jamk.fi

<

When should an organisation start vulnerability management?

Anssi Mietala

Master's Thesis
May 2020
School of Technology
Master's Degree Programme in Information Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

Description

Author(s) Mietala, Anssi	Type of publication Master's thesis	Date May 2020
		Language of publication: English
	Number of pages 48	Permission for web publication: X

Title of publication

When should an organisation start vulnerability management?

Degree programme

Master's Degree in Cyber Security

Supervisor(s)

Hautamäki, Jari and Saharinen, Karo

Assigned by

Telia Inmics-Nebula Oy

Abstract

Organisations may find vulnerability management very difficult to start conducting, but they are obligated to perform vulnerability management due to various requirements which may come from standards, regulations or business relationships.

The objective of the research was to compile an easy to understand document about cyber security program for an organisation which allows them to begin vulnerability management. To support this cyber security program a strong base for vulnerability management cyber security frameworks and cyber security maturity models needed to be compared and presented.

The research started by searching good research subjects for cyber security frameworks, cyber security maturity models and vulnerability management implantation processes. Once these research subjects were studied and similar features were compared analytically.

The comparison results and analysis found some strengths and weaknesses of the research subjects.

As the conclusion for the research there was no definite answer for all organisations, about cyber security frameworks, cyber security maturity models or vulnerability management models. The research should provide decent support for organisations to build strong basis for their cyber security program and beginning the vulnerability management.

Keywords/tags (subjects)
Cyber security, Cyber security framework, maturity model, vulnerability management

Miscellaneous (Confidential information) jamk.fi

Kuvailulehti

Tekijä(t) Mietala, Anssi	Julkaisun laji Opinnäytetyö, ylempi AMK	Päivämäärä Toukokuu 2020
	Sivumäärä 48	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: x

Työn nimi
When should an organisation start vulnerability management?

Tutkinto-ohjelma
Master's Degree in Cyber Security

Työn ohjaaja(t)
Jari Hautamäki, Karo Saharinen

Toimeksiantaja(t)
Telia Inmics-Nebula Oy

Tiivistelmä

Haavoittuvuuksien hallinnan aloittaminen voi olla suuri haaste monille organisaatioille, mutta näillä organisaatioilla on vaatimuksia tehdä haavoittuvuuksien hallintaa esimerkiksi standardien, regulaatioiden tai bisnessuhteiden kautta.

Tutkimuksen tavoitteena oli tuottaa helposti ymmärrettävä dokumentaatio kyberturvallisuudesta, joka avustaa organisaatioita haavoittuvuuksien hallinnan aloittamisessa. Kyberturvallisuuden tueksi haavoittuvuuksien hallinnan aloittamiselle tarvittiin vertailua eri kyberturvallisuusviitekehyksistä, kyberturvallisuuden kypsyysmalleista ja haavoittuvuuksien hallinnan käyttöönottoprosesseista.

Tutkimus aloitettiin etsimällä sopivia tutkimuskohteita kyberturvallisuusviitekehyksistä, kyberturvallisuuden kypsyysmalleista ja haavoittuvuuksien hallinnan käyttöönottoprosesseista. Löydettyihin tutkimuskohteisiin perehdyttiin ja niiden ominaisuuksia vertailtiin analyyttisesti.

Tutkimuskohteiden vertailussa tutkimuskohteista löydettiin niiden vahvuuksia ja heikkouksia sekä ominaispiirteitä.

Tutkimuksen johtopäätöksenä voitiin todeta, että lopullista kaikille organisaatioille sopivaa kyberturvallisuuden viitekehystä, kyberturvallisuuden kypsyysmallia tai haavoittuvuuksien hallinnan käyttöönottoprosessia ei löytynyt. Voidaan kuitenkin todeta, että tutkimus tuotti riittävän dokumentaation organisaatioiden kyberturvallisuuden rakentamiselle ja haavoittuvuuksien hallinnan aloittamiselle.

Avainsanat (asiasanat)
Kyberturvallisuus, kyberturvallisuuden viitekehys, kypsyysmalli, haavoittuvuuksien hallinta

Muut tiedot

Contents

Figures

Tables

1 Introduction

There are many reasons why organisations need to start conducting vulnerability management. These reasons can be requirements from a standard, regulations for the specific business area or from another organisation with which the organisation has a partnership with. Often, when an organisation decides to implement vulnerability management, the organisation encounters problems with technical understanding of the vulnerabilities, vulnerability mitigation and other supporting processes. Therefore, this thesis is aimed at the organisations considering to begin or are having problems with vulnerability management. The goal for the thesis is to give organisations a better understanding about vulnerabilies, the maturity of an organisation's cyber security and offer an easily adoptable vulnerability management model. The thesis is restricted to only technical vulnerabilities, which can be found with a vulnerability scanner.

According to the Finnish National Cyber Security Center (2019, 6), vulnerabilities are exploited almost immdiately and Finnish organisations do not know their own infrastructure well enough; hence, they lack capabilities to notice and react to these cyber attacks. One key risk for organisations are servers on the public internet, which are actively polled and attempted to crack using exploits from vulnerabilities (ibid., 25). NCSC-FI lists a lack of updating and password management to be developed in expectations for the year 2019 (ibid., 43).

According to Lehto, Limnéll, Innola, Pöyhänen, Rusi and Salminen (2017, 16), vulnerability exploiting was one major trend in 2016 and criminals actively search and exploit vulnerabilites. Therefore, vulnerabilities need to be found and mitigated as early as possible. The cyber security in private sector organisations works efficiently considering the common malware protection, power supply functionality, and networks. There are national challenges in cyber security due to the lack of skilled cyber security specialists. Organisations implement cyber security mostly reactively; however with some exception there is also some proactivity. Organisations fall behind in following the national cyber security strategy when it comes to creating a big picture of the status of cyber security or reaching cyber security maturity levels. (Lehto et al. 2017, 45-46)

In the International Telecommunications Union's (2017, 56) Global Cybersecurity Index 2017, the Finnish cyber security is ranked 16th on the global scale. Finland gets an extra mention about bilaterality for its activity in global organisations such as Council of Europe and the United Nations. In addition, also multilateral agreement strengthening nordic cooperation with National CERTs (ibid., 44) are mentioned. The Finnish cyber security received a low score in sectoral CERT and professional training courses (ibid., 37).

Offering organisations a better understanding and model about vulnerability management should benefit the national cyber security level of organisations as they are able to adopt vulnerability management as another layer of security. Vulnerability scanners are able to find missing updates and configuration mistakes such as default passwords.

The research is assigned by Telia Inmics-Nebula Oy. Telia Inmics-Nebula Oy is part of Telia Company. Telia Inmics-Nebula Oy was established as fusion of Inmics Oy and Nebula Oy in January 2019. On the January 2020 Telia Datainfo Oy was merged into Telia Inmics-Nebula Oy. Telia Inmics-Nebula Oy is an ICT service provider with about 500 employees (Telia-Inmics Nebula 2020).

2 Research

2.1 Research background and objectives

For small and medium size organisations it may not be easy to implement or upkeep a vulnerability management, and often organisations are not aware of their cyber security maturity either. As there is material available from organisations such as International Organisation Standardization, National Institute Standards and Technology, implementing the vulnerability management into one's own organisation may be difficult due lack of understanding the cyber security context.

The aim of this thesis is to increase the understanding of vulnerability management and to develop a common vulnerability management implementation process or suggest an existing implementation process which is not too heavy and complex for the organisations to implement. The thesis studies information and previous researches about technical vulnerabilites, vulnerability management implementation processes, cyber security maturity models and vulnerability scanners. Utilizing the research results organisations should benefit by gaining an adoptable vulnerability management implementation process and; therefore, increase the capability of their cyber security.

The research questions for this thesis are listed in below.

> How to build a solid basis to begin vulnerability management?
>
> When is the organisation mature enough for technical vulnerability management?
>
> Can there be an easily adaptable implementation process for technical vulnerability management?

A brief search from Theseus (N.d.) using this research related search words revealed that there hasn't been done a comparative research about vulnerability management implementation processes or cyber security frameworks or cyber security maturity models in this context. There are mentions of these subjects in theses, but targeted research was not found. Eventually a comparative research named Comparative Study of Cybersecurity Capability Maturity Models by Rea-Guaman, San Feliu, Calvo-Manzano and Sanchez-Garcia made in 2007 was found (Rea-Guaman et al. 2017, 2).

2.2 Research methods

This thesis uses comparative research and qualitative research in a multi-method analysis format. The chosen research methods were chosen due to the nature of existing processes and models which need to be compared to find out their advantages and disadvantages to be able to build more easily adaptable models and processes.

2.2.1 Comparative research

Routio (2007) explains comparative research as an option to research what is different and similar about chosen cases which in this thesis will be processes or models. The method of comparison is one of the most effective ways to observe differences of the selected cases and explain the differences in an easily compareable format such as a table. The comparative study has two major styles, namely descriptive comparison and normative comparison. Descriptive comparison describes and explains differences of cases and usually avoids creating changes. Normative comparison aims to observe the present state of cases and improve them in the future. This thesis aims to observe cases off vulnerability implementation processes and generate a new common implementation process or promote an existing one; thus, this research uses normative comparison as the research method. (Routio 2007.)

According to Lor (2011, 2) a comparative research is often used in social sciences, but it can be used in all science.

2.2.2 Qualitative research

Jyväskylä University Koppa is an open data storage describing that qualitative research enhances knowledge about the research topic due to there being multiple areas connected to the center of this thesis. (Jyväskylä University 2015).

Kananen describes qualitative research as any research which aims to achieve enhancement of the knowledge and gain better understanding of the subject without statistical or other quanitative means. The qualitative research analysis is utilized and a frame of reference throughout the research process to guide the research process and data collection. This thesis contains qualitatively selected literature to increase knowledge and understanding of cyber security frameworks, maturity models and vulnerability management. (Kananen 2014, 21-23.)

2.3 Research plan

The implementation of the research plan follows closely the literature reviews' discussion of cyber security frameworks, maturity models, and vulnerability management. This provides a solid and supporting basis to understand about cyber security frameworks and maturity models as well as to build vulnerability management implementation processes. The goal is to find and compare two to four cyber security frameworks, two to four maturity models and two to four vulnerability management implementation processes. These found research subjects will be compared regarding their levels of hiearchy required in the organisation and the number of steps in the process. Based on the comparison and qualitative analysis, new simplier models may be developed or existing recommended. If new models and processes are developed, they shall be compared with existing models and processes. The process of is explained below (see Figure 1)Figure 1. The research process.

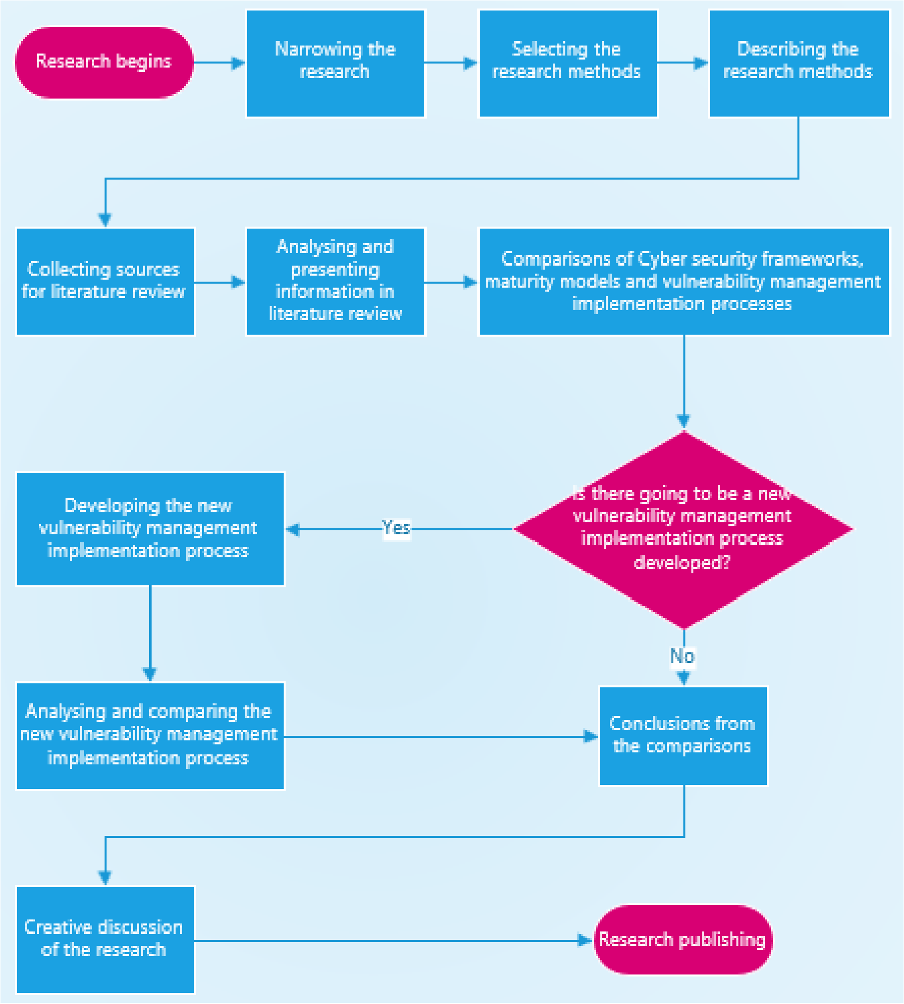

Research begins
Narrowing the research
Selecting the research methods
Describing the research methods
Collecting sources for literature review
Analysing and presenting information in literature review
Comparisons of Cyber security frameworks, maturity models and vulnerability management implementation processes
Is there going to be a new vulnerability management implementation process developed?
Yes
Developing the new vulnerability management implementation process
No
Analysing and comparing the new vulnerability management implementation process
Conclusions from the comparisons
Creative discussion of the research
Research publishing

Figure 1. The research process

3 Literature review

This literature review provides an analytical basis for the study with the aim of creating a framework in order for the reader to understand when an organisation should start vulnerability management through contrasting and comparing various cyber security frameworks, maturity models and vulnerability management processes. The review starts with the basic information about cyber security frameworks and finishes with various maturity models and vulnerability management. In understanding the major cyber security maturity models and vulnerability management tools, this thesis is able to measure and compare the dataset for this thesis accordingly.

For the literature review search engines such as Google, Google Scholar, FINNA, JANET and Melinda were used to gather possible sources to find literature to support the thesis. The used search phrases were cyber security, cyber security framework, security framework, vulnerablity management, vulnerability management model, vulnerability management process, vulnerability assessment, cyber security maturity model and maturity model. The search phrases returned vast amount of results which helped to find usable research subjects for comparison. Eventually, the literature data was decided to be obtained mostly from the original sources.

3.1 Cyber Security Frameworks

National Institution of Standards and Technology define the cyber security framework with words “The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk.” (National Institute of Standards and Technology 2018a).

The frameworks selected for this literature review had requirement that these models are known, widely used, adaptable to cyber security and contain comparable features. The selected frameworks are National Institute of Standards and Technology Cybersecurity Framework, Institutional Organisation for Standardization ISO27001 standard and Center for Internet Security Controls.

3.1.1 National Institute of Standards and Technology Cybersecurity Framework

The National Institute of Standards and Technology (NIST) was given a role to develop cyber security risk framework for critical infrastructure by the Cybersecurity Enhancement Act of 2014 in The United States of America. The purpose of the Cybersecurity Enhancement Act of 2014 ordered National Institute of Standards and Technology to identify a framework for organisations in the critical infrastructure. (National Institute of Standards and Technology 2018b, 1.)

The NIST Cybersecurity Framework is technology neutral and refer to other standards, guidelines and best practices. With the taxonomy and mechanisms provided by the framework, organisations can detail their current state of cyber security, a target state of cyber security, use continuous and repeatable processes to identify and prioritize improvement opportunities, gauge progress to the target state and cyber security risk communication for stakeholders. Organisations can use the framework as a compliance for their own requirements for cyber security. Organisations have different sizes, risks, threats, vulnerabilities and risk tolerances; however, the framework is not designed with “one-size-fits-all” approach, and it is intended to be used organisation of any size or focus to reduce and improve management of cyber security risks. Risk management is defined as a continuous process of identifying, evaluating, and responding to risks. Organisations, through the implementation of risk management services and programs, are offered the capability to assess and convey adjustments to the cyber security program they have. Additionally, the cyber security framework offers organisations the ability to assertively select and administer improvement in cybersecurity risk management for the ICS and IT environments. This framework is alterable to provide an adjustable and risk-based execution that can be used with a wide range of cybersecurity risk management processes. The risk management can cover the whole organisation or specific parts or processes. A risk-based approach is used to cyber security risk management, which contains three parts as the Framework Core, the Framework Implementation Tiers and the Framework Profiles. These three parts will be explained later in this chapter. (National Institute of Standards and Technology 2018b, 1-4.)

The Framework Core defines the required activities to achieve a desired state of a cyber security control. The Framework Core extends key cyber security outcomes recognized by stakeholders as beneficial in managing cyber security risk. The Framework Core provides a hierarchical approach with four elements which are Function, Category, Subcategory and Informative Reference. The Framework Core structure is illustrated in the image below (see Figure 2). Functions are the top-level activities and they are Identify, Protect, Detect, Respond and Recover. Each function is divided into categories which are further divided into subcategories and informative references. The Identify function concentrates on building up the foundation for managing cyber security risks by understanding the important business functions with their related and required resources. The Protect function reduces the likelihood and the effect against cyber security event. The Detect function helps to discover the occurrences of cyber security events. The Respond function helps with planning and reacting against security incidents. The Recover function reduces the time of recovery to the normal operations during an occurrence of a security incident. (National Institute of Standards and Technology 2018b, 5-8.)

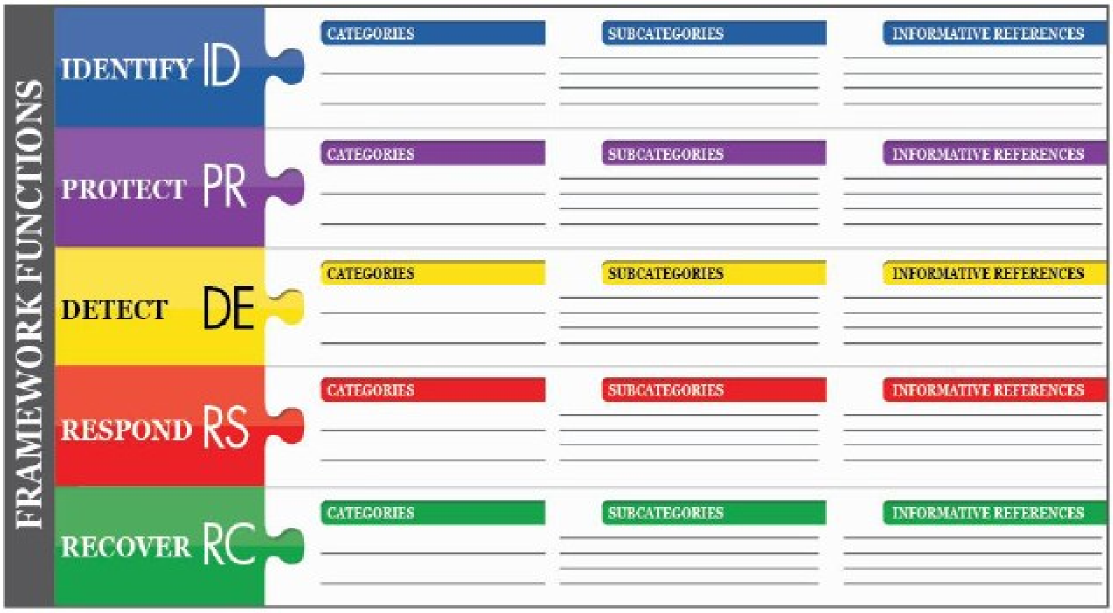


Figure 2. The structure of the Framework Core (National Institute of Standards and Technology 2018b, 6)

The tiers in the Framework Implementation Tiers measure the capability of an organisation how it assesses and mitigates cyber security risks. The tiering system has four levels, from lower to higher the tiers are Partial, Risk-Informed, Repeatable and Adaptable. At the Partial tier, the risk management is carried out ad hoc, and the awareness of risk management is very low. At the Risk-Informed tier, the risk management takes place at the higher level; however, no organisation-wide risk policy exists. At the Repeatable tier, the organisation has created a formal organisation-wide risk management process, and the security policy supports the risk management process. In the Adaptable part of the tiers, organisations will adjust their cyber security policies based upon found and learned discoveries. It is analytics driven and offers insights and preferable practices. Organisations consistently learn from the security events that take place within the organisation and in turn, share this information with a larger network. (Cipher N.d.)

A Framework Profile is a combination of Functions, Categories and Subcategories, aligned with the organisation's business requirements, risk tolerance and resources. With a Profile an organisation can build a roadmap to reduce a risk as Profiles can indicate the current and target states of cyber security. With Profiles for current and target stages an organisation can use those Profiles to create a gap analysis. A risk-based approach by prioritizing gap mitigation helps the organisation to move towards the next tier. (National Institute of Standards and Technology 2018b, 11.)

3.1.2 ISO27001 Standard

The ISO 27000 standard series is about information security management systems standards which provide universal model to implement and operate a management system. With the information security management system, it is possible to create a framework to manage and protect organisations information assets. When an organisation is developing information security management system, the most necessary standard is ISO 27001. The ISO 27001 standard gives organisation the necessary requirements to fill for information security management system. The standard introduces organisations cyclic model Plan-Do-Check-Act which is very important to make the management a continuous process. (ISO27000.org)

The essential parts for framework in the ISO 27001 standard are chapters 4 to 10. In these chapters define the context of the organisation, leadership, planning, support, operation, performance evaluation and improvement within the information security management system (SFS-EN ISO/IEC 27001:2017, 2).

To build information security management system an organisation defines the context of the organisation. This means that the organisation needs to define what and why they want establish information management system. Who are relevant parties for the information management system and what requirements they cause? An organisation needs to define a clear scope for the information management system. (SFS-EN ISO/IEC 27001:2017, 4-5)

For information security management system to be effective, a good leadership is needed; therefore, organisation’s top management involvement and commitment is required. Information security policy or policies are required and need to be enforced. The essential organisational roles, responsibilities and authorities for information security need to be assigned and communicated. (SFS-EN ISO/IEC 27001:2017, 5-6)

The information security management system related planning requires establishing a risk management for information security risks. The objectives for information security need to have a plan to achieve them. (SFS-EN ISO/IEC 27001:2017, 8-10)

Support that the information security management system requires are resources, competences, awareness, communication and documentation (SFS-EN ISO/IEC 27001:2017, 11-12).

To operate the information security management system, several processes are required, and the organisation must implement and control them. The risk assessment for information security must be carried out frequently or when changes happen. Information security risk treatment plan must be implemented. (SFS-EN ISO/IEC 27001:2017, 12)

The information security management system requires continuous or periodical evaluation of its performance by monitoring, measuring, analysing, evaluating the information security management system. Improvement of the information security and information management system can be achieved from performance evaluations. (SFS-EN ISO/IEC 27001:2017, 12-14)

3.1.3 CIS Controls

The Central for Internet Security, Inc, in short CIS, is a non-profit organisation which has collected a CIS Controls to provide a comprehensive cyber defence capability to protect systems and networks. Like the other frameworks it is not a one-size-fits-all solution and organisations must understand their criticalities. The CIS Controls are a set of best practices which have been developed by experienced IT professionals in the field of cyber defence. Due for being developed by IT professionals with first-hand experiences the CIS Controls have been able to develop into a very effective solution to combat against common or advanced attacks. The CIS Controls reflects to the five critical guidelines of an effective cyber defence which are offense informs defence, prioritization, measurements and metrics, continuous diagnostics and mitigation, and automation. The CIS Controls are meant to help organisations to prioritize their focus on the most important actions for selecting the cyber security controls to protect themselves. (The Center for Internet Security 2019, 1-3)

To scale the framework at different sized organisations the CIS Controls has introduced Implementation Groups, in short IGs). There are three Implementation Groups which organisations may use based on their cyber security capabilities. The usual division the Implementation Groups works that micro-enterprises self-classify themselves to IG1, small and medium enterprises IG2 and large enterprises IG3. Other criteria which organisations may use to identify their Implementation Group are the sensitivity of data and criticality of service, cyber security skill level and available resources for cyber security. The Implementation Groups are cumulative as for example IG2 contains all sub-controls defined in the IG1. The recommended path to implement the CIS Controls start from the lower Implementation Group Sub-Controls to the higher. (The Center for Internet Security 2019, 4-5)

The CIS Controls are divided to three major categories which are Basic, Foundational and Organisational. There are six Controls in Basic, ten Controls in Foundational and four Controls in Organisational categories. The Controls in Basic category help to secure the environment with identifying assets and vulnerabilities, basic device hardening and logging. In the Foundational category the Controls are more technology oriented. Organisational category Controls strengthen and tests the organisation capabilities against cyber threats. (See Figure 3, which shows the Controls in the framework.) (The Center for Internet Security 2019, 1-70)

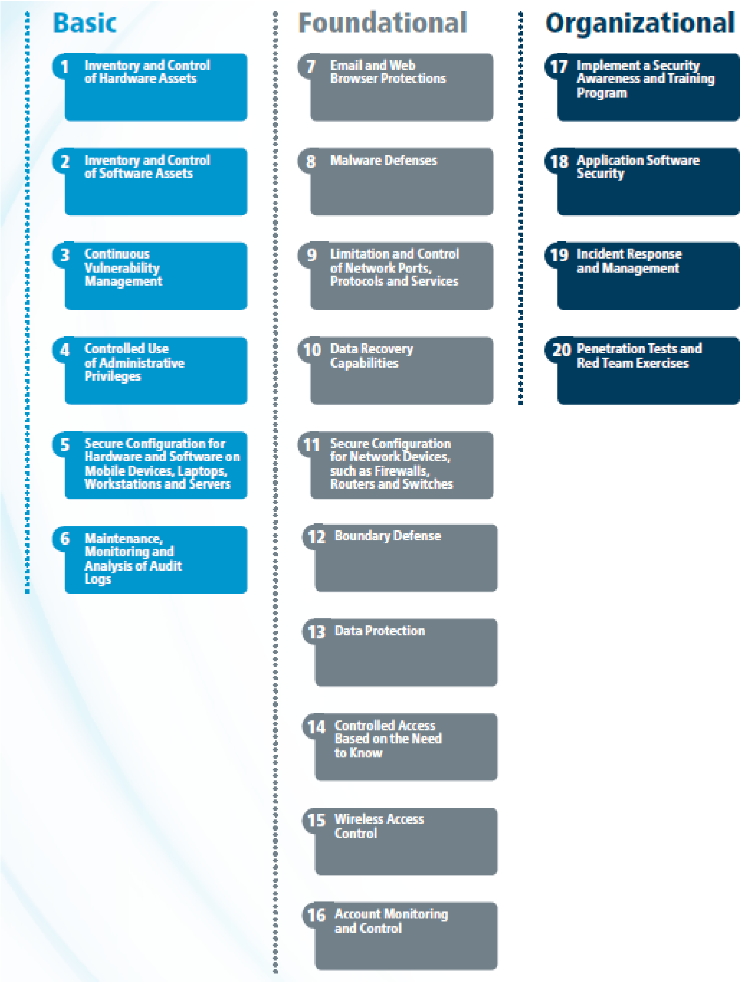

Basic
1 Inventory and Control of Hardware Assets
2 Inventory and Control of Software Assets
3 Continuous Vulnerability Management
4 Controlled Use of Administrative Privileges
5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6 Maintenance, Monitoring and Analysis of Audit Logs
Foundational
7 Email and Web Browser Protections
8 Malware Defenses
9 Limitation and Control of Network Ports, Protocols and Services
10 Data Recovery Capabilities
11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12 Boundary Defense
13 Data Protection
14 Controlled Access Based on the Need to Know
15 Wireless Access Control
16 Account Monitoring and Control
Organizational
17 Implement a Security Awareness and Training Program
18 Application Software Security
19 Incident Response and Management
20 Penetration Tests and Red Team Exercises

Figure 3. CIS Controls (The Center for Internet Security 2019)

3.2 Cyber Security Maturity Models

A maturity model is a collection of attributes, characteristics, patterns or indicators that contain the progression of capability in a discipline. The overall content of the model typically provides the best practices and may include standards or other codes of practices. In other words, a maturity model provides a benchmark against which an organisation can evaluate their current level of processes, methods, and capability of its practices. Furthermore, this allows the organisation to set goals and priorities for potential improvement. This also allows for the organisation to compare how its competitors or peers are performing overall by examining the capability of such competitors. (US Department of Energy 2014, 3.)

In order to measure progression within a cyber security maturity models, these models typically have what are referred to as levels along a scale. The Cybersecurity Capability Maturity Model (C2M2) for example, uses a scale of maturity indicator levels (MIL) of 0-3, which will be discussed in more detail in a later section. Along with each level there is a set of attributes that describe and define the level. If these attributes are present in the organisation, it has achieved the described level. The effectiveness of having such a level scale enables the organisation to determine its current and future state which is guaranteeably more mature and identify what it must do to achieve that future state. (ibid.)

The maturity models selected for this literature review had requirement that these models are known, adaptable to cyber security and contain comparable features. The selected maturity models are Capability Maturity Model, Cybersecurity Capability Maturity Model and ITScore. Other maturity models for cyber security exist and there are previous researches for example by Le&Hoang (2016) who researched maturity models supporting cyber security.

3.2.1 Capability Maturity Model (CMM)

The capability maturity model, in short CMM, is an early maturity model developed to improve quality of software development; however, it is widely applied in multiple fields and has been evolved into other cyber security maturity models. The strengths of this maturity model for cyber security lie in comprehensive management processes and it has wide coverage to be extended for security domains. (Le&Hoang 2016, 2.)

The capability maturity model has been shown to increase the effectiveness and efficiency of security programs. This is obtained through focusing on a thorough and repeatable security process, in which self-improvement becomes more automated and integrated into the operational infrastructure. (Acohido 2015.)

In the capability maturity model, there are five maturity levels, namely initial, repeatable, defined, managed and optimizing. The higher level the maturity level is the more complex and higher requirements it has. The previous maturity level requirements must be maintained on the higher level. (See Figure 4, which illustrates the maturity level progression in the capability maturity model.) (Le&Hoang 2016, 5.)

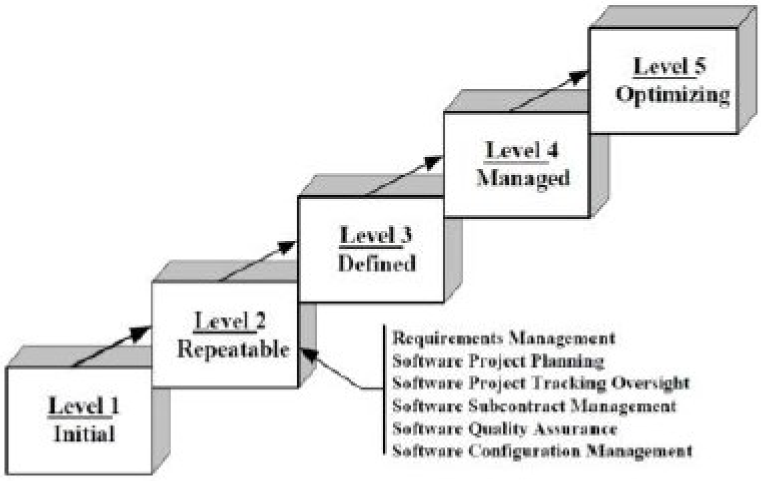

Level 1
Initial
Level 2
Repeatable
Level 3
Defined
Level 4
Managed
Level 5
Optimizing
Requirements Management
Software Project Planning
Software Project Tracking Oversight
Software Subcontract Management
Software Quality Assurance
Software Configuration Management

Figure 4. CMM maturity levels (Le&Hoang 2016, 5)

3.2.2 Cybersecurity Capability Maturity Model (C2M2)

The Cybersecurity Capability Maturity Model, in short C2M2, enables organisations to evaluate cyber security capabilities consistently. This is designed by self-evaluation methodology via a toolkit, which may be adapted later for a more rigorous evaluation in the future. The intended model is used for strengthening the cyber security capabilities of organisations, enabling organisations to consistently and effectively benchmark and evaluate their cyber security capabilities. Additionally, sharing knowledge, best practices, and relevant references across the organisation improve organisations cyber security capabilities. (US Department of Energy 2014, 1.)

There are ten domains in the Cybersecurity Capability Maturity Model and each of them represents a different grouping of a security practice. (See Figure 5, which explains the structure of domains.) These ten domains are Risk Management, Asset, Change, and Configuration Management, Identity and Access Management, Threat and Vulnerability Management, Situational Awareness, Information Sharing and Communications, Event and Incident Response, Continuity of Operations, Supply Chain and External Dependencies Management, Workforce Management and Cybersecurity Program Management. (US Department of Energy 2014, 6-8.)

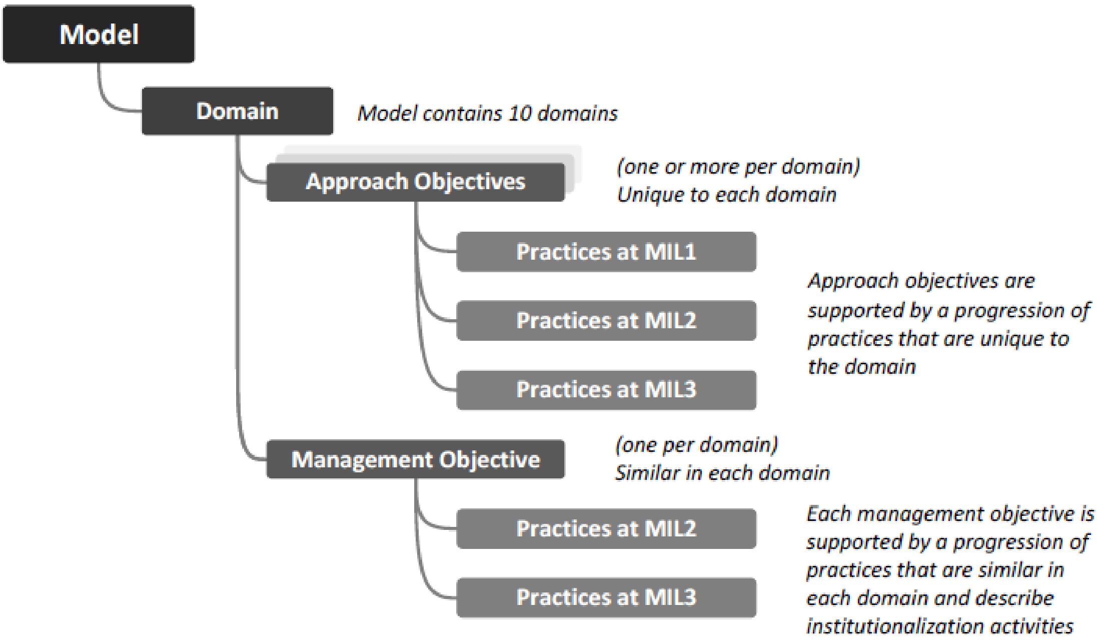

Model
Domain
Model contains 10 domains
Approach Objectives
(one or more per domain)
Unique to each domain
Practices at MIL1
Practices at MIL2
Practices at MIL3
Approach objectives are supported by a progression of practices that are unique to the domain
Management Objective
(one per domain)
Similar in each domain
Practices at MIL2
Practices at MIL3
Each management objective is supported by a progression of practices that are similar in each domain and describe institutionalization activities

Figure 5. C2M2 domain elements (US Department of Energy 2014, 7)

The Cybersecurity Capability Maturity Model defines four maturity indicator levels, known from here on as MILs (MIL0-MIL3), which are applied independently to each domain within the model. In order to understand how to apply the model correctly, there are four aspects of the MIL. The first aspect is that the maturity indicator levels apply independently to each domain, in example each organisation using the model may be operating at varying MIL indicators or ratings for each domain. For example, a company could be operating at MIL1 in one domain and MIL3 in another domain. Secondly, the MILs are cumulative within each domain, which means that to earn a MIL in any given domain, one must perform all the practices in that specific level and the levels preceding it. Thirdly, an effective strategy for using the model to guide cyber security improvement is to establish a target MIL for each domain. Finally, the achievement an organisation wishes to have with each MIL should align with the business objectives. It may not be considered cost effective or align with business goals to achieve the highest MIL in each domain. (US Department of Energy 2014, 8-13.)

The Cybersecurity Capability Maturity Model is aimed at critical infrastructure and was developed by the US Department of Energy. The main goal for the Cybersecurity Capability Maturity Model is to support organisations to assess and refine their cyber security. There are ten domains which contain sets of cyber security practices. To follow these practices, an organisation can improve their maturity in each domain and eventually reach a higher domain. The model has been adapted to provide cyber security maturity models for other critical industry subsectors such as electricity (ES-C2M2) and oil and natural gas (ONG-C2M2). (Le&Hoang 2016, 6.)

3.2.3 Gartner ITScore

Gartner ITScore offers a diagnostic tool to measure maturity for various areas such as security and risk management. ITScore concerning security and risk management focuses on improvement of security and risk management programs in six domains of security and risk management by finding gaps and risks among those six domains. These six domains are business continuity management, compliance, identity and access management, security management and risk management. ITScore measures an organisation’s maturity model at five levels based on the processes the organisation uses. With the help of ITScore it is possible to increase the visibility of security programs and their risks. It also helps to find gaps between processes and controls related to the process. These findings and information demonstrate how valuable improvements in the maturity are and help to justify costs for improvements. ITScore guides organisations in organisation structure changes to support improvements and communications to internal and external stakeholders. Improved maturity enhances business processes. (Proctor 2014, 1-4).

Gartner ITScore maturity levels are Initial, Developing, Defined, Managed and Optimizing. At the first level of maturity, Initial, the organisation’s processes may not even exist and if they exist, the processes are ad hoc, separated, unorganized and based on IT needs. A need for improvements may be recognized; however, there are no responsibilities nor program in place. At the second level of maturity, Developing, an organisation has a small group of people who have realized the need for official security program, and the management may have committed to improvements. Usually organisations have started to react on requirements, assign responsibilities and design plans for implementations. At the third level of maturity, Defined, the whole organisation is committed to a security program and its processes and the performance is measured. At the fourth level of maturity, Managed, the organisation has implemented improvements to close the identified gaps, and decisions for new improvements are designed to support business needs and associate risks. At the fifth level of maturity, Optimizing, the security program is a part of the business strategy and there is an enterprise-wide risk. (See Figure 6, where Proctor visualizes the maturity improvement through the levels in ITScore.) (Proctor 2014, 2)

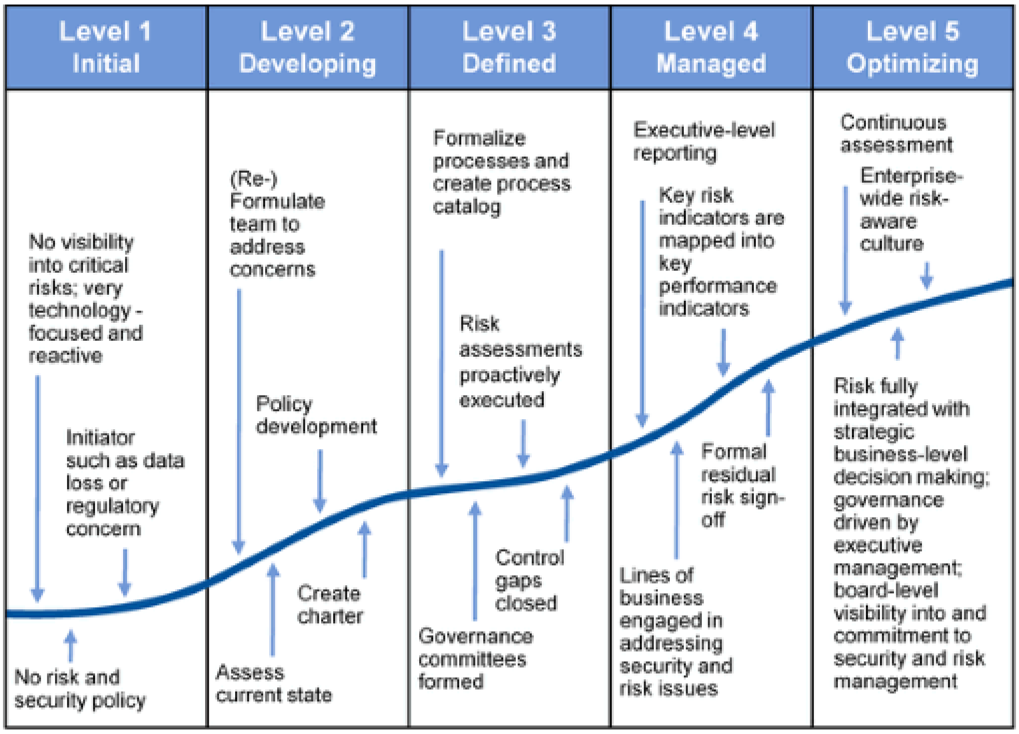

Level 1 Initial
Level 2 Developing
Level 3 Defined
Level 4 Managed
Level 5 Optimizing
No visibility into critical risks; very technology - focused and reactive
Initiator such as data loss or regulatory concern
No risk and security policy
(Re-) Formulate team to address concerns
Policy development
Create charter
Assess current state
Formalize processes and create process catalog
Risk assessments proactively executed
Control gaps closed
Governance committees formed
Executive-level reporting
Key risk indicators are mapped into key performance indicators
Formal residual risk sign-off
Lines of business engaged in addressing security and risk issues
Continuous assessment
Enterprise-wide risk-aware culture
Risk fully integrated with strategic business-level decision making; governance driven by executive management; board-level visibility into and commitment to security and risk management

Figure 6. ITScore maturity levels of security and risk management (Proctor 2014, 2)

3.3 Vulnerability management

Vulnerability management is a layer of cyber security aiming to prevent risks from being realized. With vulnerability management organsations can find threats and vulnerabilites in their devices, operating systems, services and libraries. Vulnerability management is not limited to finding vulnerabilities but also to help mitigate risks related to vulnerabilities. This literature reviewes two vulnerability management guides with requirement that they were created by trusted and known author and have comparatible structures in the vulnreability management process. These selected vulnerability management guides are SANS Institute guide for implementing a vulnerability management process and US-CERT CRR Supplemental Resource Guide for vulnerability management. Vulnerability scanners and common vulnerability scoring system are introduced to increase basic knowledge and understanding about vulnerability management in practice and are not in the scope of comparison for this research.

Palmaers (2013) describes vulnerability management as a process where IT vulnerabilites are found and their risks are evaluated. Eventually, the risks are to be assessed to be mitigated or accepted. The vulnerability management is needed to help an organisation to protect themselves against cyber-crime and its related risks. The vulnerability management is an important part of an organisations security layers for identifying and controlling security risks. With a vulnerability management process the organisation receives continous information about the vulnerabilites in the environment and the related risks. By finding and mitigating vulnerabilities and their related risks, the organisation is able to protect their assests and environment from cyber criminals accessing its networks and assets to steal information or cause other disturbance. Without implementation of vulnerability management the organisation is very unaware of IT related security risks; hence the vulnerability management can be seen as another tool for better risk management. The mature vulnerability management process allows IT Department, management and asset owners to make better decisions on remediating vulnerabilities and thus, reducing risks. The key requirements for a working vulnerability management are assigned roles and responsibilities and other stakeholders kept aware of whole vulnerability management process. The selection of the right technology to perform vulnerability scanning is required as well as proper configuration of the scans. The first scans of vulnerability scanning may produce a huge amount of found vulnerabilities; therefore, limiting the remediation to high or critical severity vulnerabilities first and later moving to other lower severity levels makes the approach easier. (Palmaers 2013, 2; Palmaers 2013, 20.)

3.3.1 SANS Institute guide for implementing a vulnerability management process

Tom Palmaers (2013) has written the paper Implementing a Vulnerability Management Process for SANS Institute. The paper describes a vulnerability management process objective, roles and responsibilities and provides a step-by-step guide of phases in the vulnerability management process.

The objective in SANS Institute guide about implementing a vulnerability management process is in detecting and remediating vulnerabilities in a reasonable timeframe. An organisation may perform a vulnerability scan very infrequently such as annually or quarterly or not at all. When vulnerability scans occur infrequently there is a possibility that a known vulnerability exists in the IT infrastructure for a very long time before the next scan finds the vulnerability. During this vulnerable period the system or systems may have been compromised before the scan has found them and mitigations against the vulnerability are done. Running vulnerability scans more frequently such as weekly or monthly allows the organisation to discover and mitigate vulnerability within a reasonable and safer time to shorten the vulnerable period as shown below. (See Figure 7 by Palmaers). Having a vulnerability management process can help the organisation to reduce risks. (Palmaers 2013, 3-4.)

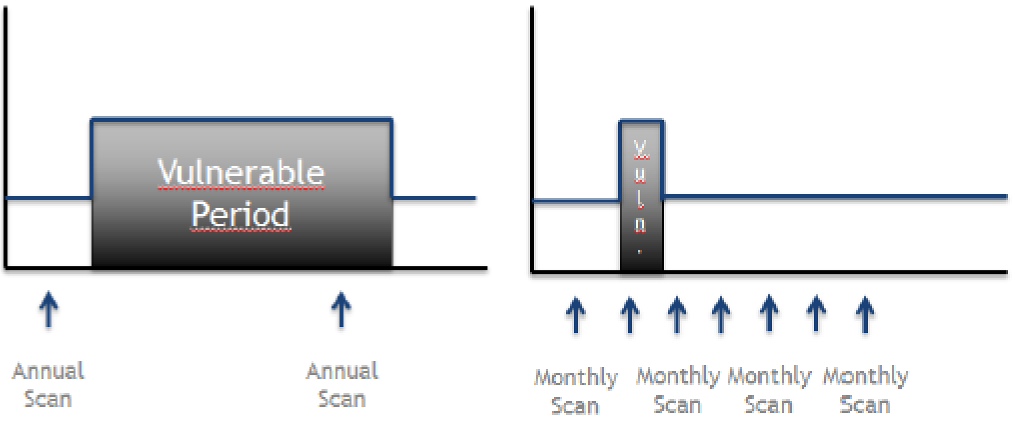


Figure 7. Vulnerable period difference in annual and monthly scanning (adapted from Palmaers 2013, 3-4)

The roles and responsibilities for vulnerability management process require that an organisation can identify Security Officer, Vulnerability Engineer, Asset Owner and IT System Engineer. The Security Officer owns and designs the vulnerability management process. The Vulnerability Engineer is responsible for configurations and schedules of vulnerability scans. The Asset Owner is the responsible for the assets in vulnerability management and makes decisions about vulnerability mitigations or accepts the risks a vulnerability may cause to the asset. IT System Engineer is responsible for remediation implementation. (Palmaers 2013, 4-5.)

The vulnerability management process of SANS Institute consists five phases, namely preparation, vulnerability scanning, defining remediating actions, implementing remediating actions and rescanning. During the preparation the Security Officer defines the scope for a vulnerability management process. First, in the scope definition it is very important to decide which systems are part of the organisation's vulnerability management process. Second, it is also important to define vulnerability scan type and whether the scan is made from the external or internal network. Third, a good rule of thumb for first scans is to keep the scope small enough, because this can limit the amount of discovered vulnerabilities to make it more manageable. Fourth, for the initial vulnerability scan a risk-based approach is recommended. When the scope has been defined Security Officer should inform the stakeholders, especially IT or whichever department is monitoring security systems should be made aware of upcoming scans. Last step in the preparation phase is to plan the scans; in example how vulnerability scans work. It is important to test scanning well in the testing environment and if possible, find out how long individual scans take. Depending on vulnerability scan configuration a single scan may take few minutes or hours. (See Figure 8, which illustrates the preparation phase.) (Palmaers 2013, 5-8.)

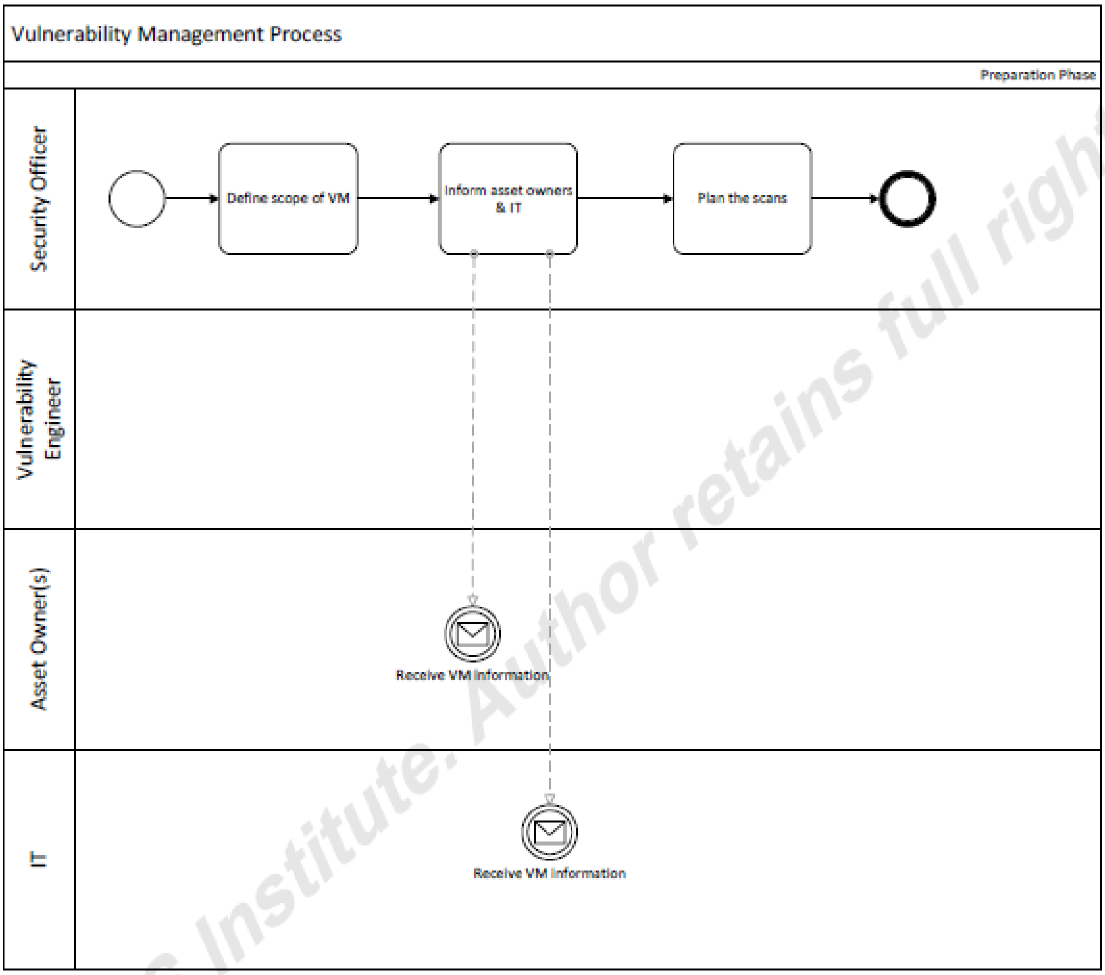


Figure 8. Vulnerability management process preparation phase (Palmaers 2013, 6)

During the initial scan phase of SANS Institute vulnerability management process, the first actual vulnerability scans are performed. It is important to monitor and report all anomalies carefully for future reference. Initial scan results contain information of which importance differs based on the recipient. For example, the Security Officer and management prefer information about the total amount of vulnerabilities and their severity. On the other hand, the Asset Owners only want information about vulnerabilities they are accountable for. Lastly, the IT department wants information about vulnerabilities with technical details and recommendations for remediation. (See Figure 9, which illustrates the initial scan phase.) (Palmaers 2013, 10.)

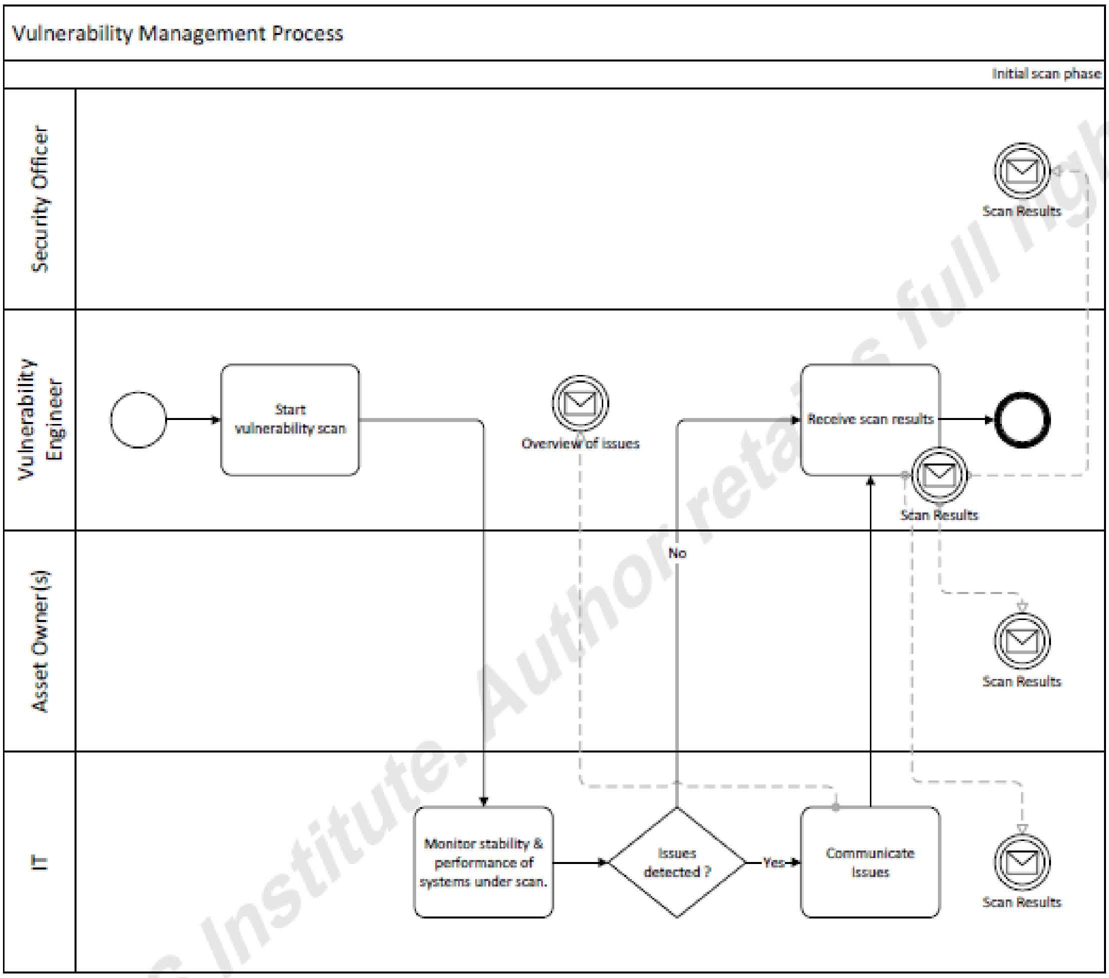


Figure 9. Vulnerability management process initial scan phase (Palmaers 2013, 10)

The purpose of the remediation phase is to decide what to do with and how to mitigate the found vulnerabilities. The Security Officer is responsible for analysing the vulnerabilities and their risks. The IT department finds out solutions how the vulnerabilities are to be remediated with technical options such as patching, access restriction or configuration hardening. The Security Officer monitors that the vulnerability remediations have proper priority to complete remediations by the deadlines set by the Security Officer. There are multiple ways to monitor remediation such as ticketing systems, spreadsheet file or built-in tracker of a vulnerability scanning product. The Asset Owners make sure to schedule the timeframes when the vulnerability remediations take place. The timeframe depends on how fast the organisation can respond to the risks. If for some reason vulnerability remediation does not remove or mitigate the risk to an acceptable level, the Asset owners should use the risk management processes for accepting the risk. (See Figure 10, which illustrates the remediation phase.) (Palmaers 2013, 11-12.)

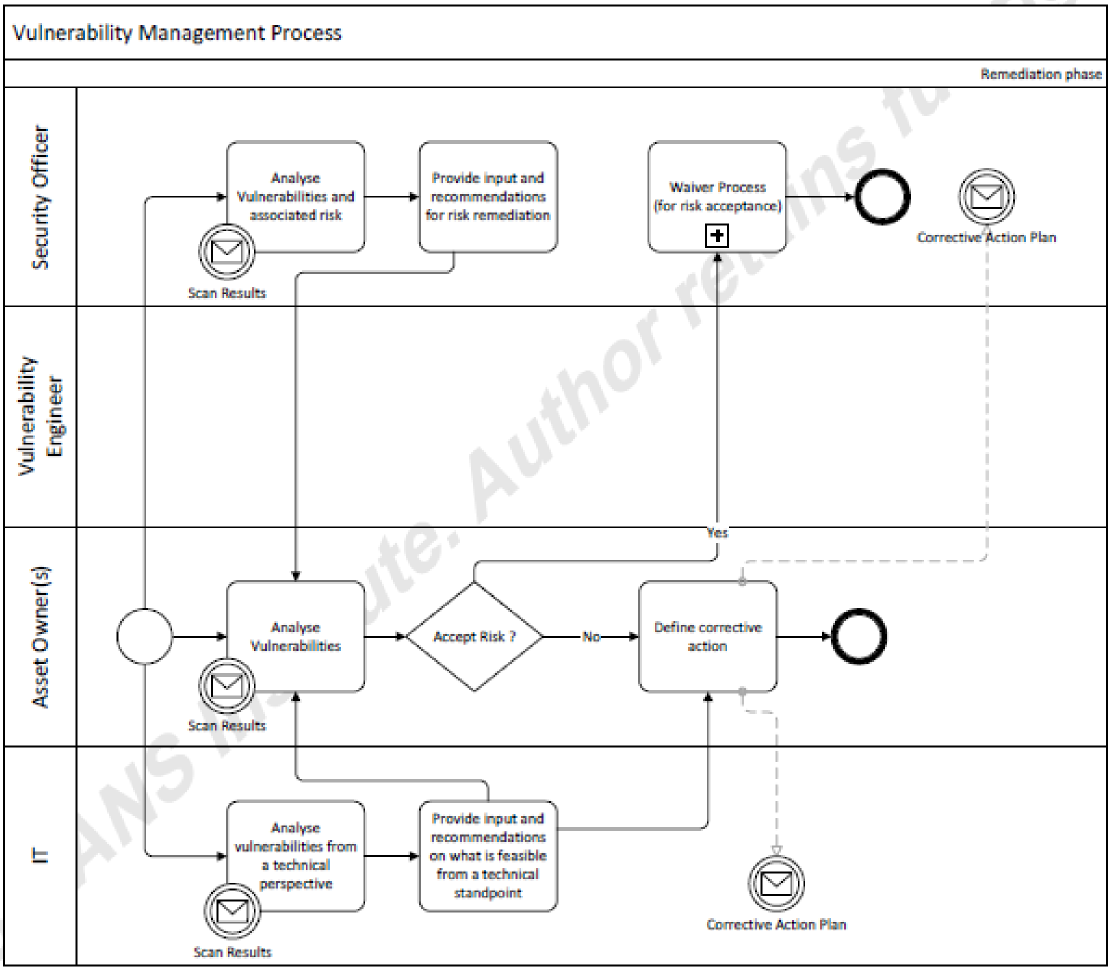

Vulnerability Management Process
Remediation phase
Security Officer
Vulnerability Engineer
Asset Owner(s)
IT
Analyse Vulnerabilities and associated risk
Scan Results
Provide input and recommendations for risk remediation
Waiver Process (for risk acceptance)
Corrective Action Plan
Yes
Analyse Vulnerabilities
Accept Risk ?
No
Define corrective action
Scan Results
Analyse vulnerabilities from a technical perspective
Provide input and recommendations on what is feasible from a technical standpoint
Scan Results
Corrective Action Plan

Figure 10. Vulnerability management process remediation phase (Palmaers 2013, 11)

The remediations should be completed before the deadline, during their scheduled timeframes, and all encountered problems should be documented. The Asset owner should define secondary and other choices for remediation based on what the IT department and the Security Officer have recommended. (See Figure 11, illustrates the implementation of remediating actions phase.) (Palmaers 2013, 13.)

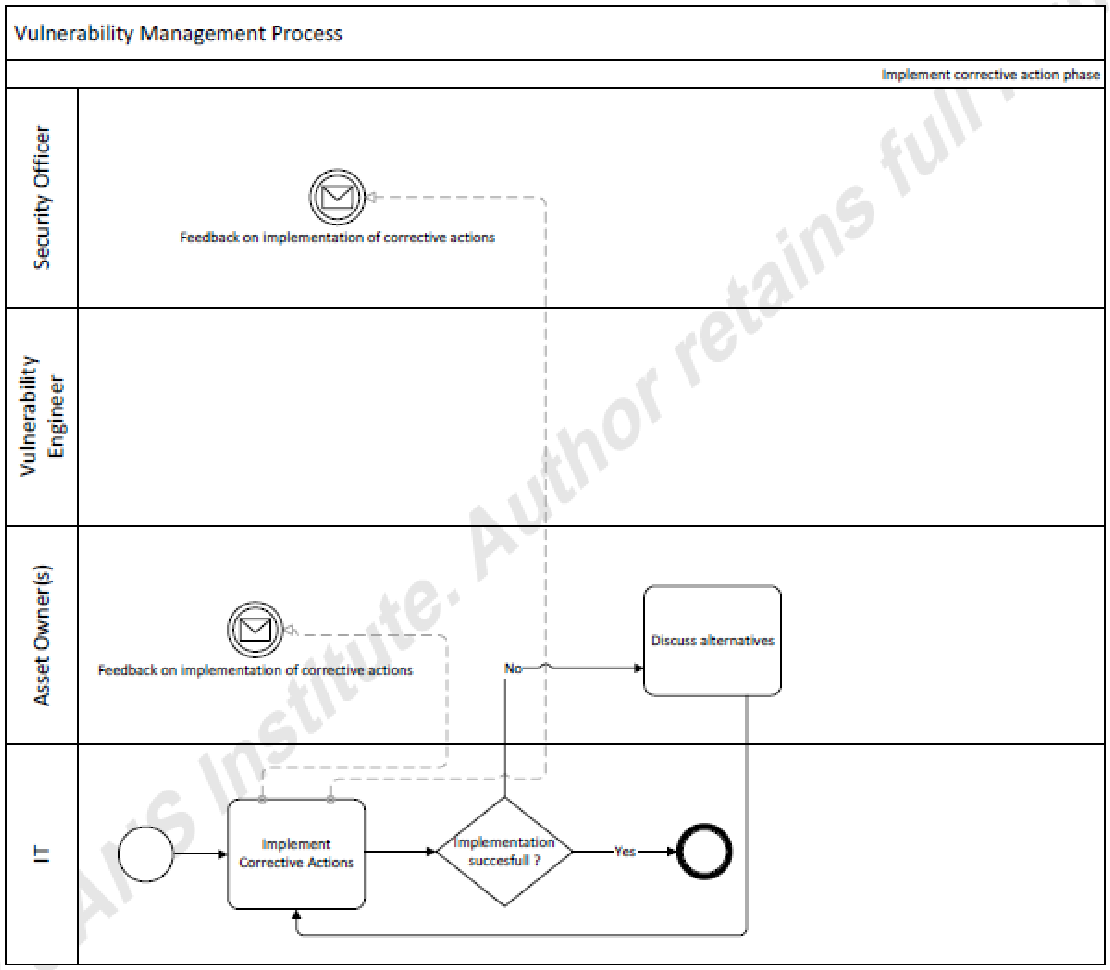

Vulnerability Management Process
Implement corrective action phase
Security Officer
Vulnerability Engineer
Asset Owner(s)
IT
Feedback on implementation of corrective actions
Feedback on implementation of corrective actions
Discuss alternatives
No
Implement Corrective Actions
Implementation succesfull ?
Yes

Figure 11. Vulnerability management process implementation of corrective action phase (Palmaers 2013, 13)

The final step for SANS Institute vulnerability management process is the rescan step where a vulnerability scan using the same scanning configuration as before verifies the efficacy of remediations. With the rescan it is possible to find possible configuration errors in scans or remediations. The rescan is usually performed after the deadline for remediations has passed. The rescan should be reported to the involved roles and stakeholders as previously in the initial scan step. After the rescan and its remediations continuous vulnerability scanning needs to be agreed on with the Security Officer and Asset Owners. The frequency of scanning and length for the remediation should be learnt from the initial scan and rescan based on how well the organisation can intake risks and is capable performing remediation of vulnerabilities. As the maturity of the organisation increases, the risk intake and remediation performance improve, and the frequency of scanning may be changed from monthly to weekly for more rapid response against vulnerabilities. Based on all information from successful scanning and remediation as well occurred problems or anomalies the vulnerability management process should be re-evaluated and improved. (See Figure 12, which illustrates the rescan phase of the vulnerability management process.) (Palmaers 2013, 14-15.)

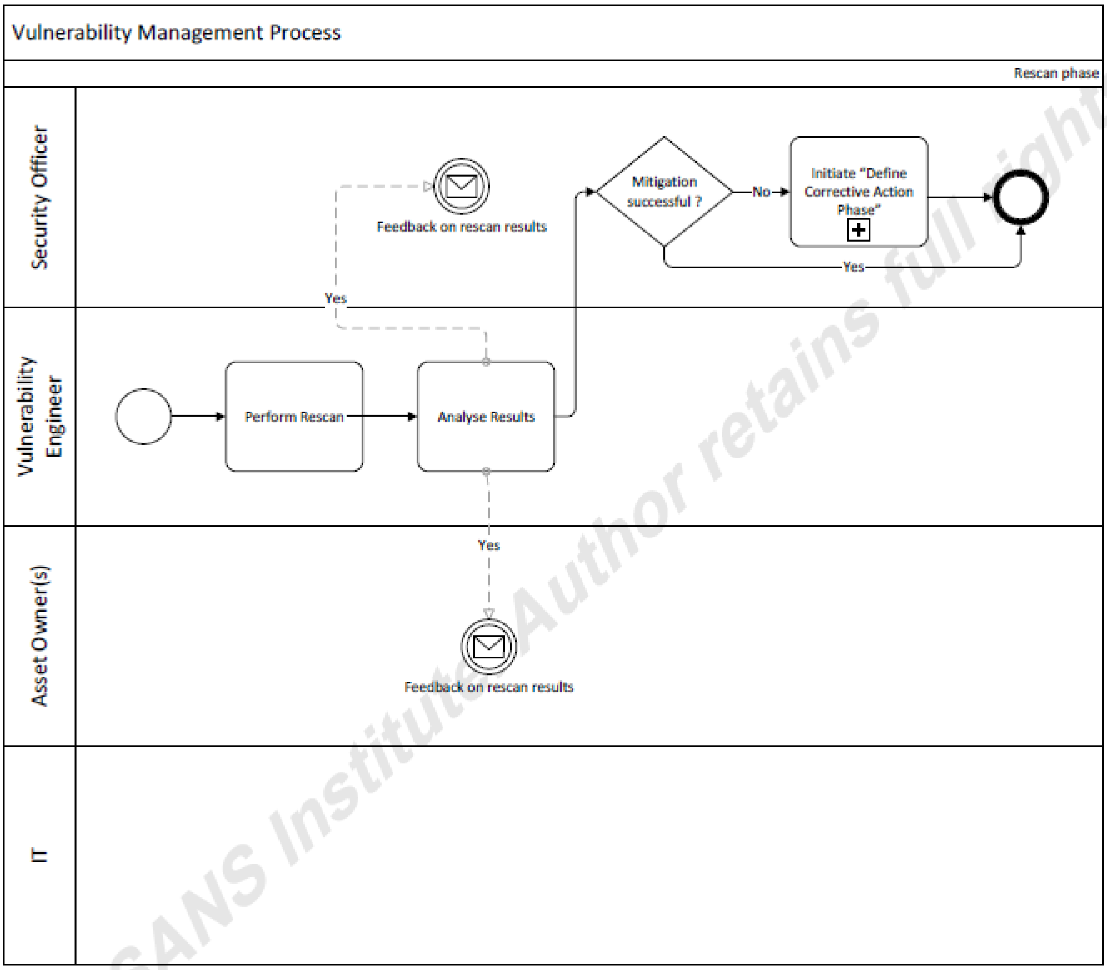


Figure 12. Vulnerability management process rescan phase (Palmaers 2013, 14)

3.3.2 CRR Supplemental Resource Guide for vulnerability management

CRR Supplemental Resource Guide for vulnerability management is fourth volume of the US Department of Homeland Security developed guide series to help organisations to improve cyber security during a Cyber Resilience Review. The Cyber Resilience Review is an assessment which helps organisations to understand and measure qualitatively their IT operations ability adapt risks against their key operational capabilities. This guide is meant to help organisations beginning their vulnerability management process and is compatible with National Institute of Standards and Technology Cybersecurity Framework. The vulnerability management process is divided into four phases Define a Vulnerability Analysis and Resolution Strategy, Develop a Plan for Vulnerability Management, Implement the Vulnerability Analysis and Resolution Capability and Assess and Improve the Capability. (See Figure 13, which describes the continuous vulnerability management process.) Also, the phases are divided further into steps, which will be introduced later in this chapter. Furthermore, this guide gives the readers better understanding about vulnerability management processes what the process implementation and running requires. The guide provides checklists to follow in various phases of the vulnerability management process. (Carnegie Mellon University 2016, 1-7.)

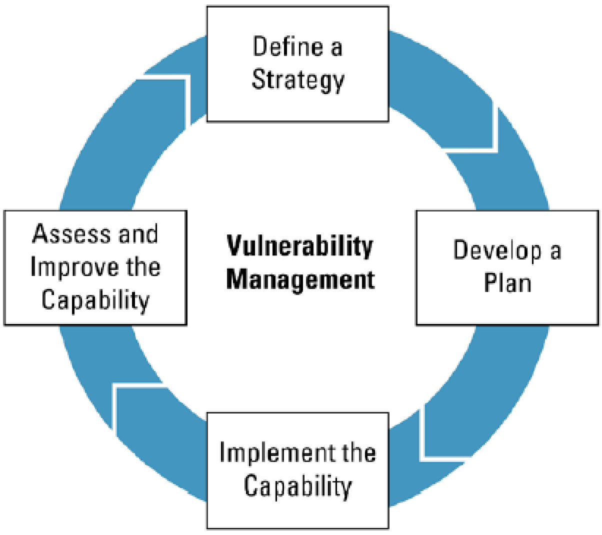


Figure 13. Vulnerability management top-level process (Carnegie Mellon University 2016, 4)

Define a Vulnerability Analysis and Resolution Strategy is a phase where reasoning, requirements, resources and goals for vulnerability management are defined consists from three steps about determining the scope for vulnerability management, selecting allowed methods for vulnerability assessment and resourcing activities. During the first step of the determining the scope an organisation must decide about assets and services to be included into vulnerability management and the level of comprehension for vulnerability assessment. This requires documentation of possible assets, services and their criticality and defining the cyberspace for operations about the vulnerability management. The second step defines allowed methods in vulnerability management, to successfully perform vulnerability assessments there needs to be support from the stakeholders and management. There may be some requirements for the organisation from regulations or legal implications which guide selection of these methods. The third step is about resourcing to have the required amount of staff and budget to perform vulnerability management as well as determining responsibilities of stakeholders to make authoritative decisions. (Carnegie Mellon University 2016, 7-10.)

Develop a Plan for Vulnerability Management is a phase where a plan about vulnerability management implementation is created and it has eight steps which are

Define and document the plan, Define measures of effectiveness, Define training requirements, Determine tools aligned to the strategy, Identify sources of vulnerability information, Define the roles and responsibilities, Engage stakeholders, Develop a plan revision process. The first step puts the developed vulnerability management strategy into action and creates a plan how the strategy will be achieved. The plan consists creating a team for vulnerability management, coordinating with risk management, setting timeframes for vulnerability remediation, defining documentation guidelines, exception handling, scheduled activity and proactive activities definition. The second step is to define process monitoring and metering for reporting. The third step defines the requirements for training the staff performing vulnerability management. The fourth step guides through the vulnerability scanning tool selection which involves researching vulnerability assessment solutions, whitelisting scanning tools to use with exception options and reviewing selected tools regularly. The fifth step identifies assets and vulnerability data sources which may require creating asset inventory database and signing up for vendor security bulletin mailing lists. The sixth step assigns departments or persons into monitoring, remediation or authorization role. The staff with monitoring role is responsible for vulnerability analysis, documenting vulnerability information about found vulnerabilities and informing staff with remediation role. The staff with remediation role is responsible for mitigating vulnerability by patching, workarounds and elevating some vulnerabilities into risk management. The staff with authorization role is responsible for making decisions based on their knowledge about their managed environments. The seventh step is to make stakeholders aware about vulnerability management and their roles in it. These responsibilities could be input about department-specific requirements and following timeframes about remediations. The eighth step develops a process to revise the vulnerability management process regularly and improve if necessary. (Carnegie Mellon University 2016, 11-17.)

Implement the Vulnerability Analysis and Resolution Capability has seven steps about performing the vulnerability management. These seven steps are Provide training, Conduct vulnerability assessment activities, Record discovered vulnerabilities, Categorize and prioritize vulnerabilities, Manage exposure to discovered vulnerabilities, Determine effectiveness of vulnerability dispositions and Analyse root causes. The first step is to ensure train the staff about the process and the tasks, so they understand the workflow and their own and others’ roles in the vulnerability management. The second step is to perform the vulnerability scanning or assessments such as penetration testing. The third step is to document discovered vulnerabilities to predefined location or system where access is restricted only to those who need the information about vulnerabilities due the sensitivity of the information. The fourth step is to analyse the found vulnerabilities to make sure that they are relevant against the target and environment, are prioritized correctly and remediation responsibility is informed to the correct stakeholder. The fifth step describes a vulnerability remediation how the vulnerability is remediated, and remediation tracked. The remediation aims to reduce vulnerability exposure and bind it to the organisation risk management. The sixth step is to validate if the vulnerability remediation succeeded for example with a vulnerability scanner rescan. The seventh step analyses root causes to understand what the cause of vulnerability occurrence in the environment and document remediation actions was to enhance remediation or prevent vulnerability to occur in the future. (Carnegie Mellon University 2016, 19-26.)

Assess and Improve the Capability phase aims to vulnerability management process regular development and consists three steps which are Determine the State of the program, Collect and analyse program information and Improve the capability. The first step is to review the current state of the program and to find the gaps against the vulnerability management process offering and the needs from stakeholders. The second step is to collect and analyse all information that the vulnerability management program has created and verify that it is aligned with the vulnerability management strategy and how effective the vulnerability management process is. The third step is to address previously found gaps and other problems in the vulnerability management process to understand what in the process needs to be improved. (Carnegie Mellon University 2016, 27-29)

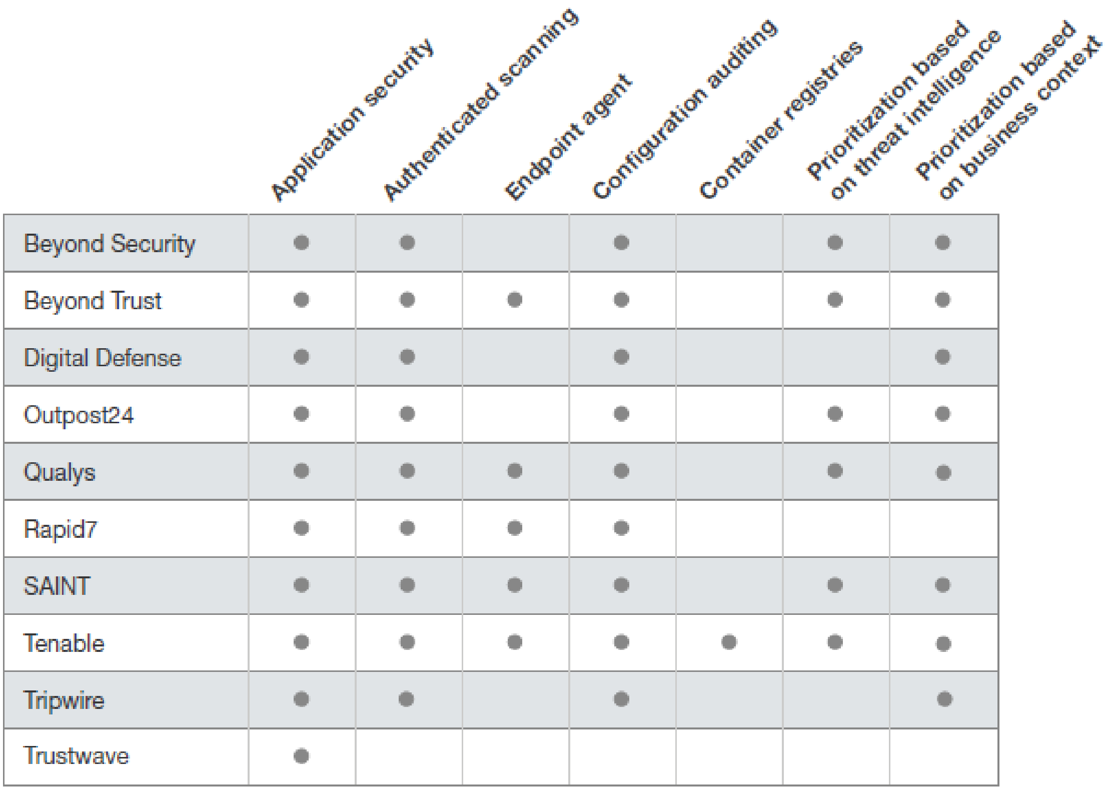
3.4 Vulnerability scanners

A vulnerability scanner is a tool to find vulnerabilities from operating system, device firmware, software or libraries for vulnerability management. Running the vulnerability scanners on a basic level does not require much technical skill from the operator as the most of the vulnerability scanning products can be operated from a graphical user interface. Palmaers (2013, 2-3) names McAfee, Qualys, Rapid7 and Tenable Network Solutions as vendors who offer commercial vulnerability scanning technology. He also mentions the existence of free open source vulnerability scanners. There are several other commercial vendors which are to be mentioned or introduced later in this chapter.

A vulnerability scanner is a technical solution which can be operated from a public or private cloud software as a service (SaaS) or on-premises. To get more accurate results the cloud based solutions require access to on-premises vulnerability scanners or otherwise the scanning is limited to organisations' public IP-addresses only or cause unnecessary risks by opening a firewall for scanning from outside to local networks. Palmaers recommends organisations to test multiple products carefully before deciding the solution because not all products meet the requirements set by the organisation. When the vulnerability scanning solution is selected the vulnerability scans need to be configured well to get the correct vulnerability information from the target and not to distrupt the target or other parts of the environment. (Palmaers 2013, 3-4.)

Vulnerability scanners provide multiple options to perform scans, and the scans should be considered to be performed either externally or internally. An external scan tries to find vulnerabilities from outside the network and can be used to validate all security layers between the scan target and the scanner. An internal scan shows vulnerabilities found inside the organisation's network. With the results it is possible to pinpoint vulnerabilities directly in the target system. When adding authentication against a scan target it is possible to gather very detailed and accurate results for the scan reports. Reporting is one key feature of most vulnerability scanning tools and a wide variety of different reports helps to assess the vulnerabilities and inform related stakeholders. (Palmaers 2013, 7-10.)

Today there are multiple vendors in the vulnerability management market while most the major market share is held by Qualys, Rapid7 and Tenable. Zelonis (2017, 5) compares multiple vulnerability management vendors with the provided features of the vulnerability scanner. These features are about application security scanning, authenticated scanning, agent based scanning, auditing configurations, container registries and prioritizating options. (See Figure 14, which illustrates the comparison of vulnerability scanner features.) (Zelonis 2017, 5-8)



	Application security	Authenticated scanning	Endpoint agent	Configuration auditing	Container registries	Prioritization based on threat intelligence	Prioritization based on business context
Beyond Security	●	●		●		●	●
Beyond Trust	●	●	●	●		●	●
Digital Defense	●	●		●			●
Outpost24	●	●		●		●	●
Qualys	●	●	●	●		●	●
Rapid7	●	●	●	●			
SAINT	●	●	●	●		●	●
Tenable	●	●	●	●	●	●	●
Tripwire	●	●		●			●
Trustwave	●						

Figure 14. Forrester Vendor Landscape: Vulnerability Management, 2017. Vulnerability scanner feature comparison (Zelonis 2017, 8)

Bhajanka & Lawson (2018) have researched various vulnerability assessment solutions to provide a guide for evaluating vendors and improving security programs. Their key findings consisted of five topics. First, all compared vendors had support for network-based and IT assets; however, for example the support of container vulnerability scanning varies. Second, the scanning against mobile technology and operational technology is almost non-exist. Third, the buyers are more interested in prioritizing analytics and remediation. Fourth, the support to scan assets on the cloud platforms is becoming available by native support or via a partnership with known cloud service providers. Lastly, the three major vendors Qualys, Rapid7 and Tenable dominate the market. The recommendations for the selection of the vulnerability assessment solution is that it should have integration options with the enterprise management or other third-party system to help assessing the workflow, options to help assessing found vulnerabilities based on the vulnerability severity or other factor. They should also consider a possibility to use multiple solutions to cover all critical assets. The measured key features of the vulnerability assessment solutions are web application scanning, cloud security posture assessment, operational technology assessment, threat and vulnerability management, breach and attack simulation tools, penetration testing, vulnerability assessment methods and analysis of vulnerability risk impact and remediation priorization. The guide compares strengths and weaknesses of the vendors or lists all their solution features to compare; in addition, it provides a good insight to what to expect from a vulnerability management solution. There are forty-five representative vendors within the whole range of features. (Bhajanka & Lawson 2018.)

3.5 Common Vulnerability Scoring System

Common vulnerability scoring system, in short CVSS, has three major version of which versions 2 and 3 are in use. The CVSS can be used to help prioritise vulnerability mitigations. (Martin 2020.)

Most vulnerability scanning tools report the severity rating of vulnerabilities based on a common vulnerability scoring system. The common vulnerability scoring system depends on how easy the vulnerability is to exploit and how severe an impact the exploitation causes. The common vulnerability scoring system has a significant flaw when the scale of critical vulnerabilities grows to find the most important vulnerabilities to remediate. (Bhajanka & Lawson 2018.)

4 Research results

4.1 Comparison of cyber security frameworks

To compare cyber security frameworks this research selects the following features:

- affiliation,
- vulnerability management controls,
- the levels hierarchy as in the number of controls and/or sub-controls,
- the amount of security focus areas and
- unique features.

The NIST Cybersecurity Framework was developed for the demand of critical industry sector in the United States of America. In the NIST Cybersecurity Framework the first level of hierarchy is Function, second is Category and third Subcategory. The NIST CSF has five security focus areas, Functions, which are divided into Categories and Sub-Categories. The NIST CSF is that it also has maturity model characteristics. The NIST CSF empathises risk management and does not contain similar guidance to implement controls such as ISO 27001 or CIS Controls. In NIST CSF the controls guide to other references such as ISO 27001, COBIT 5 and CIS Controls. (National Institute of Standards and Technology 2018b, 1-44.)

The International Organisation for Standardization, ISO in short, website (International Organisation for Standards N.d) states that ISO is independent and not tied to any country. In the ISO 27001 framework the guideline for implementing controls is in related standard ISO 27002, but the standard ISO 27001 Annex A lists all the available controls and controls in the standard. The controls have three layers of hierarchy, but the sub-controls are not evenly divided for each main control. ISO 27002 standard guides in-depth the control implementation with clear objectives, requirements and information. Technical vulnerability management is part of the ISO 27001 Annex A controls. The latest version, 2017, of ISO 27001 standard does not anymore define the security areas like NIST CSF or CIS Controls, but the ISO 27001 aims to support security thoroughly. (SFS-EN ISO/IEC 27001:2017, 15-26; SFS-EN ISO/IEC 27002:2017, 1-89)

The CIS Controls is non-profit organisation which is not affiliated to any country. In the CIS Controls the first level of hierarchy is Control and the second is Sub-control. The unique feature for CIS Controls is the Implementation Groups. The calculation of total number of Sub-controls would vary depending on the Implementation Group level. The controls have two layers of hierarchy, but the sub-controls are not evenly divided for each main control. The CIS Controls explain the reason and objective for the controls clearly and guide implementation of controls to basic technical level. Vulnerability management is a main control and a part of the Basic category in The CIS Controls. (The Center for Internet Security 2019, 2-70)

The comparable features of each cyber security framework are compared in the table below. (See Table 1.)

Table 1. The comparison of cyber security frameworks

Cyber Security Framework	NIST CSF	ISO 27001	CIS Controls
Number of security focus areas/functions	5	Not applicable	3
Hierarchy of controls	3	3	2
Number of main controls	23	14	20
Total number of sub-controls	107	114	171
Vulnerability management	Yes	Yes	Yes
Development affiliated by a country	Yes	No	No

4.2 Comparison of maturity models

To compare cyber security frameworks this research selects the following features:

- the number of maturity levels and
- the number of security domains.

Due to the reason that the Capability Maturity Model had been developed for software development, there is not a direct relation to cyber security in the Capability Maturity Model, but it has the easily cyber security -adaptable five maturity levels. The Cybersecurity Capability Maturity Model has maturity levels three MIL0-3 and ten security domains. The Gartner ITScore has five maturity levels which concentrate on six different security domains. The Gartner ITScore and Capability Maturity Model share same maturity levels, which are less complex than The Cybersecurity Capability Maturity Model maturity levels. On the other hand, The Cybersecurity Capability Maturity Model has more in-depth approach how to use the model, the other compared maturity models also have basic how to use the model instructions. A threat and vulnerability management is one of the domains in Cybersecurity Capability Maturity Model. The comparison of maturity models is presented in the tableTable 2 below. (See Table 2.)Table 1

Table 2. The comparison of maturity models

Maturity Model	Capability Maturity Model	Cybersecurity Capability Maturity Model	Gartner ITScore
Number of maturity levels	4	5	5
Number of security domains	Not applicable	10	6

4.3 Comparison of vulnerablity management processes

To compare cyber security frameworks this research selects the following features:

- the level of hierarchy,
- the number of tasks in the processes,
- the number of phases of the process and
- the number of roles or stakeholders in the processes.

The CRR Supplemental Resource Guide and SANS Institute guide for implementing a Vulnerability Management Process are presented very differently which adds some incompatibilities to comparison. The SANS Institute guide for implementing a Vulnerability Management Process the number of tasks has loops, which do not give exact number of steps in the process, therefore; the number of steps is calculated with no loops and one loop. In the CRR Supplemental Resource Guide for vulnerability management the involved roles are not clearly defined, but these roles and stakeholders are to be identified in the process. The SANS guide has two hierarchy layers; phase and process steps while The CRR guide has phases, steps and sub-steps. The SANS guide does not have clear improvement guidance about the vulnerability management program itself while The CRR guide does. The comparison of vulnerability management implementation processes is presented at the tableTable 3 below, the table continues in next page. (See Table 3.)

Table 3. The comparison of vulnerability management implementation processes

Vulnerability management implementation process	SANS Institute guide for implementing a Vulnerability Management Process	CRR Supplemental Resource Guide for vulnerability management
Number of phases	5	5
Number of steps	min 16, max 18	21

Number of sub-steps	Not applicable	61
Number of involved roles	4	Not defined
Depth of process (hierarchy layers)	2	3

5 Conclusions

Developing and maintaining a cyber security program in an organisation requires focus on multiple areas. The usual method to build cyber security is to use the onion model, where security is built with layers. Selecting the framework is good base to start building the cyber security and maturity model can be used to evaluate its quality. Vulnerability management is part of all three selected frameworks, but the importance and priority vary.

This research has followed the qualitative and comparative research methods to answer research questions. Organisations need to build solid basis for cyber security with a framework, use maturity models to evaluate and develop their cyber security program. Part of this cyber security program becomes vulnerability management. For the two first research questions “How to build a solid basis to begin vulnerability management?” and “When is the organisation mature enough for technical vulnerability management?” the straight answers are left open for organisations to select by themselves with information, knowledge and understanding provided by this research. For the third research question “Can there be an easily adaptable implementation process for technical vulnerability management?” this research concludes that both researched and compared guides, SANS Institute guide for implementing a Vulnerability Management Process and CRR Supplemental Resource Guide for vulnerability management, are easily adaptable vulnerability management implementation processes in theory.

5.1 Cyber Security Frameworks

The three compared cyber security frameworks have their own pros and cons. The complexity and resources required for implementation of the NIST Cybersecurity Framework or the ISO 27001. A small enterprise may find it difficult to implement the NIST CSF or the ISO 27001 by themselves. The NIST CSF referencing to other publications may be overwhelming with information. The NIST CSF for being developed for the United States of America critical sectors, the framework is often enforced in the country and usage in other regions may require some adaption. To have built-in maturity model is a good feature in the NIST CSF, which helps organisations to evaluate their cyber security programs maturity and evolve them. The ISO 27001 implementation for organisation is a lengthy process which may also be heavy as controls give very in-depth explanation what they require. The other benefit of ISO 27001, than a continuous security program, is that its certification is highly valued and offers many good opportunities when obtained. The CIS Controls has the most sub-controls to be implemented of the three compared cyber security frameworks, but the Implementation Groups help implementation of the framework for different size enterprises. Out of the three compared security frameworks the CIS Controls seems the most approachable.

5.2 Cyber Security Maturity Models

A cyber security maturity model helps organisations to evaluate and develop their cyber security program. The Capability Maturity Model itself is not a maturity model for cyber security, but other maturity models which have derived from it may be found useful. Yet, the Capability Maturity Model consists the basics of a maturity model and understanding it is useful. The Cybersecurity Capability Maturity Model provides a heavy, but well-organised tool for assessing the maturity of cyber security program. Threat and vulnerability management being part of the C2M2 makes it very viable maturity model for this research. Several of the C2M2 domains measure controls found in the cyber security frameworks, such as asset, change, and configuration management or identity and access management. This makes the C2M2 very compatible with cyber security frameworks. The C2M2 is aimed at critical infrastructure which sets requirements which some smaller enterprises may not be able to follow easily; therefore, the C2M2 may be more suitable for large enterprises or some medium size enterprises. The Gartner ITScore offers very simple compact maturity model which can be easily followed even with smaller enterprises. On the other hand, the data available about the Gartner ITScore was very limited and it gives rough guidelines for its six security domains to evaluate and improve. The maturity model levels, and the level definitions are clear and easily followed.

5.3 Vulnerability Management Implementation Processes

The two compared vulnerability management implementation processes are both good and offer very useful tool for implementing the vulnerability management. SANS Institute guide for implementing a Vulnerability Management Process has clear explanations with visualised step-by-step processes while CRR Supplemental Resource Guide for vulnerability management guides reader through the guide with steps and sub-steps. The SANS guide approach is very easy to follow and has useful hands on information to process with the guide. The CRR guide has built-in checklists for the beginning and the end of each phase which help to make sure that requirements are met. The SANS guide suits better for small and medium enterprises, while The CRR guide suits better for medium and large enterprises.

6 Discussion

The research was divided to three comparisons to help organisations understand more how vulnerability management can be implemented part of their cyber security program. The comparison of cyber security frameworks, cyber security maturity models and vulnerability management implementation processes limited the presented and compared subjects to two or three per framework, maturity model and process, but this allowed the research to provide wider understanding about vulnerability management place in cyber security programs. Yet, the third subject for vulnerability management implementation process would have been useful than comparing only two subjects. The problem with only two processes was very different implementation guides and comparable data was presented totally different ways.

The use of comparative research method did not provide a new implementation process, but it was still able to prove answer to the third research question.

The subject selection was initially planned to be non-affiliated and global, but still nationally developed subjects were part of the research. With nationally developed subjects, might be interesting to have Finnish KATAKRI or VAHTI-instructions part of the framework comparison. Cyber security programs and vulnerability management may be too heavy perform by small or medium size enterprises; therefore, new research opportunities open about vulnerability management and other cyber security program implementation with collaboration of information technology service provider.

References

Acohido, B. 2015. *Improving Detection, Prevention and Response with Security Maturity Modeling*. Sans Intsitute. Accessed 14 April 2019. Retrieved from: http://img.delivery.net/cm50content/hp/hosted-files/HP_ImprovingMaturityModeling_2015final.pdf

Bhajanka, P. & Lawson, C. 2018. *Market Guide for Vulnerability Assessment.* Gartner. Accessed on 22 October 2019. Retrieved from https://www.tenable.com/analyst-research/gartner-2018-market-guide-for-vulnerability-assessment

Calvo-Manzano, J., Rea-Guaman, A., San Feliu, T. & Sanchez-Garcia, D. *Comparative Study of Cybersecurity Capability Maturity Models.* Accessed on 17 October 2019. Retrieved from https://www.researchgate.net/publication/319640924_Comparative_Study_of_Cybersecurity_Capability_Maturity_Models?enrichId=rgreq-967c8b90f571b8a7f5752a72f55350d5-XXX&enrichSource=Y292ZXJQYWdlOzMxOTY0MDkyNDtBUzo1NjEyNzY3MTc0NzM3OTJAMTUxMDgzMDIwNTExNg%3D%3D&el=1_x_2&_esc=publicationCoverPdf

Carnegie Mellon University. 2016. *CRR Supplemental Resource Guide Volume 4 Vulnerability Management Version 1.1.* Accessed on 22 October 2019. Retrieved from https://www.us-cert.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-VM.pdf

Center for Internet Security. 2019. *CIS Controls V7.1.* Accessed on 22 October 2019. Retrieved from https://learn.cisecurity.org/cis-controls-download

Cipher. N.d. *A Quick NIST Cybersecurity Framework Summary.* A blog article on Cipher website. Accessed 22 October 2019. Retrieved from https://cipher.com/blog/a-quick-nist-cybersecurity-framework-summary/

International Telecommunications Union (ITU). 2017. *Global Cyber Security Index (CGI) 2017.* Geneva: Author. Accessed on 25 February 2019. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

International Organisation for Standardization. N.d. *ISO – About us.* Official website. Accessed on 7 April 2020. Retrieved from https://www.iso.org/about-us.html

ISO27000.org. 2013. *An Introduction To ISO 27001 (ISO27001).* 27000.org website. Accessed on 26 September 2016. Retrieved from http://www.27000.org/iso-27001.htm

Jyväskylä University, Koppa. 2015. *Qualitative research.* Accessed on 26 February 2019. Retrieved from https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/en/methodmap/strategies/qualitative-research

Kananen, J. 2014. *Toimintatutkimus kehittämistutkimuksen muotona - Miten kirjoitan toimintatutkimuksen opinnäytetyönä?* Jyväskylän ammattikorkeakoulu. Accessed 14 April 2020. Retrieved from https://janet.finna.fi/, Booky.fi.

Le, N. & Hoang, D. 2016. *Can maturity models support cyber security?.* University of Technology Sydney. Accessed 29 September 2019. Retrieved from https://ieeexplore.ieee.org/document/7820663

Lehto, M., Limnéll, J., Innola, E., Pöyhänen, J., Rusi, T. & Salminen, M. 2017. *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi.* Valtioneuvoston kanslia. Accessed 19 February 2019. Retrieved from https://vnk.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf

Lor, P. 2011. Chapter 4 Methology in comparative studies. Accessed on 11 May 2020. Retrieved from https://pjlor.files.wordpress.com/2010/06/chapter-4-draft-2011-04-20.pdf

Martin, J. 2020. *Is CVSS the Right Standard for Prioritization?* A blog article in DARKReading website. Accessed on 11 May 2020. Retrieved from https://www.darkreading.com/vulnerabilities---threats/is-cvss-the-right-standard-for-prioritization/a/d-id/1337712

National Institution of Standards and Technology. 2018a. *New to Framework.* Official website. Accessed on 7 May 2020. Retrieved from https://www.nist.gov/cyberframework/new-framework

National Institution of Standards and Technology. 2018b. *Framework for Improving Critical Infrastructure Cybersecurity.* Accessed 29 September 2019. Retrieved from https://www.nist.gov/cyberframework/framework

Palmaers, T. 2003. *Implementing a vulnerability management process.* SANS Insititute. Accessed on 17 February 2019. Retrieved from https://www.sans.org/reading-room/whitepapers/threats/paper/34180

Proctor, P. 2014. *ITScore Overview for Security and Risk Management.* Gartner, Inc. Accessed on 15 April 2019. Retrieved from https://cdn.ttgtmedia.com/searchSecurity/downloads/Gartner%20Security%20Research_ITScore%20Overview.pdf

Routio, P. 2007. *Comparative Study.* Accessed on 11 March 2019. Retrieved from http://www2.uiah.fi/projects/metodi/172.htm

SFS-EN ISO/IEC 27001:2017:en. *Information technology. Security techniques. Information security management systems. Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor 2:2015)* Helsinki: Finnish Standard Association SFS. Confirmed on 3 March 2017. Referenced on 22 March 2020. https://online.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID2/2/474109.html.stx, SFS Online.

SFS-EN ISO/IEC 27002:2017:en. *Information technology. Security techniques. Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)* Helsinki: Finnish Standard Association SFS. Confirmed on 3 March 2017. Referenced on 23 October 2019. https://online.sfs.fi/fi/index/tuotteet/SFS/CENISO/ID2/2/474103.html.stx, SFS Online.

Theseus. N.d. *Open Repository of the Universities of Applied Sciences.* Official website. Accessed on 5 May 2020. Retrieved from https://www.theseus.fi/

Traficom National Cyber Security Centre. 2019. *Tietoturvan vuosi 2018.* Helsinki: Author. Accessed on 19 February 2019. Retrieved from https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Vuosikatsaus_2018_tulostettava_sivuttain.pdf

U.S. Department of Energy. 2014. *Cybersecurity Capability Maturity Model*. Accessed on 14 April 2019. Retrieved from http://energy.gov/oe/downloads/cybersecurity-capability-maturity-model-february-2014

Zelonis, J. 2017. *Vendor Landscape: Vulnerability Management, 2017.* Accessed on 17 February 2019. Retrieved from https://it-securityworld.com/assets/whitepapers/Nov20170879.pdf