Joni Oksanen

Management recommendation for business-critical network infrastructure devices

Metropolia University of Applied Sciences

Master of Engineering

Information Technology

Master's Thesis

15 October 2023

PREFACE

This study was written during a challenging time in the author's life. The author had just gained a new role. The role presented new challenges to learn and overcome. During this thesis, the author got to know persons across the organization and managed to improve skills in other than just technology. The author also had a first child, for which the author needed to prepare more. The thesis was an eye-opening experience of gaining knowledge other than relying on the author's experience. It was a wonderful experience to learn about the collection of best practices, and the author had something to try to apply those practices to work directly. The most challenging step during the thesis was to think about scaling those procedures to a specific company and how they would work in the current organization's culture at the author level. The author would like to thank colleagues for helping to know systems outside the author's management. The author would like to thank the organization's supervisor, Petri Mäenpää, for encouraging and giving the author a starting point to expand their knowledge. This study also used Grammarly and Word to enhance its language. Lastly, the author would also like to thank his family for giving the author time to work on education during challenging times in our lives.

Hyvinkää, 23.04.2023
Joni Oksanen

Abstract

Author:	Joni Oksanen
Title:	Management recommendation for business-critical network infrastructure devices
Number of Pages:	52 pages
Date:	2 October 2023
Degree:	Master of Engineering
Degree Programme:	Information Technology
Professional Major:	Networking and Services
Supervisors:	Sami Sainio, Principal lecturer Petri Mäenpää, Development manager

Networking devices and their related protocols are seen as potential novel attack vectors in the organization. Zero-day vulnerabilities like Log4j have caused concern relating to network device management. These devices are a critical part of any connected company.

This thesis explores how the target organization could improve handling device management challenges. The organization wants to improve their readiness to oversee issues regarding the assets. These assets are not limited to hardware but also software-based systems. This thesis focuses on networking devices and systems that support those devices.

This work explores devices and their challenges in the target area. The main challenges in the target are related to device information, end-of-life management and communication relating the challenges. Then, NIST and ISO standards are studied to find solution suggestions for those challenges. Those standards are related to asset and security management systems. Then, based on those standards, the work suggests an improvement for the targeted company and tries to reason why work for this suggestion should be started.

This work resulted in the following suggestions for the company: improving asset management, consolidating device databases, and implementing technical risk management processes for explored devices. These suggestions contain a technological perspective instead of an organizational management perspective. The benefits of improvements can increase networking organizations' communication, awareness, documentation, and decision-making processes.

Keywords: Asset management, Risk management, Network devices

Contents

List of Abbreviations

Contents

List of Abbreviations

B2B	Business-to-business model of making business.
WLAN	Wireless local area network.
5G	Fifth generation of mobile technology.
SD-WAN	Software-defined wide area network deployment model.
NIST	National institute of standards and technology.
ISO	International organization for standardization.
ITIL	Information Technology Infrastructure Library.
SFS	Finnish Standards Association.
The U.S.	The United States of the America.
NCSC-FI	National Cyber Security Centre in Finland
UAS	University of Applied Sciences.
OSI-model	Open systems interconnection model.
IP	Internet protocol.
VLAN	virtual local area network.
SSH	Secure shell protocol.
SNMP	Simple network monitor protocol.
SLA	Service level agreement.
IPsec	IP security architecture.
SaaS	Software as a service.
ZTNA	Zero trust network access.
VPN	Virtual private network.
LAN	Local area network.
EOS	End of sale.
LDOS	Last date of support,
EOST	End of support,
EOL	End of life.
DDos	Distributed denial-of-service.
CIS	Centre for Internet Security.
CPE	Customer premises equipment.

1 Introduction

The study is for national network operator DNA Oy, part of Telenor. DNA Oy is a medium-sized corporation with approximately 1500 employees. DNA's business area is to provide connectivity service via its own or leased network for customers. This study focuses on the business-to-business (B2B) section and its managed network devices that are the foundation for the organization's corporate services. Network devices of this business sector are routers, switches, firewalls, access points, wireless local area network (WLAN) controllers and value-added systems of these pre-mentioned devices. These devices are varied and could be from different vendor partnerships. Network devices amount is in tens of thousands.

In the large customer segment, there has been an increase in the number of requirements for networking operators. These requirements are related to processes, quality of service, documentation, and fault recovery. These points are usually optional to be proven to exist by smaller B2B customers or consumer customers. Business sector customers need more than that to ensure networking operators' performance before the deal is made for connectivity services. Proving this performance is usually done by reviewing and providing documentation of said processes. Reviewing requires time from customers and the networking operator. The easier path could be to prove this by following standardization and getting processes standardized by outside organizations.

Customers also require services to prevent issues in their network instead of reacting to an existing issue. They also require that the networking devices deployed to their systems are responsibly managed and secured to prevent potential issues that might compromise their network or cause service downtime. Interruptions in the service could be costly to businesses since the services that DNA supplies impact customers directly. Operators have a unique role in enabling businesses to thrive, supplying them with a secure and maintained environment to do business in, and focusing on providing their products and services.

1.1 Business Challenge

The organization's challenge is managing devices securely and efficiently in a multi-vendor environment. The sheer number of subscription-based services and varied devices causes overhead for responsible persons. It should be explored how this overhead could be reduced or automated. The ways to manage these problems have usually been by limiting the sold devices to a specific vendor or device type and selling the bulk. The organization's device base is transforming because of new concepts like fifth-generation (5G) networks and software-defined wide area networks (SD-WAN), which require new devices and vendors that need support in addition to the old systems. These technologies are still new and constantly improved. Constant improvement causes devices and concepts surrounding these technologies to be constantly changing. New devices might come every year because of the rate of development. This constant change increases the variety of maintained devices in the environment.

Customers are now also aware of supplied vendors and demand certain vendor products or solutions that need to be tailored for those customers. This tailoring has led to increased device variance between customers.

This work aims to find ways to improve the system used to support these devices. These ways should also be based on known standards rather than the individual's experience. There should be a way to manage these varied devices effectively during their lifetime to increase the capacity of devices that fewer resources could maintain.

1.2 Objectives

This study recommends device environment management systems for development managers and system owners. The author is a part of the architecture team that is required to maintain and improve the technical aspects

of devices and provide guidance for deploying large-scale customer environments in the organization. Customer environments and how the organization manages those devices currently cannot be disclosed. This study only partially reveals the current state in its analysis. This study focuses on the following,

- Explains currently used device types.
- Explores challenges that organization faces with increased device types.
- Tries to find precedent from standardization that could solve those challenges.
- Present recommendations on what could be done to address those challenges.

In this work, the author generalizes the devices in question by type and tries to walk the fine line of not revealing too much but revealing enough to get the point across. This study could be used for similar challenges in other business areas with the same challenges in their field.

1.3 Method and Material

This study is conducted as applied research, aiming to answer specific problems and provide a solution based on known regulations and recommendations for the target organization.

This study uses the National Institute of Standards and Technology (NIST) cybersecurity framework V1.1 [1] as a base to explore standards relating to the devices in the target organization. NIST is a government organization of the United States of America (The U.S.) and provides recommendations for businesses in states. They aim to promote U.S. innovation and industrial competencies by advancing measurement sciences, standards, and technology. They aim to be world leaders in creating critical measurement solutions and promoting equitable standards. Their goal is to stimulate innovation, foster industrial competitiveness, and improve the quality of life. The organization was

founded in 1901 and is currently part of the U.S. Department of Commerce. They actively work with U.S.-based businesses to improve standardization related to their fields. Standardization in the U.S. is led by industry. NIST's role is to coordinate standardization efforts with these industries and the government. They also cooperate with similar agencies worldwide to make these standards consistent with theologies worldwide. Although only some of the information in the documents provided by NIST is required by Finnish authorities like Traficom, the information in this material generally applies to the same field. [2]

Traficom is a Finnish Transport and Communication Agency. They work in four selected fields of expertise. One of these is services for motorists. The services include but are not limited to driving licenses, vehicle registration and vehicle taxations. Other areas of expertise include: [3]

- Focus on transport services like sea and railroad traffic, railroad infrastructure, and road infrastructure.
- Provide expertise in services of digital connections where they provide regulation and licenses to use frequencies, which are critical to network operators.
- Operating National Cyber Security Centre in Finland (NCSC-FI).
- Provide security of communications for networks and services.
- Supervise and develop security in Finland.
- Provide situational awareness of the Cybersecurity landscape in Finland.

International Organization for Standardization (ISO) Standard ISO 27001 [4], which is recommended to be used by the Finnish Standards Association (SFS), is heavily used in this study along with SFS-ISO 55000 [5]. ISO 27001 is about managing security threats, and ISO 55000 is about asset management systems. These standards are explained in the theory chapter in more detail. The organization that publishes these standards for educational institutes and businesses that the study uses is SFS. SFS is a Finnish organization for standardization. They work closely with other standardization organizations. SFS ensures Finnish people and organizations can affect standardization and

regulation in their fields. They also ensure that Finnish people have access to standards in the Finnish language. They work together with ISO and the European Committee for Standardization (CEN) as their member. They evaluate and sell standards that are in effect in Finland. SFS is a non-profit organization that mainly finances its function by selling the standards. As their member, they follow regulations provided by CEN and the worldwide standardization organization ISO. [6]

ISO is a non-governmental organization of standardization. They have a global network of standardization bodies, of which SFS is a member. Their job is to develop international standards. International Standard is a documentation containing practical information and best practices. They help to make products compatible, identify safety issues, and share best practices with businesses and regulators. The benefits of standardization could be as simple as allowing two different network devices to communicate with each other. Standardization reduces the costs of operating said devices because one does not need to limit their network devices to a single vendor to provide functionality for their networks. They only develop Standards if there is a need for it. Standards are created by professionals from industry, academia, governmental, or non-governmental organizations. Their member's role is to identify said persons in their respective countries. They coordinate standardization efforts and validate standards by voting. ISO Standard is licensed. The author cannot use direct quotes of the work but will infer the material when it has influenced its writing, which is allowed under a general licence towards the education facility. [7]

This work will be conducted during a transformative period in the target organization. Security threats have encouraged the target organization to take action to ensure that current device management principles are up to date. Although this study is not part of the internal review, it is conducted from the perspective of the target organizations' corporate customer organization. The insight gained in this study could affect this team's management of the devices more closely than a higher level of review. One of this work's goals is to obtain insight into the device management principles for the internal review personnel.

The author obtained the recommendation to use the NIST Standard from the DNA Security development manager since it is readily available. Current state analysis will mostly be from the author's perspective since they are responsible for part of the mentioned device’s technical capabilities in the organization. For the other devices, the author has organized meetings with others responsible for obtaining the information from those devices and their current way of management. This information is not part of the thesis but has influenced the current state analysis chapter.

The basis for formatting this work comes from the Metropolia University of Applied Sciences (UAS) Template for Master Thesis 2021. [8] This document describes the formatting of the thesis and gives best practices for writing the work. This template recommends using Vancouver-style referencing in the thesis. Vancouver-style citations are familiar with Metropolia UAS. The author uses a referencing guide for Vancouver-style citations made by Monash University. [9]

2 Current State Analysis

This chapter lists objects related to the devices in the target organization. This chapter presents all the security or management related to a device in an organization's environment. This chapter will be heavily based on the author's experience managing these devices in the target organization. This chapter will also contain information obtained from meetings within the organization's device responsible and DNA security department influences. By exploring the device entities holistically, we might get insight into what aspects of the management of the devices need to improve the overall security management of said devices. This chapter brings forward challenges that device management has in target organizations.

2.1 Device entities

First, we will explore the devices themselves and what types are under the management of this part of the organization. What is the device's function in the system, what kind of management interfaces does this system have, and where are these systems located by nature in the environment?

Firewalls are devices that control what kind of traffic in the networks located in the system. There are a few types of firewalls for different levels of control on the traffic passing through. For our needs, we can generalize here that firewalls function as a boundary between networks. One of those networks could be a corporate, private, or public internet network. In this case, the public Internet is untrusted, and the internal corporate network is trusted. In a trusted network, it is considered that organizations know and control what it contains. In untrusted networks, it is the opposite. [10c Ch. 1]

Routers are devices that move traffic between networks. The router stores information about different networks in their route tables and decides the best path to the target destination using routing protocols and if the path is available. Routers can be in a trusted or untrusted network—routers usually just forward

traffic as efficiently as possible. Routers can also separate different networks in different route-tables. Different routing tables enable to separate networks from each other. They can also do other functions like switching or firewalls on a smaller scale. This performance is enough for small business's needs.

Table 1. Open Systems interconnection model. [11]

Layer	Short example
Application (7)	Programs
Presentation (6)	Formatting
Session (5)	Logical ports
Transport (4)	TCP, host
Network (3)	Packets
Data link (2)	Frames
Physical (1)	Cables

Switches are devices that forward frames instead of packets. A frame is a unit of data in the data link layer of the open systems interconnection model (OSI model), and a packet is a unit of data in the network layer. They differ by how they encapsulate the data they carry. The frame uses physical addresses of the devices called media access control addresses (MAC addresses), and packets use logical addresses that are internet protocol (IP) addresses. The above chart contains a brief description of the OSI model. This model contains seven layers and tries to characterize communication functions for networking and computer systems. [11] Switches are devices which extend networks physically from routers to clients like phones and computers. They are needed when devices in the target location exceed a reasonable amount to be controlled by a single device like a router. Switches can also separate devices to a different domain with a virtual local area network (VLAN). Usually, routers function as gateway devices for switches, but switches can also function as a router. These are L3 switches because they operate on layer three of the OSI model.

Access points are devices that also forward frames. They extend the network from routers or switches to a Wireless local area network (WLAN). They send data over wireless signals and extend the physical LAN network within the building. WLAN controllers orchestrate these devices. Access points can function individually, but this is not generally feasible since a single site can contain multiple access points with the same settings. This simple configuration makes managing these systems from a single source feasible.

Orchestrators are systems that manage the abovementioned hardware-based devices. They also manage the configuration of those hardware-based devices on a larger scale. They can be hardware-based or software-based. An example would be Wireless controllers, which control all access points on a specific site or customer. Orchestrators sometimes have integrated monitoring functionality.

Monitoring systems are devices that monitor the status of allocated devices. They could obtain information on devices using secure shell protocol (SSH), simple network monitor protocol (SNMP) or streaming telemetry. They are usually software-based and need an additional virtualization layer beneath. They are integral in ensuring and monitoring customer service level agreement (SLA).

Software-defined wide area network (SD-WAN) devices are the newest addition to organizations' devices. These devices combine routers' and firewalls' functionalities by creating an IP security architecture (IPsec) tunnelled overlay on top of a traditional network. These systems usually require an additional orchestrator that manages these tunnels and the configuration. These devices are usually vendor-locked to a specific vendor orchestrator, increasing the variety of devices since customers might want to acquire specific vendor products. Maintenance of these systems causes added challenges since they are vendor-specific.

In addition to SD-WAN, one of the new products consists of software as a service (SaaS) applications like zero trust network access (ZTNA) that is a replacement for traditional virtual private network (VPN) software. The target organization also

needs this software to use the service. This deployment and management of responsibilities should be determined in this case.

2.2 Device management information challenges

Based on the earlier chapter, a general understanding of devices that are the organization's responsibility can be formed. The crucial part of managing those devices is having up-to-date information on the devices—this information is required in the life cycle, monitoring, deployment guidance, debugging and SLA agreements. Once the organization has deployed something to the customer, they are responsible for said device as per agreements. They need to be aware of the status and function of the device and its history. This awareness enables the organization to meet the responsibilities of its stakeholders.

This chapter focuses on information gathered from the devices and the challenges of obtaining this information in the target organization. In this section, the author explores the devices mentioned in the earlier chapter. Target organization needs to know what information is collected and what kind of challenges there are to collect that information.

2.2.1 Collected information from the devices.

Below is a list of information the company needs to gather from the abovementioned devices. This information follows company-accepted best practices.

- organization identity.
- version.
- hardware.
- configuration.
- logging.
- licenses.
- performance.
- location.
- vendor.

Of this information, the most valuable information is the organizational identity of the service. Identity connects technical implementation to the sold environment. If there is a problem with the customer environment, the organization can match the customer site, contact and subscription to an actual implementation in the network.

Details like performance, configuration, and logging are related to support services of the products like SLA, and this identifies faults in the provided product. Configuration enables the restoration of the function of the old device in case of fault. Logging is a way for the device to inform potential problems and configuration changes in the network. Performance monitoring enables us to see congestion in the network and monitor the fulfilment of a customer SLA.

From an organizational security standpoint, essential values are vendor, version, and hardware. Vendors provide organization security notifications and updates to said versions to fix those issues and add more features as per support contracts. Knowing the version of a device gives the organization an

understanding of challenges relating to upgrading to a newer version when security or functional issue present in current firmware requires the organization to act. This way, organizations can implement controls to ensure that devices are up to date. The organization is also responsible for providing information on their devices related to their partners. This information is used to pay the support costs of the devices accurately.

Licences are paid features of the device. For example, WLAN Controllers must have licenses to manage WLAN access points. Licences also expire and need to be repurchased from the partner vendors. Licence amount information enables organizations to follow their status. Because they can expire or still need to be installed to enable product delivery, an organization can ensure the device's proper function by following this amount. There must be a way to manage these assets with monetary or operational value for the organization. Asset management is a way to manage this kind of information.

2.2.2 Challenges related to obtaining information.

One of the most apparent challenges in obtaining the required information from device entities is that there are hardware-based and software-based devices. They have different requirements and ways to collect information to manage the devices responsibly. These devices and their types are below table (Table 2)

Table 2. Device types

Device Entity	Device Type
Router	Hardware
Switch	Hardware
Firewall	Hardware
AP	Hardware
Monitoring system	Software
Orchestrators	Software or Hardware
VPN Clients	Software

The difference is that the software devices contain additional virtualization components in the servers in which they are located. They do not have dedicated physical components as hardware devices have. Information on these systems is not in the same environment as hardware devices. The number of software-based systems is also low in the organization network. The scarcity causes difficulties with maintenance because they only sometimes have the appropriate resources to maintain them. Since their management system does not overlap, these devices are maintained with lightweight models. This model means that these systems are not fully integrated into the organization. For those systems, only essential functions like backups and reachability are collected.

Hardware devices contain challenges; specifically, they have various places where they store collated information. There are a multitude of places where this information is stored. When there is a need to compile the information, it must be collected from all those separate systems that do not have integration. This lack of integration causes problems that take time and effort. One of these problems is visible in performance challenges. Diverse environments cause challenges in narrowing down the bottleneck of the system or fault location. It requires much manual work to compile a list that might narrow a performance problem to a specific device entity or a version within that device entity.

The benefit of hardware devices is that the way to obtain the information follows the standards. Therefore, information collection is conducted uniformly—for example, SNMP and Network configuration protocol (NETCONF). SNMP is defined in requests for comments (RFC) 1157 [12] as a way to communicate information and control network elements. This protocol is widely used across networking devices. [12] NETCONF is defined in RFC 6241 [13]. This protocol is a way to obtain configuration and state data from the device. The protocol's goal is to provide an interface to the device that closely follows the function of the device. [13] This protocol is not widely used but provides future networking management capabilities.

Challenges with hardware devices lie in the management types and environment of these devices. Device location also plays a part in these problems. Devices might be inside a customer environment in such a way that it is challenging to access DNA standard device management systems securely. Local area network (LAN) services are set up so that there is no direct path to manage these devices directly. These systems need to connect via a secure tunnel or connection to DNA services. These LAN environments also contain unique IP address spaces, with challenges connecting to organization management address space. As mentioned earlier, this has caused many ways to obtain the information from those devices.

Recently, connecting customer environment devices directly to cloud services where DNA experts could manage them has become possible. [14] This cloud-based solution uses the customer's Internet connection, regardless of supplier, to securely contact the cloud servers and report its existence and information mentioned in this chapter. Information contained in systems also needs to be integrated into the organization's database in cases where it is necessary to maintain the device's life cycle and state.

2.3 Challenges in end-of-life policies

This chapter describes challenges seen in target organizations regarding device end-of-life policies. There are a lot of responsibility-related issues that organizations need to solve to be able to deal with situations relating to the end-of-life (EOL) policies of the devices. For this chapter, the author focuses on first explaining the challenge with devices going to the EOL and why this is a challenge.

Hardware partners are the suppliers of physical entities, and software partners are suppliers of tools and virtual systems. They provide the devices and platforms enabling network operators to build customer services. Those services can connect partners' systems to customers' environments. All systems the partners deliver have a point in their life cycle when they need to be decommissioned. The process of partners decommissioning a product is called EOL policy. For this work, the author explores the EOL policy of Cisco [15] and Aruba. [16] These EOL policies describe and explain the steps these vendors use in communicating the decommission of a device or a system.

Figure 1. Cisco and Aruba end-of-life generalization. [15] [16]

The Aruba and Cisco EOL policies are pretty similar. They use different terms for the same concept. Both policies state that they inform the day when a device is no longer sold more than six months before the date. After this, the device goes to the end of sale (EOS). EOS usually means that the device is not manufactured anymore. The devices can still be shipped depending on the availability of existing materials. The EOS does not mean the partner stops updating the product and providing software updates and critical fixes for their devices.

Following the step comes the last date of support (LDOS)[15] or a similar term of end of support (EOST)[16]. LDOS and EOST are similar terms. So, the author indicates this date as EOL. This date means that partners no longer support that device and its software. This lack of support creates a challenge since leaving the device in a live environment is risky. The critical updates that still need to be implemented might cause the device to become vulnerable to attacks over time. There is also a problem when devices have combability issues or performance issues that cause difficult-to-solve problems to customer's networks since vendors cannot provide their expertise to solve them.

The challenge with EOL is that the hardware partners must maintain or develop the firmware or support those devices. This phase causes the network operators to either maintain or isolate those devices or change them for new models. Replacing the device usually the best option for the maintainer and the customer, but this change would cause customer service outages. New hardware change also costs, which may not be covered in the customers' current contract. Network operators also sell these devices forward to customers. With ownership, the responsibility of having an outdated system is with the customer. This responsibility causes challenges in cases where the operator should maintain this environment as per the contract, but the device change is the customer's responsibility. EOL causes security issues because the hardware manufacturer is no longer responsible for notifying their customers about issues that might be present in their older models. [15] [16] Clarifying how long an outdated device should be allowed to function on the operator's network.

The issue with these devices is that contracts are prolonged for multiple years. While this is typically a good thing from an operator business standpoint, it rarely is good from the customer's point of view. Outdated devices increase the risk of service outages and the need for action if a large-scale security threat is spotted. Vulnerabilities like Log4j [17] can stack up for those devices since the vendor does not maintain the existing device software. This risk can be mitigated by having the device in a closed environment instead of being exposed directly towards the public Internet. There is a difference in when to act.

One aspect is how the operator knows when the new device should go to EOL. This data must be apparent to all parties so the business can plan its resources more efficiently. There have been challenges with EOL where this information was not communicated clearly. This lack of data caused the organization to find new devices to meet the need and go through the procurement process again the following year since the device was outdated in a year. This mismanagement binds the testing resources and increases the amount of overhead because there is a need for a new device that needs to be maintained.

There are problems when the device is changed to a newer device. When changing a device from old to new, the existing features on the old device might not be available. These old features require the new devices to have replacements for this functionality, or operators might risk losing the customer. These features should also be documented to identify what features are in use in customer environments.

Currently, the device is changed during a fault or when there are larger re-negations of the agreement between the customer and network operator. This management has saved resources, but customers want to continue existing agreements past devices EOL. This perpetuity increases the number of devices in the network. To effectively manage these systems, there is a need for better management solutions. Those best practices are explored in the theoretical background of this work.

2.4 Challenges with communication

In this chapter, the author presents challenges with internal and external communication regarding the devices mentioned in Chapter 2.1. The word communication definition, according to a dictionary [18], is exchanging ideas, opinions, or information by a medium. Its goal is to exchange information, in this case, regarding the organization's devices. How could a company know if they would have issues regarding their devices, or how could they know if they would have delivery problems without good communication?

The organization needs help communicating their way of work or expertise of their services to their customers. This communication can be done by providing materials that explain the processes and providing references, but this can be time-consuming and not all service providers do a process the same way to be able to customers to compare them. This challenge is usually acceptable in the private sector. The problem comes with the public procurement process when the customer must be open and honest in their procurement process, and demands towards the service must be stated in detail before an agreement can be made. [19] This matter is also explored in the master's thesis by Mervi Käyty, in which one of the key findings was that the partner for public sector ICT development is usually chosen only by initial offer document and the knowledge of the supplier or the solution is not tested beforehand. [20] Usually, in these demands, the organization must prove that they follow a specific standard and that the technicians that deploy the service have enough certification to prove that they can provide quality service. This communication challenge causes organizations to strive to be standardized by a known standard like ISO or information technology infrastructure library (ITIL). Then, technicians strive to standardize their expertise with used vendor products.

Since the variance of devices mentioned in Chapter 2.1 on the company level is significant, more is needed to have overseeing persons know every challenge relating to the devices. Technicians working on delivering products only sometimes have time to communicate all issues with the products to overseeing

persons. This lack of a forum can cause a potential issue with development and management since they need correct information on the devices to make correct decisions. For example, the target company witnessed the following problem in communication. During a customer's fault, it was identified that upgrading the firmware version on a device fixed customer A problem. This problem happened again with Customer B because the problem with Customer A was not communicated to the overseeing person so that devices could be upgraded to prevent the same problem with other customers. There needs to be a better process to communicate these challenges.

3 Theoretical Background

This chapter focuses on finding solutions to perceived problems through theory. The theory is based on accepted national standards. Those standards guide how devices should be managed and what processes need to be created around device management.

The first chapter focuses more on asset management, which is a way to manage any entity that produces value. This chapter also focuses on related groups or stakeholders for those entities. There are also mentions of requirements that should be considered when planning the asset management system. The second chapter focuses on the security aspect of devices, defining risks and controlling actions to mitigate those risks. The third chapter goes through roles and responsibilities that should exist in the organization and what function those roles should have.

3.1 Asset management

This chapter describes how theory describes how asset management should be implemented in the organization. There are multiple asset management levels, which are described in the chapters below. First, there is a generalization and overview of asset management and what could be gained by implementing asset management. Then, the standard goes to how an asset management system can be implemented in the organization and what recommendations the standard provides for that system.

3.1.1 Asset management generalization

Asset management is described in the Standard ISO 55000, which states that asset management is the collection processes and functions that manage company assets [5]. Company assets include the devices mentioned in the current state analysis chapter and any entity that has value for the company. Examples of an asset could be software, process, workers, process,

configurations, or information. Asset management is a way to manage these assets and processes related to these assets. Asset management is based on four fundamental values: [5]

- Value.
- Alignment.
- Leadership.
- Assurance.

These values state what asset management tries to achieve at its core. Asset management should describe what kind of value an asset itself can provide for the corporation. This value can be not only concrete but also intangible. The organization can determine this value. The next point alignment value means asset management should be integrated across the organization. With integration, asset management could be used as a base for decision processes for those assets. The third value of leadership tries to achieve clearly defined roles and responsibilities for mentioned assets. This clarity ensures that persons with these roles understand what is expected of them. Lastly, assurance value tries to ensure that the assets meet their planned targets within the organization. This point ensures that planning and resources exist to improve those assets. [5]

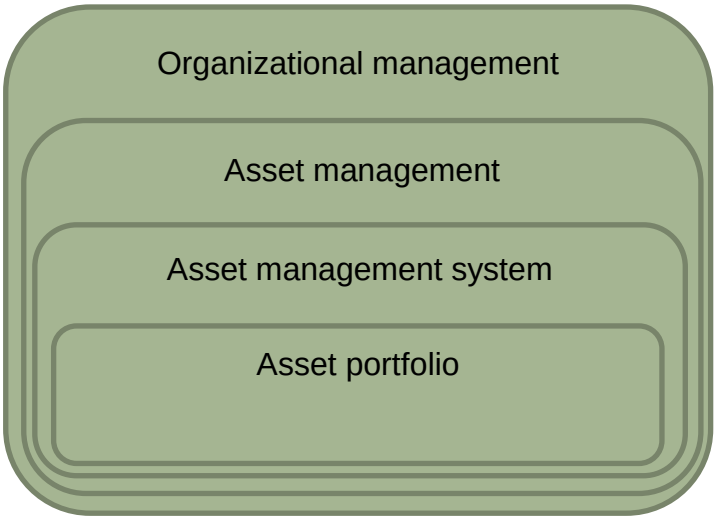

Figure 2. Asset management relation to organization management [5]

From (figure 2) states how asset management relates to the organization. Asset management is intended to be a tool for the management of an organization to release the value from those assets. The asset management system describes processes, goals and policies to manage the assets and how to achieve those targets assigned for the assets. Asset Portfolio is the collection of assets for that Asset management system that manages those assets. [5] Concerning the targeted company, the devices that are the author's responsibility lie in this portfolio as one part of the system. The improvement of those assets is part of the asset management system. This document explores these improvements more in the results and analysis chapter.

ISO 55000 explains the benefits of implementing asset management in the organization. Organizations can achieve multiple benefits listed below: [5]

- Better financial performance.
- Informed investment decisions.
- Managed risk.
- Improved services and outputs.
- Demonstrated social responsibility.
- Demonstrated compliance.
- Enhanced reputation
- Improved organizational sustainability.
- Improved efficiency and effectiveness.

The organization's leadership can benefit from asset management. Asset management can provide a base for information to make informed decisions, and knowledge of those assets could increase the financial performance of those assets. There could be places where the organization could streamline and focus its portfolio. Keeping an account of assets helps to find not-so-well-performing assets and try to improve those assets and their output. By having leadership determine and document what role or function an asset should try to meet, the development organization and leadership could have a mutual understanding and goals for that asset.

One of the essential aspects of asset management is managing risks for those assets. With the asset management system implemented, organizations could have processes to raise risks related to those devices and gain resources to discuss and mitigate those risks. Managing those risks should also be transparent and documented.

With asset management, the organization can demonstrate its compliance and social responsibility. This compliance is demonstrated by having documentation and traceability of decisions for those assets and proof of compliance with governmental edicts. This traceability demonstrates to governmental organizations like Traficom and customers that we follow regulations by having an asset management system. In addition, certificating those process organizations could have a better reputation for following known standards like ISO.

Asset management also claims to increase efficiency and effectiveness. When an asset's whole chain or responsibility is documented, the improvement in handling those assets could be justified for leadership. Organizations could know what points regarding that asset should be improved.

3.1.2 Asset management system

How the asset management system should be implemented in the organization is stated in ISO 55002.[22] These standard states that the success of an asset management system is in confirming that it is uniform across the organization. Stakeholders' interests and expectations for the assets must be recognized and documented. Below (Figure 3) is the author's interpretation of the data provided. [22]

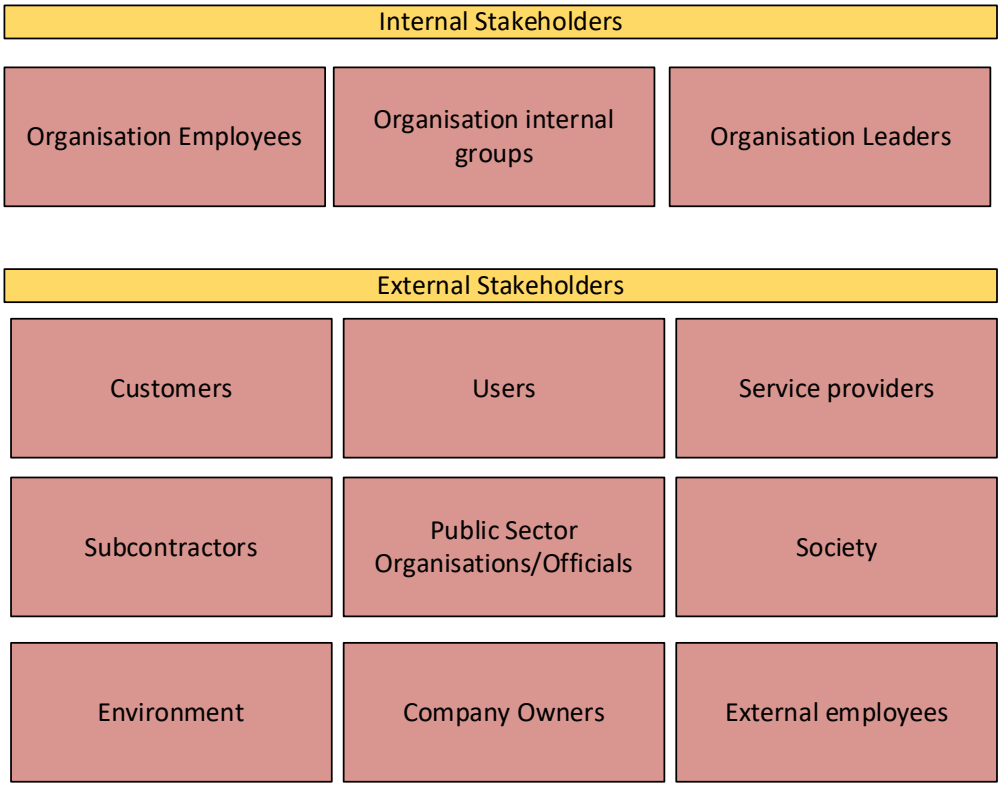

Figure 3. Stakeholders [22]

(Figure 3) can be seen as an example of a stakeholder. ISO 55002 [22] explains that stakeholders can be divided into two groups. One is internal stakeholders, which contain internal employees and groups. Another of the groups is external stakeholders, which is a larger group. These groups have expectations for managed assets. It is good to note that external stakeholders mention the environment and society. They also have expectations for the assets even if there might be no agreement between these groups regarding services provided by the company.

The standard goes on to state that stakeholders have expectations towards the device. These expectations can be values, needs, assumptions or concerns. These views from the stakeholders can have a notable effect on organizational assets and decisions made for those assets. These views or opinions should be documented and considered in the decision-making process. One of the goals of asset management is to help fulfil the needs of the stakeholders. These

expectations can also conflict with the organizational internal goals because stakeholders have different views, assumptions, and concerns. [22]

Organizations should determine the scope of the asset management system related to produced assets or services to stakeholders. These assets can be grouped and should be inspected if they can be grouped into manageable groupings. The scope of the management system should include all the assets that are significant for that function.[22]

For an asset management system to succeed in its function, it is crucial to ensure it is not separated from other functions or systems. The asset management system's data should be integrated across the organization to benefit the system most. Other systems that benefit from asset management systems are quality control, business management, accounting, security, risks, and human resources. [22] The system's benefits lie mainly in the support functions of an asset. This support is a valuable tool to improve communication and accountability for assets. These values increase the asset's value for the organization and its stakeholders.

The priority and effectiveness must be determined when creating an asset management system. Trusted processes should be used because only limited resources exist for these functions. The development of the asset management system should be stated by defining asset management policy. This policy should focus on critical issues and determine the goals of the asset management system according to an ISO 55002.[22]

When defining the asset management system ISO 55001 [21] states following requirements of ISO 55001:[21]

- context of the organization.
- leadership.
- planning.
- support.
- operation.
- performance evaluation.
- improvement.

These requirements should be considered as a minimum and not the endpoint of an asset management system. It also requires values, uniformity, leadership, and certainty within the asset management system. These systems should also be scalable to the organization's size, complexity, and importance. [22]

Asset management policy is a top-level document containing the organization's vision and values. This document provides the starting point for the organization to adopt asset management system policies. This document should contain commitments to the following subjects. [22]

- Commitment to follow laws and national regulations.
- Commitment to reach asset management system goals and appoint resources to fulfil those goals.
- Commitment to audit the asset management system and produce reports about the asset management system.
- Commitment to support stakeholders' demands.
- Commitment to honour contractual obligations.
- Commitment to improving asset management system.

After defining the Asset management policy, the organization should focus on the asset management plan. It is stated that this document does not have a pre-

defined format, but it should contain at least validation for proposed asset management systems and goals which they should affect. The document should also contain plans for action and maintenance of the asset management system. The plan should also have followed a list of plans: investments, renewal, change, improvement, decommission and plans for funding and resources. [22]

ISO 55002 [22] also gives instructions on what should be discussed and taken note of during the planning phase of the asset management plan.

1. The organization should take account of its scope, what goals and risks should be managed, and in what time cycle.
2. Asset management portfolio performance and wanted results from the assets?
3. Who is responsible for developing assets and communicating the needs of stakeholders?
4. The environment where the asset portfolio is supposed to function.
5. How do we manage risks regarding this asset management portfolio?
6. Documentation of deployment, processes, and functions.
7. Relation of capital and costs of operating the assets.
8. Outsourced functions and handling of control actions and motoring those functions.
9. Maintenance of continued operation planning, which is based on risks.
10. Known preventive measures and continued improved actions.
11. Process in which unplanned actions are prioritized.
12. Standard and technical specifications that can be applied to planning.

3.2 Risk management

In this chapter, the author explores ways to manage risks targeted towards the devices mentioned in the current state analysis chapter. Risk management is a way to manage internal or external influences that make it more challenging or impossible for the organization to achieve its objectives. Risk management

contains principles, frameworks, and processes to achieve its objectives. As with asset management, this process should be heavily integrated into leadership and how an organization is led. Managing risks helps organizations achieve objectives and make decisions at all organizational levels. [26]

The first chapter is about the risk management process, and the second chapter describes how risk management should be implemented in an organization according to ISO 31000.[26] Then, there is a chapter on control actions for those risks. These control actions are ways to mitigate known risks within the organization.

3.2.1 Risk management process

The risk management process describes ways that risk should be managed in the organization (Figure 4) is simplification of this process.

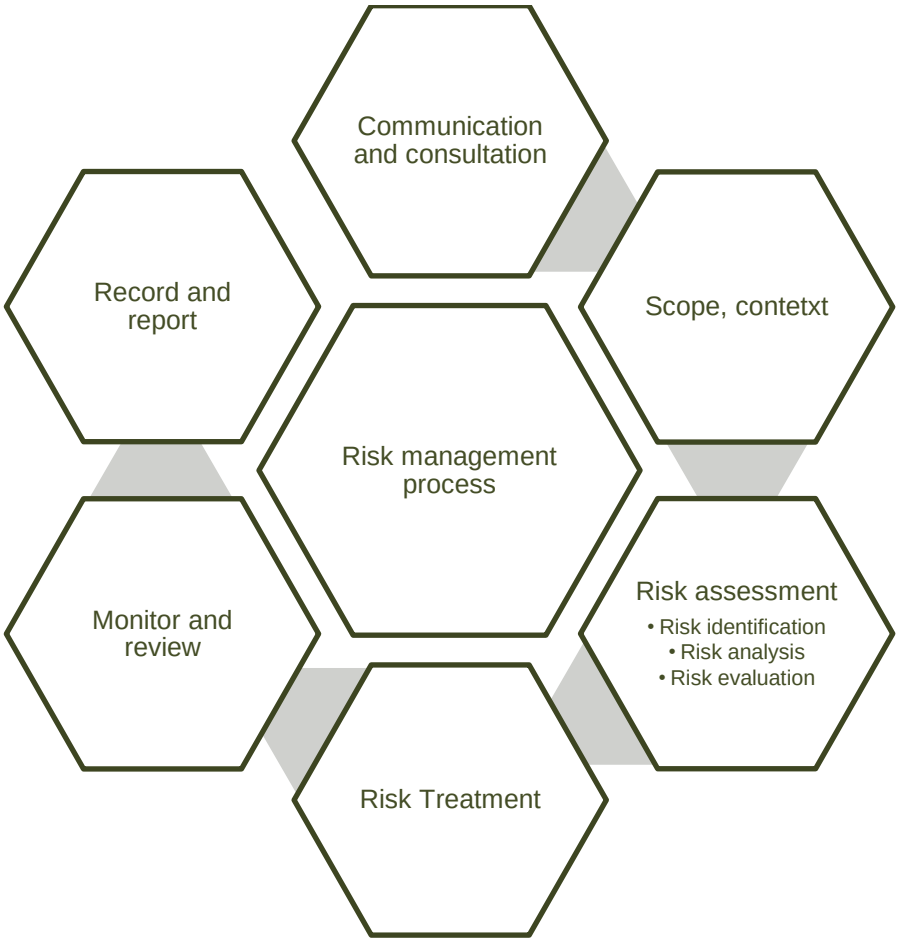

Figure 4. Simplified risk management process [26]

In (Figure 4) a typical process in risk management is demonstrated. This process contains six phases. The communication phase entails sharing information, making people aware of the risks, and understanding its reason. The consultation phase includes obtaining feedback and information to support the decision-making for those risks. The scope, context, and criteria phase's purpose in the process is to tailor the process to the organization and customize the management of the risks. Risk assessment identifies, analyses, and evaluates the risks with the stakeholders. The risk treatment phase is about managing the

risks, like removing the risk or transforming the risk with control actions. The monitoring and review phase is about improving the quality of the risk management process and should be done between any stage of the process. This review is the communication of results and information gathering for decision-making. The recording and reporting phase involves planning, gathering information and providing feedback. This step is about presenting the results to the rest of the organization and providing information for the decision-making process.[26]

3.2.2 Risk evaluation process

With a general understanding of the risk management process, how should the process be implemented? What should be considered when evaluating risks? Management of security stated in ISO 27001.[4] This standard provides recommendations on how one should implement the risk evaluation process: [4 p 8-9]

- Risk evaluation criteria should be determined.
- Risk acceptance criteria should be determined.
- Risk analysis should provide uniform results.
- Risk recognition
    - Make an analysis process for risks.
    - Recognize who owns the risk within the organization.
- Risk analysis.
    - Recognize the odds of risk realization.
    - Recognize the consequences of risk realization.
    - Determine the value for each risk.
- Risk evaluation.
    - Compare results with criteria.
    - Prioritise analyzed risks to the deployment of control actions or risk removal.
- An organization should store documentation of the risk evaluation process.

The above list provides a guide for managing security risks with nuances, with criteria in place for risk evaluation and acceptance. The organization could produce uniform results. Risk acceptance determines when risks can be approved and what risks should be controlled. These criteria should be maintained and updated.[4] There should be processes to ensure the risk evaluation process produces uniform results. These results should be uniform, competent, and comparable. Recognition of risks should be conducted by making processes for risk analysis. Also, there must be a way to identify who is responsible for said risk. Risk analysis should be done by evaluating the consequences of said risks and recognizing the likelihood of risk realization. Then, based on these risks, it should gain the value of severity. Then, risk evaluation should be conducted by comparing the result with risk acceptance criteria. Then, the risk should be sent to the deployment organization for processing or to mitigate said risk with control actions. These risks should be prioritized based on the severity of the risk. The standard also mentions that the organizations that implement risk evaluation processes should also have documentation of this evaluation process. ISO 55001 [21] also provides a similar list based on asset management. Therefore, managing risk is also a critical part of asset management.

3.2.3 Control actions

Control actions are ways to transform or change the risk defined in the risk management process.[4] These control actions are defined by standards ISO 270002 [24] and NIST SP 800-53 [23]. This chapter goes through said control actions from both standards and includes a bit from ISO 270011 [25], which contains control actions and specific instructions for the telecommunication business. ISO and NIST take a different approach to communicating the control actions. NIST has a comprehensive list of control actions, clearly stating how they relate to each other. ISO has more chosen picks that are commonly used and not grouped by formatting to find those control actions. Now, the author picks the

control actions related to devices mentioned in the current state analysis chapter and explains how the importance of this action is stated if it is mentioned.

NIST SP 800-53 divides its control actions into groups. Of these groups, the author has decided to focus on control actions mentioned in groups: [23]

- Configuration management.
- Contingency planning.
- Maintenance.
- Physical and environmental protection.
- Planning.
- System and services acquisition.
- System and information integrity.
- Supply chain risk management.

Of these groups, control actions specifically related to risk management were mentioned in the earlier chapter. However, most of the information overlapped with the earlier chapter, so it was left out. This information is worth reading to enhance risk management's importance.

Configuration management group contains the most control actions related to devices. One of the most important of these and close to the author's heart is baseline configuration. [23] For baseline configuration, the control is to produce configuration for said device that is reviewed within the organization and maintained. This process serves as the basis for customer-specific builds. Baseline configuration contains device-specific hardenings and privacy controls and reflects the device's current architecture.

Next in the same group is hardening the device. Its idea is to limit the device's functionality to provide only the necessary access to the device and restrict ports, protocols, and software. These devices usually provide more than is necessary to deploy selected services, so it is necessary to harden said device and close or restrict access to functions that are not needed for the device. ISO 270002[24]

also states that devices in the network should be monitored and managed to ensure these ports or systems stay hardened. Standard continues to state that network services and users should be separated. An example would be separating management and customer traffic for said device. The standard also states that access to those services should be limited to lessen attack surfaces that the device might provide.[23][24]

Next, the organization should define a configuration management plan. This plan contains the roles and responsibilities of said plan and establishes a plan to identify configuration items throughout the device's life cycle. Organizations can implement templates to ensure similar deployment of configuration items to this control action. [23] Templates should be done during the life cycle of device deployment, specifically when implementing the device into the network.

User-installed software should be monitored and enforced to detect unauthorized software quickly. This monitoring ensures that actions are taken if non-standard software is installed in the system, which could be vulnerable to the attacks. [23] ISO 270002 continues this control action. There should be a planned way for upgrading the software version and define how upgrading should be done. [24]

For the next group, contingency planning, the most exciting aspect for the target company is the existence of the contingency plan itself. This plan controls that business-critical functions should be identified and addresses how the system's failure can be mitigated or restored. This plan includes the responsibilities and contacts for individuals to recover from failure. According to NIST, this is an integral part of the lifecycle management of the said system and provides ways for continued operation of said system. [23] ISO 270011 also states specific requirements for telecommunication business areas. The telecommunication field must prioritize recovering services in critical functions like hospitals or government services. [25] ISO 270002 continues to broadly state that there should documented ways of action in the event of the failure of a system. [24]

The contingency plan group also contains a statement that there should be backups of,

- User-level information of the system.
- System-level information of the system.
- Backups of documentation relating to a device.

User-level information consists of backups of configuration that organizations' users can deploy on the device. System-level information like device models, software versions, and licenses should be stored safely. Backups of documentation consist of backups of information and policies and hardenings of a device. This information ensures that the business can restore the customer system with the same service. Organizations may be subject to law or regulation regarding this information.[23] ISO 270002 also mentions that organizations should make backups of their systems to recover from a failure. [24]

The next group in the NIST documents entails control actions for maintenance. There is specifically a point about controlled maintenance. With this control, one should schedule, document and review records of maintenance repair and replacement of system components. There should be a process for approving and monitoring all maintenance activities. [23] Concerning controlled maintenance, ISO 270002 states that there should also be a process for implementing secure upgrades of software versions to the production environment. [24] This point requires that device production software versions be defined for the devices, which should be monitored in the environment. Regarding this, ISO 270002 also states that there should be documentation for deploying software to targeted systems. [24]

Timely maintenance is in this same group of control actions. This control action tries to ensure that devices have the spare parts they need and support for maintenance of those devices. [23] The organization should ensure that the device supplier has support available to escalate problems of said device. An organization could also allocate enough resources with the required education to maintain said device if escalation is unavailable. Timely maintenance also

includes preventive actions like device resources being about to be exceeded, which could be monitored to prevent future device outages.

In the physical and environmental protection group, there is control action about asset monitoring and tracking. This control action ensures that a specific asset's location is known. [23] This control could mean tracking the serial number to ensure the correct device is deployed to the target system. Then, after the device lifecycle, the correct device is returned for the decommissioning process to ensure that the device and its information are not compromised during the life cycle of a device. This accounting also ensures that the device is only changed with authorization.

In the planning group of control actions, there is control action about central management. Central management is about consolidating management functions for organisationally-wide management. This control is mentioned because by centralizing management functions, the organization saves resources, and this promotes standardization and automation of said functions. This centralization also promotes the deployment of control actions across the organization. The standard also agrees that depending on resources, the organization only partially does this control action for system-level information and associated controls. [23]

The systems and services acquisition group of control actions contains two points. The first point is the acquisition process. When a new device or service is taken into use, there should be a process of having the new system meet the current controls, like controls for security and privacy documentation, a description of how the system should be developed and maintained, and which parties are responsible for said device or system. This onboarding safeguards that there would not be new devices that do not meet the required security policies. [23] ISO 270002 also states that for secure system architecture, plans should be drafted on how devices should be managed and designed. [24] If this plan did not take account of new devices to the environment, there would be a hole in the process. The second point is that system documentation should be so

the organization can secure, administer, install, and operate the device or service. This documentation aims to help personnel understand the implications of controls and to provide personnel with practical ways to manage the said device securely. [23] The importance of this documentation cannot be understated. Although documentation is rarely used during the daily operation of the device, the existence of said documentation and the distribution of this information improves the overall performance of said function. This documentation also helps the new employee who needs to learn all those recommendations from scratch.

System and information integrity is the next group in the NIST control actions related to the target organization. This group contains flaw remediation that aims to remediate system flaws related to software or firmware versions used by the devices. This remediation also includes system vulnerabilities and other flaws from upgrading or existing in the old software. The control aims to evaluate software or firmware updates before they are used in production to mitigate the side effects of such actions. [23] ISO 270002 also contains multiple points that relate to identifying threats for these devices: [24]

- There should be monitoring of threats for these devices and their software or firmware to produce related information.
- There needs to be event logs where incidents and failures should be stored.
- Clocks of those devices should be synchronized to be able to identify timeframes when something happens.

Supply chain risk management is the last group of control actions that should be included in the NIST documentation. One important group is often missed in the transformation of an organization. This point is provenance. Every system should have a point of origin or responsibility within an organization, and this responsibility can be changed. [23] In organizational transformation, the focus is often on resources, but the ownership of a system or documentation is left as it is. During this phase, it is critical that ownership of said documentation or system is found within the new organization. This process can cause problems where

people who should do the new system function in a corporation have also inferred the old responsibility of the old system since there has yet to be an evident change of responsibility during the change of organization. This lack of change in the responsibilities causes potential risks that services fall out of management.

Telecommunication business areas also have specific instructions mentioned in the ISO 270011 standard. It determines that telecommunication operators should deploy protections for distributed denial-of-service (DDoS) attacks for their networks and environment. Operators should also protect the identity of network communication information. There should be protection for IP spoofing, which protects source IP address modification. There also should be protection against malformed packets used in network devices to exploit vulnerabilities in other systems. Operators should perform detection of botnets and close those connections that have been compromised to prevent the spread of those botnets. These botnets are used in DDoS attacks inside or outside of the organization. Motoring should also be implemented inside telecommunication operators to identify if a specific connection between devices is crowded to prevent the formation of bottlenecks in the operator network. [25]

3.3 Roles and responsibilities

This chapter focuses on ISO 27001 and ISO 55000 standards. Those documents mention the responsibilities of higher management or a leader. This chapter focuses on the expectations of leaders of groups for the basis of a sound asset management system or a good security policy. ISO-based standards have less mention of what roles there are. Instead, it is mentioned that leadership should assign someone to a responsibility. The author also tries to split requirements into three levels: responsibility management, architecture, and internal stakeholders. Management in this context means someone with the resources and power to decide what will be done. Architecture means someone invested in developing or planning a system or way of work. Internal stakeholders are persons or groups that use, deploy, and maintain architecture-developed systems. The author has tried to keep these groups as general as possible.

3.3.1 Responsibilities of management

Regarding security, in general, management is expected to make an Information security policy that is used as a basis for developing the underlying security management systems or processes. [4] The same can be said about asset management since ISO 55002 states that the management is responsible for creating a culture, vision, and values that guide the policy. [22] In asset management, the involvement of the whole organization needs to be considered also, and management has the responsibility that they participate in the planning. [22]

Management is also responsible for communicating the importance of said security system and ensuring that the goals that they set are met. [4] They also define the necessary stakeholders to whom the policy is targeted. [4] They should support the leadership of others in their responsibility areas regarding security. [4] They should support the architecture in developing or enhancing the security system. [4] They should recognize the differences in culture and the conflicting needs of different stakeholders. [21] They should ensure that asset management policy conformity across the organization. [22]

Management is responsible for the time of their resources. Regarding security, there is a statement that management is responsible for appointing necessary resources to information security organizations to meet the needs of an organization. [4] Concerning an asset management system, the management is responsible for defining the scope of the asset management system and application area. [22] Management is also responsible for deciding who is responsible for developing asset management areas and their continued improvement. [22]

3.3.2 Responsibilities of Architecture

The responsibilities of architecture in an asset management system are more in participation in planning the asset management system mentioned in chapter

3.1.2. Since the asset management system is intended to be done with the participation of all the organizations,

Security standard ISO 27001 instead states many requirements for planning security procedures. The following list is a collection of responsibilities that the ISO 27001 standard state should be in design [4],

- Acceptance criteria of security risks.
- Recognizing security risks in their respective fields of expertise.
- Analyse security risks and their impact on the organization.
- Recognize owners of said risks.
- Evaluate the likelihood of risk realization.
- State goals for security.
- Recognize integrity of the integrity of information in their asset management system.

The organization's architecture should also conduct regular risk assessments for their application area. [24] They must also participate in global communities that provide standard best practices for their target group. An example of one of these groups from the author's experience is the Centre for Internet Security (CIS) workbench or a national agency like Traficom in Finland.

3.3.3 Responsibilities of internal stakeholders

Regarding asset management systems, the vital part of internal stakeholders is that their needs are documented in the asset management system for those devices. [22] One of the asset management systems' goals is to fulfil those needs and provide value for stakeholders. [22]

For security, the standard ISO 27001 has expectations for persons who deliver, maintain, or use said systems. They should be aware of the information security policy that the managers have created. They need to know how they can add to increase the security level of the system they are using. They need to be aware

of the consequences that might be caused by not following the requirements set for the system. [4]

Communication is also a critical step to success in case of security incidents. Internal stakeholders should know how to communicate internally and outside the organization. To know who should communicate what to outside and who to communicate internally about an incident in the system. They should be aware of what is communicated when communication is happening and how the communication is performed within the organization.[4]

Internal stakeholders should have documentation available if they need it to perform their functions. [4] This documentation is necessary if, for example, incidents are rare and happen occasionally, and this information needs to be remembered correctly. An example of this would be a rare system used in a single customer environment. This documentation should be shared with everyone who needs it internally. It should be appropriately stored in a place that can be accessed. This information should also be protected against accidental removal or a change. It is also necessary that the documentation states who is responsible for the documentation. If the organization is changed, there must be a process to find a new responsible for that instruction. Old information should be removed from the system so stakeholders can trust that the information provided is still valid when it is needed.[4]

4 Results and Analysis

The organization identified three points for improvement. Those key points were asset management, device database and risk management. There is data on the devices, but this data is divided into multiple systems. This information should be centralized to improve communication and decision-making for those devices. [23 p. 227] This centralization would also increase the organization's maturity level towards standardization [23 p. 227] and ensure that the organization can take part in public sector procurement processes where this standardization has become necessary [20] By improving these three points, organizations could increase their readiness to implement the standardization for the devices and services. By increasing the information on the devices, organizations could make minor improvements to the process, save time, and manage a more varied device base by having the information available. Improving these would also increase security, accountability, and customer insight and implement processes to ensure device documentation is handled.

In the following chapters, the author explains the suggested improvement points. The first author explores the benefits of increasing the readiness level of asset management. Then, the author suggests improvements that could be made to the device database. Then, the current state analysis chapter mentions the risk management process improvements for those devices. These chapters provide recommendations and guidance suggestions on how these could be implemented. The author also explains what could be gained by implementing these systems.

4.1 Asset management improvements

The difficulty of assets in target corporations lies more in asset portfolios. Too many assets concerning current documentation capability exist in a single business area. This problem is seen in the current state analysis [Ch. 2.1]. Those devices mentioned have multiple vendors. To manage this variety of vendors with

current resources. Improvements should be made within the asset portfolio of the current asset management system. These improvements are as follows,

- Visibility of all assets within a single asset management system.
- Identifying all assets within the application area.
- Assigning technical owners to all systems.

Having the visibility of assets would increase the capability of leaders to make decisions based on those assets.[5] Organizations could combat issues of combability and find people to maintain said environments or begin to migrate from the old environment to a new one.[5] By identifying assets that belong to the application area, the organization can mitigate problems from systems that are not anyone's responsibility.[5] This information decreases the time needed to solve issues related to those systems. Assigning technical owners to said systems managers could ensure those systems are developed and maintained. The assets should be maintained until they are decommissioned.[5] Without maintenance, these assets become a liability to the organization because problems related to these assets might cause network-wide problems with security or combability. All these points can function as a tool for leadership to ensure that their environment is cared for and lessen problems that might arise at their level.

The author proposes that the organization organize workshops to map devices and systems in the organization's application area and produce an asset management plan mentioned in ISO 55002 [22]. Those devices could be lightly documented in the organization's documentation system before a better place is planned for that information. Information that could be collected is as follows,

- System logs storage.
- System backup storage.
- System device database information.
- System delivery documentation.
- System maintenance documentation.
- System monitoring location.
- System maintenance location.
- System risk register.
- System readiness plan.
- System regulation from the national level.
- System stakeholders.
- System owner.
- The system is responsible for development and maintenance.

The goal of gathering this information is to evaluate if there would be the possibility of gaining benefits by combining the way assets are managed. With logs and backups, the organization might have multiple ways to implement the same function by combining the ways the organization can benefit from needing fewer systems to manage its portfolio. By streamlining systems, the organization could gain monetary benefits in lessening the cost associated with management. [5] [Ch. 3.1.1] This streamlining also ensures that the devices mentioned in those systems are centralized. This centralization increases the adaptability of standards to the organization. [23 p. 227]

By checking the system's documentation, the organization would be assured of deployment and debugging instructions for those systems. Without documentation, the delivery or support resources raise questions to the architects

or leadership that might take their time needlessly for daily operations. Documentation is also mentioned on Implementing risk management [4 p 8-9] and implementing asset management ISO 55001 [21]. NIST Security and privacy controls for information systems and organizations state that documents are evidence that control action is in place. [23 p. 47]

Then, it needs to be reviewed if any regulation might affect said system, and this needs to be documented. [23 Ch. 3] This documentation would ensure that the organization knows any restrictions or requirements related to a system set by society or government. There also needs to be information about stakeholders of the assets or devices during these workshops. These stakeholders were mentioned in the (Figure 3) Asset Management chapter. The organization could have documentation of parties related to that asset by mapping them. This information could then be used for the improvement of said asset. For example, if there is a fault with the system, we could have the manufacturer's information and see if the support contracts are still valid.

The next step after this would be to make an asset management plan, as mentioned in the ISO 55002.[22] Responsibilities should be assigned to designated architects. Their job would be to improve said documentation and uphold the risk register for the device with the partnership of the system's stakeholders. Chapter 3.1.2 provides a list that is recommended to go through during the asset management plan.

Documentation of the asset management portfolio needs also to be maintained. There might be issues if the person responsible leaves the organization. The assets would not be maintained anymore. With this, the documentation of persons who are responsible would be documented. Then, leaders could find out what assets this person maintained and find a replacement. During the asset management plan, the customer needs for said products could be reviewed and documented. The SFS-ISO 55002 [22] states that by mapping stakeholders' expectations, the organization could plan the development of the asset in question to meet the needs of the stakeholders. The organization could use

processes like customer experience mapping to enhance company internal documentation with information on stakeholder's needs.

4.2 Device database improvements

The following proposal during the study was regarding the device database. As mentioned in the previous chapter, there is a need to go through all the devices recognized as the organization's responsibility. While performing current state analysis, it was apparent that multiple distinct types of device discovery databases exist. The information from these discovery databases should be consolidated into one common database of discovered devices. [23 p. 227]

In addition, this device discovery database organization have a database where our clients and their information are stored according to customer agreements. In this database, what the customer has ordered and what was deployed should be apparent. The customer premises equipment (CPE) should be visible in this database because the technology required for the service must be documented in this system to avoid miscommunication about what is needed to deploy the service. For example, to upgrade the device from ethernet- to a fibre-based connection, the knowledge of this technology is needed for the supplied service. Documenting the virtual environments and their technology in this database is also necessary. This database needs at least have information on devices that affect customer experience. This statement would mean the device, its vendor, and installation. This database should be kept up to date with normal installation processes. This customer database needs to reflect the actual state of the network to stay valid. There should be a way to manage the following points,

- Way to manage device identity, and customer visibility to the device.
- Way to manage the change of device during fault.
- Way to manage upgrading device firmware.

To correct the above points in the customer database. There is need of a separate discovery database is needed to ensure the validity of this order

database. [27 Ch.2.5.1] This database functions differently from a device database to discover devices in our management network. Then, those devices are compared against the device database to find out if there have been errors in the device database compared to a commercial database. An example would be that there has been an error with the process, and an incorrect device has been installed at the CPE location. An organization could find faults in the process with a device discovery database and validate the device database. As the organization develops, changes like acquiring or merging organizations might cause the device database to no longer be valid. With this validating function in place, organizations could ensure that those problems are manageable where human resources are needed to manually ensure the database's validity.

These databases form a bond in that the device discovery database could validate the system itself, and the organization could ensure that it is up to date and has the means to correct the data before it becomes corrupt. If the organization has a device database that is validated with the latest information, the organization could create scripts or programs that could use this data to provide the following benefits,

- See if there are old devices in our network and update those devices.
- See if the software version has any known vulnerabilities.
- See if the software version is affected by a vulnerability automatically.
- See if the correct device is installed to location A and, at the end of its lifetime, is returned to decommission.
- See if new devices emerge to the organization network outside the correct process.
- See if a new device needs to be sold during the renegotiation of the customer's agreement because the old device is EOL.

These points also increase the environment's security by having the correct information to make decisions. With the device database information being dispersed, the Organisation could only gain some of the benefits mentioned in

the ISO 55000 standards. The benefits of hardware asset management document NISTIR 8011 [27] also collaborate with this information.

4.3 Risk management improvements

The third suggestion of the author is to implement a risk management process encompassing those systems. The goal of the risk management process would be to raise technical challenges for those systems. Those technical challenges can then be communicated in a common forum with the organization's managers, and discussions can be taken to implement control actions for those issues. Those known control actions were mentioned in chapter 3.2.3.

An example of a control action that could be implemented is as follows. The delivery organization has witnessed EOL devices in the network, which pose a risk. The risk management process would give delivery organization resources a way to inform of the risk to asset management responsible. Then, the asset management responsible could inform of the risk in a common forum and plan to mitigate it with control action or remove it entirely. The control action for said problem could be changing those devices to a new one. This risk management database could also act as a list of active control actions for said devices and give a better picture of what has been done for those devices and associated risks.

Risk management at the technical level could be implemented lightly by organizing quarterly meetings. This meeting would contain chief architects, management and technical responsible for devices. The risks would be evaluated, identified, and recognized in those meetings. (Chapter 3.2.2) This meeting would ensure that the risk management process would generate uniform results and communicate risks and their control actions as is mentioned as one of the requirements in ISO 27001 standard. [4 p 8-9] This process could also function as a way to share peer information between responsible.

The technical responsible would then need to familiarise to the following points,

- Go through risks related to their device software.
- Familiarize with common security forums of their device.
- Gather risk information from the organization about the device.
- Raise risks to risk management document.
- Plan control actions together with their peers.
- Document control actions to risk management document.

Risks could be gathered by participating in weekly meetings with the asset's stakeholders, like organized coffee breaks. In These meetings, the assets could explain their concerns about the product in a relaxed environment. There is potential and hidden knowledge in the organization. Deploying organization knows that something is a risk, but they need more time or motivation to act on those risks. By having a forum where they can express their concerns, they are not required to take responsibility for those concerns. Those risks then could be documented and raised to the knowledge of the management and the rest of the organization. Another option for gathering the risks is by organizing external audits by hiring a commercial organization that provides non-biased feedback to the organization. Outside organizations could raise issues that might not come up to system responsibility because they might be occupied with the system's development and need more time to familiarise themselves with the above points. There also is documentation available on the security hardening of these devices. Forums and organizations like Traficom and CIS Workbench could give support in solving familiar challenges with the devices. As mentioned earlier, the system responsible should have time to familiarize themselves with the organizations.

There should be a place where to document risks and control actions. Initially, this can be as simple as an Excel worksheet where a technical perspective should at least be following,

- Device risk is targeted towards.
- Consequence of risk realization.
- The value of the risk is determined by the management.
- Control actions for that risk.
- Date of the risk and control action.

This document would then be reviewed quarterly with the management and chief architects. The meetings would also provide a channel for management to communicate the risks and control actions and affect the control actions implemented for those risks. Then, management could communicate this risk to their organizations so that the whole organization could be aware of the risks and the control actions. There needs to be documentation and traceability of the risks to ensure the risk management process works.[5] [Ch. 3.1.1]

5 Discussions and Conclusions

The research question was how standards state device management and security should be conducted. Then, from those standards, derive recommendations on what should be improved to manage varied device environments more effectively under a single application area. Those improvements were as follows,

- Improving asset management.
- Consolidating device databases.
- Implementing technical risk management processes for those devices.

These points should be driven forward first because they could benefit the target organization most. Improving those aspects of device management increases the maturity of the organization's processes. Both standards, SFS-ISO 55002 [22] and ISO/EUC 27001 [4], state that the improvements need to be implemented on top of existing management processes. These standards guide how one should implement said improvements. To gain the benefits mentioned in these standards. They should be implemented across the organization's application areas. Versions of this process are in place but only sometimes extend to the technical level. SFS-ISO 55001 states that organizations should determine the level of their asset management system and its boundary. In this work, the author has recommended incorporating the principles mentioned in these standards to a technical level of these devices.

Solutions can be implemented lightly in B2B technical organizations and still gain benefits. The benefits would be having knowledge of all devices in a single environment. This environment can then be used as a base to manage known devices. When the rest of the organization can increase its maturity of device management, the information made in this asset management portfolio could then be transferred to a new system or function as an example for the rest of the organization. The validity of these improvements could be verified by having improved lead times and faster escalation to the correct department about issues

relating to devices with shared responsibility. This improvement would increase customer satisfaction and demonstrate the social responsibility of these services.

For the validity of the subject, the author states that from reading ISO and NIST standards about asset management and risk management, different persons might come to different conclusions. These conclusions are reflections of their background and unique insight. The author notes that his role as the technical responsible for managing the devices affects his ideas of what processes should be implemented and at what level. The common theme from the standards was the distribution of information and transparency. These points require resources, but those resources could manage larger environments with correct and tested processes.

References

1 National Institute of standards and technology. Framework for Improving Critical Infrastructure Cybersecurity [Internet]. 2018 [revision 16 Apr 2018; cited 2023 Feb 18]. Available from: https://doi.org/10.6028/NIST.CSWP.04162018

2 National Institute of standards and technology. About NIST [Internet]. Gaithersburg: National Institute of Standards and Technology; 2022 Jan 11 [cited 2023 Jun 17]. Available from: https://www. .gov/about-nist

3 Finnish Transport and Communications Agency. Organization [Internet]. Traficom; 2023 Jun 5 [cited 2023 Jun 17]. Available from: https://www.traficom.fi/en/traficom/about-traficom/organisation

4 Finnish Standards Association. ISO/EUC 27001:2022:fi [Internet]. 2022 [revision 01 Nov 2022; cited 2023 Feb 22]. Available from: www.sfs.fi

5 Finnish Standards Association. SFS-ISO 55000 [Internet]. 2014 [revision 13 Oct 2014; cited 2023 Feb 22]. Available from: www.sfs.fi

6 Finnish Standards Association. Finnish Standards Association SFS – The national standardization organization in Finland [Internet]. 2020 Nov 22 [cited 2023 Jun 17]. Available from: https://sfs.fi/en/finnish-standards-association/

7 International Organization for Standardization. ISO in brief_EN_2018 [Internet]. 2019 [revision Aug 2019; cited 2023 Jun 17]. Available from: https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100007.pdf

8 Metropolia University of Applied Silences. Master Thesis Template 2021 [Internet]. 2021 [revision 01 Mar 2021; cited 2023 Jun 17]. Available from: oma.metropolia.fi

9 Monash University. Vancouver Citing & Referencing style [Internet]. Monash University; 2023 [revision May 2020; cited 2023 Jun 17]. Available from: https://guides.lib.monash.edu/citing-referencing/vancouver

10 Alexandre M.S.P Moraes, Cisco Firewall,1st ed. Cisco Press; 2021; Available from: https://learning.oreilly.com/library/view/cisco-firewalls/9781587141140/

11 Cisco. OSI Model Reference Chart [Internet]. Cisco; 2021 Aug 19 [cited 2023 Jun 19]. Available from: https://learningnetwork.cisco.com/s/article/osi-model-reference-chart

12 J. Case, M. Fedor, M. Schoffstall, J. Davin. A Simple Network Management Protocol (SNMP) [Internet] Network Working Group; 1990 May [cited 2023 Jun 19]. Available from: https://datatracker.ietf.org/doc/html/rfc1157

13 R. Enns, M. Bjorklund, J. Schoenwaelder, A. Bierman. Network Configuration Protocol (NETCONF) [Internet] Internet Engineering Task Force (IETF); 2011 Jun [cited 2023 Jun 19]. Available from: https://datatracker.ietf.org/doc/html/rfc6241

14 Howard. How Cloud Managed Network Defines the Future? [Internet]. FS; 2023 Mar 16 [cited 2023 Sep 29]. Available from: https://community.fs.com/blog/how-cloud-managed-network-defines-the-future.html

15 Cisco. End-of-Life Policy [Internet]. Cisco; 2023 [cited 2023 Sep 30]. Available from: https://www.cisco.com/c/en/us/products/eos-eol-policy.html

16 Aruba. End of Life Policy [Internet]. Aruba; 2013 Aug 1 [cited 2023 Sep 30]. Available from: https://www.arubanetworks.com/support-services/end-of-life/end-of-life-policy/

17 CVE. CVE-2021-45105 [Internet]. The MITRE Corporation; 2021 Dec 16 [cited 2023 Sep 30]. Available from: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105

18 MOT Oxford Dictionary of English: communication. Kielikone Oy. Retrieved 29.9.2023 from www.sanakirja.fi/oxford_english/english-english/communication

19 Julkisten hallintojen neuvontayksikkö (JHKY). Hankintojen periaatteet [Internet]. JHKY; 2021 [revision Sep 2023; cited 2023 Sep 29]. Available from: https://www.hankinnat.fi/mika-julkinen-hankinta/hankintojen-periaatteet

20 Käyhty M. Information Systems*: Julkisen ICT-hankinnan ominaispiirteet ja haasteet*. Masters thesis. University of Jyväskylä; 2022. Available from: https://jyx.jyu.fi/handle/123456789/80926

21 Finnish Standards Association. SFS-ISO 55001 [Internet]. 2014 [revision 13 Oct 2014; cited 2023 Feb 22]. Available from: www.sfs.fi

22 Finnish Standards Association. SFS-ISO 55002:2018 [Internet]. 2018 [revision 07 Dec 2018; cited 2023 Feb 22]. Available from: www.sfs.fi

23 National Institute of standards and technology. NIST Special Publication 800-53 r5 [Internet]. 2020 [revision 12 Sep 2020; cited 2023 Feb 18]. Available from: https://doi.org/10.6028/NIST.SP.800-53r5

24 Finnish Standards Association. SFS-EN ISO/EUC 27002:2022 [Internet]. 2022 [revision 18 Nov 2022; cited 2023 Feb 26]. Available from: www.sfs.fi

25 Finnish Standards Association. SFS-EN ISO/EUC 27011:2020: en [Internet]. 2020 [revision 12 Jul 2020; cited 2023 Feb 26]. Available from: www.sfs.fi

26 Finnish Standards Association. SFS-ISO 31000:2018: en [Internet]. 2020 [revision 12 Jul 2020; cited 2023 Mar 29]. Available from: www.sfs.fi

27 National Institute of standards and technology. NISTIR 8011 Volume 2 [Internet]. 2017 [revision 12 Jun 2017; cited 2023 Feb 18]. Available from: https://doi.org/10.6028/NIST.IR.8011-2