Kimmo Fransila

Implementing NIS2 EU Directive to Large International Company in Finland

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master’s Thesis

23rd March 2024

PREFACE

The challenges that I faced in this study was more towards my persistence and time available in a day. Directives, national laws, frameworks, and certificates are not something one might call fun things to read.

However, once those things are read, one learns the ingredients very well. It also shows that, laws, certificates, and frameworks are very similar due to the nature of cyber security and crime. Then how this is implemented and, how it is mapped against real life services is a different ball game.

This thesis includes experience from my previous studies, since I have looked up items in history as well.

I would like to thank my family for allowing me to use my personal life and time to educate myself at this magnitude, I am really honored, thank you.

I also thank my employer for offering support in the form of subjects and challenges to be solved. Special thanks to Mr. Kalle Kaasalainen and Mrs. Irina Kitinprami.

Helsinki, 23rd March 2024
Kimmo Fransila

Abstract

Author:	Kimmo Fransila
Title:	Implementing the NIS2 EU Directive to large international company in Finland
Number of Pages:	xx pages + 1 appendices
Date:	23 March 2024
Degree:	Master of Engineering
Degree Programme:	Information Technology
Professional Major:	Networking and Services / Cyber Security
Supervisors:	Kalle Kaasalainen, Director, Security, Telia Finland Oyj Ville Jääskeläinen, Principal Lecturer, Metropolia

Background for this study is cybersecurity frameworks, cybersecurity specific legislation, and commercial certificates within this field and how to ensure that companies are following applicable requirements at an adequate level. The most important item is however, that the critical infrastructure is protected and prepared against any kind of cyber-attack. Telecom operators are part of that critical infrastructure.

Cybersecurity legislation is affecting an increasing number of areas in our modern societies. Companies are obliged to comply with legislation. The de facto frameworks and certificates are something that companies follow and implement voluntarily for business purposes. They also follow leading industry guidelines for protecting companies against cybercrime and in many cases offer specific control functions to fulfil the legislation.

The purpose of this thesis is to make ensure that legislative demands are fulfilled in a telecom company that is now under the NIS2 compliance umbrella. This thesis offers guidance and ensure that legal demands are fulfilled. One important note is that, when companies are working with solutions on their own to protect themselves against cybercrime. Therefore, it is important to recognize which parts of the solutions already fulfil the legal demands and what is still needed to be done.

This challenge was solved by running a companywide NIS2 implementation project.

The scope of this study is to implement NIS2 requirements efficiently to telecom company. NIST, ISO27001, and local law and regulations requirements are implemented to a certain extent as well in this case.

Keywords: NIS2, NIST, ISO27001, Cybersecurity, legislation, regulation, efficiency

The originality of this thesis has been checked using Turnitin Originality cheque service.

Contents

List of Abbreviations

AIA	Artificial Intelligence Act
BSS	Business Support Systems
DA	Data Act
DGA	Data Governance Act
DMA	Digital Markets Act
DSA	Digital Services Act
EU	European Union
FBI	Federal bureau of Investigations
GDPR	General Data Protection Regulation
ISA/IEC	ISA equals International Society of Automation and IEC stands for International Electrotechnical Commission.
ISM	Information System Manager
ISO	Information System Owner
ISO 27001	International Standard on requirements for information security management
ITIL	Information Technology Infrastructure Library
MFA	Multi Factor Authentication
NIS2	Network and Information Systems 2, European Union directive legislation
NIST CSF	National Institute of Standards and Technology (USA), Cybersecurity framework
OSS	Operations Support Systems
PDCA	Plan, Do, Check, Act. Continuous improvement cycle

1 Introduction

As the world changes, the usage of cash is decreasing in many areas around the globe. Business is going online and handled electronically. It is rather self-evident that the crime follows the money or some kind of benefit to be achieved. Therefore, there is IT crime, i.e. cybercrime. Obviously, there needs to be a balancing force, which is cybersecurity. Cybersecurity today is a basic requirement and, not something optional!

Why are governments and other instances making these laws, regulations, and guidelines for cybersecurity?

According to the Federal Bureau of Investigations, FBI in the United States, losses due to cybercrime globally are roughly 12 billion American dollars. The losses have increased by 22% compared with 2022. This is also because the increase in complaints has increased by 10%, which means that the threshold of notifying authorities about cybercrime has lowered and that the losses have become larger in size.

One thing is to manufacture secure devices with a safely written code. For example, in 2023, industry leaders released software patches for security vulnerabilities: Microsoft released over 50, Google (Android) released over 50, SAP released close to 20, Oracle released 387, and Cisco more than 50. To put this into perspective, it means that a vulnerability is found and patched every day to every week in 2023. Zero-day vulnerabilities, i.e., vulnerabilities that were unknown to the manufacturer is a weakness that can be potentially exploited by malicious instances to gain financial interest or introduce criminal disturbance to the overall working of the various products, were also made on double digits.

Now, these megacompanies, not to mention all the smaller ones, produce products that are potentially unsafe to the users and give means to criminals or state-level actors to do harm. The legislation this thesis addresses is guidelines for companies and instances that are using this vulnerable software. Companies and governments would be better off by demanding proper software and functionality in the first place. However, it needs to be recognized that this dilemma is much more diverse and more complicated than stated in this simple demand.

The above facts in 2023 thus clearly support the need for regulations and guidelines. Cybersecurity has grown into huge industry for all players. Good and bad.

There can be debate about the need for legislation and regulations about cyber security, but to ensure that nationalities can safeguard their critical infrastructure, it is important that there are guiding and binding principles that need to be followed by commercial companies and national institutes on how they protect their information systems, even if one would imagine that the commercial companies have an interest of their own to protect their business. This has not been taken as granted, and these regulations and guidelines are seen necessary to make things more secure.

Local laws in Finland describe how companies offering critical infrastructural services must apply. NIS2 is similar, but rather more demanding than the local Finnish law and regulations. Then, companies might find the competitive advantage on following ‘de facto’ certifications such as ISO 27001 or other well-known cybersecurity frameworks such as NIST CSF.

Generally, in Finland, telecommunication companies are part of the critical infrastructure; therefore, telecommunications companies must fulfil the demands of all laws and regulations in the cybersecurity area. Telcos also test their abilities and readiness towards known frameworks such as NIST CSF. Many industrial customers of these telcos demand certifications in cybersecurity and then companies usually implement the ISO 27001 certification in full or by some major parts. The company for which this thesis is written makes no exception.

The challenge in implementing legislation, regulation, frameworks, or certifications today is not that those cannot be implemented individually as such, but more on the fact that what they are describing is vastly complicated and contains numerous information systems and networks. There should be a focus on right priorities, what needs to be done first and why, and there are overlaps and items for certain specific purposes. This work on implementing this set of cybersecurity requires time, resources, and proper funding. All of which are not necessarily available. This thesis aims to give tangible guidance on implementing NIS2 in the most effective way.

It is essential to solve this challenge since such as earlier EU legislation, GDPR, and NIS2 are obligatory to follow, and if not followed, fines connected to the companies' turnover Figures can be imposed. This is also very important because the time to implement this legislation is not that long considering the IT and other systems that the telcos need to go through and verify against the NIS2. The timetable challenge is tightly connected to resources and funding.

The solution to this challenge is to make sure all preparations are done correctly, personnel time is reserved, funding in budgets, the needed work tightly organized, as is situations covered, and all overlaps and other similarities are checked and avoided if possible and needed.

The exact scope of this thesis is to focus on implementing NIS2. Not to implement NIST CSF or ISO 27001. In addition, it is assumed that the local Finnish legislation is already applied. There might be many things that overlap and are the same among all the laws, regulations, frameworks, and standards mentioned here, and those need to be noted for possible future work.

2 Guiding Laws, Regulations, and Certifications

In this chapter, all the laws, regulations, frameworks, and standards around cybersecurity are introduced on a proper level to illustrate the landscape that telcos need to fulfil. What do they contain, and on what level do they need to be applied.

To illustrate the whole landscape in this area for the European union and for Finland as an independent country, the following picture demonstrates all areas that are impacted.

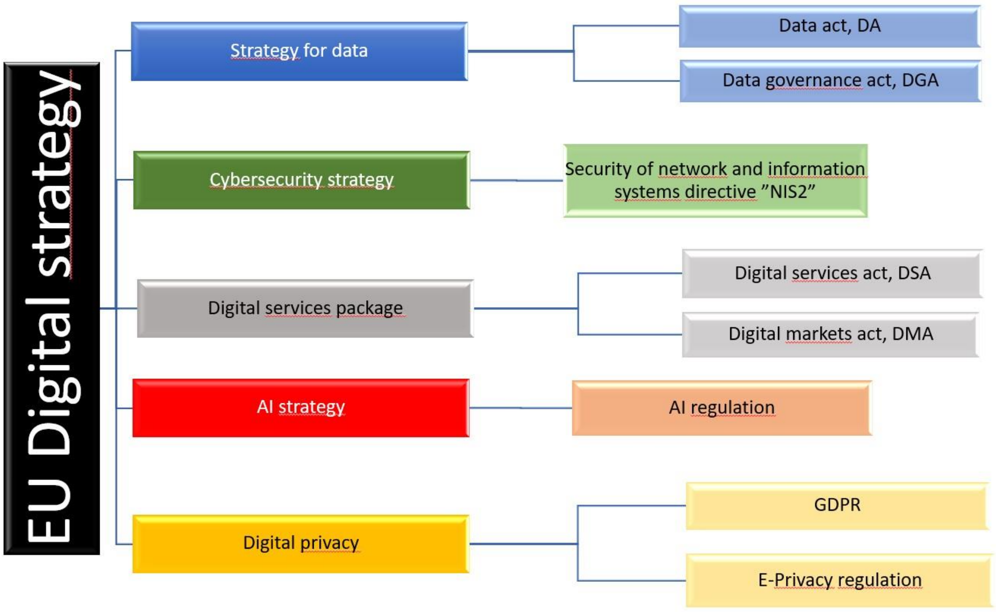


Figure 1: *Landscape of EU digital strategy*

The previous picture illustrates the European union digital strategy that everyone in the EU needs to apply. These regulations provide the opportunity and guidelines that the telecommunications companies must also follow and perhaps find a competitive advantage. All these areas are connected to each other and overlap in many cases.

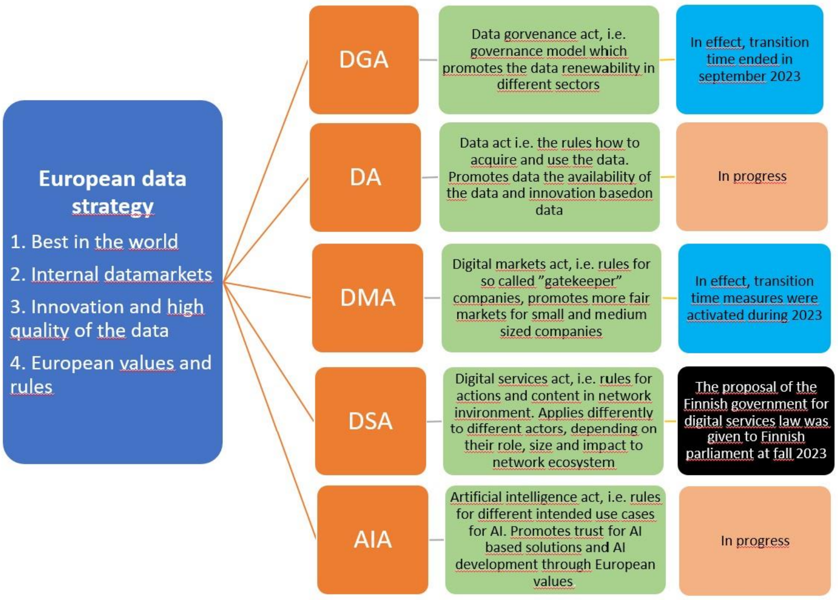

European data strategy
1. Best in the world
2. Internal datamarkets
3. Innovation and high quality of the data
4. European values and rules
DGA
Data gorvenance act, i.e. governance model which promotes the data renewability in different sectors
In effect, transition time ended in september 2023
DA
Data act i.e. the rules how to acquire and use the data. Promotes data the availability of the data and innovation basedon data
In progress
DMA
Digital markets act, i.e. rules for so called ”gatekeeper” companies, promotes more fair markets for small and medium sized companies
In effect, transition time measures were activated during 2023
DSA
Digital services act, i.e. rules for actions and content in network environment. Applies differently to different actors, depending on their role, size and impact to network ecosystem
The proposal of the Finnish government for digital services law was given to Finnish parliament at fall 2023
AIA
Artificial intelligence act, i.e. rules for different intended use cases for AI. Promotes trust for AI based solutions and AI development through European values
In progress

Figure 2: *Status of EU data strategy acts.*

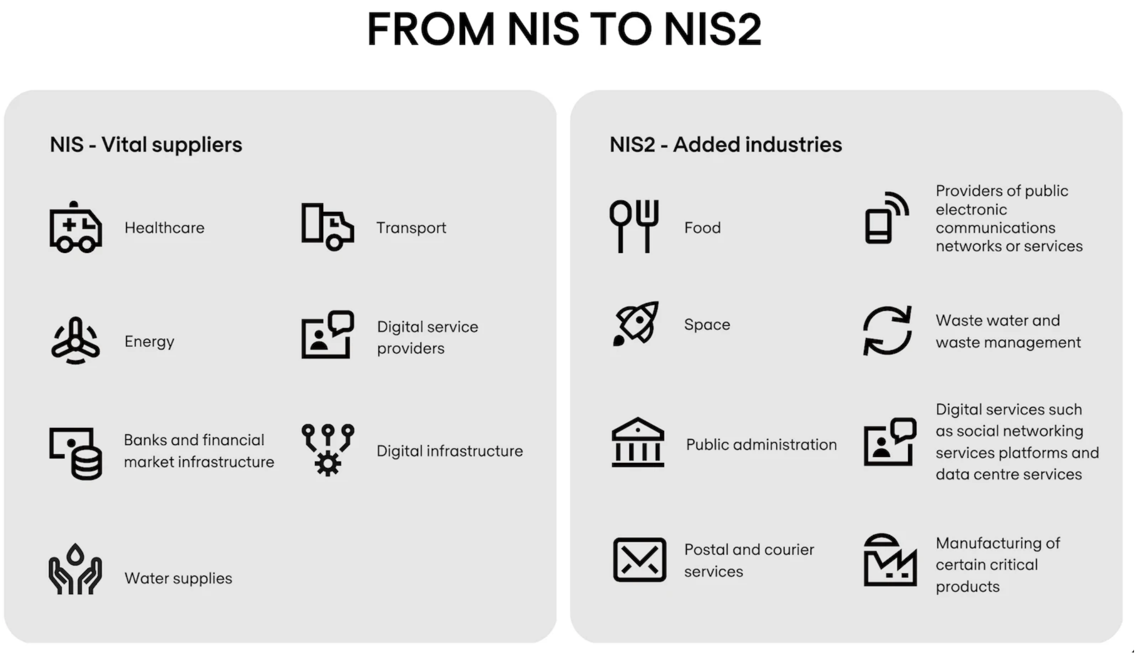
The previous picture states the status of parallel regulation regarding NIS2 in the EU. This however reveals, that implementing certain regulations is complicated. Thus, implementing enforced regulation while keeping in mind the regulation being prepared for future use.

The European cybersecurity landscape is also open to a certain extent. As it is only right, the European union amongst other countries in the world has its own separate cyber security politics and targets. This is done to safeguard the data that is used, ensure safe communications, and uphold the society and economy. The European union also actively follows the status of the implementation procedure. To ensure the cooperation and exchange of information between European countries around cybersecurity, a NIS COOPERATION GROUP has been established. NIS2 has supporting legislation such as the EU cyber solidarity act, which furthermore supports active collaboration around Europe. Europe has a European cybersecurity competence centre, ECCC [3], whose main function is to help the EU to maintain technical and industrial readiness in cybersecurity. The EU also has an agency around cybersecurity called the European Union Agency for Cybersecurity, ENISA [4], which has the task of creating and maintaining European cybersecurity certificates and increasing operative cooperation inside the EU, i.e., helping member states to handle their cybersecurity issues and coordinate EU level cybersecurity attacks and crises. In addition, EU has a stakeholder cybersecurity certification group to support ENISA on certification strategy and other relevant certification matters. If all this sounds a lot, please remember that these groups, agencies, and what have gone rather fast into concrete cybersecurity items, such as what, are the minimum network domain security measures. Also, all EU member states must have their own view on cybersecurity items, but also to ensure that all local laws are in line with EU directives. This is a massive coordination area.

This chapter contains rather detailed information, but it is vital due to the nature of the topic.

2.1 European Union Directive NIS2

Before NIS2, there was NIS (1). The first European union level cybersecurity law was introduced on 2016 and it was called NIS, Network Information Systems. Then, in 2023, NIS2 was released [1] and it needs to be enforced by every European Union member state no later than October 2024. In the NIS2 dedicated internet page [2], it is described that the typical compliance process, which includes all sorts of activities, takes approximately 12 months. In this chapter, the main difference between NIS and NIS2 is explained and the main items around NIS2.



FROM NIS TO NIS2

NIS - Vital suppliers

Healthcare

Transport

Energy

Digital service providers

Banks and financial market infrastructure

Digital infrastructure

Water supplies

NIS2 - Added industries

Food

Providers of public electronic communications networks or services

Space

Waste water and waste management

Public administration

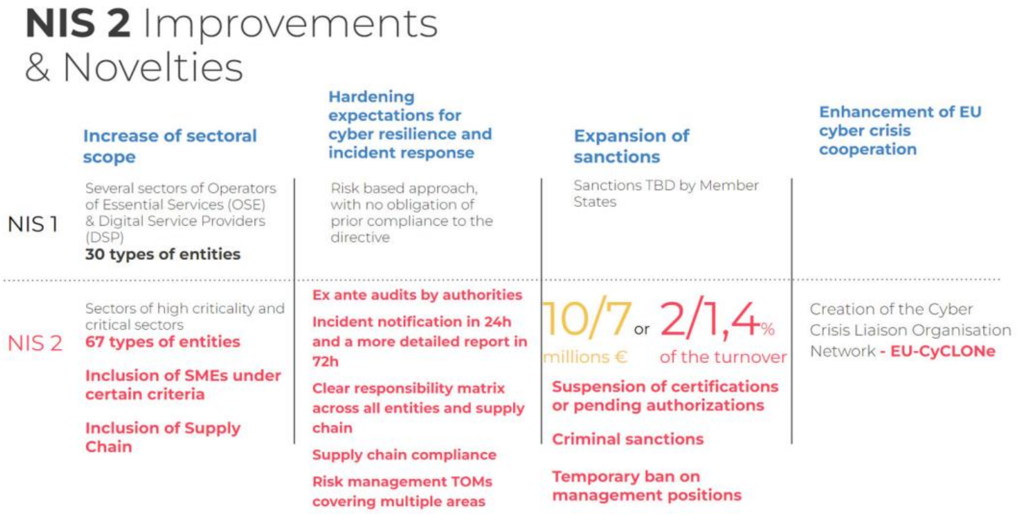
Digital services such as social networking services platforms and data centre services

Postal and courier services

Manufacturing of certain critical products

Figure 3: *Expansion of NIS2 compared to NIS.*

As indicated in Figure 1, the scope of critical industry has expanded in NIS2 to include also ‘providers of public electronic communications networks or services.’ This means that telecommunication operators are included under this legislation, and they must apply their operations to comply with this legislation.



NIS 2 Improvements & Novelties

	Increase of sectoral scope	Hardening expectations for cyber resilience and incident response	Expansion of sanctions	Enhancement of EU cyber crisis cooperation
NIS 1	Several sectors of Operators of Essential Services (OSE) & Digital Service Providers (DSP) **30 types of entities**	Risk based approach, with no obligation of prior compliance to the directive	Sanctions TBD by Member States	
NIS 2	Sectors of high criticality and critical sectors **67 types of entities** **Inclusion of SMEs under certain criteria** **Inclusion of Supply Chain**	**Ex ante audits by authorities** **Incident notification in 24h and a more detailed report in 72h** **Clear responsibility matrix across all entities and supply chain** **Supply chain compliance** **Risk management TOMs covering multiple areas**	10/7 millions € or 2/1,4% of the turnover **Suspension of certifications or pending authorizations** **Criminal sanctions** **Temporary ban on management positions**	Creation of the Cyber Crisis Liaison Organisation Network - **EU-CyCLONe**

Figure 4: *Main changes between NIS and NIS2*

Therefore, as it is now established, NIS2 is European union level legislation that needs to be followed by several industries, including telecommunication operators. What is it that companies must follow and fulfil. In this chapter the NIS2 items will be examined one by one to determine their meaning to the overall cybersecurity landscape. It is also good to mention that, NIS/NIS2 is linked to ISO 27001, NIST CSF, and ISA/IEC 62443 standards. NIS/NIS2 has many common and shared items and interests with the existing cybersecurity definitions. The following list describes on a high level what must meet be met at minimum level:

NIS2 describes thirteen main areas in cyber security, which organisations must notify as part of their cybersecurity plans and resilience.

1. Risk management and information system security i.e., having a proper process of identifying, evaluating, and managing risks. Information system security involves making sure computer systems and networks are protected against unauthorized access, theft, and so forth.

2. Incident management and reporting i.e. incident types must be identified and categorized by their severity, impact, and coverage and given related criticality level, incidents must be found, which means monitoring of the computer systems and networks must be established, resolution activity process must be in place and after incidents are solved, all of those must be recorded and reported accordingly.

3. Logging and detection are very close to incident management, here logging provides the data for detection. This area is an essential part of every company’s cybersecurity strategy.

4. Business continuity and backups, i.e. Business continuity is a plan which the companies make to ensure business activities can be carried out and continued even when something hinders the services and networks. Backups are a crucial and tangible part of the continuity plan.

5. Supply chain security and monitoring i.e., this part is one of the newest addendums compared to NIS and NIS2. All large companies use subcontractors and purchase their computer systems and network parts from third parties. Usually, security is handled through contracts, but NIS2 requires more. Supply chains must be audited regularly, and their activities and products must be monitored by regular cheques. This provides security and quality.

6. Secure system acquisition and development i.e. this refers to the process where systems to be acquired are designed, created, tested, and maintained in a way that it meets the security requirements set to it. This is an area that is very complex and sometimes time consuming. Even the specifications for the requirements require thorough and consistent expertise work.

7. Assessing the effectiveness of security measures, i.e. This is an essential part of any company's cybersecurity strategy. Once the security measures are implemented, they must be verified. There are several ways to assess these measures like, penetration testing, vulnerability scanning, intrusion detection, prevention systems, reviewing network, system and security logs, and surveys with staff. This assessment work also needs to be a continuous procedure to keep the cybersecurity measures up to date.

8. Cyber hygiene practises and training, i.e. this part is very practical, meaning that companies and individuals keep their basics in good shape. The basics can be defined, such as suing strong passwords, keeping software updated, enabling two-factor authentication, avoiding suspicious links and attachments, backing up data regularly, using antivirus and anti-malware software and educating yourself and others with the latest cybersecurity information, trends, and knowledge.

9. Encryption, i.e. This means that all business-critical data should be encrypted and protected. There are numerous ways to encrypt one's data,

and companies will find the most suitable method for their needs. This is also qn area where legislation overlapping is found. This is also a business continuity item, like in the case where the data is lost to hackers, but since it is encrypted, the hackers cannot use it and business secrets remain unharmed and secure.

10. Human resource security, i.e. This item might seem self-evident, which it is not. The main idea is to ensure that employees and contractors know their responsibilities and are suitable for the roles they are considered. In practise this means that, for example, prior to employment or contract signing, background verification is done, and during employment contract parties are ensured that they know their responsibilities and are trained on cybersecurity policies and procedures. Also, when the employment or contract is terminated, access to systems is closed and the employee and contractual party are aware of any obligations to respect the information security.

11. Access control i.e. is a vital element in cybersecurity. Here it is determined who is allowed to access what, when and why. It is also part of this that companies know who has what access to what and where and why. There are multiple ways to establish access control, to mention a few: discretionary access control, which provides case-by-case control, and mandatory access control, which is popular in government and military contexts. Role-based access control, where the aim is to provide users with only the data they need and nothing more. Attribute-based access control is the most granular access control mode. Zero trust…and so on. Point is a working access control is mandatory.

12. Asset management, i.e. Usually companies have their assets documented and they know who has them and what they are used for. In context with NIS2, it goes deeper. Assets need to be identified, tracked, and managed so that they can be used and protected effectively and efficiently. Also, a layered solution must be in place. Certain assets are more critical than

others, some assets need proper lifecycle management and development to maintain usability. Therefore, asset management controls must be in place.

13. Multi-factor authentication (MFA) i.e. as mentioned before, is part of the access control but is highlighted in NIS2 separately. MFA is a security mechanism where users provide two or more ways of authentication before accessing a system or an application. This reduces the risk of unauthorised access by malicious parties.

The above list is not comprehensive and complete. The items listed previously are the main points to be noted.

Since NIS2 is a directive, a law, it does not specifically dictate how these demands are to be fulfilled. Here companies can choose multiple ways to take this in to practice. In the following picture a few shortlisted frameworks are compared against NIS2 demands. Each entity and company decide what they want to use as a control mechanism to ensure compliance with every NIS2 requirement. The Finnish telecommunications company that is under study in this thesis chose ISO27001 as its main framework to be used as a control mechanism for NIS2.

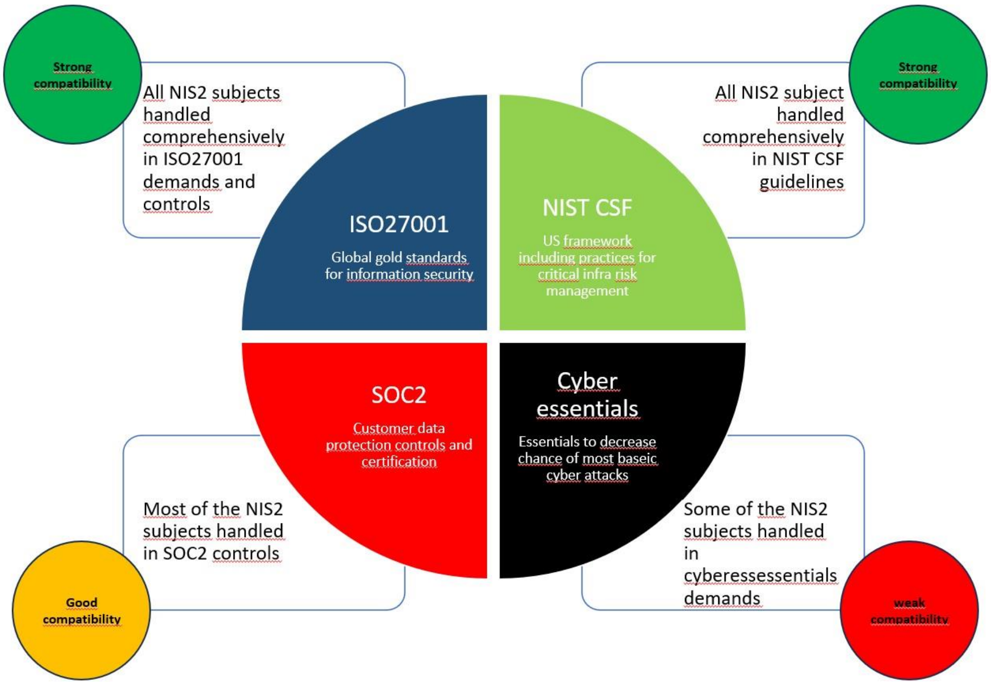

Strong compatibility
All NIS2 subjects handled comprehensively in ISO27001 demands and controls
ISO27001
Global gold standards for information security
NIST CSF
US framework including practices for critical infra risk management
Strong compatibility
All NIS2 subject handled comprehensively in NIST CSF guidelines
SOC2
Customer data protection controls and certification
Cyber essentials
Essentials to decrease chance of most baseic cyber attacks
Most of the NIS2 subjects handled in SOC2 controls
Good compatibility
Some of the NIS2 subjects handled in cyberessessentials demands
weak compatibility

Figure 5: *Which NIS2 control method to choose?*

2.2 Finnish Law 917/2014: Act on Electronic Communications Services

There are also local Finnish national laws regulating this “cybersecurity” area. The jurisdiction in here is with the Ministry of Transport and Communication and Finnish Transport and Communications Agency (Traficom). The Finnish government made their first law package in this area 2014 i.e. Act 917/2014, which of course has been updated until recent days. (1207/2020).

The objective of the act is stated in the act as follows: (direct quote)

“The objective of that act is to foster the provision and use of electronic communications services and to ensure that everyone across Finland has access to communications networks and services at reasonable conditions. A further objective of the Act is to secure the efficient and <u>interference-free</u> use of radio frequencies, to foster competition, and to ensure that communications networks and services are technologically advanced, of high quality, <u>reliable, safe</u>, and inexpensive. This Act also ensures the confidentiality of electronic communication and the protection of privacy."

The underlined parts of the Act objective are of interest to this study. It should also be noted that Traficom also issues regulations under the law to clarify certain specific areas, i.e., to be described in the next paragraph.

The interference free term mentioned in the act is related to radio frequencies, which can be interfered by various cases. If a case like this occurs, the owner of the radio frequency licence can apply for activity from Traficom and ministry to protect the frequency. How? It is something that is not defined in the act or any other regulation and will be defined case by case. Typical interference is radio frequency activity with equal of greater power in the same geographical region, like radars, etc. Also, a false base station might come into question here. It is also stated that Traficom is the official government instance in charge of cases like this.

The confidentiality of electronic communication and the protection of privacy is a bit more complicated. It can be divided into two main parts: communication between the customer and the operator and communication between the operators. In this part, the operator knows who is calling or using data to conduct the billing process. Then, the operator is allowed to know more if necessary to correct any network faults. Customer data cannot be examined if there is no customer complaint attached to it.

When transferring information between operators, the same confidentiality towards the end customer needs to be upheld, but in case of faults or technical solutions, information can be switched. No business secrets are to be endangered.

2.2.1 Traficom Regulations 66 and 67

The regulation issued by the Finnish Trasport and Communications Agency (Traficom) specifies information security requirements for telecommunication operations. Both regulations are enforced and in use today.

M66 which titles as “Disturbances in telecommunications services” defines the objectives, scope, and procedures as follows:

The objective of M66 is to ensure the detection, removal, and prevention of disturbances and threats against public communication networks and services. To ensure that users, customers, and Traficom are informed about them.

The scope of this regulation covers any disturbances in public telecommunications services, i.e., events and incidents that disturb or threaten the functionality of information security. This regulation applies to different types of communications services, such as telephone, internet, SMS, email, and mass communication services. The regulation also defines the severity grades of incidents based on their impact on communications services, users, and customers.

The procedures expected to be implemented by this regulation are as follows:

1. Monitoring functionality and information security. This means that the telecommunications operator must constantly monitor its communications networks and services to detect and prevent disturbances and threats and have adequate systems and procedures for receiving and analysing disturbance notifications and alerts.
2. Management of events that disturb or threaten functionality or information security. The telecommunications operator must have documented instructions for addressing and removing disturbances and threats and to minimise their impact. The telecommunications operator must also be prepared to take necessary measures to remove any significant disturbance or threat at any time of the day and inform Traficom of, any significant reduction in its management capacity.
3. Notifying users and customers of disturbances. The telecommunications operator must notify users and, customers of disturbances that affect the

functioning of its communications networks or services that last more than 60 minutes and affect more than 250 users and, customers. The notifications must made online, by phone, and through direct contact with customers and must contain relevant information about the disturbance, such as its cause, impact, duration, and measures available for customers.

4. Notifying Traficom of disturbances. The telecommunications operator must inform Traficom of disturbances of severity grades A, B, or C that have lasted for more than 30 minutes, by a preliminary notification, follow-up notifications, and a final report. The notifications must contain information such as the communications network or service affected by the disturbance, the severity grade, the geographical area, the impact on emergency communications, the original cause, the course of events, and the measures undertaken to prevent the reoccurrence of the disturbance.
5. Statistics. The telecommunications operator must prepare statistics twice a year on the number of functionality disturbances and information security incidents detected and managed by the operator.

M67 which titles as “Information security in telecommunications operations” defines the objectives, scope, and key requirements as follows:

The objective of M67 is to provide information security requirements for public telecommunications services in Finland, based on the Act on Electronic Communications Services and EU legislation.

The scope of this legislation is to cover general and specific information security measures for different types of communications networks and services, such as internet access, email, SMS, MMS, mobile networks, and network slicing. The key requirements are as follows:

1. Risk management, where the operator must implement risk management practises to identify, assess, and mitigate security risks related to all services and networks that the operator operates.
2. Personnel security: The operators are expected to ensure that their staff members are trained in information security practises and are aware of security protocols.

3. Physical security means that there must be measures and activities in use to protect the physical infrastructure, data centres and all critical equipment from being accessed by unauthorised people, or that it is protected against possible theft or damage.
4. Network security, in here the regulation defines that there must be measures taken to protect network components, like firewalls, intrusion detection, and access controls.
5. Service security, where all operators are required to secure their services, like encrypting any sensitive data, filtering harmful content, and ensuring that the services remain available.
6. Incident management: All operators must have processes and procedures for handling security incidents, report any breaches of security, and coordinate responses to these threats.
7. Technical standards: This, regulation also outlines the technical standards that operators must comply with, especially within mobile networks and in IP-based public telephone services.

2.3 NIST CSF

If I were to start with an illustrative Figure of this framework, it most definitely is the one that the NIST society uses itself, which is of course included in this thesis. The NIST CSF (National Institute of Standards and Technology Cybersecurity Framework, USA) was first published in 2014 as a voluntary framework to help organisations manage and reduce cybersecurity risks. It was developed by NIST in collaboration with various stakeholders from the public and private sector. The NIST CSF was updated in 2018 to version 1.1, which added some enhancements and clarifications based on feedback from users and experts. The NIST CSF 2.0 was released in 2024 and, incorporated new features and resources to address the evolving cybersecurity landscape and challenges. The NIST CSF 2.0 provides a comprehensive and flexible guide for organisations to improve cybersecurity resilience.

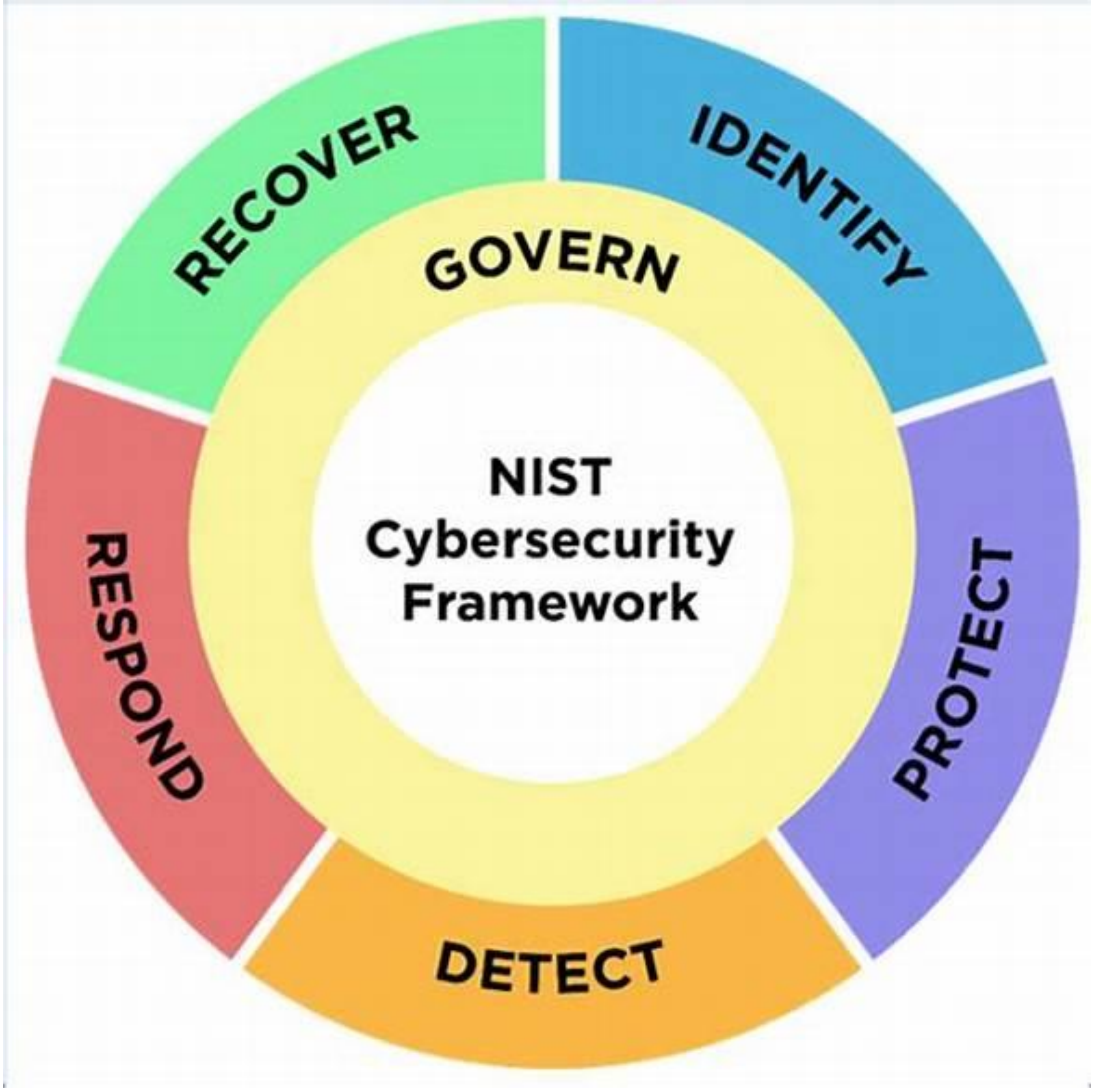


Figure 6. *Illustration of the NIST CSF main points.*

The main points of NIST CSF 2.0 are rather easily described. NIST CSF offers high-level outcomes that can be used by any organisation, regardless of its size, sector, or maturity. These outcomes help organisations better to understand, assess, prioritise, and communicate their cybersecurity efforts. Although the NIST CSF is flexible, it does not describe how the outcomes should be achieved. It links to resources that provide additional guidance on practises and controls to achieve the outcomes. The recent NIST CSF added new function called ‘Govern’, where it aims to evolve and presents an expanded scope. Lastly, NIST CSF emphasises **target profiles.** This involves understanding, assessing, and prioritising actions needed to mitigate risks and achieve cybersecurity goals. Overall, the NIST CSF provides a comprehensive and flexible guide for organisations to improve their cybersecurity resilience.

In the Figure 6 can be seen the NIST CSF main areas, and in the following, the areas are described generally.[6]

Govern

In this instance, a company or other party must understand and assess specific cybersecurity needs. The company's risks and needs must be determined. A risk strategy needs to be developed to mitigate risks and establish a defined way to create risk management policies. Companies also need to develop and communicate organisational cybersecurity practises for their specific companies. There is more, this organisational cybersecurity practises need to be taken into use in the supply chain as well. Companies need to develop a way to monitor and overlook that the supply chain is also in shape. When mentioning 'govern' it means that all the above requires continuous oversight and checkpoints to ensure that it is at the desired level.

Identify

Identifying the things that need to be safeguarded is essential. Companies and other instances, when following the NIST CSF, need to identify all their critical processes and assets. They must maintain inventories of hardware, software, services, and systems they have. All the flows in and out and between need and to be documented. Identifying does not stop here. Threats, vulnerabilities, and risks to assets must be identified and noted. Then, to follow the illustrative Figure 6, there should be a circle here too, and it is to implement lessons learned and used practise inside the company.

Protect

Where to start under the big umbrella of "Protect"? According to NIST CSF, that is where companies and other instances should start worrying about how to manage access to various systems. How can we ensure that the right people with proper tasks have access to the needed systems and resources? The user must be authenticated. In Finland, for example among the operators, the new employees must get security cheque validation from the police. Then there is managing the access management, access lifecycle, etc. Users need to be trained to be aware cybersecurity policies and procedures. All company devices need to be protected and monitored against viruses and non-accepted access. The data itself need to be protected and stored in a secure place, perhaps with multiple layers and levels of data sensitivity? The data needs to be encrypted, and as such, the encryption methods should follow technical evolution. Maintain and manage the software. This is the same topic from another perspective that was mentioned in the introduction about software producing companies. Therefore, even if the software companies create patches, it is not self-evident that those patches are installed in due time into the systems. Finally, is the backup process. It needs to be done on a regular basis, with intervals that are adequate to the system in question.

Detect

Here, the obvious thing to do is to monitor networks, systems, and facilities continuously. This monitoring also requires constant development and items from lessons learned., finding new indicators of events and possible incidents. When monitoring systems, the activities should be clear on what to do if events and incidents do occur. Those need to be determined and analysed to evaluate the impacts and scope of things. The last main point in the ’detection’ section is to provide information on the adverse events to authorised personnel and into the tools used here.

Respond

Then, when it is time to respond, it means that when a company faces an event or incident that needs attendance, they are prepared to execute an incident plan either by themselves or with relevant third parties. In this section, it is also imminent to categorise and prioritise incidents and perform the proper escalation/elevation needed. The need to collect and secure information about the incident so that it can be responded to due to facts and for future analyses after the immediate incident is handled. Notification of internal and external stakeholders is required. This is of course done in consideration of company policies on sharing data and information. To further develop a company’s response capabilities, it is sometimes good to ‘sandbox’ the incident. This means containing and eradicating the root causes or happenings of the incident.

Recover

The recovery section starts with understanding who plays roles and responsibilities in the recovery activity. Is that an internal and/or external party? The companies and other instances should have a recovery plan in place and that should be ready for execution as well. Since companies are executing, they might as well double cheque all relevant areas connected to recovery. Finally, in this section is again the communication, that recovery has been done and how successful it has been? Again, following the policies, the company has set to itself and the relevant parties.

Therefore, all in all, NIST CSF offers good guidelines, and its current version is close to many other guidelines available in the world, like NIS2 or ISO27001. However, it is not entirely a matter of taste. These guidelines can focus on high-level matters down to the last bit detail at hand. Choosing here is something that is good for giving some thoughts in the companies’ security departments.

2.4 ISO 27001

ISO has some history; it comes from the International Organisation for Standardisation. It is an independent, non-governmental, international standard development organisation, where member countries have their representatives participate in standardisation work. It was founded at the beginning 1947. So far, it has published over 25 000 international standards covering large amounts of technology and manufacturing business areas. In 2022, there were 167 national members, and it practically covers the whole globe. Their standards are named simply by stating the ’ISO’ and agreed numbering. In cybersecurity case, it is as in the subject the ISO 27001. It has sub-numbering and so on. The ISO organisation itself does not issue certificates. The certification or registration parties are responsible for granting certificates and conducting company audits. These bodies are independent of the ISO. There is a system to safeguard the bodies integrity, and it is also monitored and verified that no foul play is conducted by the parties responsible for granting the certificates. It is also appropriate to mention that Finland has developed a national tool for the government to audit information security, Katakri [9]

Katakri 2020
Tietoturvallisuuden auditointi-
työkalu viranomaisille
Kansallinen turvallisuusviranomainen

Figure 7: *Katakri*

Katakri is an information security auditing tool used by Finnish authorities to assess organisations’s capability to safeguard classified information. The scope of Katakri is not limited to government parties, but it can also help private companies and organisations in enhancing their security practises. Katakri has minimum security requirements based on national Finnish legislation and international obligations. The latest version is from 2020. In the company that this thesis focuses on, certain functionality is audited against Katakri. This thesis does not focus further on Katakri.

Another national tool to audit cloud service security is, PiTuKri [10].

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)

Traficomin julkaisuja 13/2020
PiTuKri – versio 1.1 – maaliskuu 2020

Figure 8: *PiTuKri*

The free translation of PiTuKri from Finnish to English is as follows: “Criteria to assess the information security of cloud services”.

The main objective of PiTuKri is to improve the security of authorities’ information that needs to be kept secret when processed in cloud services. PiTuKri was prepared based on Finland’s national needs but also considering international legislation and principles. PiTuKri covers various aspects, including security management, personnel security, physical security, communications security, identity and access management, encryption, and operations security. These definitions in PiTuKri are familiar from the NIST CSF and ISO 27 0001.

ISO 27001:2022 (the latest version) [7] then. The purpose and scope of this study is to specify the requirements for establishing, implementing, maintaining, and continually improving and information security management system within the organisation in question. This standard applies to companies and other entities of all sizes. Big or small. IT offers a framework to follow and implement. Being an audited company with enforced ISO 27001 certification confirms to all other stakeholders that the company has applied the system to manage risks related to data security. It is, however, not almighty, but a significant amount of dedication is in place. By implementing ISO 27001, companies have resilience against cyber-attacks. To obtain the latest version and document description of ISO 27001, it is commercially available at the ISO.org website for actual cash value the iso.org defines at any given time. There are over 100 certification demands that I will go through in a very broad and general manner. The reason for going through this massive number of descriptions is the fact that the telecom operator in question for this thesis has chosen ISO 27001 to be the main method of use for which NIS2 compliance is met. At the same time, the company hopefully gains official ISO 27001 certification. This means that ISO 27001 is probably the most tangible control method for implementing any security requirements. The following listing goes directly into the point without describing the other general items that one must do while implementing any ISO certification. [8]

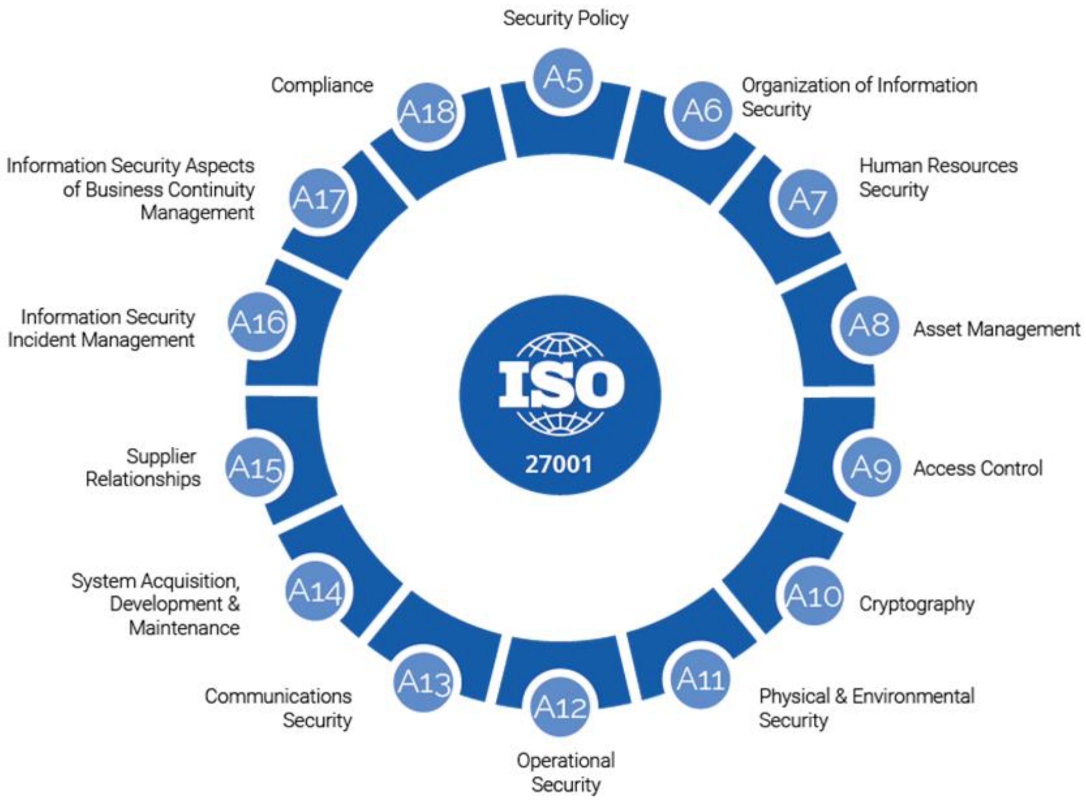

Security Policy
A5
Organization of Information Security
A6
Human Resources Security
A7
Asset Management
A8
Access Control
A9
Cryptography
A10
Physical & Environmental Security
A11
Operational Security
A12
Communications Security
A13
System Acquisition, Development & Maintenance
A14
Supplier Relationships
A15
Information Security Incident Management
A16
Information Security Aspects of Business Continuity Management
A17
Compliance
A18
ISO
27001

Figure 9: *ISO 27001 and its principal areas*

The areas in the picture and in text vary somewhat, with the numbering changes over versions and categorisation procedures at some given time.

Area 1: Encryption, management of encryption, principles of using the encryption, and controlling the encryption keys.

Area 2: Physical and environmental security, security zones, physical security zones, control of physical access to sites, offices, data centres, etc.

Area 3: The protection of offices, other spaces, and equipment, protection against external and environmental threats, working in security zones, and, delivery and hauling areas.

Area 4: Devices, protection and placement of devices, basic services in devices, and security of physical cabling.

Area 5: Maintenance of the devices, removal of protected devices, how to protect devices and assets taken outside security premises, secure decommissioning of devices, including recycling.

Area 6: Devices without supervision, clean desk policy, secure usage of devices, guidance, and duties.

Area 9: Documented guides, change management, capacity management, and separation of development, testing, and production environments.

Area 10: Protection against malware and, backup procedures

Area 11: Logging, protecting logs, and admin, and user logging.

Area 12: Synchronisation (devices), management of software in production, software installation to production, management of technical vulnerabilities, limiting installations in user devices and, auditing mechanisms of information systems.

Area 13: secure communication environment, network security management, network management, securing network services, transferring data, data transfer policies, agreements and procedures, and electronic communication. Confidentiality agreements.

Area 14: Acquiring, developing, and maintaining systems, security demands concerning information systems, analysing and defining information security demands, protecting application services in public networks, protecting application events, development- and supporting process security, policy of safe development, management procedures towards changes in systems, technical audits of platforms after changes, restrictions and/or limitations concerning changes, principles of secure system design, secure development environment, external development principles, system security testing procedures, approval procedures of systems, testing material protection

Area 15: Relationships to supply chain and other third parties, information security with supply chain relationships, information security policies among supply chain partners, security of supply chain agreements, management of supply chain services, auditing supply chain services, and supply chain change management

Area 16: management of information security, procedures, and duties, reporting of information security events, reporting of information security weaknesses, evaluation of information security events and decision making in here, responding to information security disturbances, and learning from information security disturbances.

Area 17: Business continuity and information security, information security continuity, planning of information security, executing information security, auditing information security, fault tolerance, and ICT service availability.

Area 18: Complying with demands, applying regulative and agreement demands, immaterial rights, protecting recordings, conducting information security audits, applying security policies and standards, and auditing technical demands.

Area 19: information security policies, Company management guidance regarding information security, organising information security, internal organisation, information security roles and responsibilities, official governmental contacts, contacts to relevant stakeholders, information security in project management, mobile devices and remote working, policies concerning mobile devices and, remote working.

Area 20: Personnel security, before the start of employment, background cheques, during employment, management responsibilities, information security awareness and training, disciplinary process, and ending or changing employment.

Area 21: Management of assets to be protected, responsibilities of the assets, documenting the assets to be protected, ownership of the assets, acceptable use of the assets, and classification of information.

Area 22: Access control, business demands for access control, access control policies, access to networks and services, and access management. User registration and removal, issuing access, management of access issuing, user identification data management, access right re-evaluation, deleting or changing access rights, user responsibilities, access management of systems and applications, data restrictions, safe access, password management systems, control and management systems, source code protection with access control.

2.5 Summary of the Regulative Message

One must comprehend that regulation, laws, and certifications on whatever area of expertise are wide and thoroughly thought packages and that they require an extensive amount of time for anyone to fully understand what needs to be understood and make it clear for themselves. Usually also more than one person who understands it is better, so you can cross verify one’s views and agree.

It is then yet another thing to start implementing a regulation or certification. One needs to define and reserve resources, time schedule, and budget for the work itself as well as possible changes needed to make to the current surroundings to fulfil new demands. It is a good thing that the governmental party has recognised these facts and given time for companies and other instances to do the work required to be applicable to the new law or certification.

The legislative party has also motivated to the companies to find resources and financing for this work in the form of fines related to their global revenue. The fines can be a maximum of 10 million euros or 2% of the global annual revenue. Then, each company can build their own business case for this work and start finding resources and financing. So, it is compulsory!

However, despite the mandatory aspect, these regulations, frameworks, and certifications are made carefully and with the assumption that if the companies and other instances follow those guidelines, they are well protected against malicious activity from cyberworld bad elements. As stated in the beginning, there is a lot of that activity going on all the time, and if the companies neglect that, they might end up suffering larger financial impacts than the fines introduced by regulators.

As I mentioned before, companies do think carefully if there are other gains to be achieved other than fulfilling legislation and gaining improved cyber security. For example, getting certified might open new business possibilities, i.e., new customers, new partnerships, increased revenue, better brand credibility, etc.

3 Current State Analysis and Implementation

It is not that the company referred to in this thesis must start from scratch. Many things are already done properly at this point when referring to cybersecurity or NIS2. The legislation or certification that precedes NIS2 has already woken up companies. These include the General Data Protection Regulation, GDPR, Data Governance Act, DGA, Data Markets Act, DMA, ISO 27001, which can be partially applied or focused to specific area, local Finnish Katakri and PiTuKri audit demands, and so on.

There has been voluntary protection built against cybercrime from the very beginning of the digital era.

3.1 Finnish NIS2 Project Members View on Progress.

A short questionnaire was presented to the Finnish employees of the project. There are sixteen members of which eight answered the questionnaire. The questionnaire was administered in February 2024 and was conducted anonymously with company tools. These answers will be discussed further in the chapter “Discussions and Conclusions”.

The questions were as follows:

1. “Do you know that you are part of the NIS2 implementation project?”
2. “You have participated in workshops to define controls for some security questions? Have you found that valuable?”
3. “Do you know what is expected from you now and in the future regarding NIS2 EU directive?”
4. “What would you do differently or improve in the project?”
5. “What is good about the project? Your evaluation grade for the project between 1-5, where 1 is poor and 5 is very good”.

General view regarding question number 1: Seven out of eight agreed that they are aware that they are in this project. However, four of those seven said that more clarification on why they are involved, or what kind of responsibilities they have in there and in the future with results and services.

General view regarding question number 2: five out of seven answered yes or in an agreeable way. There were remarks like “the meeting were very security personnel oriented and service-related questions were not addressed” or “not very well prepared or informed beforehand”, “results of the workshops not shown”.

General view on question number 3: Six out of eight did not know what was exactly expected of them and only one knew for sure. Due to the secretive atmosphere, many respondents felt that they were unaware of future steps after the NIS2 implementation project and “go live” date.

General view on question number 4: In this case the questions were more open, so the answers were like as well. The main points focus on time spent and remaining. The respondents would focus on exact NIS2 requirements instead of broader and more detailed ISO 27 001 demands. The workshops should be targeted more to personnel which are responsible for those platforms and services and not to all. More funding was included in the Wishlist. Personnel do not like the ‘closed’ more or secretive feeling in the project.

General view on question number 5: The average score is 2,6. The comments were as follows: “it’s been good to go through the standards”, “its missing raising NIS2 awareness to everyone”, “it will eventually improve our ways of working more professionally and unified way”, “always good to have focus on security”, “let’s be polite and give them a 2 because of the effort”.
This is Appendix 1.

3.2 People and Training

Personnel in this company have been trained for many years with information security and in recent years on cybersecurity. This has also been mandatory. Some of the work includes handling customer information, and personnel have the right and obligation to know under what circumstances customer data and information can be viewed. (for solving customer problems and only for that!)

Cybersecurity training, however, has grown more when the attacks also targeted individual persons. DDoS attacks and SW patch delay issues to systems have been common knowledge for a long time in cybercrime scenes for telecom operators globally. I believe can be said as the general statement for the entire ICT industry.

Today, cyber- and information training has grown to cover more cybersecurity areas and is in good shape. Of course, people are people, and things vary. Despite the status remark in the last sentence, it must be said that people are the biggest vulnerability and need to remain as the focus area for continuous improvement.

When stating that the biggest vulnerability that can be considered is with people, it is the fact that the number of personnel participating in NIS2 implementation is only a few. When remembering GDPR implementation, getting personnel committed and increasing the knowledge on what is happening was totally at a different and higher level. Yes, NIS2 is more technical than GDPR, but when considering the personnel churn in the technical area and since the NIS2 demands are connected to tasks, equipment, systems, products, and services, there should be more information spread needed amongst personnel.

At this point of the implementation project employee training regarding NIS2 is non-existent. There is a good trend on general and hot topic cyber security micro trainings in the company all the time.

So, cyber security training is not forgotten, but things personnel need to know about NIS2 and how it effects on their daily lives after October 2024 are currently based on a few intranet articles. The general adaptation/coverage/hit rate on intranet article information amongst personnel is between 40 to 50% based on the company intranet report 2014. The assumption here is that this percentage of information penetration through intranet articles being released into company’s personnel has not changed much since 2014.

Employee training among NIS2 implementation project personnel is not higher than that among other personnel, and it relies on person own interest and willingness to learn NIS2 directives.

Here the NIS2 implementation project is lacking. The project, of course, has time until October 2024 for introducing this big time to general personnel, but since the project personnel is also lacking training, this becomes a challenge.

3.3 Networks

Networks have always been connected to an Operational Technology (OT) of a kind, the OSS. All network elements can be accessed locally, but they are behind physical locking and alarm-generating protection. Today, as technology has evolved and eavesdropping equipment can be fitted to very small places, a theoretical possibility is that the operator purchases infected connectors, which could be then installed with current processes and remain unnoticed for a period, depending on how much data these eavesdropping devices would send and what threshold are set by the operator monitoring the data flow. However, as said, it is theoretical since the instance trying to get these devices to the network would have no idea where they would be deployed and what data they could receive. Not all data are worth knowing. A massive spread of malicious devices for operator’s networks would cost a fortune for attackers and it would be found out, as it needs to be so massive.

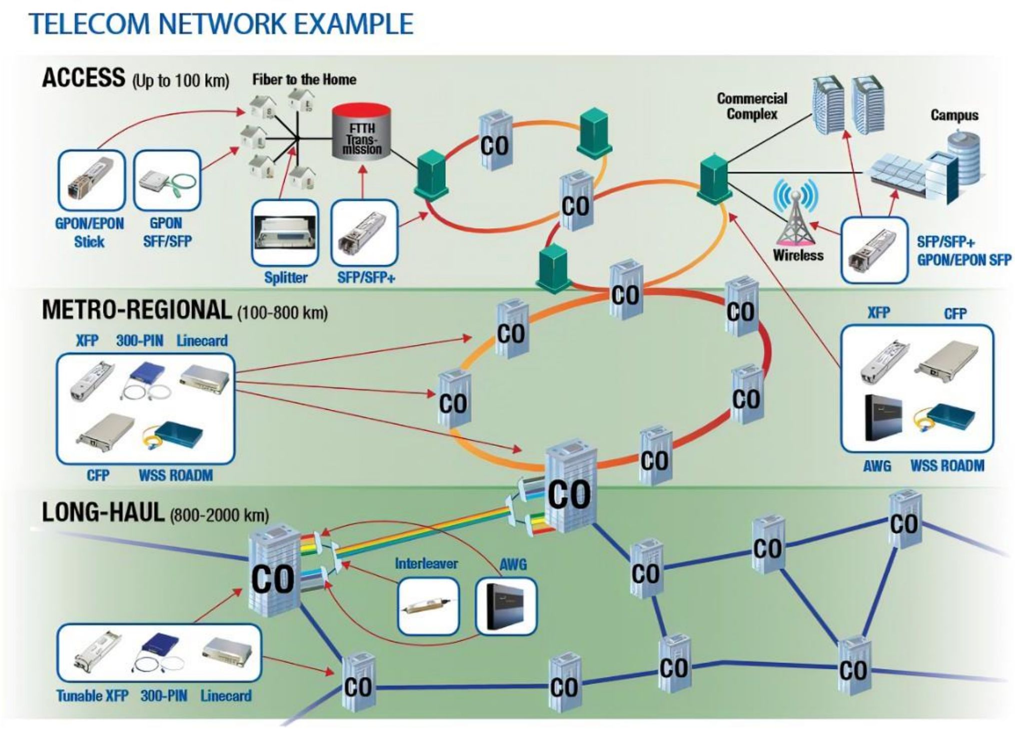


Figure 10: *Illustration on network composition*

Physical cables, Fiber cables are dug down to ground and could be accessed for malicious intrusion: however, there is always a breakage and therefore an alarm, that something is wrong. It will always be inspected, and it will reveal unauthorized connections.

Mobile network base stations and radio interfaces then. In Finland, all the operators operate 2G, 3G, 4G and 5G networks, of which the 3G network is one that all the operators have committed to closing in the coming years. The radio interface can be interfered with a false base station (often called stingray base stations) and an, IMSI catcher. In many cases, the user device must send IMSI (International Mobile Subscriber Identity) information to the base station via the radio interface, and for some short time it is unprotected. This IMSI number can be found and then in the false base station, it can be used to connect further data communication to this IMSI number and gain the call or data session information. In theory, that is. The data is then encrypted. In 2G, it is encrypted with A5/3, in 3G much better than in 2G, in 4G with 128bit encryption, and in 5G with 256bit encryption. In the future the quantum computers may decipher 128bit encryption in real time, but not today, and not to mention 256bit encryption which is the case in 5G communication. The legislation discussed in this thesis does not focus too much on network and system technologies. Networks and systems need to be run with the latest software version and, the latest patches. The project also assumes that networks are managed with best practise models.

3.4 Monitoring

Monitoring networks, systems, and services is a must, and it is done efficiently by the operator. Monitoring as a function is not simple. As mentioned in this thesis, all the event and alarm levels must be defined and categorised and then implemented into the monitoring system. Personnel must be trained to further develop the system and backup systems.

Even then, there are millions of events and alarms each month that need to be managed and incidents solved, and systems fixed. The Information Technology Infrastructure Library (ITIL) named process 'service operation' is well established and followed in the company.

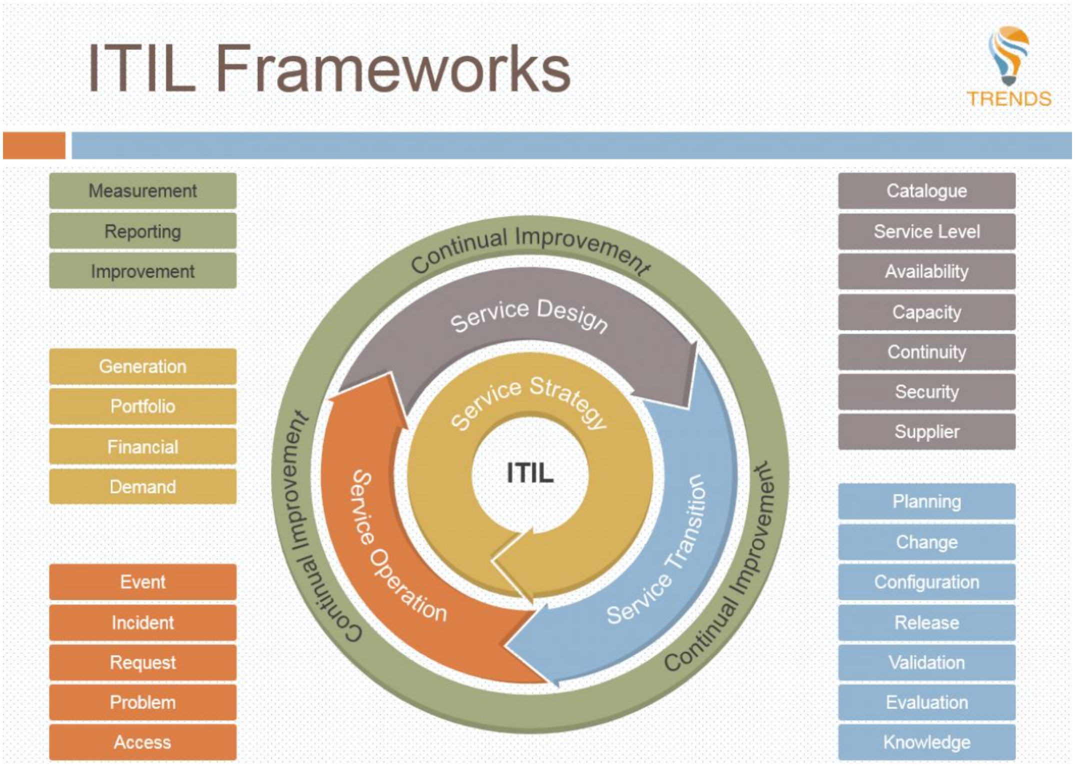


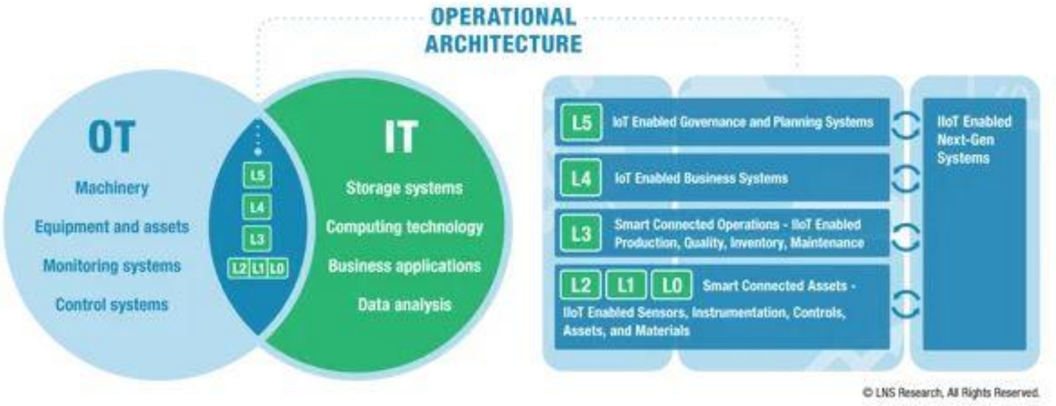
Figure 11: Illustration of *ITIL Frameworks*

Automation is the biggest thing now and ensuring that NIS2/ISO 27001 demands are 'hard coded' in there.

On the hardware/software side, the service operation function is also dependent on OSS and BSS systems, so it shares their vulnerabilities. The actual monitoring function is then safeguarded and secured in multiple ways against multiple threats.

3.5 Operations Support Systems

Operations Support Systems are operational technology and, OT network operating systems. These systems are usually connected to a certain product line of an equipment manufacturer. Telecom operators as product lines from Cisco, Nokia, L.M. Ericsson, Huawei, and maybe some more? All these manufacturers have OSS systems of their own against which the telecom operator's personnel must be trained. This is also a part of the technology area, where NIS2 does not focus too much on, ISO 27001 focuses to some extent.


OPERATIONAL ARCHITECTURE
OT
Machinery
Equipment and assets
Monitoring systems
Control systems
L5
L4
L3
L2 L1 L0
IT
Storage systems
Computing technology
Business applications
Data analysis
L5 IoT Enabled Governance and Planning Systems
L4 IoT Enabled Business Systems
L3 Smart Connected Operations - IIoT Enabled Production, Quality, Inventory, Maintenance
L2 L1 L0 Smart Connected Assets - IIoT Enabled Sensors, Instrumentation, Controls, Assets, and Materials
IIoT Enabled Next-Gen Systems

© LNS Research, All Rights Reserved.

Figure 12: *Illustration on how OT and IT align.*

The OSS is not connected to "outside" world, it is connected to the network in question and company-specific databases, monitoring systems, business support systems (BSS), and workflow systems. Personnel plays a crucial role here, they can do harm unintentionally by making mistakes or, in theory, deliberately. There is no special protection introduced in OSS systems other than what the manufacturer has provided and what the operator has built. A proper access management system applies here done by the operator, so even if one could have physical access to a node accessing networks, they would have to know the access credentials to the systems. If personnel do not have separate equipment to connect to network elements, an attack to the personnel's equipment and man in the middle attack has a small chance. However, time-dependent access is in use, and the attacker would not have long time to meddle with the network. Personnel equipment is protected by default and the granted access levels and access credentials narrow the possibilities of malicious parties for a network breach to close to zero. There are theoretical possibilities because networks are connected to networks, and by default, they are complicated and require careful planning and execution to be functional. In this complicated world, there might be cybersecurity vulnerabilities that have not yet been found.

3.6 Business Support Systems

Business Support Systems are systems connected to billing, commissioning customers to the networks and services, reporting, and agreement systems.

In many ways, it could be considered OT on the OSS side, except that it is not. BSS is more widely connected, and there are cloud instances and services used, which multiplies the BSS 'network' spread.

This makes BSS more vulnerable when considering cybersecurity. That is not a weakness as such, if the operator is aware of it, then adequate protection procedures can be introduced, and BSS and data can be safeguarded.

This is something that is partly in the 'technology box' when NIS2 is involved but also strongly in the information security area, thus making NIS2 and ISO 27001 more strong.

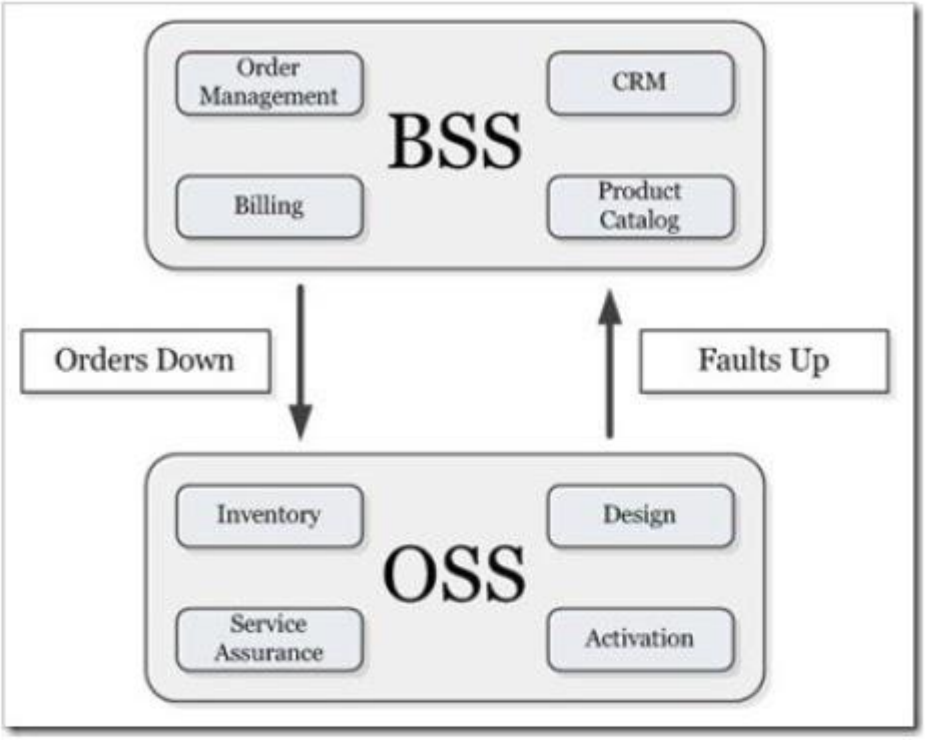


Figure 13: *How BSS and OSS interact*

The current state in the BSS area is also under change, practically all the time. There are old products, old billing systems (not outdated), and all sorts in between up to new products and new systems. BSS is also closer to traditional IT, with servers and operating systems closer to off-the-shelf products, not so closed systems like in OSS and network side. (even though future technology evolution moves to that direction in networks too!)

3.7 Services and Classic IT

Services in telecommunications are all connected to communications and various networks. For consumers, the usual services are mobile network subscription and mobile phone, internet connection either via mobile network or fixed network, landline home phone service. For enterprises, those are too valid for their employees, but enterprises need more extensive offering like connectivity, cloud services, managed services (SaaS etc.), Internet of Things (IoT), Voice over IP (VoIP), video conferencing, data storage, hosting, cybersecurity services for example.

The above-mentioned services are all of different age, capability, and condition, no matter how well they have been updated and maintained. These services are then built over numerous servers, with backup servers, firewalls, etc. The entire IT stack is behind there. These servers are then connected to networks and made available to all customers. Therefore, there is connection to live networks, the internet.

This is something that needs to be handled extra carefully. There is information security, confidentiality, GDPR, cybersecurity, and some more to consider and be applicable.

The current state here is “above the waterline”, there are no unauthorised accesses, the actual services are behind firewalls, and there are actions to mitigate, for example, DDoS attacks. This scenery is complicated to handle technically. Change management is something that should be on their toes all the time. The technology behind all services requires constant upgrades, integrations, refarming, and rehosting, and because many things are connected to many other things, the technical handling of things here is a handful of things. When you add the demands from NIS2, GDPR and so on, you multiply the complexity. Now, as stated, different areas vary from their security maturity level, but all areas are in acceptable terms, but there is not time to rest and not continue focusing on here plus more automation is needed. In general, one could say that, with automation, you can reduce human error very much.

3.8 Risks and Risk Assessment

The risk section is currently managed well in the company. There are other regulations and certifications that have driven this area. There is a risk management system that starts from individuals up to high-level strategy execution.

A process that evaluates, mitigates, introduces, or closes risks on a monthly basis. Everyone in the company is entitled and expected to speak up in case they see a situation that is a risk.

Risks are then evaluated depending on their severity on impact and monetary impact. The risk schema rises from the team level to departments and units up, to the top management. If mitigation requires extra resources or financing, it can be managed through normal budgeting because the risk process is integrated into all other processes.

However, the current state can benefit from a more detailed view in risk handling. There needs to be the high-level severity-financial impact view, but also practical hands-on risk-based activity, like does this service need multi factor verification (MFA) or not, what is the business continuity, and does this need other security measures or not. All this is based on the practical risk assessment which this ISO 27 001 is designed to deliver.

As mentioned earlier in this thesis, there is a risk management process in place in the company. This risk assessment meant here is connected to each asset and service and their current situation towards NIS2 and what is the probability in can be finalised during the project.

Of course, the risk assessment here includes the same classification as the company process with severity and monetary impact in a way in which the controls and activities are mapped against each other in the asset list.

When compiling the risk assessment, the usage and collaboration of project personnel is vital. The experts of each area play a key role in defining the risk levels and controls that are adequate. There must be a combined technical and financial/business evaluation done for the full risk assessment.

Now this is taking time, and getting all the needed personnel into this work is a challenge. There is some ‘automated’ risk evaluation done on assets and services that share similar backgrounds either in technology or business or in both. This is not ideal, but it saves time and resources and, gives acceptable results. This way of working does not prevent changing the risk levels in the future if seen as more suitable?

3.9 Documentation and Record Keeping

In general, the company in question has extensive documentation, as it has been a long-time requirement from commercial and technical points of view. The company has made many agreements with customers and, vendors, such as telecommunication manufacturers, cable manufacturers, power companies, insurance companies, banks, and third-party suppliers. There are product descriptions, service descriptions, guidelines, and manuals.

The technical part is also extensive, all technical equipment and embedded systems have manuals and system manuals, and every single equipment is documented on what is its place in networks, in the assets.

The current statement is good, but not perfect. There are minor things missing or the documentation is delayed, which might cause challenges to change management. As described in the chapter “services and classic IT” the landscape is so massive that the documentation is challenged to keep up with the dependencies. If then in the manual there is a note saying that the hard drive lifecycle is 6 years, is that picked up and notified in activity? There are IP routing tables that change quite often, and if the change documentation is delayed, it might cause incidents? Not every product or service is connected to every piece of hardware equipment and personnel expertise. Service or product alarm level definitions vary on the monitoring end based on things that are under change and therefore not always at the right level. Examples on documentation challenges are extensive and there is room for improvement. When it comes to NIS2 or ISO 27 001 demands, the company will survive.

The documentation and record keeping in the company in question for this thesis is on an adequate level. It is not perfect, and, in some cases, it is distributed to several instances so that it is a challenge to gain all the benefits that well-written documentation could provide.

The real challenge for documentation is timing, how up to date information is and when it is due? Sometimes documentation updates or generation lacks behind.

The record keeping is time wise ok since it is generated mostly automatically. That is not the case with documentation, and that is something to be developed in the future. For the NIS2 implementation part, the documentation is not the part that will drag the acceptance of the company capabilities towards the directive. The example is again if a certain hardware part has a lifecycle span of xx years, is that going to pop up automatically or does it rely on personnel's awareness of this subject? If the worst-case scenario is that the company cannot make backups or keep data safe because of this, it is a failure. Usually in the example cases, the manufacturer releases a technical note highlighting these issues and the company personnel should detect the urgency.

Documenting cybersecurity-related events and incidents, or guidelines and procedures, the situation is at a good level.

In my view, the company is very well equipped to support any documentation and record keeping demands that NIS2 introduces. There is always room for improvement, but still.

Systems that are used for storing documentation and record keeping are also improving with time. New ways are introduced to keep it safe and secure, distributed, and available for enriched usage for multiple benefits.

3.10 Identify Critical Assets and Services.

Identifying critical assets and services is fundamental. This part needs to be performed extra carefully. All assets, equipment, systems, networks, products, services, and knowledge need to be identified and considered, and analysed in this implementation project.

This work alone in a large telecommunications operator takes time and requires resources, dedication, and prioritising.

When this has reached an acceptable level, the project can start connecting more personnel into the project who have more in-depth knowledge about the actual systems then. In ITIL, there are defined roles like Information System Manager (ISM) and Information System Owner (ISO), which the company has also adapted. These roles and personnel connected to those roles need to be involved. Same goes for security and legal related personnel and product managers. The project management of course needs to up to date with driving the project and making sure the documentation of this part is done in the way it best supports the project and future needs.

Therefore, whilst describing what needs to be done above, it has been done so in the company connected to the thesis. The only part that requires more attention is the personnel connected at this point, but that is something the project can change as it progresses.

The actual list of assets and services was documented as sort of list, where the ISO 27001 controls were connected, and workshops were held with experts from personnel to define the criticality level and actions connected to that. The levels are business critical, mission critical, and non-critical. Based on criticality, their predefined controls needed to be fulfilled. This part of the work was time consuming and tedious.

3.11 Security Measures and Incident Response

Under this topic, there are two things that also require separata handling. Security measures are defined by the project based on risk evaluation and with different approaches based on service type and its composition in the network service structure. There can be multi-factor authentication (MFA) used in some cases, but some might require more and/or different protective ways. Security measures also include ways of working from a working point of view, how is the working process connected to a specific service or product, and can there be new or improved security measures? The security measures in the company are concentrating through data classification. Which data are sensitive, and which are not so sensitive? Then, the obvious, strict access control, like MFA mentioned earlier. In addition, the monitoring of accesses to networks and systems must occur. This can be defined as monitoring suspicious working hours, odd locations, etc. Encryption is part of the measures, training of people, regular backups, protection against malware, and awareness of surroundings.

Incident response is something that is usually is done after something has happened. However, these procedures must be defined beforehand as much as possible.

These procedures study critical and major alarm situations and responses to those, then there are incidents that do not necessarily produce alarms that need to be thought of and prepared for. Important note is that this incident response is connected to cybersecurity incidents.

So, the main points here that the implementation project is doing:

Preparation.

There has been an incident response team established sometime in the company and an incident response plan. The company has the necessary tools and knowledge for incident detection, investigation, and evidence collection. All these are things mentioned in the cybersecurity guidelines.

Detection and analysis.

Fast identification of cybersecurity incidents. Understanding the scope and usage of tools and competences. This is something that the company works with a lot and collaborates with authorities and cyber security companies. Yet again, an area with continuous focus.

Containment and resolution of cybersecurity incidents.

Isolation and mitigation of the incident, root cause elimination, and overlap of these phases. Again, an area that is in use at the company.

Recovery.

Restoring normal operations as fast as possible. Data restoration, if infected? Testing and validation that everything is ok. This part is also duly noted, and all employees have understood what prolonged downtime would cause to company reputation and income.

Lessons learned.

Ensure there are adequate post-incident activities and that lessons are learned so that no similar attack would be successful again. Continuous development of processes. This is an area that is not falling back, but one that requires constant focus and development.

3.12 Reporting and Notification

Topic with two things here again. Reporting is reserved for authorities and perhaps for large enterprise customers of this company. The notification audience includes consumer customers, small and medium businesses, and governmental authorities and large enterprise customers.

Therefore, reporting collects more cybersecurity incidents and events, and documented activity based on the incidents and lessons learned section. Notification is a one-time bulletin for everyone to be alerted or informed.

For reporting the data collection and a systematic approach to the whole process is important. Usually, reports are built with a specific structure and agreed measurement points, which are mutually beneficial and agreed. These measurement points can be changed at any time but are usually agreed for a longer period for data consistency.

There is a standard tradition in the company for these activities already so the changes in this area are minor, perhaps some tweaks on the reports?

The project also ensures that this area gets continuous focus and emphasis for NIS2/ISO 27 001 and other future needs.

3.13 Collaboration with Authorities

In Finland, the collaboration is concentrated to one governmental instance, the Traficom National Cyber Security Centre (NCSC) [12]. There are agreed and well-known procedures in place to report any incidents and events with, for example, the telecom industry and NCSC. The ISO 27 001 does not define Finnish demands separately, but this part is also in good shape. NSCS also assists companies and organisations with cyber security guidelines for various specific areas. This part is active and working.

NSCS keeps publishing active alerts from known cybersecurity incidents and informs companies and organisations nationally.

Traficom is also a party that is the Finnish national instance responsible for assuring NIS2 implementation in Finland with the companies and organisations in scope. Therefore, reporting on the progress of NIS2 implementation in the company is ongoing towards authorities.

The project ensures that all national collaborations is done accordingly.

3.14 Resources and Budgeting

In the project definition, the needed resources, dedicated time of key personnel, and monetary budget for possible IT and other changes were safeguarded. Time as a resource is scarce and might be function that needs to be revisited.

Time as a resource that is not flexible, if changes are needed, it will take time to develop concrete demands, gather personnel availability, rewrite code, and adjust all that to the currently popular Agile SAFe [13] way of working and getting it to exactly right agile release train.

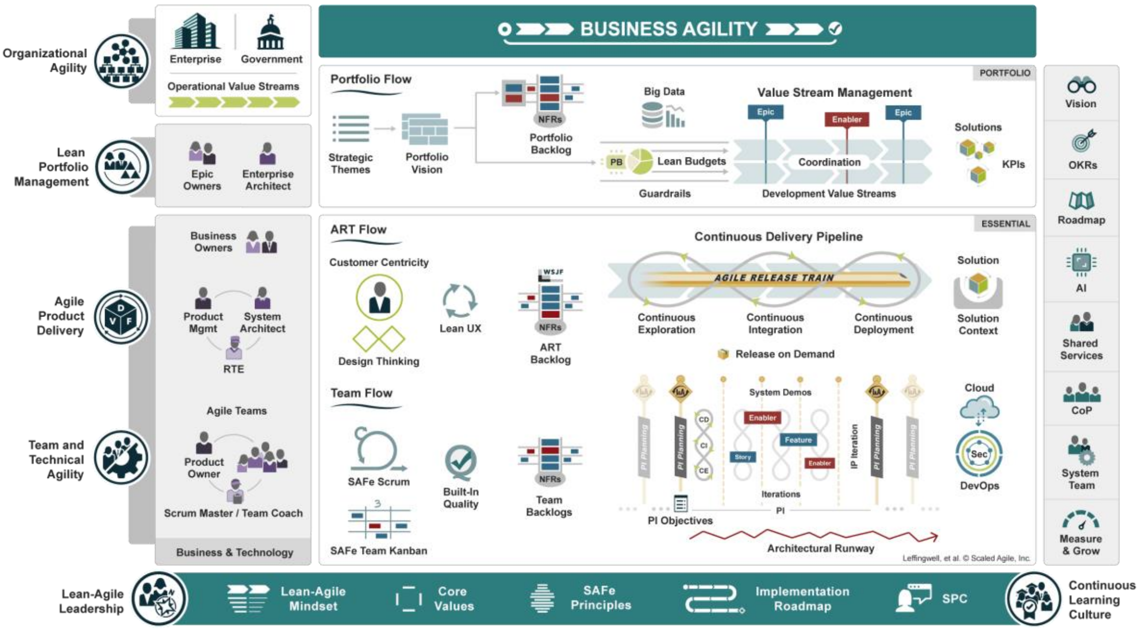


Figure 14: *Illustration of the Agile SAFe framework.*

However, the need for large IT changes in the company is minimal, since the main cybersecurity and information security measures have been taken into practise for some time. However, it is not 100% sure that, every system is up to date with NIS2 and ISO 27 001 demands, and this gives the project uncertainty towards available time against the demands. This uncertainty is irrelevant to personnel resources and monetary funding.

So, in here, personnel time is not an issue, nor is funding. The main vulnerability here is time.

3.15 Auditing and Testing

There is a consulting function that assists the company in driving and coordinating the NIS2/ISO 27 001 implementation project. The internal auditing and testing are aimed to be done by this consulting function.

Auditing is a straightforward item, going through all the points one by one and checking those points, for example, on three level grading, done, needs development, not done.

Testing certain cybersecurity functions on a company equipment, systems, and applications is yet another larger task.

Testing needs to be planned, test cases chosen, executed, and results evaluated and fixed like in continuous improvement. Testing will take time, especially if multiple testing rounds are required.

Testing is a part of the implementation project task list and will, be done. The biggest concern here is once again the availability of time.

3.16 Third-Party Suppliers and Contractors

To some extent, a new demand is introduced in NIS2 and that is the third-party suppliers and contractors must fulfil the same cybersecurity demands as the original company.

This demand makes sense since the old saying: “you are as strong as the weakest link” applies in this case. If a cybercriminal element can use a company third-party suppliers and contractors, they might as well access the original company. The threats are many.

In the project, all third parties are identified, listed, and documented, and contractual demands are implemented. Also, actual auditing of third-party activity in this area is planned. Therefore, it is not only placing written demands, but verifying those as well.

The main concern is that third-party suppliers and contractors are a wide audience and are multiple in numbers. Time might be a factor in here too. The positive angle here is that the demands now introduced by NIS2/ISO 27 001 are similar to what the industry is currently using in many cases.

3.17 Continuous Improvement

Why is a model for continuous improvement is good? This thesis began by painting the threat. Threat evolves, protection must also do so too to maintain a balance or preferably a slight lead.

In general, continuous improvement models answer the “why” question through a simple plan-do-check-act (PDCA) cycle example. [14]

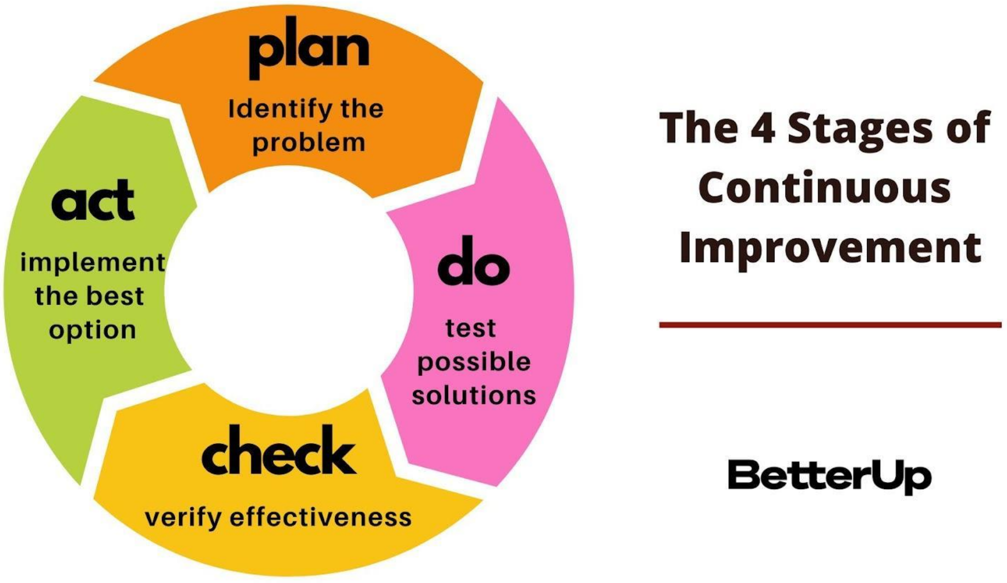


Figure 15: *Example of the PDCA cycle.*

This PDCA method to implement continuous improvement is just an example of how continuous improvement can be achieved.

In the company, the methods used for continuous improvement vary depending on the context and per division/department. The main point is that this is a widely used procedure across the company and is also an area where, the demands from NIS2/ISO 27 001 are certainly met.

In the implementation project this is also notified through the demands and preparation to fulfil those as expected in the NIS2/ISO 27 001.

4 Discussions and Conclusions

The main goal for this NIS2 implementation project is to ensure that the company is fully aligned with the directive demands in October 2024. That should be the clear number one target, and the rest of the ambitions should follow on a reasonable distance.

There should also be a clear vision of why NIS2 needs to be implemented. Because of increased threats in the cybersecurity landscape. In that respect, NIS2 is only a good thing for the company and for the industry. Not something you must do, and not something that people and personnel see as necessary evil. Training and information should follow and ensure that the interpretation of personnel concerning NIS2 is correct.

Risks were introduced in the previous chapters.

Now being part of the implementation project and when other members were interviewed, the goal is unclear. NIS2 yes, but also ISO 27 001. Is that too much? Should the focus be on NIS2-related ISO 27 001 demands first and the rest of the ISO 27 001 later when the needs of the legislation are fulfilled? This approach would save time. When looking at the interviews of the implementation project members, only half of the interviewed were fully aware of the fact that they were members of the project. Most of them agree that it is useful to participate in workshops. The most worrying part is that the majority of interviewed personnel are expected out of them regarding NIS2. It is a positive sign that, everyone was willing to give guidance on how to improve the running of the project. Now, if this interview is to be concluded, it does not give good remarks on scope and expectation for the employees on their future and NIS2 directive responsibilities.

Time is something that always needs to be followed and kept alive in project management. So far, nothing has been alarmingly late and there are no implications that the implementation project would fail, but there are significant risks that could be mitigated if taken care of immediately.

Time might become a risk when there is a specific date as a deadline. This is the case with the NIS2 implementation project. There are multiple things that consume time, and it is spent worthlessly. As we all might agree, sending an email to someone else takes a few minutes, but we do not know how much time is then gone when, the email is read, not to mention when the email message creates activity?

The multiple things are related to workshops deciding risk assessments, definition of measures to fulfil the NIS2 demands, possible IT changes, possible OSS changes, possible BSS changes, and agreeing and auditing supply chain demands. Even if the project is perfect in defining the project schedule, the risk of losing time is imminent. With this very complicated project, landscape time remains a variable that should be taken seriously. It needs to be self-evident that everything takes time, and if time could be saved by performing short cuts or going under the fence where it is at its lowest, take it. Saving time should be one of the biggest priorities in such projects.

People and training are areas of risk. Even though laws bind citizens and legal entities regardless of whether they are aware of the law or not, legal entities, companies are more expected to know the laws that are effective in their line of business. Companies are constructed by employees. So, this makes the personnel’s awareness of NIS2 vital for the company. Therefore, it is important that as many as possible in the company’s staff are aware of the NIS2 demands. The turnover of people in the company is approximately 10% annually, which means that every tenth person changes or leaves a position in the company. If only the ones currently working with services, systems, and platforms are introduced with knowledge on NIS2? What about the people who stand in as new service owners? Is there a training package concerning NIS2 then available? Documentation is good, but if the personnel do not know about it or are expected to Figure it out on their own, the company faces a challenge. Personnel not knowing the legislation does not put them in trouble, but the company is responsible anyway and is subject to fines defined by the NIS2 directive.

The need for training personnel about NIS2 is now shown to be vital. The next questions are how? When? By whom. Obviously, training needs planning, and this is not solved by sending the document to personnel about the NIS2 directive and say: “absorb”. So, planning and time are needed here too. Time is relative as we know, in training it is a bit more flexible, the training does not have the same deadline as the legal bindings.

5 Summary

It is a good idea to use ISO 27 001 certification demands as a control method to achieve NIS2 directive demands while simultaneously trying to get certified by ISO 27 001. A good idea does not necessarily mean that it is feasible or doable in the same exact package. ISO 27 001 is a very detailed and specific certificate and getting that done for the first time takes time. Maybe, too much time to reach the deadline for NIS2. ISO 27 001 will increase the workload of personnel working on the project.

Time is always a factor in any given project or activity everywhere. In a project way of working, there are some good standard ways to ensure its management. There are project milestones that either are reached on time or not. Time allocation can be divided based on resource allocation and estimated workload. Nothing fancy in there. If there are problems in time management, there should be a plan for mitigating them. There should be a plan on what to prioritise if time is an issue. As described many times in this thesis, some things are more important than others and those plans should be revisited as the project advances. Project resources can then be directed towards work which more benefit the number one target of the project.

Therefore, ensure the time is used wisely and fitted to the timeframe available as number one priority.

Training is another topic in this summary. Education of employees at all levels is crucial. Everyone in the company should know the following main topics:

- Understanding the NIS2 directive.
- Understand the basic cybersecurity practices in the company.
- How to handle any cybersecurity incident and how to respond?
- Why backups and business continuity are important.
- Safe use of company IT systems and networks.
- Everyone should know best practices for protecting sensitive information.

Then, there should be more dedicated training NIS2 directive lead personnel. I.e. the personnel who are responsible for making security measures into the systems and networks and make sure they stay that way and are updated. They should continue with topics like.

- Deep understanding of NIS2 and its impact on critical infrastructure.
- How to implement robust cybersecurity measures for critical assets?
- Develop incident response capabilities and risk management.

<u>The NIS2 directive implementation project must take care of personnel training and reserve sufficient time and resources to do it well.</u>

If either of these points, training of personnel, and/or time management are performed poorly, this project will fail at one point.

References

1 European commission directive: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive // 17.10.2023

2 NIS2 directive page: https://nis2directive.eu/nis2-requirements/ // 25.10.2023

3 European Cybersecurity Competence Centre, ECCC: https://cybersecurity-centre.europa.eu/index_en // 25.10.2023

4 European union agency for cybersecurity, ENISA: https://www.enisa.europa.eu/about-enisa // 25.10.2023

5 ETSI. Mobile-edge Computing, White paper. <https://portal.etsi.org/Portals/0/TBpages/MEC/Docs/Mobile-edge_Computing_-_Introductory_Technical_White_Paper_V1%2018-09-14.pdf>. Accessed 17 Dec 2023.

6 NIST CSF, National Institute of Standards and Technology CyberSecurity Framework, NIST Cybersecurity Framework 2.0: Resource & Overview Guide // accessed 13th March 2024.

7 ISO 27001:2022 certification // https://www.iso.org/standard/27001 accessed 13th of March 2024.

8 ISO 27001 certification items // ISO 27001 | Digiturvamallin sisältökirjasto accessed 13th of March 2024.

9 Katakri, Finnish governmental national audit tool for information security // Katakri – tietoturvallisuuden auditointityökalu viranomaisille - Ulkoministeriö (um.fi) accessed 13th March 2024

10 PiTuKri, Finnish governmental national audit tool ofr cloud services // Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) (kyberturvallisuuskeskus.fi) accessed 14th March 2024.

11 ISO 27001 demand frameworks // ISO 27001 | Digiturvamallin sisältökirjasto // accessed 17th March 2024

12 Traficom NCSC // Homepage | NCSC-FI (kyberturvallisuuskeskus.fi) // Accessed 18th March 2024

13 An introduction to Agile SAFe framework // SAFe 6.0 (scaledagileframework.com) // accessed 21st March 2024

14 Example of continuous improvement // Continuous Improvement: 6 Stages to Follow and Why It's Important (betterup.com) // accessed 21st March 2024

Appendix 1

.

Appendices

Appendix 1: Interviews of NIS2 Implementation Project Members

NIS2
implementation(1-8)

Appendix 2: List of Figures

12: Illustration of OT // Picking the Right Operational Technology Initiative to Drive an Operational Architecture Effort (lnsresearch.com) // Accessed 17th March 2024

13: Illustration of BSS and OSS Interaction // OSS and BSS Systems (nitscookbook.blogspot.com) // Accessed 17th March 2024

14: Illustration of AGILE SAFe framework // SAFe 6.0 (scaledagileframework.com) // Accessed 21st March 2024.

15: Illustration of PDCA cycle // Continuous Improvement: 6 Stages to Follow and Why It's Important (betterup.com) // Accessed 21st March 2024.