggal, A.T. (2024, January 22). *The 72 Biggest Data Breaches of All Time [Updated 2024]*. Retrieved May 11, 2024, from https://www.upguard.com/blog/biggest-data-breaches

Van Dijk, V. (n.d.). *4 different Definitions of Cybersecurity from NIST*. Security Scientist. https://www.securityscientist.net/blog/the-definition-of-cybersecurity-according-to-nist/

von der Leyen, U. (2021, September 15). *2021 State of the Union Address by President von der Leyen* [Speech transcript]. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701

Wilhelm, E. O. (2016, February). *A brief history of the General Data Protection Regulation*. Iapp. https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/

Wolford, B. (n.d.). *What is GDPR, the EU's new data protection law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/

Žukauskas, P., Vveinhardt, J., & Andriukaitienė, R. (2018). Philosophy and Paradigm of Scientific Research. In *www.intechopen.com*. IntechOpen; Intechopen. https://doi.org/10.5772/intechopen.70628

Appendices

Appendix 1. The CRA Annex I

ESSENTIAL CYBERSECURITY REQUIREMENTS

Part I Cybersecurity requirements relating to the properties of products with digital elements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(a) be made available on the market without known exploitable vulnerabilities;

(b) be made available on the market with a secure by default configuration, unless otherwise agreed between manufacturer and business user in relation to a tailor-made product with digital elements, including the possibility to reset the product to its original state;

(c) ensure that vulnerabilities can be addressed through security updates, including, where applicable, through automatic security updates that are installed within an appropriate timeframe enabled as a default setting, with a clear and easy-to-use opt-out mechanism, through the notification of available updates to users, and the option to temporarily postpone them;

(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

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

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

(g) process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended purpose of the product with digital elements (data minimisation);

(h) protect the availability of essential and basic functions, also after an incident, including through resilience and mitigation measures against denial-of-service attacks;

(i) minimise the negative impact by the products themselves or connected devices on the availability of services provided by other devices or networks;

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

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

(l) provide security related information by recording and monitoring relevant internal activity, including the access to or modification of data, services or functions, with an opt-out mechanism for the user;

(m) provide the possibility for users to securely and easily remove on a permanent basis all data and settings and, where such data can be transferred to other products or systems, ensure that this is done in a secure manner.

Part II Vulnerability handling requirements

Manufacturers of products with digital elements shall:

(1) identify and document vulnerabilities and components contained in products with digital elements, including by drawing up a software bill of materials in a commonly used and machine-readable format covering at the very least the top-level dependencies of the products;

(2) in relation to the risks posed to products with digital elements, address and remediate vulnerabilities without delay, including by providing security updates; where technically feasible, new security updates shall be provided separately from functionality updates;

(3) apply effective and regular tests and reviews of the security of the product with digital elements;

(4) once a security update has been made available, share and publicly disclose information about fixed vulnerabilities, including a description of the vulnerabilities, information allowing users to identify the product with digital elements affected, the impacts of the vulnerabilities, their severity and clear and accessible information helping users to remediate the vulnerabilities; in duly justified cases, where manufacturers consider the security risks of publication to outweigh the security benefits, they may delay making public information regarding a fixed vulnerability until after users have been given the possibility to apply the relevant patch;

(5) put in place and enforce a policy on coordinated vulnerability disclosure;

(6) take measures to facilitate the sharing of information about potential vulnerabilities in their product with digital elements as well as in third-party components contained in that product, including by providing a contact address for the reporting of the vulnerabilities discovered in the product with digital elements;

(7) provide for mechanisms to securely distribute updates for products with digital elements to ensure that vulnerabilities are fixed or mitigated in a timely manner and, where applicable for security updates, in an automatic manner;

(8) ensure that, where security updates are available to address identified security issues, they are disseminated without delay and, unless otherwise agreed between a manufacturer and a business

user in relation to a tailor-made product with digital elements, free of charge, accompanied by advisory messages providing users with the relevant information, including on potential action to be taken.

Appendix 2. The CRA Annex II

INFORMATION AND INSTRUCTIONS TO THE USER

At minimum, the product with digital elements shall be accompanied by:

1. the name, registered trade name or registered trademark of the manufacturer, and the postal address, the email address or other digital contact as well as, where available, the website at which the manufacturer can be contacted;

2. the single point of contact where information about vulnerabilities of the product with digital elements can be reported and received, and where the manufacturer's policy on coordinated vulnerability disclosure can be found;

3. name and type and any additional information enabling the unique identification of the product with digital elements;

4. the intended purpose of the product with digital elements, including the security environment provided by the manufacturer, as well as the product's essential functionalities and information about the security properties;

5. any known or foreseeable circumstance, related to the use of the product with digital elements in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, which may lead to significant cybersecurity risks;

6. where applicable, the internet address at which the EU declaration of conformity can be accessed;

7. the type of technical security support offered by the manufacturer and the end-date of the support period during which users can expect vulnerabilities to be handled and to receive security updates;

8. detailed instructions or an internet address referring to such detailed instructions and information on:
(a) the necessary measures during initial commissioning and throughout the lifetime of the product with digital elements to ensure its secure use;
(b) how changes to the product with digital elements can affect the security of data;
(c) how security-relevant updates can be installed;
(d) the secure decommissioning of the product with digital elements, including information on how user data can be securely removed;
(e) how the default setting enabling the automatic installation of security updates, as required by Part I, point (2)(c), of Annex I, can be turned off;
(f) where the product with digital elements is intended for integration into other products with digital elements, the information necessary for the integrator to comply with the essential cybersecurity requirements set out in Annex I and the documentation requirements set out in Annex VII.

9. If the manufacturer decides to make available the software bill of materials to the user, information on where the software bill of materials can be accessed.

Appendix 3. The CRA Annex III

IMPORTANT PRODUCTS WITH DIGITAL ELEMENTS

Class I

1. Identity management systems and privileged access management software and hardware, including authentication and access control readers, including biometric readers
2. Standalone and embedded browsers
3. Password managers
4. Software that searches for, removes, or quarantines malicious software
5. Products with digital elements with the function of virtual private network (VPN)
6. Network management systems
7. Security information and event management (SIEM) systems
8. Boot managers
9. Public key infrastructure and digital certificate issuance software
10. Physical and virtual network interfaces
11. Operating systems
12. Routers, modems intended for the connection to the internet, and switches
13. Microprocessors with security-related functionalities
14. Microcontrollers with security-related functionalities
15. Application specific integrated circuits (ASIC) and field-programmable gate arrays (FPGA) with security-related functionalities
16. Smart home general purpose virtual assistants
17. Smart home products with security functionalities, including smart door locks, security cameras, baby monitoring systems and alarm systems
18. Internet connected toys covered by Directive 2009/48/EC of the European Parliament and of the Council (1) that have social interactive features (e.g. speaking or filming) or that have location tracking features
19. Personal wearable products to be worn or placed on a human body that have a health monitoring (such as tracking) purpose and to which Regulation (EU) 2017/745 or (EU) No 2017/746 do not apply, or personal wearable products that are intended for the use by and for children

Class II

1. Hypervisors and container runtime systems that support virtualised execution of operating systems and similar environments
2. Firewalls, intrusion detection and prevention systems
3. Tamper-resistant microprocessors
4. Tamper-resistant microcontrollers

Appendix 4. The CRA Annex IV

CRITICAL PRODUCTS WITH DIGITAL ELEMENTS

1. Hardware Devices with Security Boxes
2. Smart meter gateways within smart metering systems as defined in Article 2, point (23) of Directive (EU) 2019/944 of the European Parliament and of the Council (1) and other devices for advanced security purposes, including for secure cryptoprocessing
3. Smartcards or similar devices, including secure elements

Appendix 5. The CRA Annex V

EU DECLARATION OF CONFORMITY

The EU declaration of conformity referred to in Article 28, shall contain all of the following information:

1. Name and type and any additional information enabling the unique identification of the product with digital elements
2. Name and address of the manufacturer or its authorised representative
3. A statement that the EU declaration of conformity is issued under the sole responsibility of the provider
4. Object of the declaration (identification of the product with digital elements allowing traceability, which may include a photograph, where appropriate)
5. A statement that the object of the declaration described above is in conformity with the relevant Union harmonisation legislation
6. References to any relevant harmonised standards used or any other common specification or cybersecurity certification in relation to which conformity is declared
7. Where applicable, the name and number of the notified body, a description of the conformity assessment procedure performed, and identification of the certificate issued
8. Additional information:

Signed for and on behalf of:

(place and date of issue):

(name, function) (signature):

Appendix 6. The CRA Annex VI

ANNEX VI

SIMPLIFIED EU DECLARATION OF CONFORMITY

The simplified EU declaration of conformity referred to in Article 13(20) shall be provided as follows:

Hereby, … [name of manufacturer] declares that the product with digital elements type … [designation of type of product with digital element] is in compliance with Regulation (EU) 2024/2847.

The full text of the EU declaration of conformity is available at the following internet address: …

Appendix 7. The CRA Annex VII

CONTENT OF THE TECHNICAL DOCUMENTATION

The technical documentation referred to in Article 31 shall contain at least the following information, as applicable to the relevant product with digital elements:

1. a general description of the product with digital elements, including:
(a) its intended purpose;
(b) versions of software affecting compliance with essential cybersecurity requirements;
(c) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;
(d) user information and instructions as set out in Annex II;

2. a description of the design, development and production of the product with digital elements and vulnerability handling processes, including:

(a) necessary information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;
(b) necessary information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence of the provision of a contact address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates;
(c) necessary information and specifications of the production and monitoring processes of the product with digital elements and the validation of those processes;

3. an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained pursuant to Article 13, including how the essential cybersecurity requirements set out in Part I of Annex I are applicable;

4. relevant information that was taken into account to determine the support period pursuant to Article 13(8) of the product with digital elements;

5. a list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union, common specifications as set out in Article 27 of this Regulation or European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 pursuant to Article 27(8) of this Regulation, and, where those harmonised standards, common specifications or European cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential cybersecurity requirements set out in Parts I and II of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or European cybersecurity certification schemes, the technical documentation shall specify the parts which have been applied;

6. reports of the tests carried out to verify the conformity of the product with digital elements and of the vulnerability handling processes with the applicable essential cybersecurity requirements as set out in Parts I and II of Annex I;

7. a copy of the EU declaration of conformity;

8. where applicable, the software bill of materials, further to a reasoned request from a market surveillance authority provided that it is necessary in order for that authority to be able to check compliance with the essential cybersecurity requirements set out in Annex I.

Appendix 8. The CRA Annex VIII

CONFORMITY ASSESSMENT PROCEDURES

Part I Conformity assessment procedure based on internal control (based on module A)

1. Internal control is the conformity assessment procedure whereby the manufacturer fulfils the obligations set out in points 2, 3 and 4 of this Part, and ensures and declares on its sole responsibility that the products with digital elements satisfy all the essential cybersecurity requirements set out in Part I of Annex I and the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.
2. The manufacturer shall draw up the technical documentation described in Annex VII.
3. Design, development, production and vulnerability handling of products with digital elements
   The manufacturer shall take all measures necessary so that the design, development, production and vulnerability handling processes and their monitoring ensure compliance of the manufactured or developed products with digital elements and of the processes put in place by the manufacturer with the essential cybersecurity requirements set out in Parts I and II of Annex I.
4. Conformity marking and declaration of conformity
   4.1. The manufacturer shall affix the CE marking to each individual product with digital elements that satisfies the applicable requirements set out in this Regulation.
   4.2. The manufacturer shall draw up a written EU declaration of conformity for each product with digital elements in accordance with Article 28 and keep it together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The EU declaration of conformity shall identify the product with digital elements for which it has been drawn up. A copy of the EU declaration of conformity shall be made available to the relevant authorities upon request.
5. Authorised representatives
   The manufacturer's obligations set out in point 4 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the mandate.

Part II EU-type examination (based on module B)

1. EU-type examination is the part of a conformity assessment procedure in which a notified body examines the technical design and development of a product with digital elements and the vulnerability handling processes put in place by the manufacturer, and attests that a product with digital elements meets the essential cybersecurity requirements set out in Part I of Annex I and that the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.
2. EU-type examination shall be carried out by assessing the adequacy of the technical design and development of the product with digital elements through the examination of the technical documentation and supporting evidence referred to in point 3, and the examination of specimens of one or more critical parts of the product (combination of production type and design type).
3. The manufacturer shall lodge an application for EU-type examination with a single notified body of its choice.

   The application shall include:

   3.1. the name and address of the manufacturer and, if the application is lodged by the authorised representative, the name and address of that authorised representative;

   3.2. a written declaration that the same application has not been lodged with any other notified body;

   3.3. the technical documentation, which shall make it possible to assess the conformity of the product with digital elements with the applicable essential cybersecurity requirements as set out in Part I of Annex I and the manufacturer's vulnerability handling processes set out in Part II of Annex I and shall include an adequate analysis and assessment of the risks. The technical documentation shall specify the applicable requirements and cover, as far as relevant for the assessment, the design, manufacture and operation of the product with digital elements. The technical documentation shall contain, wherever applicable, at least the elements set out in Annex VII;

   3.4. the supporting evidence for the adequacy of the technical design and development solutions and vulnerability handling processes. This supporting evidence shall mention any documents that have been used, in particular where the relevant harmonised standards or technical specifications have not been applied in full. The supporting evidence shall include, where necessary, the results of tests carried out by the appropriate laboratory of the manufacturer, or by another testing laboratory on its behalf and under its responsibility.
4. The notified body shall:

4.1. examine the technical documentation and supporting evidence to assess the adequacy of the technical design and development of the product with digital elements with the essential cybersecurity requirements set out in Part I of Annex I and of the vulnerability handling processes put in place by the manufacturer with the essential cybersecurity requirements set out in Part II of Annex I;

4.2. verify that specimens have been developed or manufactured in conformity with the technical documentation, and identify the elements which have been designed and developed in accordance with the applicable provisions of the relevant harmonised standards or technical specifications, as well as the elements which have been designed and developed without applying the relevant provisions of those standards;

4.3. carry out appropriate examinations and tests, or have them carried out, to check that, where the manufacturer has chosen to apply the solutions in the relevant harmonised standards or technical specifications for the requirements set out in Annex I, they have been applied correctly;

4.4. carry out appropriate examinations and tests, or have them carried out, to check that, where the solutions in the relevant harmonised standards or technical specifications for the requirements set out in Annex I have not been applied, the solutions adopted by the manufacturer meet the corresponding essential cybersecurity requirements;

4.5. agree with the manufacturer on a location where the examinations and tests will be carried out.

5. The notified body shall draw up an evaluation report that records the activities undertaken in accordance with point 4 and their outcomes. Without prejudice to its obligations vis-à-vis the notifying authorities, the notified body shall release the content of that report, in full or in part, only with the agreement of the manufacturer.

6. Where the type and the vulnerability handling processes meet the essential cybersecurity requirements set out in Annex I, the notified body shall issue an EU-type examination certificate to the manufacturer. The certificate shall contain the name and address of the manufacturer, the conclusions of the examination, the conditions (if any) for its validity and the necessary data for identification of the approved type and vulnerability handling processes. The certificate may have one or more annexes attached.

The certificate and its annexes shall contain all relevant information to allow the conformity of manufactured or developed products with digital elements with the examined type and vulnerability handling processes to be evaluated and to allow for in-service control.

Where the type and the vulnerability handling processes do not satisfy the applicable essential cybersecurity requirements set out in Annex I, the notified body shall refuse to issue an EU-type examination certificate and shall inform the applicant accordingly, giving detailed reasons for its refusal.

7. The notified body shall keep itself apprised of any changes in the generally acknowledged state of the art which indicate that the approved type and the vulnerability handling processes may no longer comply with the applicable essential cybersecurity requirements set out in Annex I, and shall determine whether such changes require further investigation. If so, the notified body shall inform the manufacturer accordingly.

   The manufacturer shall inform the notified body that holds the technical documentation relating to the EU-type examination certificate of all modifications to the approved type and the vulnerability handling processes that may affect the conformity with the essential cybersecurity requirements set out in Annex I, or the conditions for validity of the certificate. Such modifications shall require additional approval in the form of an addition to the original EU-type examination certificate.

8. The notified body shall carry out periodic audits to ensure that the vulnerability handling processes as set out in Part II of Annex I are implemented adequately.

9. Each notified body shall inform its notifying authorities concerning the EU-type examination certificates and any additions thereto which it has issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of certificates and any additions thereto refused, suspended or otherwise restricted.

   Each notified body shall inform the other notified bodies concerning the EU-type examination certificates and any additions thereto which it has refused, withdrawn, suspended or otherwise restricted, and, upon request, concerning the certificates and additions thereto which it has issued.

   The Commission, the Member States and the other notified bodies may, on request, obtain a copy of the EU-type examination certificates and any additions thereto. On request, the Commission and the Member States may obtain a copy of the technical documentation and the results of the examinations carried out by the notified body. The notified body shall keep a copy of

the EU-type examination certificate, its annexes and additions, as well as the technical file including the documentation submitted by the manufacturer, until the expiry of the validity of the certificate.

10. The manufacturer shall keep a copy of the EU-type examination certificate, its annexes and additions together with the technical documentation at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer.
11. The manufacturer's authorised representative may lodge the application referred to in point 3 and fulfil the obligations set out in points 7 and 10, provided that the relevant obligations are specified in the mandate.

Part III Conformity to type based on internal production control (based on module C)

1. Conformity to type based on internal production control is the part of a conformity assessment procedure whereby the manufacturer fulfils the obligations set out in points 2 and 3 of this Part, and ensures and declares that the products with digital elements concerned are in conformity with the type described in the EU-type examination certificate and satisfy the essential cybersecurity requirements set out in Part I of Annex I and that the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.
2. Production

   The manufacturer shall take all measures necessary so that the production and its monitoring ensure conformity of the manufactured products with digital elements with the approved type described in the EU-type examination certificate and with the essential cybersecurity requirements as set out in Part I of Annex I and ensures that the manufacturer meets the essential cybersecurity requirements set out in Part II of Annex I.
3. Conformity marking and declaration of conformity
   3.1. The manufacturer shall affix the CE marking to each individual product with digital elements that is in conformity with the type described in the EU-type examination certificate and satisfies the applicable requirements set out in this Regulation.
   3.2. The manufacturer shall draw up a written declaration of conformity for a product model and keep it at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The declaration of conformity shall identify the product model for which it has been drawn up.

A copy of the declaration of conformity shall be made available to the relevant authorities upon request.

4.Authorised representative

The manufacturer's obligations set out in point 3 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the mandate.

Part IV Conformity based on full quality assurance (based on module H)

1.Conformity based on full quality assurance is the conformity assessment procedure whereby the manufacturer fulfils the obligations set out in points 2 and 5 of this Part, and ensures and declares on its sole responsibility that the products with digital elements or product categories concerned satisfy the essential cybersecurity requirements set out in Part I of Annex I and that the vulnerability handling processes put in place by the manufacturer meet the requirements set out in Part II of Annex I.

2.Design, development, production and vulnerability handling of products with digital elements

The manufacturer shall operate an approved quality system as specified in point 3 for the design, development and final product inspection and testing of the products with digital elements concerned and for handling vulnerabilities, maintain its effectiveness throughout the support period, and shall be subject to surveillance as specified in point 4.

3.Quality system

3.1.The manufacturer shall lodge an application for assessment of its quality system with the notified body of its choice, for the products with digital elements concerned.

The application shall include:

(a)the name and address of the manufacturer and, if the application is lodged by the authorised representative, the name and address of that authorised representative;

(b)the technical documentation for one model of each category of products with digital elements intended to be manufactured or developed. The technical documentation shall, wherever applicable, contain at least the elements as set out in Annex VII;

(c) the documentation concerning the quality system; and

(d)a written declaration that the same application has not been lodged with any other notified body.

3.2.The quality system shall ensure compliance of the products with digital elements with the essential cybersecurity requirements set out in Part I of Annex I and compliance of the vulnerability handling processes put in place by the manufacturer with the requirements set out in Part II of Annex I.

All the elements, requirements and provisions adopted by the manufacturer shall be documented in a systematic and orderly manner in the form of written policies, procedures and instructions. That quality system documentation shall permit a consistent interpretation of the quality programmes, plans, manuals and records.

It shall, in particular, contain an adequate description of:

(a)the quality objectives and the organisational structure, responsibilities and powers of the management with regard to design, development, product quality and vulnerability handling;

(b)the technical design and development specifications, including standards, that will be applied and, where the relevant harmonised standards or technical specifications will not be applied in full, the means that will be used to ensure that the essential cybersecurity requirements set out in Part I of Annex I that apply to the products with digital elements will be met;

(c)the procedural specifications, including standards, that will be applied and, where the relevant harmonised standards or technical specifications will not be applied in full, the means that will be used to ensure that the essential cybersecurity requirements set out in Part II of Annex I that apply to the manufacturer will be met;

(d)the design and development control, as well as design and development verification techniques, processes and systematic actions that will be used when designing and developing the products with digital elements pertaining to the product category covered;

(e)the corresponding production, quality control and quality assurance techniques, processes and systematic actions that will be used;

(f)the examinations and tests that will be carried out before, during and after production, and the frequency with which they will be carried out;

(g)the quality records, such as inspection reports and test data, calibration data and qualification reports on the personnel concerned;

(h)the means of monitoring the achievement of the required design and product quality and the effective operation of the quality system.

3.3. The notified body shall assess the quality system to determine whether it satisfies the requirements referred to in point 3.2.

It shall presume conformity with those requirements in respect of the elements of the quality system that comply with the corresponding specifications of the national standard that implements the relevant harmonised standard or technical specification.

In addition to experience in quality management systems, the auditing team shall have at least one member experienced as an assessor in the relevant product field and product technology concerned, and shall have knowledge of the applicable requirements set out in this Regulation. The audit shall include an assessment visit to the manufacturer's premises, where such premises exist. The auditing team shall review the technical documentation referred to in point 3.1 (b), to verify the manufacturer's ability to identify the applicable requirements set out in this Regulation and to carry out the necessary examinations with a view to ensuring compliance of the product with digital elements with those requirements.

The manufacturer or its authorised representative shall be notified of the decision.

The notification shall contain the conclusions of the audit and the reasoned assessment decision.

3.4. The manufacturer shall undertake to fulfil the obligations arising out of the quality system as approved and to maintain it so that it remains adequate and efficient.

3.5. The manufacturer shall keep the notified body that has approved the quality system informed of any intended change to the quality system.

The notified body shall evaluate any proposed changes and decide whether the modified quality system will continue to satisfy the requirements referred to in point 3.2 or whether a reassessment is necessary.

It shall notify the manufacturer of its decision. The notification shall contain the conclusions of the examination and the reasoned assessment decision.

4. Surveillance under the responsibility of the notified body

4.1. The purpose of surveillance is to make sure that the manufacturer duly fulfils the obligations arising out of the approved quality system.

4.2. The manufacturer shall, for assessment purposes, allow the notified body access to the design, development, production, inspection, testing and storage sites, and shall provide it with all necessary information, in particular:

(a) the quality system documentation;

(b)the quality records as provided for by the design part of the quality system, such as results of analyses, calculations and tests;

(c)the quality records as provided for by the manufacturing part of the quality system, such as inspection reports and test data, calibration data and qualification reports on the personnel concerned.

4.3.The notified body shall carry out periodic audits to make sure that the manufacturer maintains and applies the quality system and shall provide the manufacturer with an audit report.

5.Conformity marking and declaration of conformity

5.1.The manufacturer shall affix the CE marking, and, under the responsibility of the notified body referred to in point 3.1, the latter's identification number to each individual product with digital elements that satisfies the requirements set out in Part I of Annex I.

5.2.The manufacturer shall draw up a written declaration of conformity for each product model and keep it at the disposal of the national authorities for 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer. The declaration of conformity shall identify the product model for which it has been drawn up.

A copy of the declaration of conformity shall be made available to the relevant authorities upon request.

6.The manufacturer shall, for a period ending at least 10 years after the product with digital elements has been placed on the market or for the support period, whichever is longer, keep at the disposal of the national authorities:

(a) the technical documentation referred to in point 3.1;

(b) the documentation concerning the quality system referred to in point 3.1;

(c) the change referred to in point 3.5, as approved;

(d) the decisions and reports of the notified body referred to in points 3.5 and 4.3.

7.Each notified body shall inform its notifying authorities of quality system approvals issued or withdrawn, and shall, periodically or upon request, make available to its notifying authorities the list of quality system approvals refused, suspended or otherwise restricted.

Each notified body shall inform the other notified bodies of quality system approvals which it has refused, suspended or withdrawn, and, upon request, of quality system approvals which it has issued.

8.Authorised representative

The manufacturer’s obligations set out in points 3.1, 3.5, 5 and 6 may be fulfilled by its authorised representative, on its behalf and under its responsibility, provided that the relevant obligations are specified in the mandate.