Teemu J. Tiainen

Cyber security services reporting framework

Helsinki Metropolia University of Applied Sciences

Industrial Management

Master's Thesis

30 April 2021

Metropolia

It has been truly the best and the worst time to complete studies and the thesis project during the COVID-19 era. Little could anyone predict at the end of year 2019 that the world would change so drastically for the study period. Originally, I embarked to a journey to meet new people and to gain insights to other industries besides IT. The journey turned out to be an exploration of myself, what I aspire professionally in the long-term and what kind of person I am as a life-long learner. The industrial management program and thesis project have been a great way to turn a new page career-wise and have helped me tremendously to lay a solid foundation for new knowledge about strategy, management, business and cyber security.

I want to thank my case company management for the opportunity to study in the program and for their constant push to develop the organisation along with the full support for the final project. I want to thank all the internal and external stakeholders who have participated and given their valuable input through interviews, workshops and discussions. And I would also like to thank my colleagues in the business team for their valuable peer support.

I thank my thesis instructor Dr. Thomas Rohweder for the guidance and brilliant lectures as well as M.A Sonja Holappa for steering my professional language and pushing me to take an extra mile with the thesis content. I want to thank Dr. Juha Haimala and Dr. James Collins for the excellent Industrial Management study program. And I also want to thank my fellow students for their insights to other industries and successful group assignments with special thanks to Walter and Tytti for their peer support.

My deepest gratitude and thanks go to my wife for the support and being there for me throughout this process. Special thanks also to my two sons for understanding the amount of work and effort I had to put to the study. Hopefully I have set an example for you to study and work hard in the future.

The studies were very intense but when considering it all, it has been very rewarding. I have started new chapter career-wise and cannot wait to learn new things every day.

Teemu J. Tiainen
Espoo
April 30, 2021

Author Title Number of Pages Date	Teemu J. Tiainen Cyber security services reporting framework 111 pages + 3 appendices 30 April 2021
Degree	Master of Engineering
Degree Programme	Industrial Management
Instructors	Dr. Thomas Rohweder, Principal Lecturer M. A. Sonja Holappa, Senior Lecturer

The objective of this study is to create a cyber security services reporting framework to enable reporting to cyber security stakeholders of customer that supports business needs of customer to improve security posture. The case company provides managed cyber security services, and the reporting of the services is done differently for each customer and the current reporting structure is mainly focusing on operative and technological aspects without bringing additional value to customer business needs. The cyber security services have been provided only for a few years and the case company is looking for a solution to improve and harmonise the reporting of cyber security services supports customer's business needs to improve security posture.

The study includes four stages that are performed according to the research design that is the research approach. The first stage is the current state analysis stage of the strengths and weaknesses of the current reporting structure and deliverables. The second stage is a literature review where knowledge and best practices to overcome weaknesses are compiled as the conceptual framework. The third stage is a co-creation stage to create a proposal for reporting framework together with internal and external stakeholders based on the findings in the previous stages. The fourth and last stage is a multiple step validation of the proposal by the internal and external stakeholders to validate the final proposal for cyber security services reporting framework. The study also includes a recommendation for the steps to implement the framework in the case company.

The outcome of this study is a comprehensive cyber security services reporting framework that incorporates the customer and service provider relationship and responsibilities. The framework describes best practice for cyber security management. The cyber security management includes cyber security target setting through risk management. The framework describes what and how the service provider reports the outcomes of cyber security services to improve security posture of customers.

The initial steps for the implementation of the framework are included in the study. The framework has received positive comments and the implementation plan has received management support to move forward with the development of cyber security services reporting.

Keywords	Cyber security reporting, cyber security reporting framework, continual service improvement, cyber security posture, cyber security management, cyber resilience, cyber security risk management

Metropolia

Contents

Appendices

Appendix 1. Questions of the current state analysis

Appendix 2. Questions of Data 2 – external stakeholder interviews

Appendix 3. Validation questions – external validation

List of figures

List of tables

1 Introduction

During past two decades the businesses have quickly turned from brick-and-mortar style of businesses to digitalized businesses. As today the global internet penetration is around 59% of world population that translates that approximately 4,6 billion persons have access to Internet and can use the digital services. (Clemens, 2020) The cybercrime is rising constantly, and businesses need to implement cyber security measures to protect their business systems, software, devices and data communications networks against any cyber threats. This sets also new demand and requirements for the top management and boards of any business to run their as securely as possibly in the digital world. (Traficom, 2020)

The companies and especially the top management of business has the responsibility to ensure first and foremost the safety and privacy of their employees and customers in the digital world but not forgetting the business continuity. Since the business has moved to digital world this has led into a situation where cybercrime has emerged and developed quite rapidly in the past few years. Finnish Economic Research Institute (ETLA) has investigated cyber threats and crime and published a report in December 2020. The report shows that the number of data breaches reported to the police has increased year by year. When comparing year 2018 to the 2020 forecast at the end of November, the number of data breaches has doubled in Finland.

Cybercrimes are also reported by Finnish Transport and Communications Agency TraFiCom's (Traficom) Cyber security Center, and the study shows that data phishing has increased by 67%, the number of cyber scams has more than quintupled and, overall, cyber security anomalies have almost tripled compared to 2019. The increase can be partly explained by the continuing pandemic, which has also taken criminals to remote offices to plan and commit crimes. Finland is not alone with this phenomenon, but the growth figures are very well in line with global trends which are also presented in the study. (ETLA, 2020)

Traficom has published a guide for management board about their responsibilities regarding cyber security. The business and cyber security are therefore the responsibility of the top management in any company. This sets the requirement for company management to understand cyber security matters to assess the current security posture and cyber risks to make correct decisions how to improve the security posture and to minimize the risks from business continuity perspective. The companies are facing increased

requirements to respond more quickly, learn new things and can invest in the right technologies and services to mitigate the business risks posed by cyber security threats. (Traficom, 2020 & ETLA, 2020)

This study focuses on reporting on cyber security services to companies who are purchasing cyber security as a service and their aim is to have mature cyber security posture as part of their business.

1.1 Business Context

The case company is a Finnish public limited company who is offering telecommunication and digital services for both consumers and corporate customers. The company operates worldwide in digital services and employs about 5000 professionals. The corporate structure is presented in Figure 1.

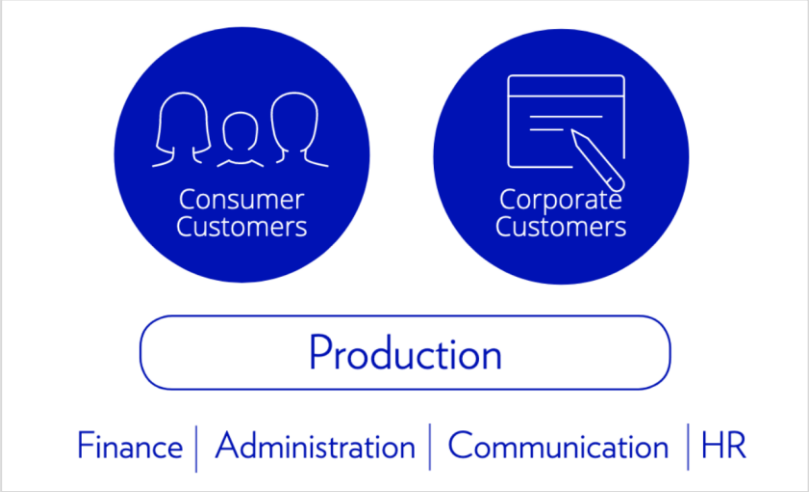


Figure 1. The structure of the case company

The focus on this thesis is on cyber security services that are delivered for the corporate customers. The company has existed for over 140 years, but the cyber security services business has been offered to customers only since 2015. The cyber security business is divided into business and production responsibilities. The business is responsible for the profit and loss of the services and ensuring services are valid and meeting customer expectations. The main responsibility of the production team is to deliver the services as per agreed with the agreed customers and team is responsible for developing people,

processes and tools to meet the requirements and expectations on daily basis. The cyber security services management and delivery organisation is visualised in figure 2.

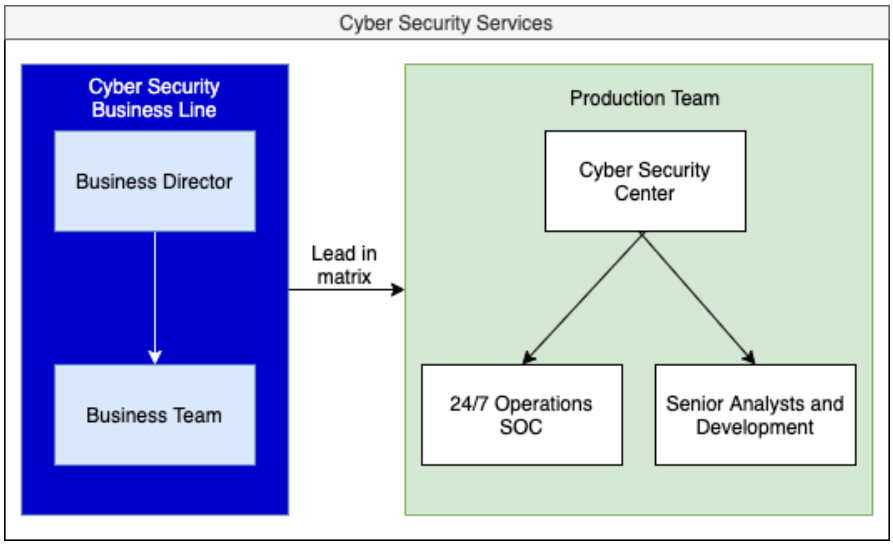


Figure 2. The structure of the cyber security services management and delivery

The author of this study works as a business lead in the cyber security services business team that is part of the Connectivity business line in Corporate Customers business unit.

1.2 Business Challenge, Objective and Outcome

The cyber security services unit are part of corporate customers business unit. Since 2015 the customer amounts have risen steadily, and technologies along with reporting requirements have evolved. Cyber security has been raised as a management topic and well-informed top management considers it a priority to understand the security posture and how risks are managed within their business.

The Case company offers cyber security services for several customers, but the reporting of the services is done differently for each customer based on the historical needs and requirements. The current reporting structure is mainly focusing on the operative and technological aspects and brings mainly added value to the customer business needs through the incident management process and judgment by team participating to the service governance. Without proper reporting the customers do not have visibility and understanding of their cyber security posture and they are not able to make educated decisions where and how to improve the cyber security posture.

The objective of this thesis is to create a framework for reporting on the cyber security services. With clear and meaningful reporting, the stakeholders of customer's cyber security team will have understanding of how they can support their business by improving their cyber security posture. The outcome is a framework for reporting on the cyber security services.

1.3 Thesis Outline

The study consists of seven sections and four stages. The business challenge and outcome of this study are introduced in this section. The third section and first stage of the research design was to understand the current state of the cyber security reporting by interviewing by the internal key stakeholders. The goal and outcome of this stage was to gain deep knowledge and understanding from current reporting process, structure and deliverables including the customer requirements and their maturity level. The outcome of this stage includes validation of the business problem and identification and documentation of the current report structure along with Strengths and Weaknesses-analysis of it.

The fourth section describes second stage of research design where relevant literature is user to create conceptual framework based on the weaknesses found in the current state analysis stage. The outcome of this stage is a conceptual framework that includes elements of cyber security posture management process and the reporting of it. The fifth section describes the third stage of research design how the elements of conceptual framework were used to co-create a draft proposal for cyber security services reporting framework with the input from both external and internal key stakeholders. The outcome of third stage is a proposal for reporting framework. The sixth section and final stage is the validation stage of the proposal with both external and internal stakeholders. The last section contains the conclusion of the study through summary and analysis of the study.

This study does not include the implementation of the reporting framework and neither does it include the process development for service reporting. The study is limited to analysing the current state of the reporting framework and to create and recommend a framework to be used with cyber security services governance in the case company. The following section describes the project plan of the study along with the details of the research approach and design, and collection and analysis of data.

2 Research project plan

The previous section described the business challenge, objective and outcome of this study. This section describes the research approach, data collection and analysis methods used in this study. It includes a research approach and design that describe the different stages of this study.

2.1 Research Approach

Saunders et al. (2009) define research as something that people undertake to find out things in a systematic way. This increases their knowledge. Systematic research is based on logical relationships where data collection methods from various sources is gathered and assembled in a manner that results are interpreted to be meaningful and can be used to find out 'things' about the research subject. The 'things' is the clear purpose of the research. (Saunders et al., 2009; 4-5)

According to Baimyrzaeva (2018) basic research which is also known as academic or foundational research is expanding knowledge of something and the results are universal. The goal of basic research is to advance and expand human knowledge about the world and explain the nature of things or how they work. When a study aims for direct and immediate relevance to business and addresses the issues that are seen as important and are presented in actionable format it called applied research. Applied research improves the understanding of the particular business or management problem and the findings of practical relevance bring value to the organisation. (Saunders et al., 2009; 5-11, Baimyrzaeva, 2018; 6-10)

Kananen (2013) describes design research as a combination of development and research. Conducting only research is not merely enough. The design research requires qualitative methods in all stages of design research. The methods can be divided into collecting data and analysis. When development work is documented by using scientific methods to produce reliable and new knowledge that is one of the criteria of science. The objective of the design research is subject to continuous development in organisations. The design research produces functional and practical solutions in order to improve operations in organisations. (Kananen, 2013: 20-22, 102)

When there is no clear definition what something is and the deliverables of it, Saunders et al. (2009) describe this as a subjectivist view where social phenomena are created

from the perceptions and consequent actions of social actors. In a service entity context this means that services are produced through social interactions between service provider and customer and are under constant revision. Therefore, the definitive entity in question is constantly changing, and researchers must seek to understand the subjective reality of the customers from it. (Saunders et al., 2009; 111)

This study is conducted using design research together with qualitative methods. Design research was chosen as the research approach as this study focuses on a specific activity in the case company. Design research is aiming to produce new knowledge and recommendation how to improve the activity in this specific context for the case company. This was the key reason why design research was selected as the most suitable method to conduct this study and the key reason why qualitative data collection method is selected instead of the quantitative method. Existing professional literature and frameworks were utilized to create the conceptual framework and they heavily contributed to the outcome of this study. The outcome is new knowledge in this context. The implementation of the recommended framework is not included in the objective or outcome of this study.

2.2 Research Design

The study consists of four stages that follow a systematic research method to achieve the objective and the outcome of this research. The business objective and motivation behind the research were described in detail in the previous section. The condensed version of objective and the stages with descriptions, data sources and outcomes leading to the final business outcome are described in Figure 3.

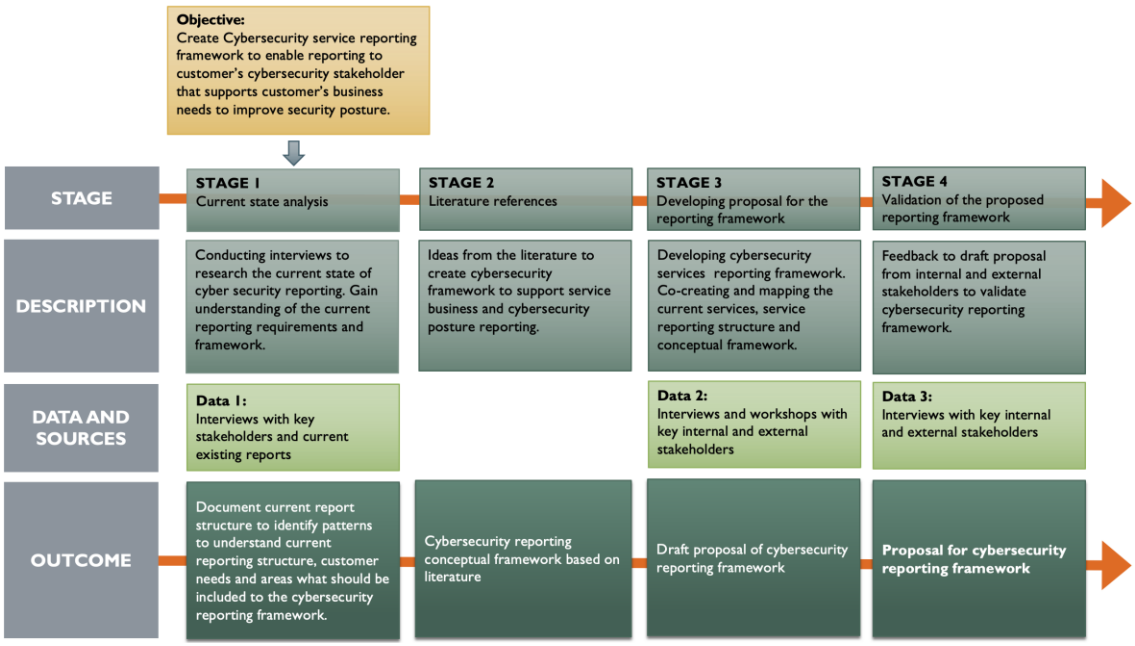


Figure 3. Research design of this study

The first stage is the current stage analysis stage. The outcome of the stage is to get deep understanding of the current reporting structure and identify patterns that possibly could be the existing reporting framework which is not documented when current stage analysis stage is started. This is achieved by interviewing all internal key stakeholders that are participating to the customer reporting process directly or in-directly but have relevant information about reporting. The stage was started by creating semi-structured interview questions that were based and created on high-level definitions of 'service' and 'cyber security'. Then all stakeholders were interviewed individually over Teams one-to-one meeting. After the interviews the current state of reporting structure was analysed, documented, and verified. The analysis includes the current reporting structure along with its strengths and weaknesses.

The next stage is to find ideas from literature for cyber security services reporting framework. This stage had the focus on designing service reporting in customer and service provider context, define the service metrics and measures and other deliverables to determine how they are in relationship to the cyber security posture elements of customer. The key question to research is how case company can contribute through the service reporting to the continuous improvement of cyber security posture. The outcome of this stage was conceptual framework.

As illustrated in Figure 2, the third stage was to develop a proposal for the reporting framework. The stage aimed to co-create a draft proposal for the services reporting

framework that would map the current services, services reporting structure and conceptual framework into one framework. This was done through co-created workshops with the internal key stakeholders and one to one interviews with the external key stakeholders.

The final and fourth stage was to validate the proposed reporting framework. Feedback from the draft proposals was gathered to receive improvement ideas and to validate the draft proposal. The outcome of this stage was the proposal for cyber security reporting framework to be used with services.

2.3 Data Collection and Analysis

Data was collected and drawn from various sources to this study. The data was collected from the internal and external stakeholders through interviews and workshops. The three data collection rounds are presented in the following three tables that each represent the data collection round. The data collection was conducted in all other stages besides ‘literature references’ stage.

Table 1. Details of interviews, workshops, and discussions in Data1

DATA 1 - CURRENT STATE ANALYSIS						
#	Source	Internal or External	Collection method	Topic	Time	Documented
1	Business Director	Internal	Interview (Teams meeting)	Planning current State of Cyber security services reporting interviews	Date: 16.12.2020 Time: 08:00-08:30	Field Notes
2	Senior Cyber Security Analyst 1	Internal	Interview (Teams meeting)	Current State of cyber security services reporting	Date: 17.12.2020 Time: 12:13-13:34	Field Notes
3	Business Team Member 1	Internal	Interview (Teams meeting)	Current State of cyber security services reporting	Date: 21.12.2020 Time: 12:48-14:30	Field Notes
4	Senior Cyber Security Analyst 2	Internal	Interview (Teams meeting)	Current State of cyber security services reporting	Date: 29.12.2020 Time: 10:03-11:18	Field Notes
5	Services Development and Back Office Team Member 1	Internal	Interview (Teams meeting)	Current State of cyber security services reporting	Date: 29.12.2020 Time: 13:08-14:46	Field Notes
6	Services Development and Back Office Team Member 2	Internal	Interview (Teams meeting)	Current State of cyber security services reporting	Date: 30.12.2020 Time: 09:07-10:18	Field Notes
7	Senior Cyber Security Analyst 3	Internal	Interview (Teams meeting)	Current State of cyber security services reporting	Date: 30.12.2020 Time: 11:08-12:00	Field Notes
8	Business Team Member 2	Internal	Interview (Teams meeting)	Current State of cyber security services reporting	Date: 31.12.2020 Time: 10:04-11:07	Field Notes
9	Business Team Member 3	Internal	Interview (Teams meeting)	Current State of cyber security services reporting	Date: 4.1.2021 Time: 14:33-16:00	Field Notes
10	Senior Cyber Security Analyst 4	Internal	Interview (Teams meeting)	Current State of cyber security services reporting	Date: 5.1.2021 Time: 14:10-14:55	Field Notes
11	Services Development and Back Office Team Member 3	Internal	Interview (Teams meeting)	Current State of cyber security services reporting	Date: 8.1.2021 Time: 12:15-13:25	Field Notes
12	Services Development and Back Office Team Member 4	Internal	Interview (Teams meeting)	Current State of cyber security services reporting	Date: 8.1.2021 Time: 15:11-16:04	Field Notes
13	Services Development and Back Office Team Member 5	Internal	Interview (Teams meeting)	Current State of cyber security services reporting	Date: 8.1.2021 Time: 16:13-17:25	Field Notes
14	Service reports in document management system.	Internal	Document (Service Report)	Perusal of the most recent service reports produced to customers.	Date: 15.1.2021	Customer A report Customer B report Customer C report
15	1 Senior Cyber Security Analyst 1 Business Team Member 1 Services Development and Back Office Team member	Internal	Email inquiry (To validate initial version of CSA framework)	Validate the initial Current State of reporting framework documented based on the answers received in interviews that will be presented in workshop results.	Date: 17.1.2021 Time: 20:13	Email replies and Fields Notes
16	Business Director	Internal	Interview (Teams meeting)	Current State Analysis initial results walkthrough	Date: 19.1.2021 Time: 08:00-08:30	Field Notes
17	1 Senior Cyber Security Analyst 3 Business Team Member 3 Services Development and Back Office Team member	Internal	Review meeting (Team interation to validate findings)	Current State Analysis results workshop. Validate and discuss findings.	Date: 22.1.2021 Time: 09:00-10:00	Powerpoint Presentation, Field Notes
18	All interview participants	Internal	Email inquiry (validate CSA framework)	Current State Analysis results delivery for comments	Date: 22.1.2021 Time: 13:06	Email

As seen in Table 1, Data 1 was collected through interviews in the current state analysis stage. The data was mainly collected through individual interviews that were conducted as theme interview as semi-structured approach focusing on the current state of reporting using both structured and open questions. The data was recorded to field notes and analysed after the interviews. The analysis results including the reporting model along with its strengths and weaknesses were verified through workshop and distribution of the results to all participants. Table 2 presents the data collection to gain input and insight for creating the initial recommendation for cyber security service reporting framework.

Table 2. Data 2 collection

DATA 2 - CREATING THE INITIAL RECOMMENDATION FOR REPORTING FRAMEWORK						
#	Source	Internal or External	Collection method	Topic	Time	Documented
1	Business Team Member 3	Internal	Interview (Teams meeting)	Discussion about knowledge found in Current State Analysis-stage.	Date: 1.3.2021 Time: 10:00-10:35	Field Notes
2	Business Director	Internal	Interview (Teams meeting)	Discussion about knowledge found in Current State Analysis-stage.	Date: 1.3.2021 Time: 10:35-11:45	Field Notes
3	Business Team Member 1 Business Team Member 2 Business Team Member 3 Business Director	Internal	Document (Workshop material)	Delivery of Conceptual Framework theory material	Date: 1.3.2021 Time: 14:16	Field Notes
4	Business Team Member 1	Internal	Interview (Teams meeting)	Discussion about knowledge found in Current State Analysis-stage.	Date: 2.3.2021 Time: 15:00-16:00	Field Notes
5	Business Team Member 2	Internal	Interview (Teams meeting)	Discussion about knowledge found in Current State Analysis-stage.	Date: 11.3.2021 Time: 12:45-13:00	Field Notes
6	Business Team Member 1 Business Team Member 2 Business Team Member 3 Business Director	Internal	Document (Workshop material)	Delivery of workshop material and condensed version of Conceptual Framework theory	Date: 12.3.2021 Time: 10:42	Field Notes
7	Business Team Member 1 Business Team Member 2 Business Team Member 3 Business Director (present 14:00: - 16:00)	Internal	Workshop (Teams meeting)	CSA and Conceptual framework presentation. Co-creation of high-level framework based on knowledge gained through conceptual framework. Setting goals and recommendations for the initial framework.	Date: 12.3.2021 Time: 14:00-17:00	Field Notes
8	Business Team Member 1 Business Team Member 3 Business Director (present 15:15: - 15:35)	Internal	Workshop (Teams meeting)	Comments based on the draft version for proposal. Co-creation through improvement ideas to draft.	Date: 19.3.2021 Time: 15:15-16:00	Field Notes
9	Key Customer 1	External	Interview (Teams meeting)	Interview through semi-structured questions to validate elements to be included in the proposal framework and understanding reporting expectations from customer perspective.	Date: 26.3.2021 Time: 9:30-11:00	Field Notes and Voice recording
10	Key Customer 2	External	Interview (Teams meeting)	Interview through semi-structured questions to validate elements to be included in the proposal framework and understanding reporting expectations from customer perspective.	Date: 26.3.2021 Time: 12:30-14:18	Field Notes and Teams meeting recording
11	Key Customer 3	External	Interview (Teams meeting)	Interview through semi-structured questions to validate elements to be included in the proposal framework and understanding reporting expectations from customer perspective.	Date: 29.3.2021 Time: 12:00-13:27	Field Notes and Teams meeting recording
12	Key Customer 4	External	Interview (Teams meeting)	Interview through semi-structured questions to validate elements to be included in the proposal framework and understanding reporting expectations from customer perspective.	Date: 30.3.2021 Time: 8:15-9:20	Field Notes and Teams meeting recording
13	Key Customer 5	External	Interview (Teams meeting)	Interview through semi-structured questions to validate elements to be included in the proposal framework and understanding reporting expectations from customer perspective.	Date: 31.3.2021 Time: 14:34-16:22	Field Notes and Teams meeting recording
14	Business Team Member 1 Business Team Member 2 Business Team Member 3 Business Director	Internal	Workshop (Teams meeting)	Feedback and recommendations of external stakeholder interviews. Walkthrough of draft framework	Date: 6.4.2021 Time: 10:30-12:00	Field Notes

In the next round of data collection, data was collected from cyber security business team members of case company through workshops and from external key customers through one-to-one interviews. The business team members were participating to creation workshops where knowledge gained through the conceptual framework was utilized to set requirements and goal for initial recommendation. After the co-creation session, the data of cyber security management in customer organizations was gathered from various customer organization and to be able to analyse and compared against goals and requirements set in the internal workshops. Due to COVID-19 situation all workshops and interviews were conducted as virtual meetings.

The table 3 presents the final data collection round where Data 3 was gathered as feedback to validate the initial recommendation for cyber security services reporting framework.

Table 3. Data 3 collection

DATA 3 - VALIDATION OF THE RECOMMENDED FRAMEWORK						
#	Source	Internal or External	Collection method	Topic	Time	Documented
1	Business Team Member 1 Business Team Member 2 Business Team Member 3 Business Director	Internal	Document (Material for internal validation)	Delivery of materials for validation. External stakeholder interview results, summary and description of recommendations, proposal for draft framework.	Date: 6.4.2021 Time: 17:41	Email distribution and field notes
2	Business Team Member 1	Internal	Interview (Teams meeting)	Discussion about proposal framework to clarify operational and tactical level frameworks and metrics.	Date: 8.4.2021 Time: 13:45-14:00	Field notes
3	Business Team Member 1	Internal	Email Response (validate proposal framework)	Validation feedback of the proposal framework	Date: 8.4.2021 Time: 14:20	Email
4	Business Director	Internal	Email Response (validate proposal framework)	Validation feedback of the proposal framework	Date: 8.4.2021 Time: 14:43	Email
5	Business Team Member 1 Business Team Member 2 Business Team Member 3 Business Director	Internal	Email (validate proposal framework)	Response to validation feeback and questions received.	Date: 9.4.2021 Time: 16:05-16:31	Email distribution
6	Business Director	Internal	Interview (Telephone call)	Discussion about proposal framework and PREVENT-aspect of the operational metrics	Date: 9.4.2021 Time: 16:05-16:31	Field notes
7	Business Director	Internal	Email Response (validate proposal framework)	Response to the PREVENT-aspect of metrics in framework proposal	Date: 9.4.2021 Time: 16:23	Field notes
8	Business Team Member 3	Internal	Interview (Telephone call)	Discussion about proposal framework	Date: 9.4.2021 Time: 16:54-17:10	Field notes
9	Business Team Member 1 Business Team Member 2 Business Team Member 3 (Present 10:00 - 11:04) Business Director Key Customer 1 (Present 9:58 - 11:03) Key Customer 2	External and Internal	Workshop (Teams meeting)	Presentation of weaknessess found in current state analysis, conceptual framework and recommendations generated in Data 2 stage. Presenting the proposal framework. Validation of recommendations and proposed framework.	Date: 15.4.2021 Time: 9:58-11:25	Field Notes and Teams meeting recording
10	Business Director	Internal	Interview (Teams meeting)	Feedback of workshop. Peer review and feedback of thesis draft sections 1-5. Validation of proposed framework and next steps regarding it.	Date: 16.4.2021 Time: 08:00-09:03	Field notes

As shown in table 3, the validation included internal validation discussions before external and internal stakeholder validation workshop. And the final step being the validation discussion with the business director who introduced the business problem and is ultimately responsible validating the outcome of this study and the suitability of it for the case company.

The next section explains in detail how the current state analysis stage was carried out to collect data 1 as described above and what the analysis revealed regarding the current state of cyber security reporting in case company.

3 Current State Analysis

This section describes the current state of cyber security services reporting. It explains how the current state analysis was conducted to find out the strengths and weaknesses of the current reporting framework. The previous section contained the data collection principles and an overview of how the data was gathered at this stage.

The current state analysis stage was conducted in the order of identifying key stakeholders, collecting data through individual interviews, analysing data collected through interviews, documenting existing reporting framework based on data collected, verifying documented existing reporting framework and data analysis workshop with internal stakeholders. The section also visualises the existing reporting service framework that was documented based on the interview data and analysis.

Definition of cyber security was studied before the current state analysis was started to ensure that meaningful questions about the cyber security services were created and asked from internal stakeholders. There is no one and true definition for cyber security since companies and states define the cyber space appropriate for themselves. Schatz et al. (2017) investigated definition of cyber security and have created based on their analysis the most representative definition for 'cyber security' as follows:

> *"The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space. The concept includes guidelines, policies and collections of safeguards, technologies, tools and training to provide the best protection for the state of the cyber environment and its users." (Schatz et al., 2017; 66)*

The goal of the current state analysis was to find relation between IT services that cyber security. The questions in the current state analysis aimed to understand the customer organisation, risk management process and how service provider is aligned with them and how the reporting is linked to the management of cyber security and how the reporting is currently created, containing and delivered to the customers.

3.1 Overview of the Current State Analysis Stage

The data collection was started by having a meeting business director who initially introduced the business problem to be solved. He gave a short introduction how the reporting was currently done and who were the key internal stakeholders who are participating in

the reporting process by directly interfacing with the customer, developing the services or otherwise participating in the delivery of the reports. At this point the assumption was that reporting is quite much dependant on the senior cyber security analyst named per customer and the reports are not properly unified.

I contacted all named individuals separately and asked if they could participate in the study. The participation was not mandatory, and all individuals kindly volunteered to participate in the interview. The 12 interviews were held between 17.12.2020-8.1.2021.

The interview questions can be found in appendix A. The questions are semi-structured and steering of answers was avoided but some questions were asked to clarify the original answer if it was too vague or more information was needed to understand the answer. There were originally 16 open and semi-structured questions developed for the interview to find out the current state of reporting. The last question was “any other business” where we would discuss with the interviewee if there is something they would like to elaborate and if there is something that was missing from the questionnaire. Interviewee 4 pointed out that one direct question about cyber security posture could be added. A direct question about cyber security posture (Q10) was added to the questionnaire for the remaining interviews.

3.2 Data collection for current state through interviews

The interview was done by using virtual one to one web meetings due to the pandemic situation and physical meetings for this purpose were not allowed by company policy and generally not recommended by the state. The interviews followed the same pattern. The purpose of the interview, study and objective were explained to the interviewee. For the interviewee it was emphasized that there are no right or wrong answers but we are interested in the reality of the current state so we can analyse the strengths and weaknesses. Then background information from the interviewee was asked regarding their role, responsibilities and participation in the reporting process. The interviewee saw the question on their screen and the answers were documented simultaneously to the field notes. The interviewee only saw their own answer. After each question the answer was confirmed from the interviewee that if they are happy with the answer documented, should something be added or removed and did the answer capture the essence of their

answer. When the answer was accepted by the interviewee the interview moved to the next question.

After the interviews, an analysis was conducted for the answers. All four senior analysts mentioned in their interviews that a base template for reporting has circulated among staff but there is no agreed base template. The base template was studied along with three customer reports that were identified as most suitable candidates to present the current state of reporting. Based on the interviews the answer groups with similar kind of answers were identified. The groups were divided based on the work roles and how is the role participating to the reporting to the customers and what is their role. The answers were first grouped per answers group and analysed how similar the answers were. And after group analysis, the groups were analysed by comparing to other groups. The interview grouping and the group descriptions are presented in figure 4.

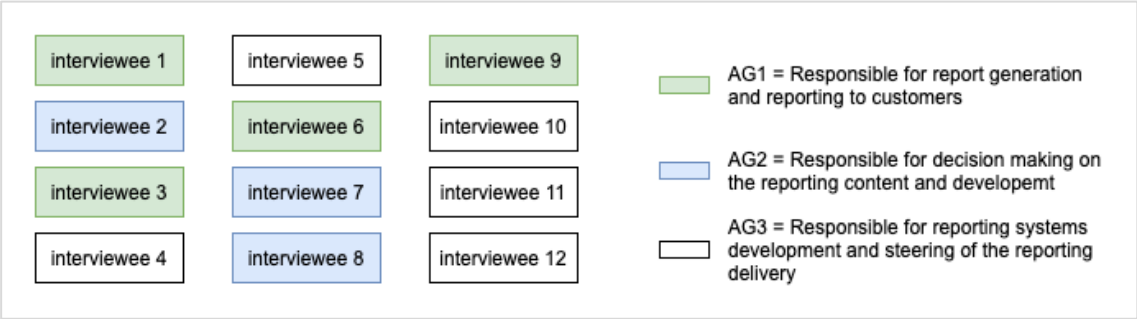


Figure 4. Interviewee grouping to answer groups

This made it possible to understand the current and the reality of the reporting process and content more clearly since more emphasis was placed on the answers that concerned the actual reporting of the participants who actually were doing the reporting instead of the individuals who were only contributing to the process.

3.3 Analysis of the data collected through interviews

In general, the interviews provided highly valuable input for this study and to the next stages. Some things were agreed in all answers such as the common base template requires improvement, and some work was already under development to unify the base template since as it was assumed the reporting varied from customer to customer but there were common denominators.

3.3.1 The strengths found through data

From the interview data there were six strengths found. The majority of people thought that current process produces the required outputs for customers due to the fact that people are committed to delivering the reports for customers. This has also resulted in a situation that reporting is very customer-oriented and as discussed earlier the base template has evolved with each customer to a certain direction. The focus of the reporting is heavily focusing on the operational and tactical level matters. It was also stated that the reporting meetings are held as per agreed with the customers and they are working as intended. It was also mentioned by several people that the case company has the needed resources to develop the reporting if there are new needs or requirements.

3.3.2 The weaknesses found through data

The weaknesses are linked to the strengths. Since there was a strong focus to be customer-oriented it was mutually pointed out in each interview that the case company is not using any cyber security services reporting framework. There was one question (Q15) to name or identify a reporting framework, but no single framework was named or identified. Cyber Security Frameworks and Control frameworks were mentioned a few times. It also became evident that the reporting terms are not unified. This is due to technologies where identical matters are named differently. This can cause confusion internally as well as with customers. It was also brought up that not many customers push for their needs and requirements to push reporting development further and it was more expected that the service provider suggests new items and content for reporting. It was also mentioned that there is minimal linking between the service reporting and the business and risks of the customers and identifying threats towards the customer is solely relying on the expertise of the case company analysts.

3.3.3 Out-of-scope findings through data

It is worth mentioning that there were other weaknesses related to reporting found through the interviews. These were identified as process related weaknesses and are therefore out-of-scope from this study. The premise for why the process is unclear and undocumented is the lack of a framework. When the framework is established, it should

support the execution of reporting tasks. This also contributes to the relevance of this study.

3.4 Current reporting framework based on data collected

One objective for the current state analysis was to identify patterns and gain understanding about reporting in a manner that the current framework could be identified and documented. As previously mentioned, the reporting varied between customers but there were similar patterns and goals mentioned in many cases. Based on the information collected a draft of the current reporting framework was documented.

The initial description of the current framework was validated by sending it to initial evaluation through email to couple of key stakeholders. One comment was sent back and small correction to initial description was made. Figure 5 contains the general reporting framework as usually used with services.

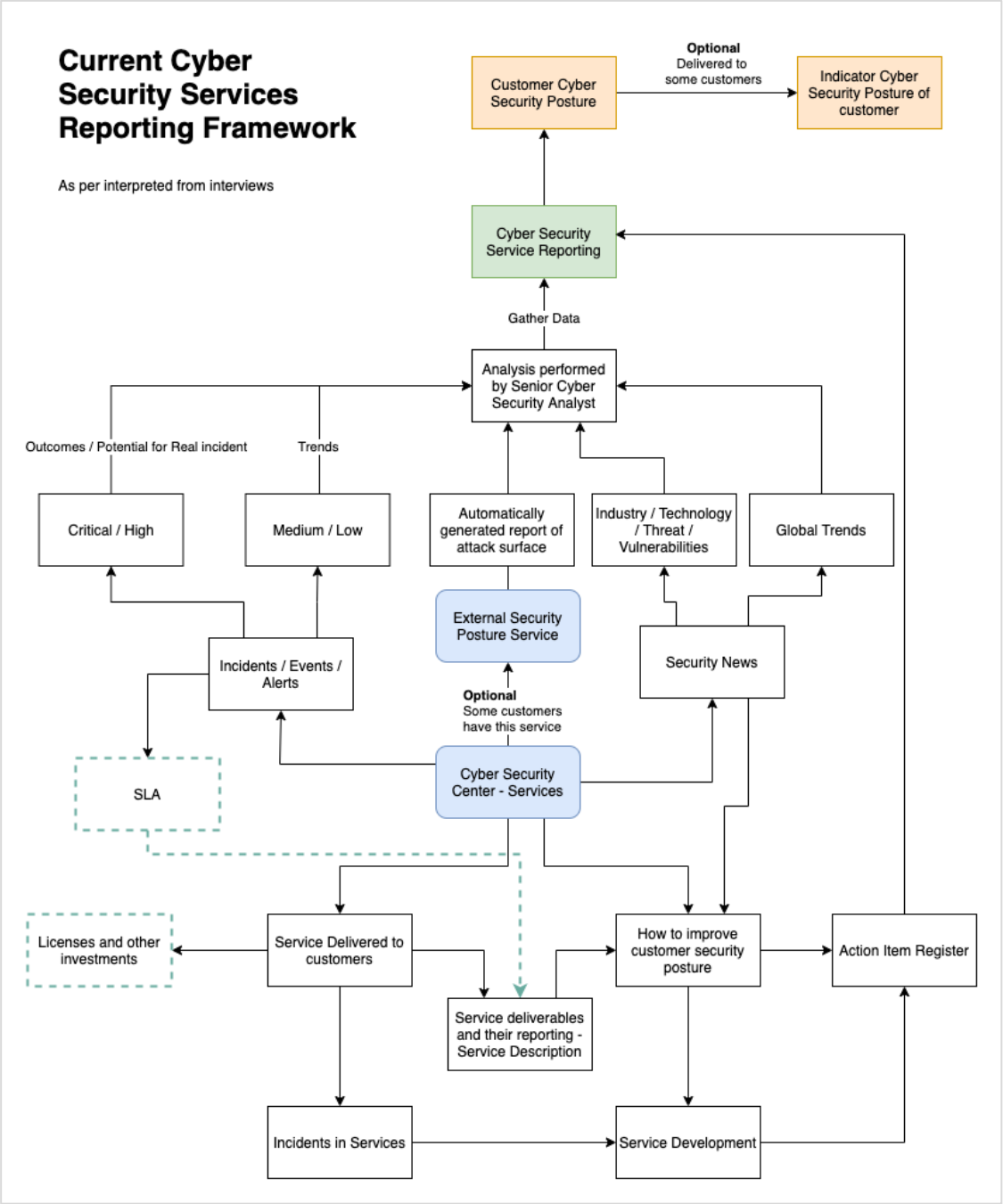


Figure 5. Reporting framework documented and perceived based on the current state data

The blue boxes represent the Cyber Security Services that are delivered to the customer. The dotted line boxes represent rarely reported topics. The white boxes are actions, data and deliverables of the service that are contributing cyber security reporting. Green box is the reporting itself and orange box represents the customer cyber security posture. To

some customers an agreed indicator of cyber security posture is reported but it is presenting the cyber security posture based on cyber security service activities and news of the last month and in for some customers this was not done at all.

The framework underlines the original assumption. The data collection and analysis from it is mainly done by Senior Cyber Security analysts and the report content is highly dependable on their efforts. As mentioned, the reporting is not tied to customer risks or business and focuses mainly on the operational aspects of Cyber Security Services. The focus of reporting revolves around the incidents that are classified either high or critical severity. Many customers are lacking the external security posture service that would help radically identifying the attack surface and possible threats and vulnerabilities towards the customer environment.

3.5 External stakeholder ideas on the scope of the reporting framework

A second objective of the current state analysis stage was to identify valid ideas what should be considered to be part of the cyber security services reporting framework. Question 16 placed the interviewee in the position of top management of a company and had the power to specify requirements what should be reported to them so they would know the state of cyber security posture in their imaginary company.

Various topics were mentioned. The most common question to be answered by reporting was “How secure are we and what we should do next?”. The route to get the answers to these questions on the other hand was very different among the interviewees. The requirements given by interviewees through this question were not overlapping and there was no single requirement stated as de facto requirement to be reported to the top management. This is an indicator as well that the topic is relevant to be investigated.

Altogether 49 different reporting requirements were presented through this question. After some analysis there were certain themes rising from the data. The requirements were then grouped to different category groups based on the content of requirement. The reporting areas identified from data are presented in table 3.

Table 4. Suggested reporting categories identified from data

#	Reporting category	How many mentioned
RC1	Business, risks and investments	12 persons
RC2	Current security posture	10 persons
RC3	Development and roadmap	7 persons
RC4	Operational data and systems protection	5 persons
RC5	Policy, compliancy and regulations	5 persons
RC6	Comparison to industry and competitors	3 persons
RC7	Culture and awareness	3 persons
RC8	Business continuity, impact and cost	2 persons
RC9	Service and Service management	2 persons

Each reporting requirement content was analysed to which category it could be placed by its essence. One requirement was placed only to one category where it suited best by the essence of the content. The categories were used as a reference category when the search from the literature was done what could be included to the conceptual framework.

3.6 Verifying initial reporting framework and data analysis workshop with internal stakeholders

Before presenting the results and outcomes of the current state analysis stage to all internal stakeholders, the material was presented to the business director who initially set the problem. The results and outcomes were as expected, and the business director validated that the findings are relevant, and the problem was still valid, and solution is worth to pursue.

All interview participants were invited to workshop where data, analysis, outcomes of the current state stage were presented and discussion about their validity was open. Half of the interview participants were able to join the session. After the presentation five session participants confirmed that the documented current reporting framework looks good and presents the current state of reporting. Same applied for the strengths and weaknesses. The discussion about reporting categories raised some questions. One participant raised the question:

> *Are you sure you haven't influenced our answers about risks and business with the order of questions and small clarifying discussions? (interviewee 4)*

The order of questions was thought to follow the process from generation to the reporting to the board room. The question was open ended and placed as almost a final question in the interview and there were other questions between risk and business questions. This set requirement to be researched and validated from the external stakeholders since the reporting is aiming to suit the needs and requirements of customers.

When discussion about the need of framework for service provider and reporting categories carried on, a discussion about the service providers responsibility and the robustness of framework were raised. The discussion tried to find answers to these questions:

> *We should think carefully that we do not create too robust framework. Can we even find 'answers' to all areas? (interviewee 9)*

> *What is the responsibility of service provider in regards of customer cyber security posture? (interviewee 4)*

The questions are valid. The cyber security space and posture are very broad topics. The objective and outcome of this study is to find suitable solution for the case company. Both of the questions were considered and kept in mind when the conceptual framework from literature was researched and built. And to mitigate the issues the draft proposal was validated in the stage 4 by internal and external stakeholders. The analysis and results from the current state data was placed to digital workspace where all stakeholders have access, and they were informed about the location and encourage to be in contact should there be any questions or comments regarding the findings or study.

3.7 Key-findings summary

The current state stage findings were documented version of the current reporting framework and the strengths and weaknesses of it.

The strengths and weaknesses identified are presented in the table 3. The table also includes common weakness identified in the interviews that relates to whole reporting process. The reporting process development is out of this study and the objective of this study is developing a framework for cyber security services reporting. Therefore, the process-related weaknesses are marked with out-of-scope identifier, but it is worth to

mention them since this is essential information for the case company in the long run when framework is implemented.

Table 5. Summary of strength and weaknesses found in the current state analysis

#	Strength
S1	The current process produces the outputs required.
S2	The persons involved with the reporting and committed to deliver the reports to their customers.
S3	Reporting aims to be very customer-oriented and developed on customer needs on each service.
S4	The reporting is focusing to the operational matters quite thoroughly.
S5	The organisation is capable of developing reporting.
S6	Operational and Tactical level reporting meetings are working as indented.
#	**Weakness**
W1	No reporting framework used or identified.
W2	The reporting terms and deliverables should be unified.
W3	Typically customers do no have many requirements to push the reporting further and are expecting service provider to develop the reporting alone.
W4	Customers business and risk engagement to the services is minimal.
#	**Out-of-scope from the study**
O1	Process is based on the historical actions and is not documented.
O2	Clear ownership of the reporting process end-to-end should have named owner.
O3	The requirement gathering and development process could be more cleared.
O4	There are different views between teams and individuals about the reporting process.

Each of the strengths are identified with a unique identifier S*n*. The weaknesses are identified unique identified W*n* and out-of-scope weaknesses O*n* identifier. The study will focus on the weaknesses W1 to W4.

3.8 Key-findings to elaborate

The study must not solely focus on the weaknesses. There was input from the interviews and workshop that must be taken into account while finding solution through literature. The relationship and responsibilities between customer and service provider in the cyber security services context must be researched. That part of research should contribute to the reporting structure and what cyber security service framework should include.

In the following section 4 ideas for cyber security service reporting framework are searched from academic literature and already existing known frameworks. The focus of search is on weaknesses found in the current state analysis stage.

4 Ideas for cyber security reporting framework from literature and frameworks

Section 4 discusses about existing knowledge that was found from relevant literature and existing known frameworks. Section 3 outcome listed four main weaknesses and the literature search was focusing to find ideas and clarifications to find suitable solutions to each weakness and take into account reporting categories identified in the current state analysis interviews. The outcome of this section is a conceptual framework that is presented in visual format which is developed based on the relevant reviewed literature.

The search of the literature and review of it in this section is divided into three sub-sections. The first sub-section is focusing on the determining the cyber security posture elements from the service provider perspective. This was approached through definitions of cyber security space, cyber security and cyber security posture of a company. Then study discusses about the relationship between customer and service provider in cyber security and cyber security services context. Also, the questions raised in the current state analysis results workshop are considered when the relationship and responsibilities are determined. Through these topics and context, the cyber security posture elements and responsibilities from the perspective of service provider are determined. The aforementioned discussions relate to weaknesses W3 and W4 found in the current state analysis sections. When those aspects of the cyber security services are understood, the second sub-section of literature search focuses on finding relevant solutions to create cyber security services reporting framework from service provider viewpoint. Ideas and solutions from literature related to weaknesses W1 and W2 were searched. In the third sub-section, the conceptual framework is designed based on the literature. Each sub-section topic discusses about the rationale and the relevance for this study.

The described literature search approach and logic is presented in figure 6.

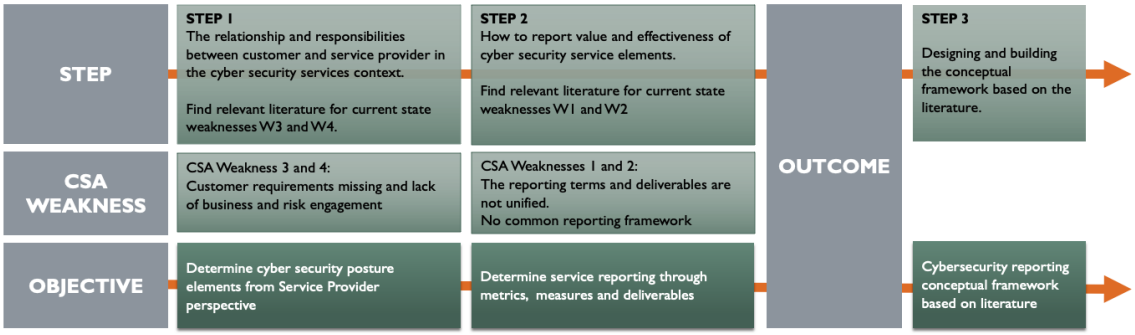


Figure 6. Literature search approach and logic

Figure 7 contains the relations of each search area and the related weakness to it. The weaknesses and topics contain the ideas and knowledge that were used to build the conceptual framework that is the outcome of this section.

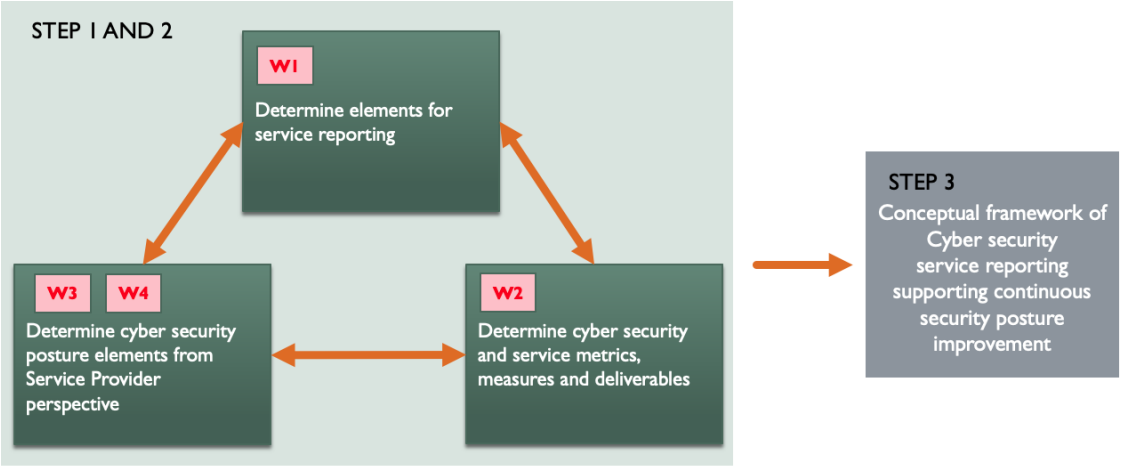


Figure 7. Weaknesses and relation of search areas that literature search is focusing on

The final step and sub-section of the section 4 summarizes the findings and knowledge gained in section 4 that led into the visualized conceptual framework of cyber security services reporting.

4.1 Determining the cyber security posture elements

In the current state analysis section, the definition of cyber security from Schatz et al. (2017) was introduced. This sub-section examines these elements mentioned in the definition and how they are linked to the cyber security services delivery and reporting.

4.1.1 Definition of cyber space

Fourkas (2004) has defined cyberspace consisting of three layers that technical, geographical and social. The characteristics people, space and time along with geography are contributing to the spatial conception and embodiment in contemporary society and development of the cyberspace is influenced by economic and technological development. (Fourkas, 2004; 2)

According to Limnéll et al (2014) the cyber space is an operating environment in which ecosystems of bits and the physical world are mixed. The inactivity of bits might be reflected in the physical world as negative affect. A cyber-safe operating environment requires an overall goal, for which each member of the ecosystem produces its own subgoal. Changes in cyber space are rapid and difficult to predict. The sub-objectives should be coordinated in a manner that overall cyber security can be achieved. The most important element is building and strengthening trust to each ecosystem that they can be trusted as safe and functioning environments. (Limnéll et al., 2014: 24-26, 29, 40, 74)

From this we can conclude that cyberspace is everywhere, evolving constantly and rapidly and has constant affect to all users and organizations through technological and social interactions that reflect to physical realm. There are so many variables what are affecting the reality of cyber space of an organization, that each organization can be considered to be unique in the context of cyber space. Also, the environments of organizations are most likely intertwined and dependable from each other and line cannot be drawn where cyber space of one customer environment starts or ends. Therefore, each organization should focus on making their own environment or in other words their own ecosystem as safe and secure as possible.

4.1.2 Cyber security of an organization

Traficom (2020) published a guide for management boards for their responsibilities regarding cyber security. The responsibility is to understand benefits from digital technology, but it is equally important to understand the risks related to them. These responsibilities start from the management board. Cyber security risks or in short cyber risks should be dealt as other business risks. The organizations should define their technical environment that is most critical for achieving business objectives and use cyber security measures to protect the environment. If organization is collaborating with service providers, the service providers must be included to the risk management practices of the company. (Traficom, 2020; 3, 10-11)

When we combine this conclusion with sub-section 4.1.1 ecosystem definition a conclusion can be drawn that each company has a responsibility to ensure their cyber security risks and possibilities are treated accordingly so that their ecosystem meaning cyber space environment can be trusted and considered to be secure by other ecosystems.

The section 3 introduced the definition of cyber security by Schatz et al (2017). The definition states that risk management should focus on the confidentiality, integrity and availability of data and assets used in cyber space. The protection of data, users and cyber environment is achieved by using guidelines, policies, safeguards, technologies, tools and training or some combination of these. Bauyk et al. (2012) explain that goals and mechanisms of cyber security can be reflected and achieved by three triads. The triads are presented in figure 8.

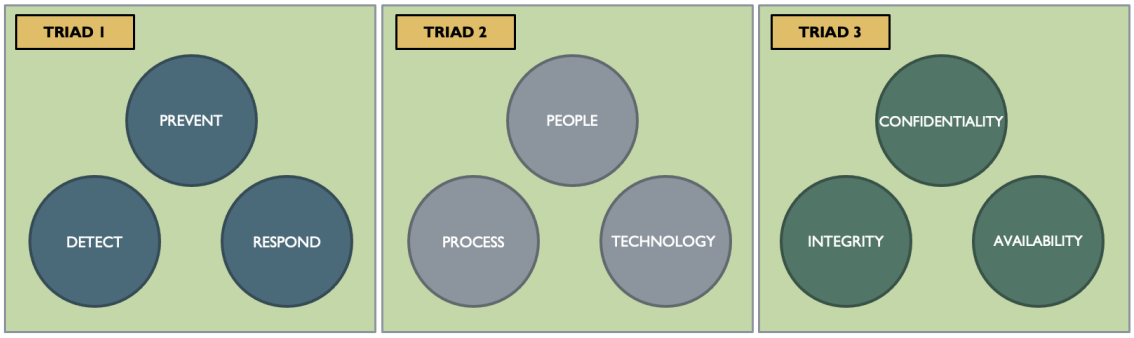


Figure 8. Three triads to achieve cyber security goals.

The triad 1 focuses on the operations of cyber security. The goal is to 'prevent' all attacks but since it is not possible, 'detection' capability of threats and attack progress preferably before they cause any damage is required. The third step 'respond' represents the capability to respond to attacks with countermeasures when they are detected. If the 'prevent', 'detect' and 'respond' triad capabilities fail, the 'respond' capability changes to 'recover' capability of business-critical systems step. The triad should be developed in the continuous improvement loop. (Bayuk et al., 2012; 2)

Triad 2 is focusing on that the triad 1 capabilities can be achieved. Triad 1 requires the people, processes and tools to observe, maintain and manage the routines and systems to accomplish their mission and to achieve cyber security goals. (Bayuk et al., 2012; 2-3)

Triad 3 addresses the confidentiality, integrity and availability of the information. Confidentiality ensures the access to certain information is granted for intended individuals only to protect the sensitivity of information while integrity ensures the authenticity, accuracy and provenance of the information. Lastly, availability refers that information is accessible by indented users. (Bayuk et al., 2012; 3)

When triads are combined the cyber security of an ecosystem could be defined how Bayuk et al. have defined cyber security through the triads:

> *Methods of using people, process and technology to prevent, detect and recover from damage to confidentiality, integrity and availability of information in cyber-space. (Bayuk et al., 2012; 3)*

From these statements we can make a conclusion that companies must make efforts to improve their cyber security environment constantly with continuous improvement methods and one way to observe and consider organizational cyber security dimensions is through the three triads.

4.1.3 Cyber security management and objectives of an organization

Limnéll et al. (2014) state management of cyber security happens through organization strategy and must be taken into consideration in all organization processes. Implementing cyber security requires the organization to have common standards, controls, practices, reporting, situational awareness, and incident management. Absolute safety cannot be achieved, but the organization should set the desired level of safety. The aim must be to create a cyber-secure operating environment, but this cannot be created alone, but requires seamless and flexible cooperation between different actors. (Limnéll et al., 2014; 40, 44, 55-58)

Both Whitman et al. (2011) and Bayuk et al. (2012) state that setting goals and targets through strategy is necessary to respond to the cyber security needs and requirements by an organization. They both also describe this an iterative process how the cyber security goals and targets are defined to support overall strategy and create a comprehensive cyber security posture. Whitman et al. use term program where tactical level and operational level goals and actions are defined. Bauyk et al. on the other hand state that cyber security is part of the of the program where goals and objectives are defined. The next step is to implement the necessary steps to achieve the goals and objectives. Both books mention International Organization for Standardization's ISO27000-series and National Institute of Standards and Technology NIST cyber security framework as good frameworks to help and guide the implementation of cyber security. But it is stated as well as that implementing known framework does not guarantee that cyber security goals

and objectives are reached. The frameworks should be adapted to meet the cyber security needs of the organization. The whole company should be aware of the cyber security goals and objectives and be accountable in their all actions that they in accordance with them. (Bayuk et al., 2012; 11-12, 39-40, Whitman et al., 2011; 39-44)

Both authors deliver key message that organizations should not try to reinvent the wheel but should find a suitable framework to help and guide organizations. It is also good practice to understand the uniqueness of each organization and carefully evaluate how the framework will fit to the needs of and organization.

Both Whitman et al. and Bayuk et al. refer controls as safeguards that are protecting the environment from threats and attacks and ensuring the acceptable use of the systems and information. According to Whitman et al. (2011) the controls can be divided into three broad categories that are managerial, operational and technical controls. Managerial controls cover security processes whereas operational controls are controls that are developed and integrated into the business functions to address operational issues such as disaster recovery and incident response planning. The managerial and operational controls are supported and complimented by technical controls which address specific technical components that relate to identification, authentication, authorization and accountability. NIST and ISO standards are mentioned by Bayuk et al. (2012) as good sources to evaluate technological operations. Also, the controls must be managed, monitored and maintained accordingly. (Bayuk et al., 2012; 10-13, 39-40, Whitman et al., 2011; 39-44)

Whitman et al. (2011) are pointing out that not only technical controls are enough to secure systems and information. The controls require input from strategic level through processes and operational controls are looking into situations where technical controls have failed for a reason or another. The standards yet again help organizations to discover and implement controls.

Bayuk et al. (2012) and Whitman et al. (2011) emphasize the monitoring the performance, effectiveness and progress and how critical it is to justify the spend and resources used to cyber security. The metrics should be meaningful and correspond to the goals and objectives of cyber security program or policy. A metric is a generic term that refers to measure certain things in a comprehendible way in the relational world to draw conclusions about. Cyber security cannot be a direct object of metric or measurement

since there is no defined measure and metric for it. Therefore, cyber security needs to be measured through other things and drawing conclusions about them. The metrics and their measurement need to be linked to the objectives and should be devised at the same time as goals and objectives are set. This way the progress, performance and effectiveness of cyber security can be measured and reported. (Bayuk et al., 2012; 11-13, 40 Whitman et al., 2011; 46)

Figure 9 contains the concept for cyber security management cycle that is a systematic process and includes reporting of performance, effectiveness and progress of cyber security.

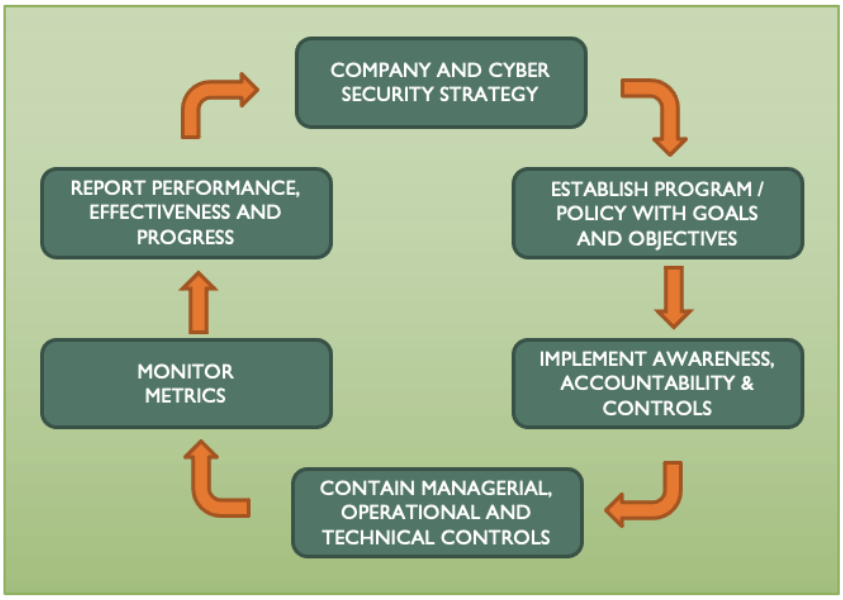


Figure 9. The cyber security management cycle based on Whitman et al. and Bauyk et al.

From this we can conclude that the cyber security management cycle can be similar in every company and it must respond to the changing needs and requirements set by the company itself and cyber space where it operates. The objectives and goals that set the requirements for controls, metrics and reporting are in some extend company specific and require planning. Or if the services include standard controls along with metrics and measures, they should be evaluated how they are contributing to the organization's goals and objectives.

4.1.4 Cyber security risk management process

According to Limnéll et al. (2014) a risk means the possibility of some negative event in the future. Risks cannot be fully countered, but they can be addressed in a variety of ways, such as avoiding, embracing, limiting, mitigating, moving or learning to live with them. This is done through risk management, where risks are assessed, addressed and the means are chosen to cope with the remaining risks and their potential negative effects. Risk management takes place as a systematic and continuous process consisting of risk management planning, risk identification and analysis, continuous monitoring and reassessment of risk development, implementation of corrective actions, communication, reporting, other documentation and coordination. The risk always includes an assessment of the probable occurrence of the negative event in the future and its effects. (Limnéll et al., 2014; 108-110)

NIST Cybersecurity Framework Core 1.1 (2018) consists of five concurrent and continuous Functions that are ‘Identify’, ‘Protect’, ‘Detect’, ‘Respond’, ‘Recover’. NIST defines risk management an ongoing process to identify, assess and respond to risk. Through the five functions organization can obtain a high-level strategic view of lifecycle of management of cyber security risks. Each organization will have unique risks, different threats and vulnerabilities. Risks are determined by likelihood and event will occur and potential resulting impacts and each company has their own risk tolerance and willingness to spend to solutions or controls. The cyber security risk management process is aiming to measure risks along with costs and benefits. The risk management process should support the reaching of objectives that are set in in the cyber security strategy. The measurement of organizational objectives, supportive cyber security outcomes and how the cyber security outcomes are implemented and managed is beyond the scope of NIST Cyber Security Framework. According to Stallings (2019) organizations get input to risk analysis through the risk identification that is identification of assets, threats, controls and vulnerabilities. (NIST, 2018; 2-4, 20, Stallings, 2019; 85)

Limnéll et al. (2014) underline that the digitized processes of companies are the most critical objects for the company, which affect the company's performance and are dependent on the cyber environment. They are also the most important targets in terms of opportunities and risks for the company. Cyber-exposed processes can be divided into four categories, which are digital business processes, digital customer experience, information in digital form, and staff productivity. Of these, the company should look for

threats and opportunities. The risks associated with the threats and opportunities need to be identified in order to manage them. (Limnéll et al., 2014; 170-179)

The main goal of the risk management process is to identify threat and vulnerabilities to business assets in order to implement controls. The risks and controls must be evaluated, monitored, reviewed and reported in order to update and improve them. (ITU-T X.1055, 2008; 1-7)

High-level risk management process is illustrated in figure 10.

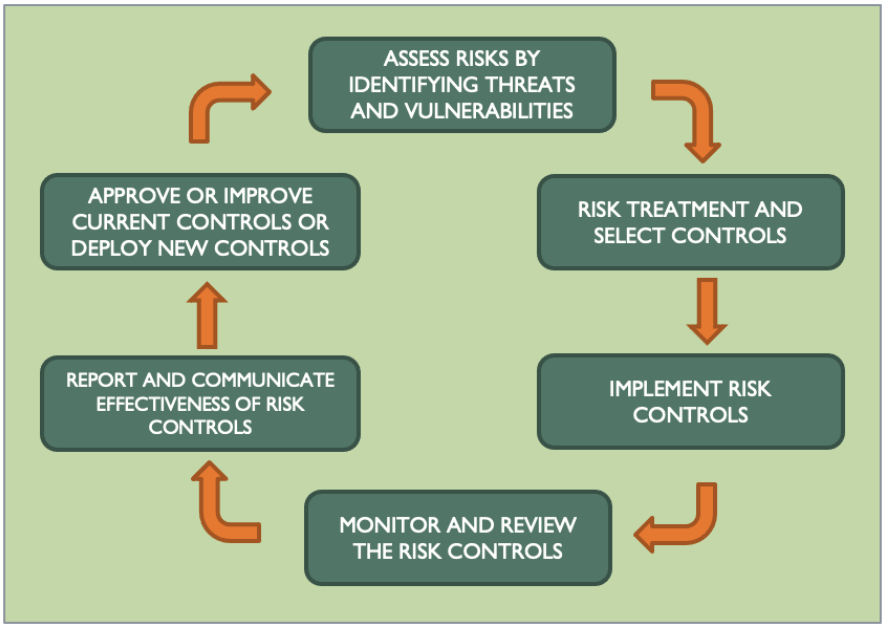


Figure 10. High-level risk management process adapted from NIST, Limnéll et al. and ITU-T

From these statements we can interpret that risk management process for digital processes and ecosystems is a top priority to any organization who want to improve their cyber security posture. The risk management process must be carried out with a systematic approach and requires monitoring, reviewing and communicating the risks, opportunities and results. The reporting of the controls links also to the risk management process and it should link to the identification of assets, threats, and vulnerabilities. The communication aspect means that delivery of a report alone is not enough, but results require dialogue between the reporting stakeholders about the effectiveness so that improvements to controls can be decided and deployed.

4.1.4.1 Threats

Whitman et al. (2011) define threat as possibility of negative effect on an asset that has not yet occurred but the possibility of it occurring exists. Stallings (2019) classifies asset as anything that has value for the for the organization and requires protection. The asset can be hardware, software, information or business asset. According to Whitman, the possibility of negative effect contributes to risk likelihood to be increased. Threat agents are specific actors of threat categories who seek access or damage assets for any reason. The threat agents can be human but not just limited to them since they can take other forms such as forces of natures or 3rd party actors who accidentally cause negative effects such as power or network outages. Based on threat assessment, an organization places necessary controls to mitigate the negative effects to assets. The controls can be policies, practices, processes and/or technological. (Whitman et al., 2011; 6, 13-14, Stallings, 2019; 85)

Center of Internet Security (CIS, 2021) classifies the threats through five alert levels. The threat levels, descriptions and colour coding are presented in figure 11.

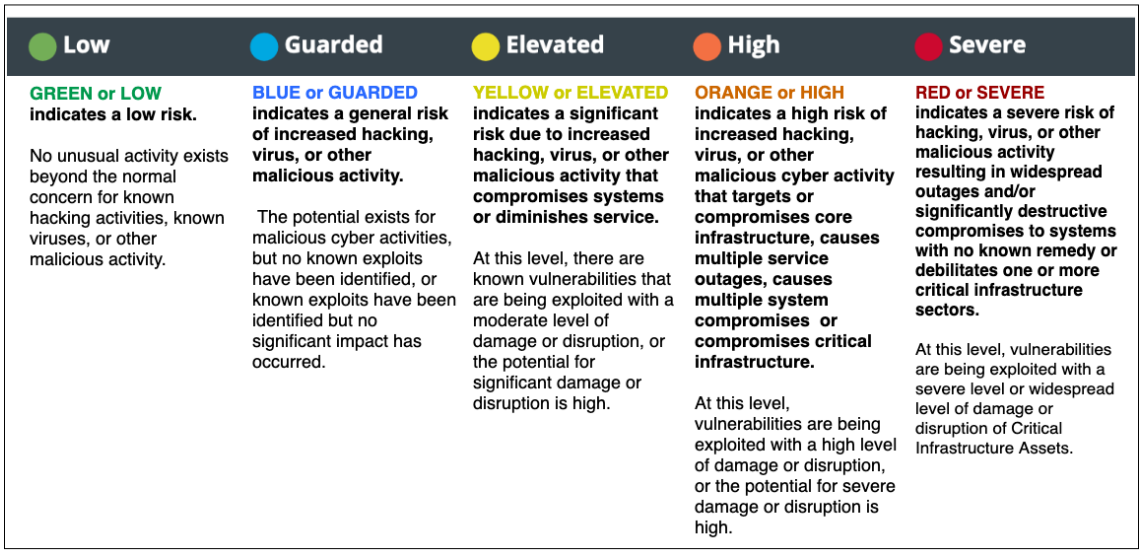


Figure 11. Threat alert levels adapted from CIS (2021)

CIS also has also defined formula to calculate the alert level. Severity is calculated by adding first together the values of criticality and lethality and then the system and network countermeasures are added together. The added figures are then used in an equation where countermeasures are subtracted from the added value of criticality added to the

lethality. The severity calculation result can vary between negative eight (-8) to positive eight (+8) and the result value will present the severity level. Each of the lethality, criticality, system countermeasures and network countermeasures have definitions how they receive their respected value between one and five. Figure 12 contains the threat severity formula and value ranges for different severities. (CIS, 2021)

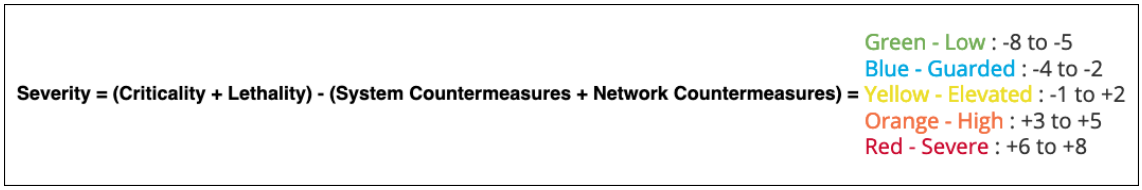


Figure 12. Severity calculation formula adapted from CIS (2021)

The alert level determinations by CIS seem to be bit outdated from some parts but the idea seems to be that they give examples how to determine the levels in each organization and apply them in the threat severity formula.

All of the aforementioned factors underline that the threat management process is an integral part of the risk management process and organizations should prepare themselves to identify several types of threat from outsider to insider threats and from accidentally to intentionally caused negative effects. This requires understanding of the organizations most important assets and processes and the business in general to choose and apply right controls. It is good practice that the threat severity levels are determined to ensure people evaluating threats are discussing in the terms regarding threat severity. This can be done by any method and CIS threat severity calculation formula is one approach.

4.1.4.2 Vulnerabilities

Foreman (2009) defines vulnerability as a weakness in systems, processes and strategies. The definition is aligned with how Limnéll et al. (2011) describe that the vulnerability starts to exist when an actor has a possibility to utilize the flaw in the system. Stallings (2019) on the other hand describes that vulnerabilities are exploits that can be used by threats to cause harm to assets. He continues the definition that vulnerability can be triggered either accidentally or intentionally but then there has been a weakness or flaw

in a system's security procedures, design, implementation or controls. (Stallings, 2019; 102)

Foreman (2009) describes vulnerability management as a cyclical process to identify, classify, remediate and mitigate vulnerabilities and it is linked to risk management process and Limnéll et al. align to this by stating that the vulnerability management process aims to systematically identify, classify, alleviate or fix vulnerabilities or reduce the number of them. The vulnerability management requires both technology and processes where processes guide the use of technology and tries to understand what systems and components compose the IT environment and their exposure. The vulnerability management should be running as a management sponsored security program that has defined processes, goals and policies how it supports business. The vulnerability management process can be linked to regular ITIL processes such as change, incident, problem and release management with agreed service level agreements (SLAs), objectives and agreed measures to meet the business requirements. Regular reports need to be delivered in governance meetings to verify that service level agreements are met. Figure 13 represents the conceptual idea how vulnerability management intertwines with ITIL incident management process and forensics service provided by a security operations team. (Foreman, 2009; 1, 5-6, 45, 181, 189-191, 214, Limnéll et al., 2014; 110)

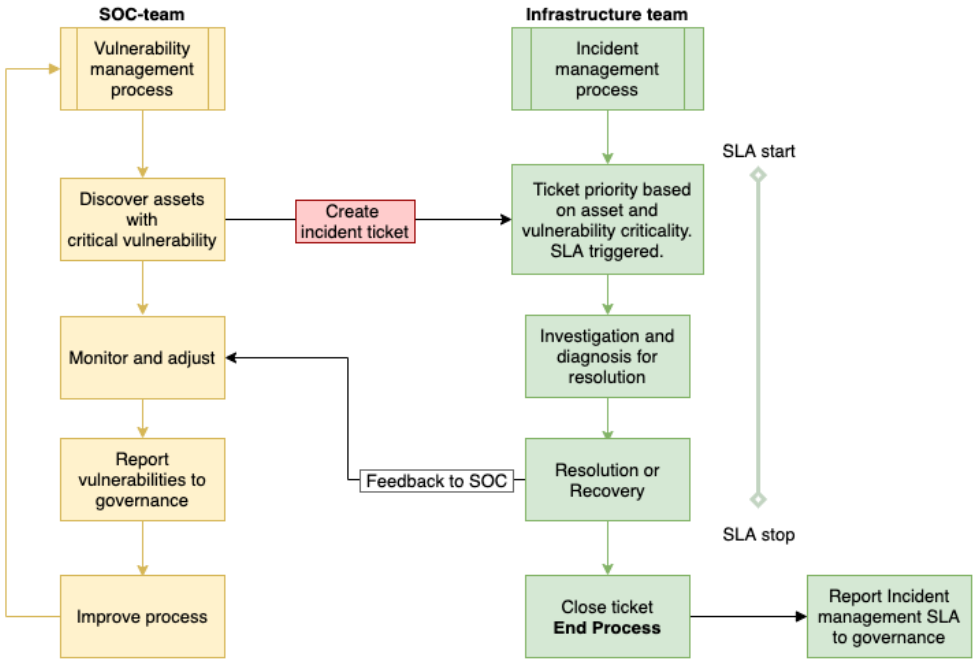


Figure 13. The conceptual idea of ITIL Incident management and vulnerability management process working in interaction based on Whitman

Foreman states that security controls and known standards can be used in conjunction with vulnerability management process but the vulnerability management process needs to work on its own and contribute to the standard. (Foreman, 2009; 3-5)

As Foreman suggests, the key point is that vulnerability management should be done as well as a systematic process and it should be tied directly to incident management process to mitigate possibilities for exploits with effective process and measurable SLA. The problem currently is that vulnerabilities are found every day from every organization. How to prioritize and measure the effectiveness of vulnerability management is a broad topic since there are several stakeholders involved to discover, analyse and remediate them. This requires collaboration between all stakeholders to create meaningful reporting and visibility to vulnerability exposure levels and actions taken in each organization. As Foreman suggests, effective vulnerability management requires constant reporting that should aim for organizations to have visibility of the vulnerability exposure and ability to prioritize the unpatched systems and software.

4.1.4.3 Risk control planning

Whitman et al. (2011) tell that risks need to be managed since it is extremely unlikely to reduce risks to zero. Each organization has their own risk appetite or risk tolerance where vulnerabilities, exploitability and controls are evaluated against the potential cost and gain of the perpetrator. The security controls are implemented to reduce the likelihood that perpetrator can exploit and benefit from vulnerability. (Whitman et al., 2011; 122-123)

Stallings divides risk control planning to following models. Planning can be done by either quantitative and/or qualitative assessment. In both models the target is to find controls where benefits outweigh the security control costs. When vulnerabilities are controlled, the remaining risk is called residual risk. Finding the optimal cost point varies from organization to organization but it is always the lowest point of total cost curve that represents the risk tolerance and costs proportion. In figure 14 the cost analysis of risk or in this case cyber security controls is presented. (Stallings, 2019; 107-109)

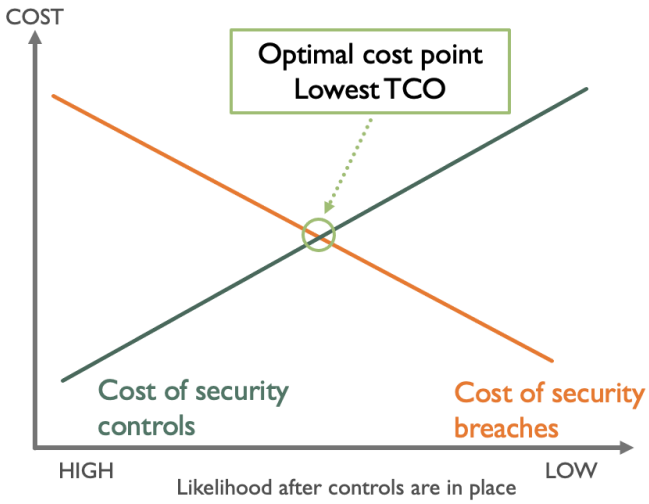


Figure 14. Cost analysis of cyber security controls adapted from Stallings (2019)

This sets a requirement to service provider to collaborate with organizations to find and plan the suitable level of risk tolerance and cyber security controls. But the organizations themselves are responsible for risk management process and setting the correct level for risk appetite.

The cost is depended on many factors. Stallings (2019) mentions for example length of downtime, amount and effect of adverse publicity, cost to recover and rest of the factors being difficult to estimate and introduces standards and methods such as ISO27001, FAIR and ISO27005 to assess risks. Whitman et al. (2011) introduces several ways to do the cost-benefit analysis. He mentions methods such as Annual Loss Expectancy-formula, Feasibility analysis, OCTAVE-method and Microsoft Risk Management approach. (Stallings; 108-116, Whitman et al., 2011; 124-141)

Heyburn et al (2020), have created typology for measurement of costs for a specific breach and not general cyber security costs. The cost types are direct costs and indirect costs. Both cost types are tied to timeframe that is be divided in short, medium or long term but the there is no specific time lime what they are exactly considered since cyber-attacks can last from hours to days. They have found altogether 41 different cost categories that organizations should think and evaluate in case of specific breach. (Heyburn et al., 2020; 22-25)

From these cost methods we can conclude that calculating the cost-benefits is depending on the organization what method they see the most suitable for their organization to

calculate and evaluate what is the optimal cost point. A service provider can help organizations in planning phase by giving their views how certain direct and indirect costs are generated from past experiences from the additional services service providers provides when organization is facing a cyber-attack. The responsibility of risk cost planning resides in the customer organization.

Both Stallings (2019) and Whitman et al. (2011) state that in all scenarios the management is responsible to assess and determine acceptable risk. Whitman et al. (2011) have generalized the process by three tier model where executive management sponsor is ultimately accountable for defining acceptable risk on tier 1. Tier 2 a named risk management team focuses to prioritizing risks by assessing and defining functional requirements to mitigate risks. The tier 3 is operational level where controls are implemented and operated. The risk management team then measures the effectiveness of security solutions and steers operations and reports back to executive management. Figure 15 illustrates a risk management and control planning process. (Stallings, 2019; 113, Whitman; 142-143)

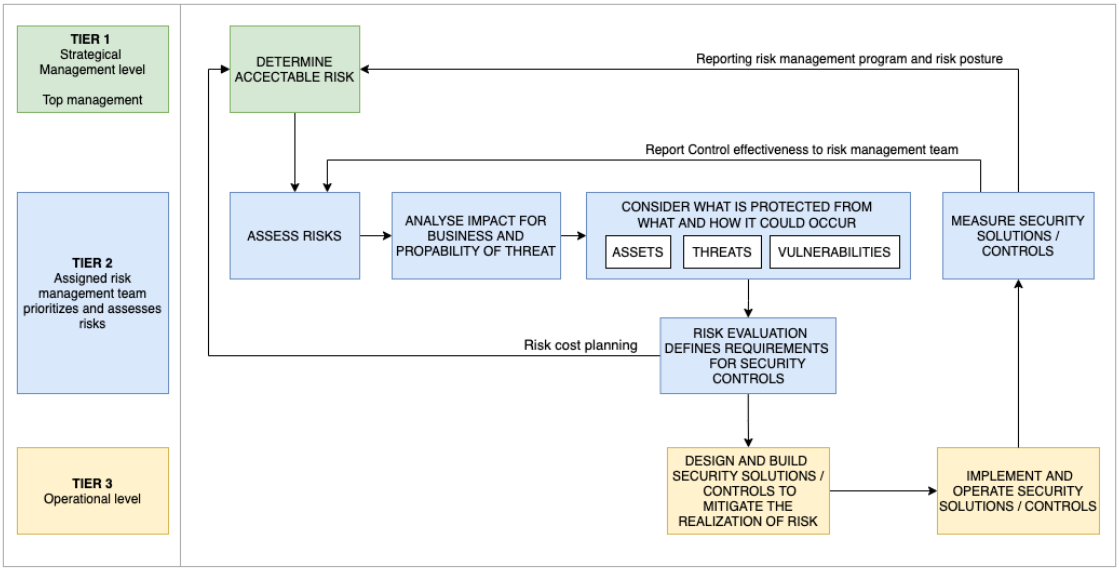


Figure 15. The conceptual idea how control solutions are planned through risk management process and reported back to stakeholders based on Whitman, Limnéll and Stallings

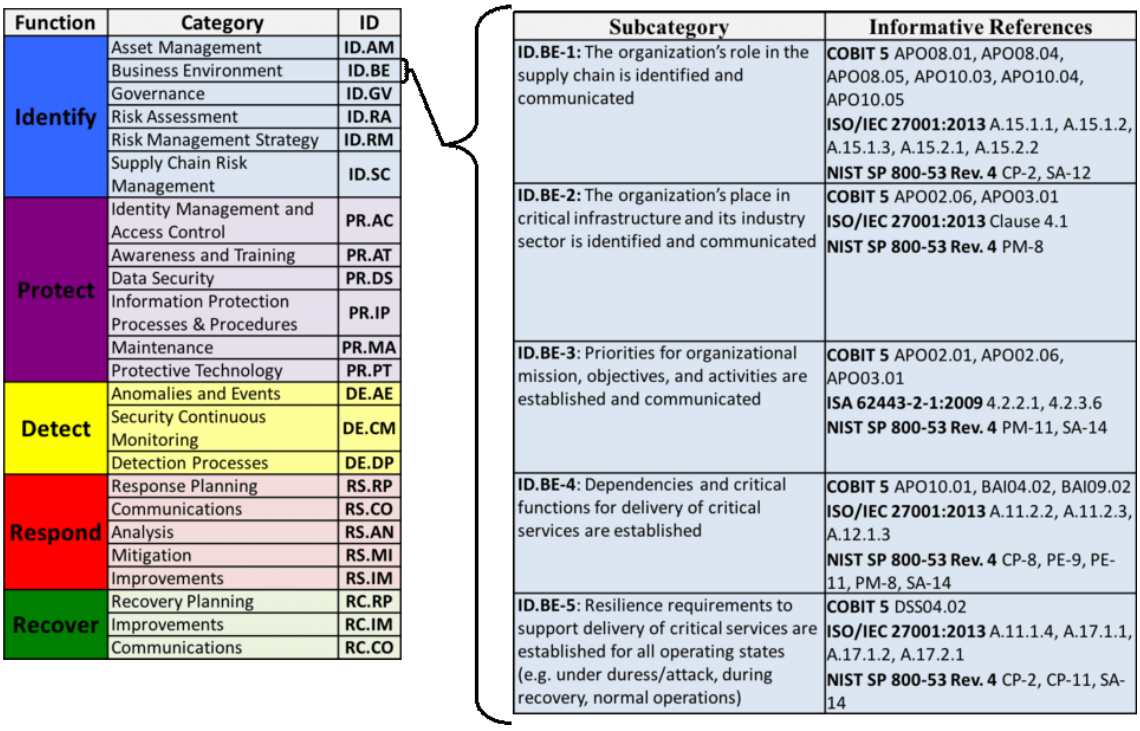
Limnéll et al. (2014) define the measurement should happen through metrics that are agreed upon and should be closely related to the business process. The security plan, implemented at the operational and tactical level, includes operational plans and projects aimed at reducing cyber risks and increasing cyber resilience. The security plan can be

divided into three main categories: situational snapshot, effective cyber security management and response to incident situations. They mention that the ‘SANS Twenty Critical Controls for Effective Cyber Defense’-document can be used as the framework for the cyber security plan. (Limnéll et al., 2014; 180-181, 188-189, 197)

With SANS Twenty Critical Controls for Effective Cyber Defense-document Limnéll points the management to a direction to have at least some sort of requirement for basic hygiene for cyber security related matters since as both Whitman et al. and Stallings state that management is responsible for determining the acceptable level of risk and appoint organization to manage and operate risk management processes and controls. Reporting and communication back to all risk management stakeholders about risks and controls metrics and measures is therefore important in any organization.

4.1.4.4 Risk control management through frameworks

As earlier introduced, NIST Cybersecurity Framework 1.1 (NIST CSF, 2018) provides framework to manage cyber security risks. The framework contains also mapping to other cyber security frameworks and the controls in them. The other control listing standards are ISO27001, COBIT 5, NIST SP-800-53 rev.4, CIS Critical Controls, The International Society of Automation (ISA) standards. This document is available from all organizations from https://www.nist.gov/cyberframework/framework and contains over 500 rows of mappings currently. In figure 16 an example of mapping the CSF function to category and its subcategory where suggested controls are listed.



Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Subcategory	Informative References
ID.BE-1: The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **ISO/IEC 27001:2013** Clause 4.1 **NIST SP 800-53 Rev. 4** PM-8
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
ID.BE-4: Dependencies and critical functions for delivery of critical services are established	**COBIT 5** APO10.01, BAI04.02, BAI09.02 **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	**COBIT 5** DSS04.02 **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-14

Figure 16. Example of mapping to controls to NIST CSF 1.1 (2021)

This does mean that controls should be mapped from each control framework but merely presents that there are several ways how to implement the control for certain risk.

For example, in the Identify ID.BE-2 has controls from COBIT 5, ISO27001 and NIST SP 800-53. The wordings and content of each individual control aims to minimize the risks to Business environment but wording in this instance of each control is different. The controls are presented in figure 17.

IDENTIFY (ID)	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06 - Communicate the IT strategy and direction **COBIT 5** APO03.01 - Develop the enterprise architecture vision **ISO/IEC 27001:2013** Clause 4.1 **-** The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system. **NIST SP 800-53 Rev. 4** PM-8 **-** CRITICAL INFRASTRUCTURE PLAN Control: The organization addresses information security issues in the development, documentation and updating of a critical infrastructure and key resources protection plan.

Figure 17. The control definitions of ID.BE-2 subcategory in other standards

The other standards do not map to each subcategory in NIST CSF 1.1. The key takeaway from the NIST CSF 1.1 is that covering each of the categories and subcategories will contribute to efficient risk management process that leads into improved cyber security program. The program then leads into continually improving cyber security posture through having controls in place. The controls can be from any standard or created for the purpose of organization but the bottom-line is that the control must fulfil the intention of the subcategory in the framework.

The CIS control framework 7.1 (2019) is collection of best practices to mitigate perpetrators to do negative affects to systems. As the document states, the controls can be mapped against regulatory and compliance frameworks. The controls aim to be prioritized set of actions that implementable, usable, scalable and compliant to any industry or government requirements. The controls are specific set of technical measures to detect, prevent, respond and mitigate the damages of most common attacks. Using the controls requires still the organizations to understand what is critical to their business and what are the adversarial actions that could have impact to assets or business data that might hinder the business or operations. The controls and sub-controls are divided into three different implementation groups (IG) that represent the size the hygiene and advancement level of controls. The IG1 is meant for small businesses and also considered as essential for success or in other words the minimum level of basic hygiene of cyber security. IG1 is then followed by IG2 and IG3 where IG2 aimed for organizations who have some IT competencies and usually are medium to large business. IG3 is aimed for enterprises who can afford to spend dedicated resources to cyber security activities. In all cases it is recommended to perform risk assessment. Figure 17 contains the IG group and their definitions. (CIS, 2019; 1-5)

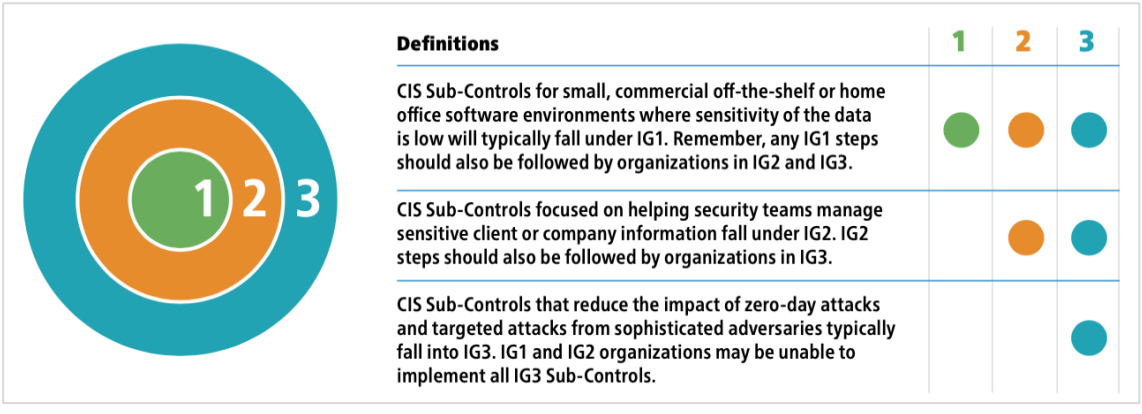


Figure 18. CIS controls 7.1 Implementation groups (CIS, 2019; 5)

The CIS 20 controls are divided into Basic, Foundational and Organizational groups and each of them have a vast number of sub-controls. Each group has a definition, why that control is critical, followed by a list of technical controls and the implementation group recommendation.

CIS Control 3: Continuous Vulnerability Management

Sub-Control	Asset Type	Security Function	Control Title	Control Descriptions	Implementation Groups		
					1	2	3
3.1	Applications	Detect	Run Automated Vulnerability Scanning Tools	Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●
3.2	Applications	Detect	Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.		●	●
3.3	Users	Protect	Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.		●	●
3.4	Applications	Protect	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●
3.5	Applications	Protect	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	●	●	●
3.6	Applications	Respond	Compare Back-to-Back Vulnerability Scans	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.		●	●
3.7	Applications	Respond	Utilize a Risk-Rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.		●	●

Figure 19. Example of CIS control and sub-control list. (CIS, 2019; 16)

In figure 19 the CIS Control 3 – continuous vulnerability management and its sub-controls are presented. The sub-controls 3.4 and 3.5 present basic controls that are part of IG1 and should be implemented to all organizations no matter in what business or size they are. The rest of the sub-controls belong to IG2.

The CIS control Implementation Group model works very well as a framework to evaluate and prioritize what controls should be implemented in all cases and what controls are more advanced and should require mapping to risk management process if they are needed.

4.1.5 Cyber security frameworks

All cyber security frameworks are developed to help organizations to evaluate and develop their cyber security capabilities and manage cyber related risks. There is a hefty number of different frameworks and standards available nowadays and this study introduces couple of them. Against each of the framework there is critique but all of them have supporters as well. One thing in common in each framework is that the organization must define what is their approach to cyber security and what kind of maturity they are aiming for in the short- and long-run. NIST Cybersecurity Framework and CIS Controls were introduced in the study earlier as a management tools in the risk management process but are also considered as cyber security frameworks in the study context. The presents some other frameworks that could be used to evaluate and develop the cyber security in any organization that service provider might encounter.

4.1.5.1 TAG Cyber controls

TAG cyber states that NIST CSF and the detailed NIST 800-53 requirement combination is very large and comprehensive way to approach cyber security. And in the other end of the spectrum, they state that using CIS Controls is more viable approach to reduce enterprise risk. To suite the practical needs of large enterprises, they have developed more hands-on approach to evaluate the enterprise security. Figure 20 contains the 54 controls that are organized to six categories.

Enterprise Controls	Network Controls	Endpoint Controls	Governance Controls	Data Controls	Service Controls
1 Deception-Based Security	10 Public Key Infrastructure	19 Anti-Malware Tools	28 Digital Risk Management	37 Data Privacy Platform	46 Research and Advisory Services
2 Intrusion Detection/Prevention	11 Cloud Security Solutions	20 Endpoint and EDR Security	29 Crowdsourced Security Testing	38 Content Security	47 Information Assurance
3 User Behavioral Analytics	12 DDOS Security	21 Hardware Security	30 Cyber Insurance	39 Secure File Sharing	48 MSSP and MDR Services
4 Data Leakage Protection	13 Email Security	22 ICS/IoT Security	31 Governance, Risk, Compliance (GRC)	40 Data Encryption	49 Large Security Consulting Firms
5 Firewall Platform	14 Infrastructure Security	23 SIEM Platform	32 Incident Response	41 Digital Forensics	50 Small Security Consulting Firms
6 Application Security	15 Network Monitoring	24 Mobile Security	33 Penetration Testing	42 Enterprise Asset Inventory	51 Security Staff Recruiting
7 Web Application Firewall	16 Network Access Control	25 Password/ Privilege Mgmt	34 Continuous Attack Simulation	43 DevOps Security	52 Security Training and Awareness
8 Web Fraud Prevention	17 Secure Access/ Zero Trust	26 Authentication Security	35 Identity and Access Management	44 Vulnerability Management	53 Advanced Security R&D Support
9 Web Security Gateway	18 Attack Surface Protection	27 Voice Security	36 Threat Intelligence	45 Threat Hunting Tools	54 Value-Added Solution Providers

Figure 20. TAG Cyber controls for 2021 (TAG, 2020)

The control list is aimed for larger enterprises to measure their cyber security program completeness. Should the organization not need some control they can leave it out with their own discretion. (TAG, 2020; 6-7, 13)

The TAG cyber control is quite comprehensive list with focus on controls. Even though organization would use this a model for the enterprise controls, the practice still would be to link the control needs to business targets and risk management process which is indeed one of the control categories. Having a control for the sake of control is not the best practice as we have discussed earlier in this study. But the control list offers quite extensive list what organizations could consider as risk controls.

4.1.5.2 Standard of Good Practice (SOGP)

Information Security Forum (ISF) that has over 400 global member organizations. ISF is an independent, not-profit organization specializing in cyber security and information risk management. According to ISF, their Standard of Good Practice (SOGP) covers some cyber security related practices and disciplines in a more detailed coverage. (Chaplin 2017).

The SOGP 2016 version has been divided into 17 categories and 132 topics that are ran in three principal activities as a systematic on-going process. The first phase is planning and defining requirements specific for a given organization and developing policies and processes for managing cyber security. The second activity is implementing and managing controls and third activity is assuring the business continuity enablement and monitoring, assessing and improving the implemented cyber security controls and reporting them back to planning for cyber security. (Stallings, 2019; 9-12)

In meeting between author of this study and ISF, where ISF as an organization and the most recent version of SOGP was presented. The standard has extended to 135 topics and some areas have received update and enhancements. The SOGP also includes metrics tied to the individual topics and mappings to other frameworks such as NIST, ISO27001, COBIT and CIS. The SOGP 2020 version framework is presented in figure 21. (ISF, 2021)

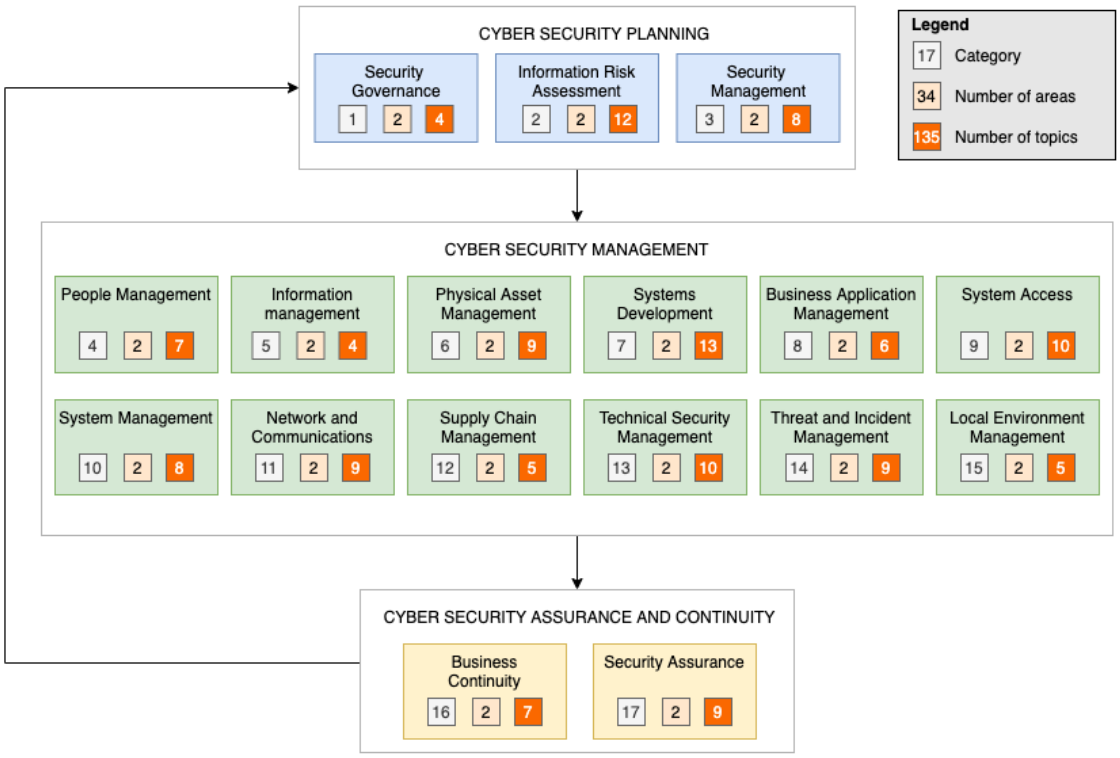


Figure 21. Categories, areas and topics in the SOGP 2020

SOGP has really good approach to managing cyber security as a systematic process. The 2020 version has the same number of categories, but the number of topics has grown to 135. Compared to NIST CSF, getting hands to SOGP material requires paid ISF membership. Both NIST and SOGP are robust frameworks that any enterprise could consider to be used to understand and manage cyber risk as part of the business strategy.

4.1.5.3 ISO27000 series

ISO27000 series is a set of standards that aim for organization to have an efficient information security management system (ISMS). As the name states, it is management system where goals and policies are set by management to enable organization to systematically improve the organization's information security to achieve business objectives. The core of the ISO27000 enables ISMS is the risk assessment and management practices to protect the assets. The known standards are 27001 which set the ISMS requirements and 27002 that provides framework of security controls. The 27001 meaning the ISMS can be certified by independent certification bodies. The certificate ensures the

company executives and partners that security capability has been funded and implemented accordingly to meet security requirements set by the organization themselves. When Stallings compares ISO27002 and ISF SOGP he mentions that ISO27002 does not cover some important topics such as threat intelligence and system decommissioning that are covered in ISF SOGP and he continues that ISF SOGP is far more detailed. (Stallings, 2019; 12-17)

The biggest advantage of the ISMS based on ISO27001 requirements is that it can be certified. With the certificate organizations can show other ecosystems that the area in the scope of certified ISMS is handled systematically in regards of risk management, systematic security improvements are expected, and the organization has top management engagement and enough resources assigned to constantly improve security.

4.1.5.4 Library of Cyber Resilience Metrics

The Netherlands Organisation for applied scientific research (TNO) has collaborated with several Dutch banks on a research program to create a framework to ensure appropriate level of cyber resilience by measuring the cyber security capabilities through metrics that are linked to the 'cyber kill chain'-model developed by Lockheed Martin. The framework is divided into 10 categories that contain 47 metrics. The framework is presented in figure 22. (TNO, 2017; 5-7)

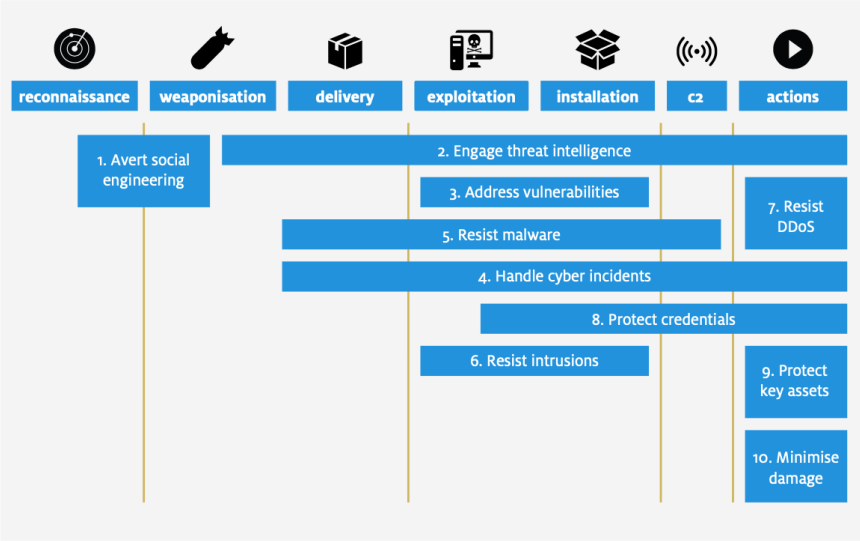


Figure 22. The cyber resilience framework by TNO (TNO, 2017)

TNO states that traditional security metrics focus on the existence of security controls and on fulfilment of specific security requirements. Their metrics aim to reveal the actual status and performance rather than having just tick in a box of fulfilment. (TNO, 2017; 5-7)

The TNO framework has good mix of organizational and technical metrics. They try to tackle the whole spectrum of the three triads and their framework is based on the known Advanced Persistent Threats (APT) attack scenarios and offers way to analyse and plan requirements how to be resilient against them. The framework is created for financial sector, but it can work in any organization facing similar threats. The framework topics from one to ten can be considered as good examples of security targets and high-level metrics the organization should be setting themselves.

4.1.6 Cyber security service provider role and responsibilities in development

Jacobs et al. (2016) have studied existing standards, frameworks and best practices to create a framework for the development of business cyber security capabilities (BCCapDev Framework). According to them there are no existing cyber security capability development framework existing that is modular, reusable and independent to changes in standards, frameworks or best practices while being industry neutral. They have studied definition of capability and have accumulated from various resources that capability is something what is or needs to be done, is clearly defined and provides solutions to its parent capabilities to reach objectives and outcomes by the combination of processes, knowledge, skills and behaviours of people, tools and systems, technology and organization. They have divided the framework to six levels and each level defines what is done and by who. (Jacobs et al, 2016; 51-53)

The Level 0 describes the responsibility of board of directors that are responsible to create business strategy that is complying to all national and international laws, regulations and standards that translate into organizational strategy and policy. (Jacobs et al., 2016; 53-54)

Level 1 describes how an internal governing and controlling body is appointed to place documents created at Level 0 to practice. This requires risk-based approach to determine cyber threats and cyber risks. Only through understanding risks and threats can organization prioritize the development of cyber security capabilities. They mention cyber

security risk management frameworks can be used from organization and standards such as ISO/IEC 31000, ISO/IEC 27005, ITU-T X.1055, NIST, ENISA, ISACA, ISO/IEC 27001 & ISO/IEC 27002 and SANS. The main point is to have ongoing operational model such as ISACA's plan-build-run-monitor that is run by the internal controlling body that usually run by CISO. (Jacobs et al., 2016; 54-55)

Level 2 describes organizational structure of the business. Each organization is different and might be operating in several countries where different normative and authoritative requirements, laws and regulations are applicable. (Jacobs et al., 2016; 54-55)

Level 3 are the capabilities that organization has determined the business cyber security capabilities. These should be used in conjunction with enterprise architecture, people, processes and tools/technologies that enable and support the cyber security capabilities. Wakaru (2010) tells that in ITIL, capability is the ability of a service organization that is consisting of people, processes, applications, Configuration Items (CI) or IT service to carry out an activity. Jacobs et al. (2016) have chosen NIST CSF to represent the capabilities and completeness of business cyber security but only on a category level. They mention that NIST CSF is considered flexible capability framework and it can be used in conjunction with other requirements and frameworks that have input or output applicable to the business. The development of technical capabilities should measure effectiveness and performance of the technological capability. They state that these operational models and skills requirements can be provided by outsourced service provider. (Jacobs et al., 2016; 55-57 & Wakaru, 2010)

Level 4 describes the structures needed to support the capabilities from Level 3. For example, the respond capability requires Security Operations Center (SOC) that has people and skills, processes and technologies. The structure might consist of internal or outsourced resources or both. (Jacobs et al., 2016; 57)

Level 5 describes the structures policies, processes and technology specific procedures that need to be aligned with business. The structure might consist of internal or outsourced resources or both. (Jacobs et al., 2016; 57-58)

The BCCapDev Framework quite nicely defines the Service Provider role in the development of cyber security capabilities in any organization. The concept for how to develop cyber security capabilities based on business requirements is presented in figure 23.

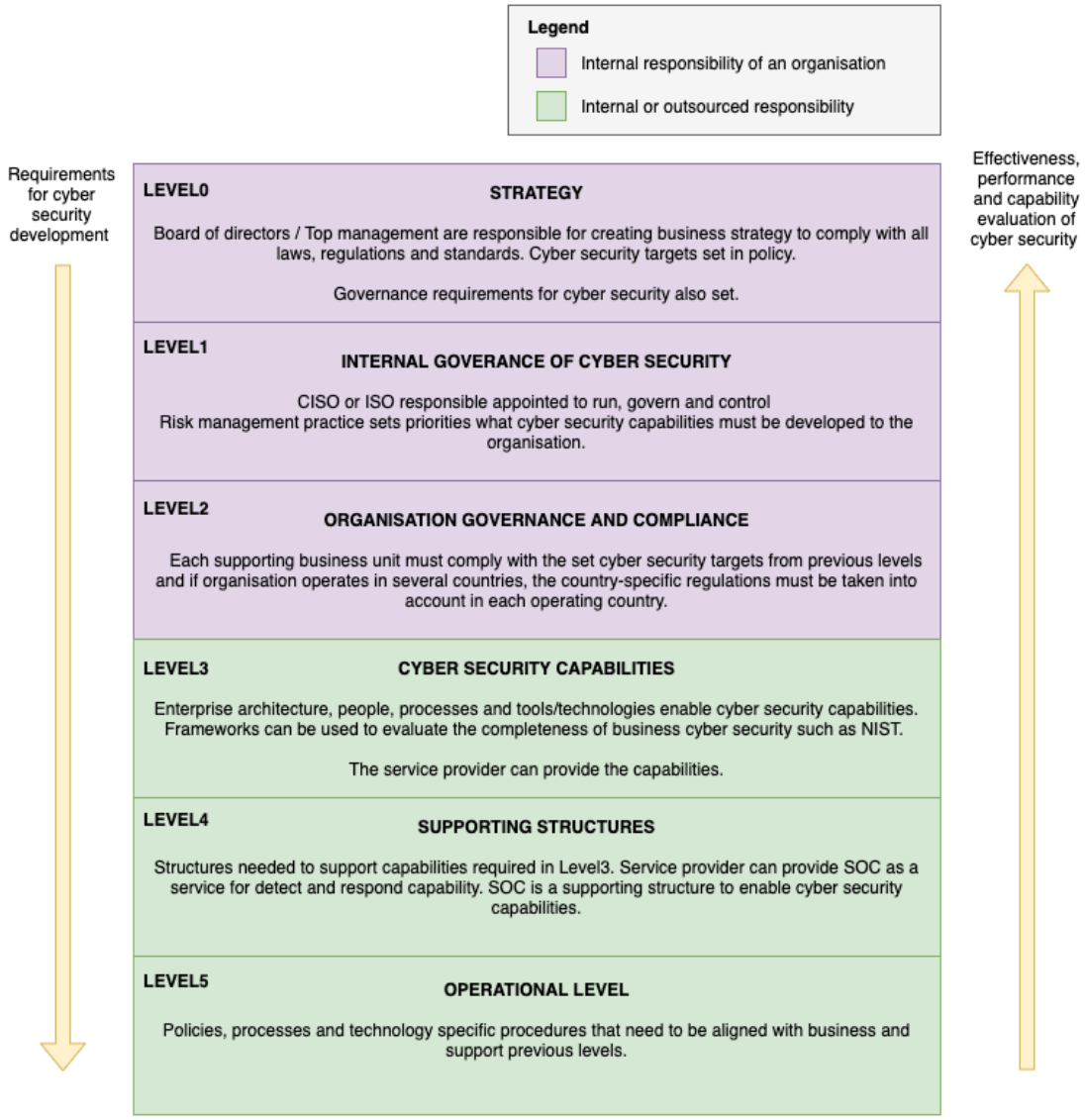


Figure 23. The concept for developing cyber security capabilities in an organization through business requirements based on Jacobs et al.

The capabilities can translate into cyber security posture or cyber resilience. The key takeaway from the BCCapDev Framework is that like in any other frameworks, setting the cyber security objectives and risk management are the responsibilities of the organization. The activities are divided among top management and the assigned controlling body by the top management. The risk management process cannot be outsourced but rather it requires participation from all internal and external stakeholders of the organization.

The service provider can help then with enterprise architecture to ensure proper technical and process components, but the cyber security should be built-in to those and capabilities should be developed accordingly and not as an afterthought. It is up to the organization to decide what capabilities are outsourced and what are done in-house. The Service Provider role and responsibilities start from the capabilities that are aiming to fulfil the objectives. The required controls or countermeasures that support capabilities need to be identified in the risk management process. On the other hand, the NIST CSF and SOGP give strong indication what are the cyber security capabilities that are required by any organization whereas TNO Cyber resilience sets the high-level cyber security targets that then require capabilities. All the mentioned frameworks should be used in conjunction with people, processes and tools triad to ensure the controls are working as intended.

Katzan (2012) describes cyber security service as a collaborative service. In this method service providers and clients collaborate and share responsibilities to supply the service. All the controls that are implemented to the organization form a collaboration group that try to achieve mutually beneficial results and it might be that cyber security service provider is not responsible for all controls. When cyber security is delivered as a service, the distinction between service provider and customer is often blurred than strictly defined. (Katzan, 2012; 71-77)

The study of Katzan underlines the need of a strong partnership in cyber security services if an organization wants to achieve successful outsourcing and required capabilities. This sets requirements for reporting practices to be transparent and it should always suggest ways how to improve collaboration between service provider and customer, capabilities and service deliverables. But the customer must also engage to services by clearly telling the targets and give correct requirements through risk management process or even include the service provider as stakeholder in the risk management process.

4.2 Service reporting elements

The second step in this section is to find relevant literature to weaknesses related to reporting metrics, measures and deliverables that were not unified across customer base and organization did not identify or use consistently any reporting framework. This sub-

section gathers elements such as metric, measures and other deliverables for the reporting of value and effectiveness of cyber security service.

4.2.1 Definition of service

ITIL Central (2005) states that around in 1988 IT Infrastructure Library (ITIL) saw its daylight. It was developed by UK government's Central Computer and Telecommunications Agency (CCTA) to standardize the best practices how to run IT infrastructure and IT services. In the year 2021 best practices of ITIL and the framework in general have been iterated many times over and has been globally accepted as the de facto standard to request and provide IT services. The biggest advantage from the ITIL being widely accepted is that the customers and service providers use the same terminology. Axelos (2011) states that both customer and service provider understand the needed service attributes in a same manner to ensure that services are delivering the outcomes and value that is expected by the customer organization. (ITIL Central, 2005 & Axelos, 2011)

Khalilian et al. (2017) describe that services delivered to customers need to be reported in a manner that the report includes metrics of service activities, functions and processes. These are usually Service Level Agreements (SLA), KPIs (Key Performance Indicators), Service Level Management (SLM) and Service Level Targets (SLT) that are implemented through IT service management framework (ITSM) such has ISO/IEC 20000 or Information Technology Infrastructure Library (ITIL). The aim of the service reporting is to measure, audit and align the service provider and customer to verify the successful outsourcing by clearly showing the status of implementation by monitoring trends and performance against service targets that should guarantee the quality and outcome of the service. The target metrics are defined and reached through agreement between parties. Good reporting shows the value of service for both customer and the service provider (Khalilian et al, 2017; 1737).

Cyber security services are a subtype in the wide range of IT services, and it was identified in the current state analysis that the key stakeholders are working in the IT departments of customer organizations. ITIL is considered to be the de facto standard for delivering IT services in general and that is used in other departments in the case company to provide IT and network services. This makes using the ITIL terminology and governance models in the cyber security services highly feasible since they are then aligned with all other services in terminology, governance and delivery wise.

In the ITIL-framework there is a clear definition for what is a service and IT service.

> *A service is a means of delivering value to customers by facilitating the outcomes customers want to achieve without the ownership of specific costs and risks. (Axelos, 2011)*

> *IT service: A service provided by an IT service provider. An IT service is made up of a combination of information technology, people and processes. A customer-facing IT service directly supports the business processes of one or more customers and its service level targets should be defined in a service level agreement. (Axelos, 2011)*

The capabilities and resources are used by organization to create value in the form of goods and services. The ITIL framework also stipulates that service will deliver the value for business when both utility and warranty are realized. Utility means that service is fit for purpose which means that the customer gets what they want by either ensuring the service performance is on a desired level or constraints have been removed. Warranty means that service is fit for use which means that how the service delivered. This means that service needs to have capacity and be available for service consumers and must be secure enough. For incident or disruptions, continuity plans should be made in advance. Illustration how utility and warranty together create is illustrated in figure 24. (Axelos, 2011)

Figure 24. Illustration of service utility and service warranty creating value of the delivered service

The customer needs need to be understood and the demand must be translated into attributes of the service. That will result to increased probability that service will deliver the desired outcomes that translate into value the service provides. (Axelos, 2011)

The definitions set requirement that services should identify what outcomes are expected from the customer business and the services should have service levels agreed in the

service level agreement to ensure the outcomes. The utility and warranty cover the people, processes and technology scope. The cyber security services usually provide capabilities along with technological outputs therefore it is evident that service provider and customer need to work in tandem to improve performance and remove constraints and work together to ensure the warranty. This sets requirement for reporting to report and suggests improvement to each area to ensure that value is created in the short, medium and long-term future.

4.2.1.1 Service value chain and continual improvement

ITIL version 4 is built around service value system (SVS) that is comprised of guiding principles, governance, service value chain, practices and continual improvement. ITIL focuses on the value delivery through a service value chain (SVC) through six activities that are plan, improve, engage, design & transition, obtain/build and deliver & support that is the core element of ITIL Service Value System (SVS). The SVC is illustrated in figure 25.

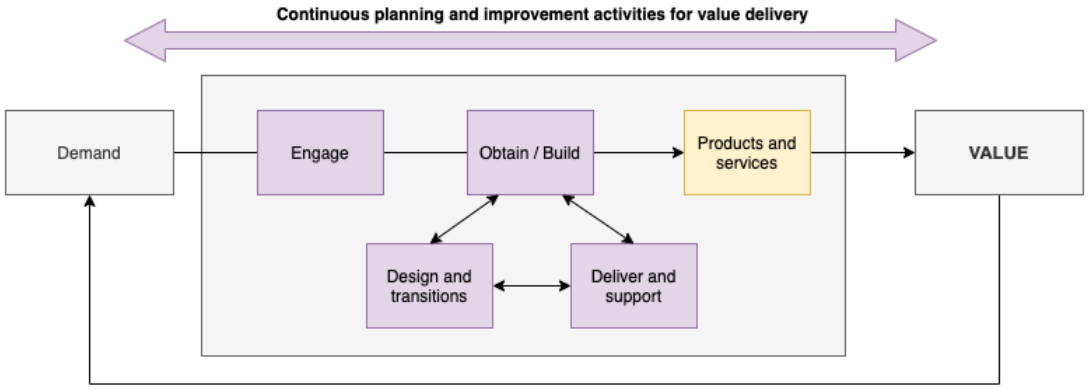


Figure 25. The conceptual idea of ITILv4 service value chain (SVC) to ensure value delivery

Once service is designed the value streams should be subject to continual improvement which is a separate ITIL practice. There are total of 34 practices in ITIL version 4 that are designed for performing work or accomplishing an objective. The continual improvement model is illustrated in figure 26.

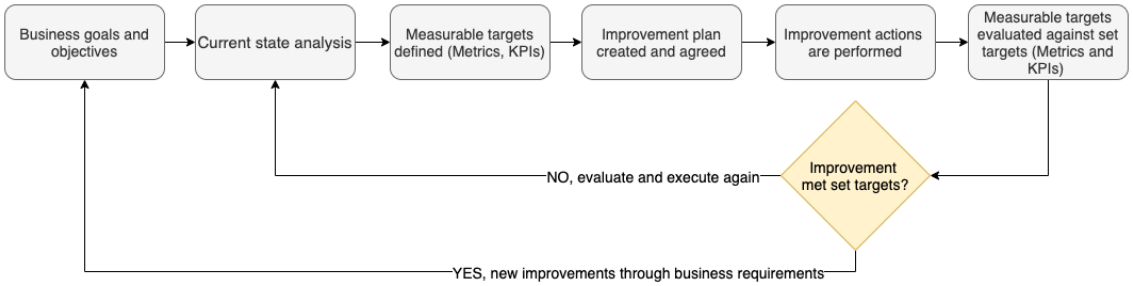


Figure 26. The concept of continual improvement model

Key performance indicators (KPI) along with critical success factors (CSF) are important metrics used to evaluate the success in meeting an objective. They are planned and decided in the 'Business goals and objectives'-step with clearly defined measurable targets. CSFs represent the set goals. Based on the CSFs, a set of related KPIs are defined. Operational KPIs should represent the efforts by the whole team that business goals are met, and targets should be set in the context of proving value for the organization. (Axelos, 2019)

Continual service improvement is therefore integral part to deliver any services. This again emphasizes the collaboration aspect of service development but also highlights that improvement goals and objectives should have measurable baseline and targets that success of improvement can be verified. The ITIL does not state what are the units of measures for measurable targets and neither it states if they should be quantifiable or qualitative. Therefore, it is important that service provider and customer agree about the targets together, but the vision, mission, goals and objectives should be derived from the business of customer.

Bainey (2016) does not talk about CSFs, but according to him KPIs are monitored and managed to guide decision making. The KPIs and services both follow lifecycle that aims for continuous improvement results, outputs, outcomes and performance. The KPIs are presented in a scorecard or dashboard. The goal of them is to monitor and manage outputs by measurable outcomes. The goal of them is to monitor and manage outputs by measurable outcomes that are linked to objectives. Industry best practice is ITIL in the IT service delivery life cycle. (Bainey, 2016, 339-344)

Similar process for service lifecycle and continuous service improvement is described by Bainey as they are described in ITIL. Bainey emphasizes that the KPI monitoring, measuring and managing should guide the decision making. The key point is that the units of measures should be translated and communicated in a manner that they support decision making through reporting.

4.2.1.2 Service Level agreement

To offer and provide services for customers a clear business-based targets for service levels need to be established. This ensures that services are delivered properly. This requires monitoring and measuring against these targets. The service level means that one or more metrics have been defined what is expected or achieved to constitute the service quality. Service Level Agreement (SLA) is the common tool to measure the performance of services. The SLAs have requirements must be related to a defined 'service' which relates to defined outcome and not simply operational metrics. The outcome and operational metrics must be understood and used by all parties and reflect to agreement what was discussed between service provider and service consumer. The Service Level metrics and measures should be a truthful reflection of the customer's actual experience and the level of satisfaction of the whole service. (Axelos, 2019)

Service level agreement aims not just outputs but also ensures the expected quality and tries to measure it. ITIL does not directly state how the actual experience and level of satisfaction should be measured. This will be most likely achieved by combining technical units of measures and getting subjective feeling of quality and satisfaction from customer using the service. This yet again requires communication and dialogue between service provider and customer in the service governance activities.

Feglar (2005) has created synthesis that SLAs should be defined risk management process. The SLA creation starts with scope definition. Then the risk management process starts with asset, threat and vulnerability analysis and risk is then treated accordingly to approve the risk level and choosing right countermeasures eventually leading to responsibility assignment between service provider and customer to generate SLA package based on the responsibilities. The process for SLA to cover security is illustrated in figure 26. This complements to the definition of Katzan that cyber security is a collaborative service. (Feglar, 2005; 61-70)

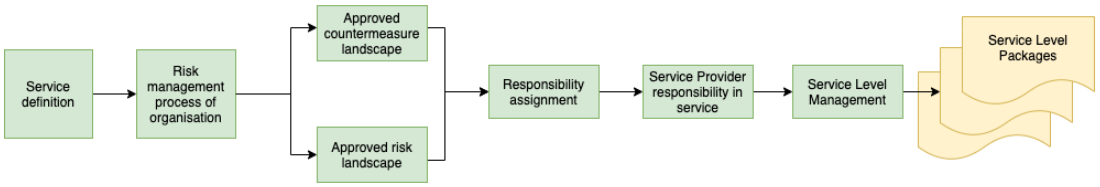


Figure 27. Service Level Management if SLAs Cover Security adapted from Feglar (2005)

The SLAs can be most effectively created when the customer is engaged. ITILv4 has list of helpful items to discover from customer and these can be for example base metrics, measurement and ongoing progress discussions that can be complimented by asking the customer about their business, goals, objectives and measurements for the current and coming year. The service level should hold 'Key business-related measures' including the 'business metrics' that indicate what customer values as important and can be a bundle of SLA metrics or specific business activities related to sales, projects or operational function. The business-related measure should be presented in written format for example 'getting an ambulance to site of an accident within x minutes 24/7'. The 'Operational metrics' are low-level indicators of various operational activities and can include for example system availability, processing times, response and fix times. The keep it simple and practical guideline states that if a service, process, action or metric fails to provide value or produce a useful outcome, it should be eliminated. (Axelos, 2019)

Building the correct SLA package for cyber security services requires collaboration understanding of customer's business and risks so that the responsibilities can be agreed accordingly. This is the correct way to build services and their processes and actions that can be measured and translated into KPIs and metrics that are translated into critical success factors that support the customer business, and they can be used for decision making that was one requirement for service reporting.

4.2.1.3 Service measurement and reporting

Bainey (2016) states that the measurement system aims for improving the operational excellence of the company by enabling view to utilization of IT resources, strategic value integration and evidence-based decision making. The strategic level defines and adjusts the goals, strategic directives and alignment with IT whereas operational level defines and adjusts the goals of IT and establishes accountabilities for IT service delivery along with performance measures. This includes the Service Level Agreements (SLA) and Key

Performance Indicators (KPI) for outsourced contracts that need be aligned with performance results that are presented to stakeholders to highlight issues, accomplishments and continuous improvements. (Bainey, 2016, 6-18)

Bainey discusses that measuring and reporting should be divided into strategic and operational levels. The report should help the customer organization to align services that performance results, issues, accomplishments and continuous improvements from IT services can be reported and presented to the strategical level stakeholders.

In ITILv4 measurement and reporting is one of the 34 practices. Measurement and reporting practice is used to decrease any uncertainty from decision making and continual improvement. This requires collection of relevant data on various managed objects and valid assessment of this data. The managed objects are most likely connected along with their metrics and indicators therefore they should be assessed in appropriate context. Even a customer survey can be part of the Service Level reporting. According to ITILv4 a good report answers to questions: how far are we from our targets and what bottlenecks prevent us from achieving better results? Table 4 for contains description how the measurement and reporting practice contributes to each activity in the service value chain. (Axelos, 2019)

Table 6. The measurement and reporting practice contribution in the different service value chain activities

Plan	Strategy enablement through reporting. Reporting supports decision-making by evaluating current performance of products and services. Needs for improvement or new products or services are discovered through reporting.
Improve	Constant monitoring of performance. Reporting aligned to support continual improvement and value creation.
Engage	Reports are providing correct and up to date information for stakeholders.
Design and transition	Report information supports management decisions at every stage before go-live of products and services.
Obtain/build	Development and procurement are transparent. Reporting enables effective management and integration to all other value chain activities.

Deliver and support	Reporting enables management of products and services that currently deployed to customer. Correct, up-to-date, and sufficient performance information of the products and services are presented to stakeholders.

In all cases the reporting is aiming to support good decision-making and the content of report depends on the context related to the topic, context and the recipients of the report. (Axelos, 2019)

The decision making is a pivotal attribute for reporting and is highlighted by both ITIL and Bainey. Fact and evidence-based decision making can be achieved by having proper measurable targets that are derived from business needs. But as ITIL states the report should be created and delivered to serve the right context and recipients.

4.2.2 Cyber security metrics and measures

According Black et al. (2008) cyber security requires metrics for decision making, performance improvements and accountability. The notion here is that statement of Black et al. for cyber security metrics is not different from ITILv4 metrics. Black et al (2008) also describe metrics being quantifiable, observable and objective data supporting metrics that organization has set requirements for measuring IT security performance. Attributes of effective metrics include ability to identify weaknesses, determining trends for better security resource utilization and judging the successes or failures of implemented security solutions that translates to controls and countermeasures. (Black et al., 2008; 1)

According to Bakshi (2016) good metrics are constantly measured, data gathering is easy and expressed in units of measure and are contextually specific. The metrics are divided into means-based and ends-based metrics that are further divided into technology, process and service metrics where technology and process metrics are referred as operational metrics. The technology metrics are measuring the aspects of the technology and how it is functioning whereas process metrics measure specific aspects of process and only the processes that are critical should be included to the management report. Service metrics are focusing how the service is provided according to ITIL practices. The measures that are expressed in units of measure should be translated to management to provide meaningful statement if the metric is meeting the expectation of the technology, process or service metrics. (Bakshi, 2016; 1-7).

Bakshi divided the metrics into three categories. They support the people, process and tools-triad and also prevent, detect and react-triad. He also underlines the division between operational and strategical reporting by suggesting that management reporting is done through key process metrics.

In the most literature related cyber security there is a clear division what is a metric and what is a measure. Black et al. state that metrics and measures need to be defined separately and define metric and measure as follows:

> ***A measure*** *is a concrete, objective attribute, such as the percentage of systems within an organization that are fully patched (Black et al, 2008; 2)*
>
> ***A metric*** *is an abstract, somewhat subjective attribute, such as how well an organization's systems are secured against external threats or how effective the organization's incident response team is. An analyst can approximate the value of a metric by collecting and analyzing groups of measures (Black et al, 2008; 2)*

Metrics and measures aim to verify security controls compliance with policy, processes or procedures, identify strengths and weaknesses of policy, processes and procedures and finally identifies trends both within and outside the control of organization. Black et al. (2008) recommend that metrics are decided first and after that the concrete measures are defined. The metrics should be designed accordingly to each governance level meaning that strategical level metrics are more abstract and tactical level metrics focus for example to the effectiveness of certain security control. The metrics can be therefore divided to higher-level metrics and supporting metrics where higher-level metrics are used for decision making. The reports for metrics are generated by collecting and analysing measures. The trend study aims to organization to monitor security performance over time to identify areas for improvement in the security posture of organization. (Black et al., 2008; 1-2)

Cyber security metrics do not differ from metrics introduced in ITIL section. The cyber security literature uses terms operational and tactical meaning the same thing depending on context. It seems that in military context tactics come before operations and in business context the operations come before tactical layer. Therefore, we can conclude that Black et al. also suggest that cyber security metrics are divided to strategical and operational metrics and operational metrics are contributing higher-level strategical metrics that are used for decision making. They also suggest including trends to identify improvement areas. This sets a requirement for service provider to analyse the metrics and trends to create suggestions for improvements for cyber security posture.

4.2.2.1 Known problems with cyber security metrics and measures

Black et al. (2008) point out that here are problems with metrics and measures. There are no universal metrics and measures that can be applied to all organizations. The usual problems relate to the accuracy and imprecise measure definitions along with when qualitative measures are used there are no well-defined scales or units of measures. In cyber security both quantitative and qualitative measures need to be used and therefore the context of measures and metrics is very important. They should be evaluated and altered over time since the meaning of them changes when for example security posture, knowledge and technologies evolve in an organization. As in ITIL, collecting some metrics and measures should be stopped if they do not provide any more value. (Black et al., 2008; 3-6)

By context Black et al. mean different operational environments and organizations with different goals and objectives. They emphasize that metrics and measures need to be defined or at least finetuned to suit the context and if they are not serving the purpose re-iterated or even removed from reporting.

The same issues are mentioned in the article of Meyer (2016) where several industry experts explain their approach to cyber security metrics and measures. Key statement is that there is no standard set of KPIs, and each organization must develop its own based on their risk appetite. Other route would be to develop clear metrics where the organization stands with its capability to detect, respond and recover from attack. This could be done by benchmarking against guidelines and standards such as NIST CSF. And the article points out that the security strategy and risk management process are the enablers for the cyber security. (Meyer, 2016; 30-32)

4.2.2.2 Mapping metrics and controls to cyber security frameworks

Krumay et al. (2018) did a systematic literature review to investigate existing cyber security metrics and controls and map them against NIST CSF which they call de facto standard among CISOs since the previous research has shown that it is most commonly adopted globally and is supporting the CIS controls, COBIT, ISA standard and ISO 27001 standard. Their study covered over 9000 pre-selected scholar articles which were scrutinized to 56 papers to rule out overlapping metrics and controls. They ended up with 1378 units of metrics and controls that they further investigated which finally resulted in

1053 unique units to be analysed. From this we can conclude that the cyber security metrics and controls can really be different from organization to organization and from approach to approach to the cyber security. (Krumay et al., 2018; 1-7)

What makes the study interesting, is the disproportion of the metrics and controls between the different NIST functions. The ‘Identify’ and ‘Protect’ functions together had 86,82 % of metrics and controls mapped against them. The remaining ‘Detect’, ‘Respond’ and ‘Recover’ functions had the rest but the focus was mostly on ‘Detect’ with 8,06 %, ‘Respond’ 4,03 % and ‘Recover’ 1,09 %. The research was done on literature but from this we can conclude that many organizations and literature is focusing on the fundamental capabilities in cyber security. This also means that there might some hardships to find benchmarking even on the NIST CSF function level. There were also some units that did not fit to any NIST CSF functions. They were placed around topic areas that were organizational climate, monetary aspects, executive involvement, ethics, general management, IT service levels, cognitive response, procurement, business value and natural disaster. Even though NIST CSF is considered to be most important risk management framework, this shows that NIST CSF is not full proof even if it would be fully covered by the metrics and controls since there might organizations that requires other areas or functions to be covered by metrics and controls. (Krumay et al., 2018; 9-13)

During the research of this study, it has come evident that various frameworks can be used in conjunction with each other. And mapping frameworks to other frameworks can be done as we have presented mapping of other frameworks to NIST and SOGP to other frameworks and so on. The mappings include the mapping of high-level metrics as well as the mapping of operational level metrics. But some of the categories in frameworks can be left without mapping from other frameworks. As previously stated, none of the frameworks is flawless but the main cyber security aspects are covered quite well and are overlapping in each of them. From this we can conclude that there is no single framework covering all areas and metrics of cyber security.

4.2.2.3 Presenting cyber security metrics and controls in the service report

Snyder et al. (2020) have looked into measuring cyber security and cyber resilience through red and blue teaming. The conclusion in their study for presenting metrics for cyber security and cyber resiliency is that there is no simple “dashboard” that will show

the status cyber security and cyber resiliency. The perpetrators and defenders are constantly evolving techniques, tactics and procedures with rapidly evolving technologies. The main point of metrics for organization is to evaluate how the metrics look compared to the reality. And evaluating metrics also requires expertise and judgment from work force and leaders. Recommendation is to divide metrics for decision-level and working-level metrics. The working-level metrics contribute to decision-level metrics, but this does not remove the requirement that when needed the working-level metrics are brought to attention of decisionmakers, but the focus then should be on systemic issues. By this Snyder et al. also describe dividing metrics to strategic and operational levels. This works very well with the division of metrics to higher-level and supporting metrics by Black et al. and Bakshi. Black et al. (2008) also point out that organizations need to alter their measures and metrics over the time. Metrics usually are initially measuring basic security controls but when organizations mature so should the metrics and measures since the desired level is reached and organization may want to answer new questions through metrics and measures. The high-level metrics may stay the same but at least the low-level metrics need to change and evolve. (Snyder et al., 2020; 39-43, Black et al., 2008; 5-6)

Metrics should be combination of performance/efficiency and effectiveness measurements. Universally the effective, adaptive and strong cyber countermeasures are technical and are operating at the working-level. The cyber metrics should be part of the risk management process to deal with the uncertainty and all members of the organization need to be involved with that process. This sets a requirement that culture for cyber security must be in place and all personnel need to be trained to have skills making the environment more cyber safe. The reporting should not just be a report and it should include communication. (Snyder et al., 2020; 39-43)

Snyder et al. highlight the importance that metrics and controls alone are not enough. The whole organization needs to be cyber security oriented through training to reduce the attack surface of perpetrators. The metrics and controls therefore should be communicated not only to decision makers but also to the whole organization, so they are aware how their environment is looking from the perspective of cyber security.

4.3 Designing and defining the cyber security reporting conceptual framework

This section has discussed about the cyber security, how it can be defined and developed and how metrics and measures should be defined to constantly develop cyber security through continual improvement practice that is in-built to services. The ambiguous relationship between service provider and customer in collaborative cyber security was later discussed. The conclusion from this sub-section is that cyber security is rapidly changing and evolving systematic process that secures and enables the critical digital business ecosystem of any organization.

The organization must ensure their own ecosystem is cyber secure and trusted by others. The company management is responsible for setting goals, targets, policies and resources for cyber security. The aforementioned matters vary from organization to organization. All organizations must have the three cyber security triads (Figure 8) at the disposal of the organization to have basic cyber security capabilities in place. The common practice is to approach this through risk management process where threats and vulnerabilities set the requirement for controls and countermeasures to secure the business-related assets that are delivering the outcomes and business results. Organizations cannot outsource the risk management process but should involve all relevant stakeholders to the process to ensure risks are treated properly. Ultimately the top management of organization is responsible for risk management process. In the figure 28 the relationships of the cyber security are illustrated.

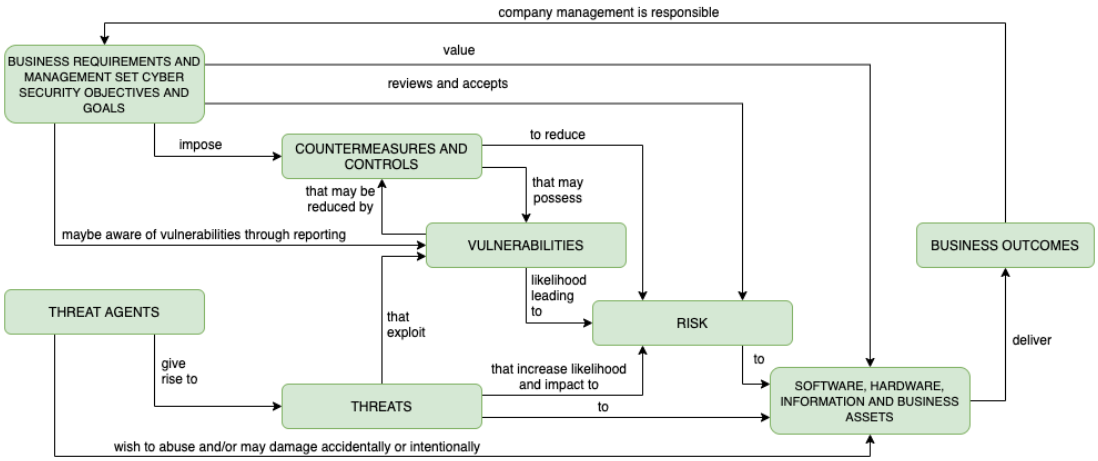


Figure 28. Cyber security relationships illustration based on Whitman et al., Stallings, Bayuk et al. and Limnéll et al.

The development of cyber security is a systematic process that need to be in collaboration by service provider and customer. The services need to deliver the value that is expected from them. Usually, cyber security services provide controls to risks. The most common and recognized risk management framework is NIST CSF that can be utilized to verify if all aspects of cyber security risks and capabilities are covered. But there are some critics that NIST CSF does not cover all aspects of cyber security management in certain organizations so there are other frameworks that can be utilized to evaluate the cyber security capabilities and risks in organization and study has presented some of them. One option can also be that the service provider or organization develops their own framework based on the existing frameworks to ensure the cyber security objectives and goals are reached.

Reporting of cyber security services are aiming for development of the cyber security services. This is done through metrics and measures. Usually, the metrics are divided into high-level and operational metrics so they can be steered and evaluated in the right decision-making forums. The metrics cannot be blindly believed, and cyber security reporting and development also requires expertise and good judgment from all stakeholders. Also, the metrics and measures are organization dependent and should be chosen correctly and the chosen metrics should be systematically evaluated and developed to represent the reality of cyber security landscape in an organization and outside of the organization. Figure 29 contains the conceptual framework created based on the literature.

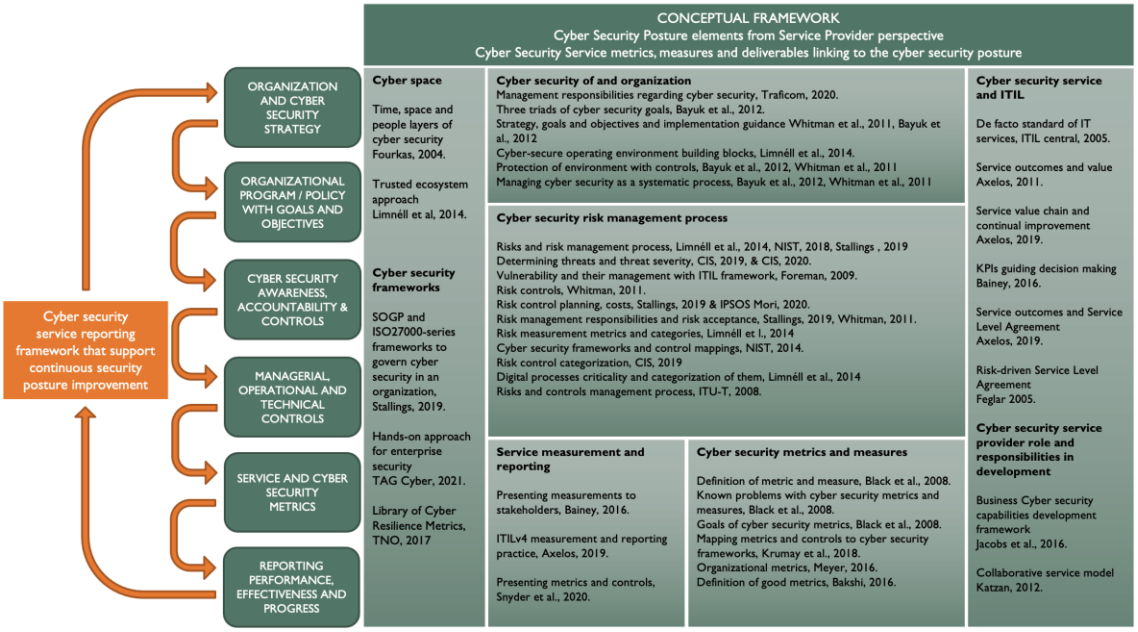


Figure 29. The conceptual framework of this study

The conceptual framework is based on finding solutions to weaknesses found in the current state analysis and combining the search areas of cyber security posture elements of an organization from service provider perspective and linking them to cyber security service metrics, measures and deliverables in to one conceptual framework. As it came evident in the section 4.1, the cyber security needs to be managed and developed with a systematic process. The continuous cyber security management process and the phases for cyber security posture is illustrated in the left side of picture with orange arrows and dark green boxes as the first element. The second light green elements are the existing knowledge linked to each phase of the cyber security posture management and development. The cyber space, frameworks, service and the development run through all phases of the cyber security management process. The risk management is the pivotal central piece of cyber security management and it needs to be linked to each area in the framework. All of the actions, processes, technologies and other service aspects need to be managed and governed through reporting that needs to reflect the reality of customer's cyber security services and cyber security posture. The reporting is communication and collaboration tool for the service provider and customer to make decision and prioritize development areas should they be in any area of the three cyber security triads.

The conceptual framework assumes that customer have linking of business and cyber security strategies which is managed by risk management process that includes the management of cyber related risks. Also, the services should include a working governance model that enables collaboration of customer organization and service provider through reporting.

In the section 5 the conceptual framework is utilized to co-create the initial proposal for cyber security services reporting framework that enables the continuous improvement of cyber security posture of customer organizations. The conceptual framework is evaluated against the strengths and the weaknesses found in the current state analysis and the initial proposal framework will also incorporate the strengths and eliminate the weaknesses to solve the original business problem set by case company management.

5 Creation of the initial recommendation for reporting framework

This section describes the steps taken to create initial recommendation for the cyber security services reporting framework. The initial recommendation was created by using the findings from the current analysis, the conceptual framework and stakeholder co-creation. The section contains detailed description of the steps and process how the initial recommendation creation was performed.

5.1 Overview of the proposal building stage

The focus in the proposal building stage is to co-create a reporting framework that would enable the development of the cyber security posture of the customer organisations of the service provider where the emphasis is placed on the weaknesses found in the current state analysis stage. The initial recommendation for the framework was created through two separate workshops where the participants from the case company business team gave their input as to areas from the conceptual framework need to be included to the framework. The draft framework was iterated a few times over internal communication channels. Input for the initial recommendation for the framework was then gathered from key external stakeholders who are and would be using the services and are the key stakeholders and consumers of reporting. Separate interview sessions were held by each external stakeholder to verify the customer processes and requirements regarding cyber security management, development and reporting.

Due to COVID-19 situation all the internal workshops and interviews contributing to Data 2 were held as virtual online meetings. The co-creation commentary, discussions and debates were captured to the field notes. Also, between the workshops, input was requested through email from the business team members to comment and contribute to the framework creation. Suggestions for topics and questions to the stakeholder interviews were also gathered from the business team members prior to interviews.

The external key stakeholders providing Data 2 were suggested by the business team members. The individual interviews focused on understanding cyber security management processes, development practises, expectations and other inputs that are considered crucial for successfully implementing the framework to use at case company in the

future. The second focus area was to receive input and suggestions for further improvements before the validation stage and the third and final co-creation workshop for the initial recommendation of the framework.

The third and final workshop comments, data and input translated to recommendations from external key stakeholders were presented to the business team members. The data was pre-analysed and formatted in a manner that decisions on which ideas to bring in or leave out from the initial recommendations was possible. The last step was to iterate the decisions and recommendations from the final co-creation workshop into the initial proposal for the cyber security services reporting framework.

5.2 Summary and descriptions of recommendations from data 2 collection

The recommendations are derived from co-creation sessions for data 2 collection rounds. The recommendations are intended to overcome the weaknesses identified in the current state analysis by utilizing the conceptual framework and input from internal and external stakeholders. The recommendations are divided to different segments based on the weakness. Each recommendation has a unique identifier assigned. The recommendations were taken into consideration when the initial recommendation for the cyber security services reporting framework was built. Figure 30 contains the recommendations co-created based on the weakness 1 found in the current state analysis stage.

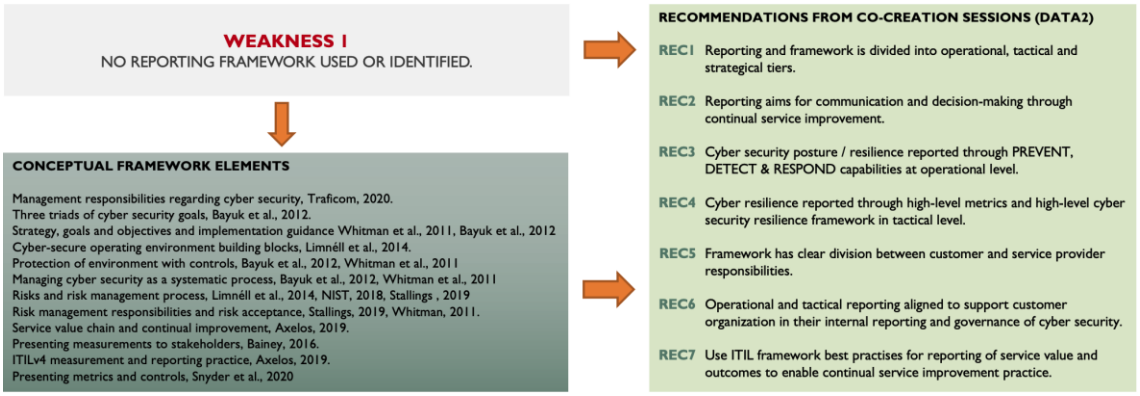


Figure 30. The co-created recommendations for weakness 1

As shown in figure 30, seven recommendations for framework base generation were identified. The recommendations include topics to divide the framework in to three levels,

guidance to the metrics and frameworks and how reporting supports and aims for communication and decision-making. The descriptions of the recommendations are gathered to table 7.

Table 7. Descriptions of recommendations REC1 to REC7

#	Recommendation	Description of recommendation
REC1	Reporting and framework is divided into operational, tactical and strategical levels.	Reporting is divided into operational, tactical and strategical levels to support the current case company governance model. The strategical level is the customer organization level in regards of cyber security services reporting.
REC2	Reporting aims for communication and decision-making through continual service improvement.	All the frameworks, metrics, measures and reporting material provide input to the decision-making and continual improvement practice.
REC3	Cyber security posture / resilience reported through PREVENT, DETECT & RESPOND capabilities in operational level.	The daily operations revolve around the prevent, detect and respond processes that people and technologies produce. When respond activities are low, the focus on reporting shifts to detection of incidents or other pro-active aspects of delivering cyber security services.
REC4	Cyber resilience reported through high-level metrics and high-level cyber security resilience framework in tactical level.	The individual control capabilities are too low-level for top management of customer organizations. The framework on tactical level should aim for holistic view of cyber security capabilities and resiliency that is not focusing to individual environments. The customer should be able to use the framework in their internal governance of cyber security.
REC5	Framework has clear division between customer and service provider responsibilities.	The service provider provides the agreed services. The customer has responsibility for risk management process and service provider only produces input to these through reporting. If deeper engagement to risk management or threat intelligence process is required, then there is a clear distinction between managed security services and consultancy services.
REC6	Operational and tactical reporting aligned to support customer organization in their internal reporting and governance of cyber security.	The continual service improvement practise needs to verify customer is receiving the reports and data that support their internal reporting and governance. The reports provide direct input to customer internal reporting.

REC7	Use ITIL framework best practises for reporting of service value and outcomes to enable continual service improvement practice.	ITIL has iterative processes for value chain and value recognition. The continual service improvement practise aims that services are providing value and required outputs to customers. The metrics and service content are evaluated in the continual service improvement practice. The output from this practice is taken to the service provider's development process.

Figure 31 contains the co-created recommendation for weakness 2 through the conceptual framework elements to unify the reporting terms and deliverables

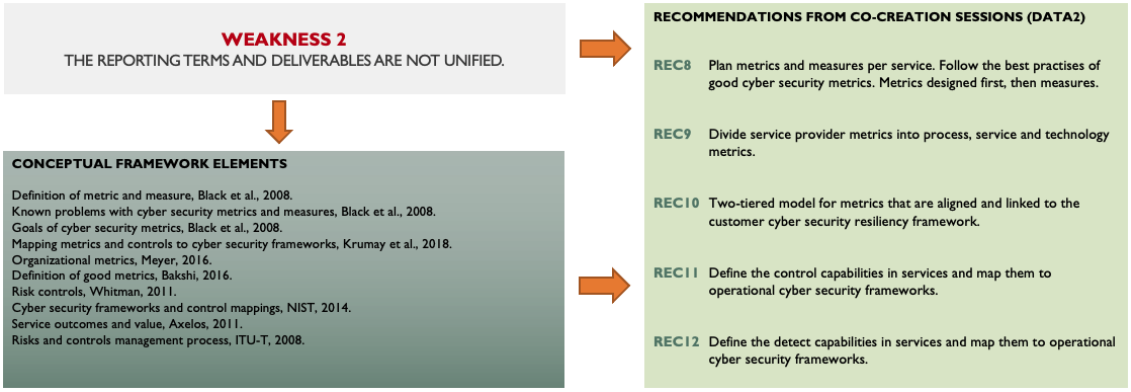


Figure 31. The co-created recommendations for weakness 2

To unify the reporting terms and deliverables, a total of five recommendations were created. The recommendations are related to the best practices of metrics and reporting of them and how to report the prevent and detect capabilities of individual services. The descriptions of recommendations for weakness 2 are described in table 8.

Table 8. Descriptions of recommendations REC8 to REC12

#	Recommendation	Description of recommendation
REC8	Plan metrics and measures per service. Follow best practises of good cyber security metrics. Metrics designed first, then measures.	The services are planned pre-determined metrics and measures. The metrics and measures are rolled to services and not to customer environments to keep the service metrics reporting standardized.
REC9	Divide service provider metrics into process, service and technology metrics.	Each service has these characteristics. The process metrics aim to report prevent, detect and respond capabilities that people and technologies provide. The service might contain other metrics. The technology is mostly sold as a Service, but the technological metrics are reported as well in the name of transparency. The other flavour of technological metrics is that customer organisation and service provider both rely on a technology that is provided for both as a service. Measuring those technologies should be done if technology enables the measuring.
REC10	Two-tiered model for metrics that are aligned and linked to customer cyber security resiliency framework.	The service itself has metrics. These metrics are representing the service and controls related to that service. The operational level looks into individual services and incident process metrics. The service metrics are combined to represent the higher-level cyber resiliency metrics in the tactical level reporting and mapped against the cyber security resiliency framework to represent the current status of customer's cyber security posture.
REC11	Define the control capabilities in services and map them to operational cyber security frameworks.	The controls are divided into categories. The controls are divided into three categories from essential to advanced. The mapping what we are proving and capable of providing through services. This supports the continual service improvement practise and roadmap thinking and planning.
REC12	Define the detect capabilities in services and map them to operational cyber security frameworks.	Both perpetrators and defenders are developing new techniques. This requires constant development of detection capabilities to understand if organization is capable of detecting new exploits in their environment. The detection capabilities inside the services are developed at the operational level.

The third recommendation area to gather requirements from customer organizations for developing the services and reporting is seen in figure 32.

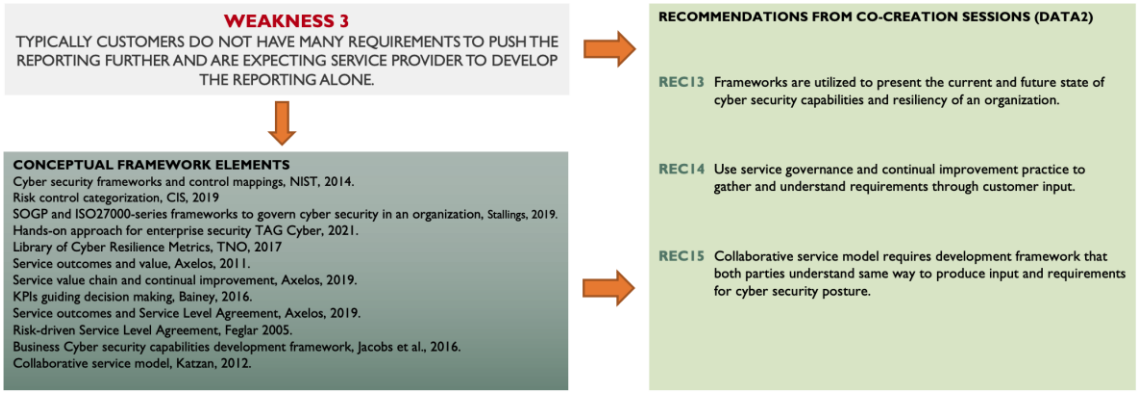


Figure 32. The co-created recommendations for weakness 3

To ensure that customers are engaged to reporting, three recommendations were created. The recommendations include guidance to the service governance practices and how reporting is supporting it through mutually understood and used frameworks. Table 9 contains the descriptions for recommendations for collaboration through the reporting framework.

Table 9. Descriptions of recommendations REC13 to REC15

#	Recommendation	Description of recommendation
REC13	Frameworks are utilized to present the current and future state of cyber security capabilities and resiliency of an organisation.	One single framework is not enough. Different areas and governance levels of reporting require different frameworks and delivery of "message". The frameworks operate as discussion and evaluation benchmarks. This enables service provider to benchmark their customer organisations to each other that is also commonly requested by the customers.
REC14	Use service governance and continual improvement practice to gather and understand requirements through customer input.	The continual service practice requires input from customer as well. The continual service improvement practice expects that customer sets requirements for cyber security targets through risk management process. The cyber security capabilities and controls needs to be designed against these requirements.

REC15	Collaborative service model requires a development framework that both parties understand same way to produce input and requirements for the cyber security posture.	The framework used by the service provider needs to be agreed and approved by customer. To deliver services efficiently, the service provider needs to use standard set of frameworks and tools to produce outputs from data. The customer should adopt best practices, but the framework should be created in a manner that it suits the governance models of customers. This ties back to REC4 and REC5. The governance and development models need to be described in the service descriptions.

The fourth and final recommendation area to engage the risk and cyber security management to the framework is in figure 33.

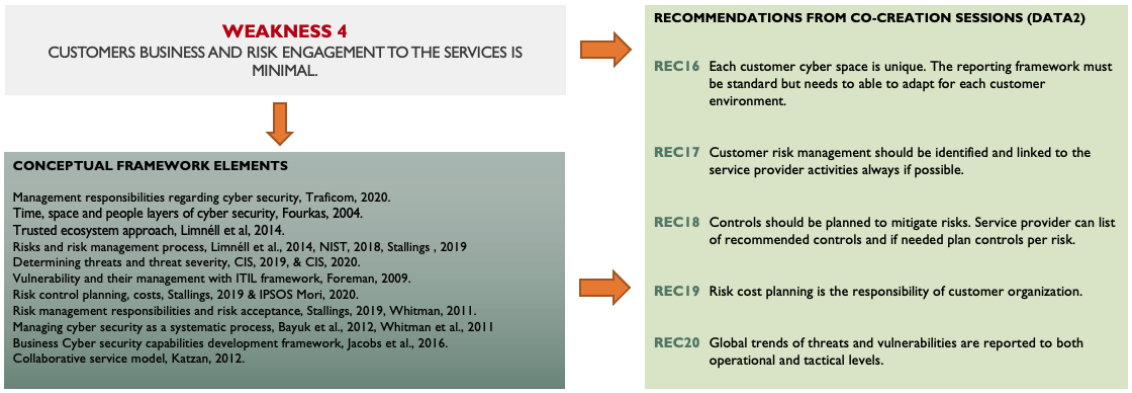


Figure 33. The co-created recommendations for weakness 4

Engaging customer business and risk management to the cyber security reporting received five recommendations. The unique features of each customer need to be understood and considered, but a standardized approach to the cyber security strategies of customers require the framework to have relationships, responsibilities and input models described. Table 10 contains the descriptions for recommendations for customer cyber security and risk management process linking to the reporting framework.

Table 10. Descriptions of recommendations REC16 to REC20

#	Recommendation	Description of recommendation
REC16	Each customer cyber space is unique. The reporting framework must be standard but needs to able to adapt for each customer environment.	The service provider must be able to adapt to each customer ecosystem. The cyber security target setting, and risk management process are running within customer organization with customer processes. The service provider requires provide input and output to these processes. If service provider is engaged to risk management process this happens through consultancy services and not through managed services.
REC17	Customer risk management should be identified and linked to the service provider through reporting.	Customers are running their own risk management process. The cyber security risk management is part that process. The customers are evaluating and managing risks by themselves and they expect input to that process in some extend from service provider such as identifying new risks or suggesting controls to certain risks if requested by customer. The risk management process input and output should be described in the reporting framework.
REC18	Controls should be planned to mitigate risks. Service provider can list of recommended controls and if needed plan controls per risk.	The services and controls that service provider is providing should be linked to customer risks. The control overview is visualised in framework. The controls are divided into different categories. The recommended controls start from essential category, followed by intermediate and the advanced category. This helps planning and identifying required controls and measuring the efficiency of implemented controls.
REC19	Risk cost planning is the responsibility of customer organization.	The risk cost planning is customer responsibility. Service provider cannot determine the cyber-attack related costs to customer. The service provider can help customers by giving input to direct costs through expertise from previous cyber security incidents handled by case company. These are costs related labour and other always occurring costs when organisations are facing cyber security attacks. The reporting supports customer cost planning and return on investment calculations.
REC20	Global trends of threats and vulnerabilities are reported to both operational and tactical levels.	Service provider provides lightweight threat analysis in the managed services. The content is based on global threat landscape analysis. The output is a short summary of seen and potential threats to raise customer awareness and to be utilized in the threat intelligence evaluation in their internal risk management process. Service provider can provide customer-specific threat intelligence services separately.

5.3 Description of the recommendation creation workshops and interviews

This section describes how the Data 2 was drawn through workshops and interviews to be utilized for co-creating the recommendations for the framework. The section is divided into internal workshop and external interview descriptions.

5.3.1 Gathering internal initial recommendations

The internal recommendation gathering started by having one to one discussion with each business team member. The focus was on discussing the findings that were made in the current state analysis and what the weaknesses are that the reporting framework should overcome and what the elements from the conceptual framework are to be utilized in the framework. One other point of the interviews was that the delivery of materials before first workshop would not be totally new and it would be easier to go through the briefing material.

The conceptual framework theory materials were stored to the virtual workspace of the business team on the 1st of March. Each member was notified about the location of materials and was asked to get familiarised with it and give comments from the content of the material before the first workshop. Only comments received about the conceptual framework materials were discussed in the one-to-one interviews and the comments were positive and each team member saw the benefit already at this point to develop framework with using both the existing knowledge and the experience that team members possessed.

5.3.2 The first internal co-creation workshop

The first internal workshop took place on the 11th of March 2021 as a virtual meeting. The workshop material was distributed in advance to all business team members. The material was in PowerPoint presentation format. The presentation contained the weaknesses of the current state analysis, description of the logic how the knowledge was gathered to overcome weaknesses, the conceptual framework and breakdown of each conceptual framework element that followed the same structure as it is in this study. The workshop started by going through the weaknesses, the information gathering process and the conceptual framework. Then each topic of the conceptual framework was introduced in

presentation format and discussed if they should be included to the framework including ‘how’ and ‘why’ discussions.

The first bigger debate was in the early stages of the workshop. The discussion revolved around the robustness and goal of the reporting framework and could the case company even create and execute reporting through a framework that is touching a very complex and vast topic of cyber security management and cyber security posture of a customer organisation. This was due to the fact that the main focus in the reporting has been previously on the operational and technological aspects of the service. After some discussions the business director, who was the person who initially introduced the problem for this study, defined the goal and purpose for the framework that the workshop should aim for as follows:

> *We are aiming to build a framework that we understand the reporting relations and how reporting should be done. After that we can start planning our services and operations to follow that best practice in the future. It does not mean it will be immediately implemented but will act as a guideline and a reference for us to develop our reporting capabilities. (Business Director)*

The statement clarified for everyone participating to the workshop that the feasibility of the reporting framework was not just tied into the capabilities that case company currently possess. The capabilities were taken into consideration, but it was also identified as a strength in the current state analysis stage that case company has all the necessary means to develop reporting further. This meant that all participants understood that we are creating the ‘to be’-state of reporting without any strict timeline when the whole framework or parts of it should be implemented to the production.

The risk cost planning discussion was very sound. It was mutually agreed that the service provider cannot provide exact costs for risks. The consensus was that it is not ruled out from the framework but is part of the customer’s risk control planning where the service provider can help for example by providing examples for realised costs in cyber-attack cases that the service provider encounters during the service lifecycles of all customers. The risk cost planning is done in the cyber risk management process of the customer organization. This is marked as recommendations REC5 and REC19.

There was much discussion about frameworks. They were dissected thoroughly and there were previous experiences from many of the frameworks mentioned. The discussion topics included, should the frameworks be followed strictly or should the metrics only be utilised from them. Two of the business team members pointed out that metrics are just metrics, the most important thing is to understand why and for what purpose are they used. This led into a conclusion if mapping all the services and the operations is even possible with one single chosen framework.

The metrics discussion led into another discussion about metrics. It was concluded that the metrics need to be divided into two tiers as suggested in the conceptual framework. The epiphany was that in a service provider and customer organization context the metrics cannot be called operational and strategical metrics. This discussion led into a recommendation that the reporting framework needs to be divided into three levels that are strategical, tactical and operational levels. The customer is running the strategical part of the framework. The Service provider is operating on both operational and tactical levels in the managed services. Both have different focus in the context of the framework. The operational level, as the name indicates, focuses on the operational matters while tactical level is used for collaboration between the service provider and customer organization to receive input from the strategical matters of customer in the form of cyber security targets, risk management process and other requirements for cyber security services. The service provider aims with the tactical level reporting to provide valid input for the internal reporting and cyber security management process of customer. It was agreed that this requires continual service improvement practices and a framework that is clearly presenting the cyber security resiliency of a customer environment in a manner that it could be used with the top management of the customer organizations. The discussions led into conclusion that the operational level metrics and the frameworks need to contribute to the tactical level metrics and the frameworks. The recommendation REC1, REC6, REC8, REC10 and REC14 were based on these discussions and supports REC5 and REC19.

Next, the discussion covered the risk management process and controls. The discussion started from the responsibilities. It was unanimously agreed that the customer is responsible for the risk management process. It was clearly stated between business team members that the framework must clearly indicate the responsibility areas of the service provider and customer even though we are talking about collaborative services. This

resulted into recommendation REC5. This should also help customer and service provider distinguish what is included in the scope of the managed service and what are the service aspects that are separately ordered consultancy services. One business team member described the responsibility of the service provider as follows:

> *Our managed cyber security services mainly produce controls for risks. When the controls are placed to a framework, the main objective for framework and reporting is to provide data in number, traffic lights or other data format that the customer can make decisions based on those. (Business Team Member 1)*

This was a good remark and supports the conceptual framework elements that state that reporting is communication and decision-making. This led naturally to the discussions of controls. One business team member saw this as a very good approach that controls are mapped to categories that are starting from the essential and gradually evolving through the intermediate level controls to the more advanced controls. The controls then sit nicely to the roadmap thinking and continually improving cyber security posture and cyber resiliency thinking. This resulted also in the discussion that the controls have prevent and detection capabilities. Therefore, it was suggested that it would make sense to divide the capabilities to separate coverage frameworks for prevention and detection. The recommendations REC2, REC11, REC12 and REC18 were based on these discussions.

The controls discussion led eventually to the metrics discussion again. But now the focus was on the operational level metrics. It was already discussed that the operational level metrics are contributing to the tactical level metrics. It was accepted by all team members that the metrics are divided into process, service and technology metrics. Since the case company is mostly offering the cyber security service with ‘as a service’-approach, it makes sense that all areas of the services are covered metrics wise so that the customer can rely on that the services are delivered as the service that was acquired. This ties back to the conceptual framework ITIL approach of delivering services and ensuring the value of the service whilst following best practices of the cyber security metrics. The biggest concern around the metrics was that it was suggested that the metrics would be tied to the critical digital processes of customers. This was considered too cumbersome approach at this point since it would be impossible at this time and age to map the services and their metrics to the digital processes of customers. The mapping of the customer digital processes to the service reporting framework was unanimously decided to

be left out. The recommendations REC7 and REC9 were created through these discussions.

The biggest concern regarding the risk management process and mapping it to the reporting framework was the threat intelligence. The vulnerability management and open-source intelligence management come naturally through the respective services that are available in the service catalogue of case company. The customers are expecting to receive each month a threat analysis of the global threat landscape. It was decided that the reporting framework includes a light-weight threat and vulnerability analysis summary of the global threat situation. This recommendation is identified with the identifier REC20. More robust threat intelligence and analysis based on a customer agreed hypothesis is offered as a separate service. The workshop ended to a small presentation of a high-level architecture of the reporting framework illustration.

5.3.3 The second internal co-creation workshop

Between the first and the second workshop a draft of the initial recommendation framework was created by the author of this study. It included the elements that were discussed and recommended during the first workshop.

The second workshop was held on the 19th of March 2021. The focus was on the draft version and giving feedback for it and setting the objectives for the external stakeholder interviews. Business team member 3 gave a solid feedback from the reporting of controls part of the framework:

> *I was bit vary about this framework, but I am liking this control part quite much and I can see the benefits of reporting them based on separate frameworks. (Business Team Member 3)*

There were pointers given how to polish the framework for example by making it clearer that the operational framework is comprehensible by the internal and the external stakeholders and that it represents the modular service catalogue. Positive comments were made about the strategical aspect of the service reporting that belongs to the responsibility of the customer organisation. The consensus was that the draft comprehensively represents how the customer should do their cyber security management and reporting processes, but it was unclear whether the customer organisation is managing them as they were presented in the draft. This led directly to the need to focus on finding out how

the cyber security management and the risk management processes are handled in the customer organisations. The recommendation REC17 was created to tackle this concern. Other key topics to find out from the external stakeholders were the threat management of their environment and industry, how they are managing the current detection and control capabilities, could they give input from their risk management process to the cyber security service provider and what are the general expectations regarding the reporting and the cyber security posture management from the service provider. The business team suggested diverse group of key customers to be interviewed.

The draft of the tactical part of the reporting framework was presented as well. As mentioned earlier, the tactical reporting level is the interface between the operational and the strategical levels in the service provider and customer organisation context. The concept of the tactical level was accepted but it was agreed that it lacked the feedback loop to the development process of the service provider. It was agreed that the continual development practice of the tactical level requires more extensive details. The idea of a 'cyber resilience'-framework as the centre piece of the tactical level was accepted as well and this resulted in the recommendations REC4 and REC13 that are supported by REC10. With the following feedback and recommendations, the next stage was to plan interview questions for the key external stakeholders and make a request for them to be interviewed.

5.3.4 External stakeholder interviews

The key customers to be interviewed to gather input from the external stakeholder perspective were suggested and decided by the members of business team. The stakeholder companies varied from a globally operating company with thousands of employees to a 30-person strong company that is responsible for mission critical infrastructure with a common denominator that all the companies require very strong and constantly developing cyber security posture and resilience by nature of their business. The companies represented the energy, maritime, retail and industrial manufacturing industries.

All of the suggested five key customers accepted to be interviewed. The individual interviews were held between 26th of March and 31st of March 2021 as a virtual video meeting with details documented in Data 2 table in section 2. Information about the thesis was included to the interview invitation where the topic and objective along with the outcome of this study were explained. Each of the sessions followed the same pattern. First the

thesis problem and the objective together with the outcome were introduced followed by presenting the research design approach. Then the publicity of thesis material and the purpose for interview were gone through in more detail. After that the interview started. All of the interviewees accepted that the virtual meeting is recorded. Exception was the first interview where there was a technical problem and due to time constraint, it was mutually decided to do only an audio recording of that interview. All other video meetings were video recorded. Even though the sessions were recorded, field notes were captured during the interview. The interviewee saw on their screen one question at a time and the field notes that were written down during the answer. The discussions were in Finnish, but the field notes were written directly in English. It was stated to the interviewee that they can rectify the essence of their answer and if needed they are allowed to add or remove parts from the field note.

The interview questions are attached as Appendix 2 to this study. There was total of 16 questions but some of the questions had logic inside them depending on the first answer given to the initial question. The questions were created to understand the strategical management and the cyber security strategy process in the customer organisations.

From the answers it was identified that in each organisation there was some sort of cyber security management process. One organisation had even strategy that they are running three-year strategical cyber security program with goals and targets set for that strategy period. None of the interviewees had the ultimate responsibility for cyber security in the form of being either management team or management board member in their organisation. In each organisation, the top management or management board sets the very high-level goals for cyber security. All the interviewees were responsible for enabling and developing the cyber security capabilities, operations, operations management and cyber security in general in their organisations. The reporting chain to top management varied from one step to a few steps but in all cases the cyber security topics to the management team were reported by the interviewees. All the interviewees can be described by having a long history, background and experience working in the IT industry and cyber security.

It was identified through the answers that there were two topics that top management had set for targets and were keen to hear about them through reporting. The first topic was that how their operations are secured. Or in other words, is the organisation capable of ensuring that they can do their business now and in the long run. It was up to the

reporter to create a message that is suitable and comprehensible for the audience. Some audiences require just verbal descriptions such as ‘bad’, ‘good’ or ‘excellent’ or some organisation parts wanted to see numbers and percentages. This highlights the fact that the service provider should support the customer internal reporting with both more generic cyber resilience outlook and in the other end of the spectrum by providing concrete metrics. Some organisations included threat condition snapshot for the top management, but the high-level threat condition reporting seemed to be a bit cumbersome since it is quite hard to populate the exact summary of the threat condition. This has been added as recommendation with identifier REC16 but supports REC15 that is tying back to REC4 and REC5.

The second common topic was that that how is the cyber security developing in the organisation. This touched the cultural through awareness and training of personnel and as well as the processes and technologies that are providing the cyber security capabilities. The operational development was reported monthly and the longer span roadmaps were presented and reported occasionally. These tied back to the initiatives that the cyber security team had set based on the targets set by the top management. The majority of the interviewees recommended that is a good practice to include development activities to all reporting since it is reported by them back to the top management.

All companies had the cyber risk management process in place. In all companies it was part of the company risk management process that was run by the CFO or a separate risk management organisation. The cyber security teams were responsible for the identification of the risks to operations that directly ties to the business outcomes. The risks were prioritised, and investments were assigned through the risk assessment process. The assessment was done by either FAIR-method or likelihood and impact matrix but the companies who had adopted the likelihood and impact analysis method made more thorough analysis of the business impact. All of the organisations used threat and vulnerability management process in conjunction with risk assessment but the manners and depth of them varied greatly. One organisation was relying on the current light-weight threat analysis provided by the case company while on the other end of spectrum from one key customer there was expectation that the service provider knows what is critical for the customer organisation and acts accordingly regarding the risk management process even with the current set of services. 40 % of interviewees did not see benefit from a service provider participating to the risk management process and 60% saw the benefit through advocacy in the risk control planning. Also, there was an expectation from two

interviewees that the service provider proactively identifies risks and especially operational risks. One company used an external service provider to run the risk management process but had not considered that the managed services provider would also run the risk management process for them. The conclusion from the risk management process in the customer organisations is that they do exist but vary greatly from organisation to organisation. Therefore, the reporting of cyber security services can only produce input to that process by evaluating the overall cyber resilience and controls efficiency performance and coverage. The company or an industry specific threat intelligence without agreed service scope is hard to achieve and report. And the same conclusion applies to the vulnerability management. These interview findings support the recommendation REC20.

The questions of using cyber security frameworks varied from company to company greatly and frameworks were used differently. ISO27000-series was mentioned three times as a guideline how to manage security in a company and it was not officially certified in any company. Other frameworks that were mentioned Traficom Kybermittari, Mitre ATT&CK, NIST CSF, NIST 800-63, IEC62443 and CIS 20. One interviewee mentioned that one standard is not enough, since in a global company, the framework should be used in context of business and geography. Other interviewee also pointed out that the standards are evaluated against systems and their maturities can vary from top notch to immature or from legacy to recently deployed in their quite large operational environment. Hence it is hard to evaluate the whole organization against one standard. One organization had performed an audit against CIS 20 in the recent months and the feeling from it was very positive. Using an audit and the framework enabled them to have a clear gap analysis what could be improved in their environment. A roadmap based on the findings was built and supported by the top management and the management board. And it turned out that the management board had suggested the audit. Four out of five said they would see benefit that the development of cyber security capabilities of a customer organisation would be followed through a mutually agreed framework. The conclusion was that frameworks are and should be used when suitable. The benefits mentioned by interviewees were that the service provider and customer would have common goals and objectives, targets are set together, service provider can show their ideas what should be taken forward, benchmarking between service provider customers, thinking holistically and not just point solutions and lastly, the capability to understand what is delivered and offered by the service provider to the customer. The last benefit tied to the fact that service provider is offering also other services besides cyber security services

to that customer. This is marked as recommendations REC13 and REC15. The one interviewee who was hesitant to see benefits could see the benefit if not only one framework is followed but some flexibility is in the usage of the frameworks and the updating of the frameworks is mostly automated.

The interview questions about the metrics were another hard topic from service provider perspective. There was a variety of metrics used in the organisations and they varied greatly from organisation to another. The operational metrics are quite known through the current reporting but to the internal reporting, the customers added their own metrics as well. The reporting to the top management happened in some format in each organisation on a monthly basis. The metrics reported to the top management varied between none and the most cumbersome metric from the service provider viewpoint was a 'high-level threat condition of the company'. The organisation reporting this had their own way how to produce this metric for their top management. Other metrics mentioned were related to GDPR requests, security coverage of servers, incidents, cyber security incident trends to name a few. Eventually all of the metrics boiled down that the top management was mostly interested about the business impact. And more importantly how something might affect the customer's customers. This directly ties back to the secure ecosystem thinking and the ITIL service value chain approach. Three out of five interviewees told that it would be beneficial to align the metrics from the strategical metrics to the operational metrics that the service provider produces. This has received recommendation identifier REC4. The expectations included timeline linking of service provider and customer internal reporting, dissection of incidents that they would include more lessons learned approach in the reporting in the format that the part of reporting would answer to questions 'what we have learned from incidents', 'what can be improved' and 'how we can protect our organisation from similar cases'. The expectation was that the traditional KPIs, incident metrics, threat condition metrics and what businesses they have had an impact are aligned to provide input for the business risk management. One interviewee described the existence of metrics:

Input to business risks is always the reason for metrics. (Key customer 5)

When interviewed about the key metrics that are expected in general from the cyber security services, there was no clear consensus about them. Two interviewees were happy with the current metrics used in services. Three others mentioned that the most important key metric is the number of critical or high-level cyber security incidents. When

these incidents realize and are reported, the incidents should be dissected and reported very thoroughly. The expectation from one interviewee was:

> *When critical incidents are handled, we would require an analysis on these to present the true state of our cyber security. The analysis should in a format that we can take it upstairs along actionable suggestions to reduce risks in the future. (Key customer 4)*

The other notable mentions for the key metrics besides incident metrics included, threat intelligence, ‘does the service work’ and weekly/monthly development metrics. There were no concrete suggestions about these metrics. This has no clear recommendation but the recommendations REC3, REC11, REC12, REC13 and REC14 needs to receive input from incident reporting.

When asked how the service provider could help and contribute to the internal reporting of the customer organisation there were 12 concrete suggestions. Most of them are mentioned already in the previous analysis since some suggestions were discussed under the previous questions. One recommendation was that the service provider reporting should be already in a such format that it could be presented directly to the top management while some others suggested sparring about reporting to the top management or creating different report views to different audiences in the customer organisation. This similar suggestion was mentioned four times but with little bit different wording and angles. From this we can make a conclusion that the service provider reporting must support the internal reporting of customer organisations. Another notable mention was that one key customer suggested that the reporting would be presented through the prevent, detect and response-triad. The triad approach is marked as recommendation REC3. And while the response activities are low, the activities and reporting of the cyber security then naturally shifts to the prevent and detect areas of the service. And final notable suggestion was that collaboration is required between the service provider and the customer organisation and the reporting should support the collaboration.

The final part of the interviews concentrated on expectations from service provider to enable cyber security improvement in the customer organisations. The general expectation is to convert the operational data to actionable items along with advice and recommendations. One key customer mentioned that their organisation would like to understand if they are capable of detecting necessary things related to cyber security. And one

customer suggested that maybe in the future the raw data could be transferred to the customer's own data warehouse to improve their internal reporting.

The relevant recommendations that were mentioned multiple times by the external stakeholder interviews were transferred after the interview data analysis as recommendations derived from Data 2. After completing the interviews and analysis of them, the feeling from the external stakeholder interviews was very positive and valuable information, insight and recommendations for the case company reporting framework was obtained.

5.3.5 The third internal workshop – co-creation based on results of customer interviews

The third and final workshop before releasing the initial recommendation for validation was held the 6th of April 2021. The workshop started by presenting the results of the key customer interviews followed by the list of recommendations drawn from both internal and external key stakeholder sessions. The approach to cyber security strategies in the customer organisations was discussed in more detail, including the linking of risk management process to it. The discussions revolved around how the risks from daily operations are truly taken into consideration in the cyber risk management that translates into business risks and how they are eventually linked together. The recommended framework takes this into account by having a clear division between the customer and service provider responsibilities. And the service provider has clear approach to reporting controls and cyber security capabilities. It is up to the customer to build the linking of these and service provider can help in this matter if the customer sees benefits and added value from this.

The framework discussion was held next. It was a pleasant surprise that Traficom's Kybermittari was recognised but it was thought that it might be too complex to be used as part of the continuous services. The framework approach is thought to be good idea, but it must be built in a manner that it suits for the purposes of the managed services and fulfils the needs of both customer organisation and service provider.

The discussion about the key metrics was held in a general level. It was accepted that the two-tier metric approach is necessary. It was also identified that the higher-level metrics need to be designed together with customer organisations since they require common vision and development from both parties. This supports also the design metrics first approach.

A change from previous sessions to the framework was done through the customer organisation feedback by adding more emphasises on the critical incidents and it was raised as a separate reporting area. On the other hand, this does not surprise since incidents is a concrete and almost tangible reporting topic to be taken to the top management in customer organisations to justify the need and necessity of cyber security and costs related to it. It was considered to be very valuable feedback from the customers that the proactive approach to cyber security is part of the reporting as a standard practice if there are not that many incidents during a reporting period. The reporting in this case should be focusing more on the prevent and detect aspects of the services. This relates to recommendation REC3. The prevent aspect of the reporting was considered to be cumbersome and there were some concerns that how this could be included to the framework, but the general feeling was that this should be included in the framework.

A mutually agreed framework between the service provider and customer got full acceptance based on the customer feedback. It was now seen as an integral part of the tactical level where steering and decisions of the cyber security posture is done. The framework was identified also as a clarifying element to link the customer organisation strategical level requirements and activities to the service provider. Again, the business team emphasized that the reporting framework must have clear division between the customer organisation and service provider responsibilities especially if they are concerning threat intelligence and costs related directly to the customer organisation.

The next step in the co-creation workshop was to go through all of the recommendations gathered from the internal workshops and external interviews and recommended framework draft. And if at this point there were suggestions to add or remove any of them.

The draft framework was walked through. The framework did not raise that many questions and it was perceived to be really good by the business team members. One recommendation to the illustrated framework was suggested. The threat aspect of the managed services should be clarified. The emphasis should be on the term ‘threat assessment from global threat landscape’ and make it clearer that it only includes the global threat landscape assessment, and it does not deep dive into customer-specific threat intelligence. This was a remark to avoid any misunderstanding what the threat assessment actually includes in the reporting framework, since the customers have the possibility to purchase separate customer-specific threat intelligence service.

At the end of the workshop, it was agreed that the results of the customer interviews, recommendations along with their descriptions and the slightly modified recommended framework is distributed to all business team members and the framework moves to the validation stage.

5.4 Description of the initial recommendation for cyber security services reporting framework

The framework was based on the conceptual framework originally. The first version was divided only into strategical and operational levels with focus on controls and using one framework to cover the cyber security posture of customer. The framework evolved through iterations taking into consideration the recommendations of each workshop and the interview sessions. The initial recommendation for cyber security reporting framework for case company is visualised in figure 34.

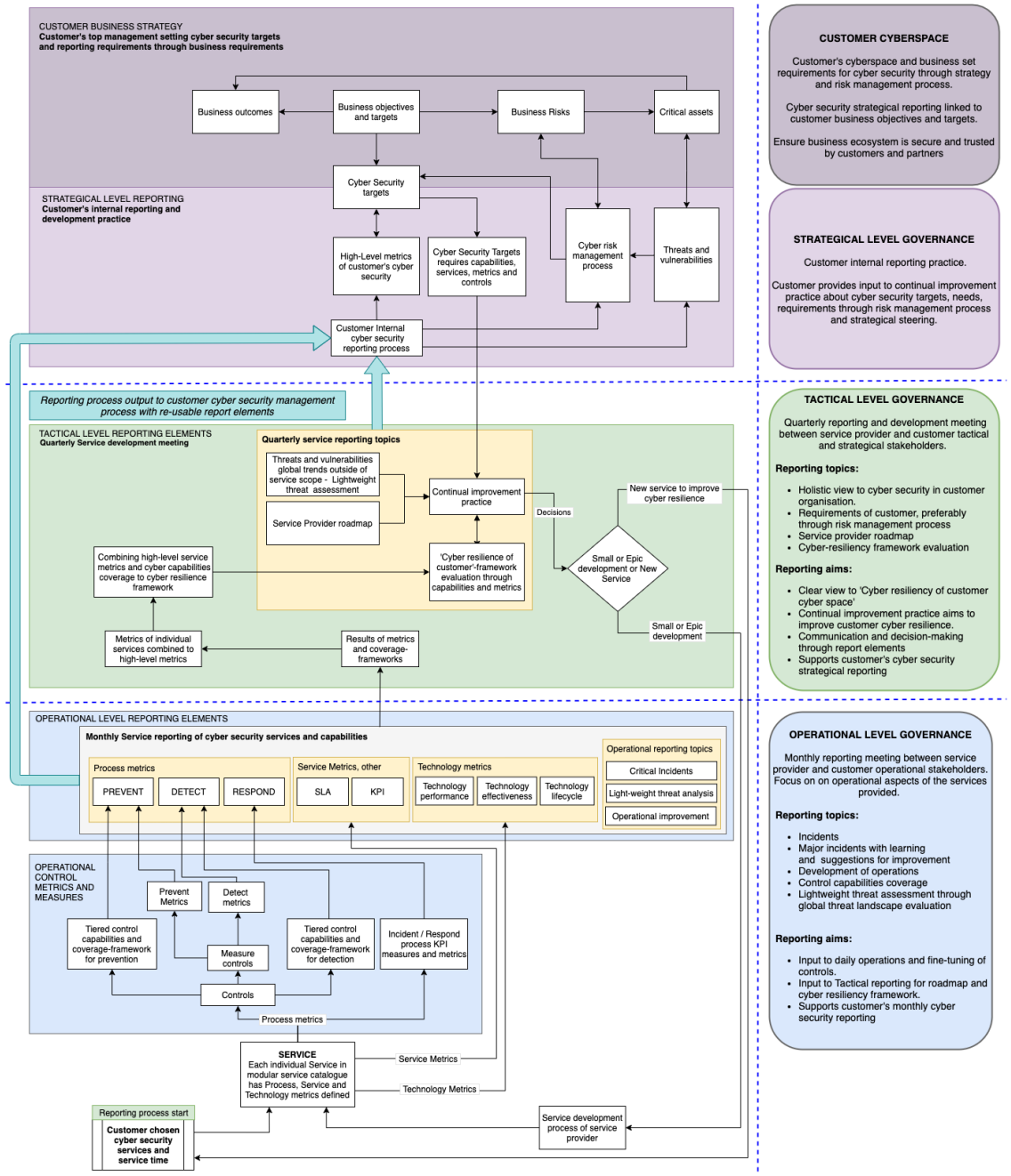


Figure 34. The initial recommendation for cyber security services reporting framework

A total of 20 recommendations were drawn from the co-creation sessions to support the findings from the conceptual framework and overcome the weaknesses found in the current analysis stage. The co-creation of initial recommendation for the reporting framework was done successfully and the validation of the initial recommendation for framework validation is described in section 6.

6 Validation of the proposed cyber security services reporting framework

Section 6 describes the validation of the proposed initial cyber security services reporting framework. The section begins with a general description how the validation stage was performed followed by the detailed description of the key stakeholder evaluation of the proposal. The key stakeholder evaluation includes the description of the validation feedback that led into the final adjustments for the framework that is the outcome of this study. Finally, this section describes the final proposal and validation steps with the internal and external stakeholder before the final validation by the business director of cyber security services of the case company who initially defined the problem and set the objective for the study.

6.1 Overview of the Validation Stage

The validation of the framework was performed in three separate validation rounds. The first validation round was carried out in conjunction with the final co-creation workshop through evaluation and distribution of produced materials after the workshop. This enabled each internal team member to evaluate the recommendations and the initially proposed framework thoroughly and individually to provide meaningful feedback and perform validation for them. The feedback and especially the initial internal validation from the internal stakeholders was required to evaluate the framework content and maturity to move to the second validation round that was agreed to be done in collaboration with key external stakeholders.

After the internal validation round, a second validation round where both internal and external key stakeholders participated was held as an online virtual meeting to get the feedback and validation for the framework from the customer organisation perspective as well to support the internal validation. All the same stakeholders that participated in co-creating the initial recommendations were invited to the second validation round collaboration session, but some invited stakeholders were not able to participate in the session due to their previously agreed engagements. The second validation session started by introducing the business problem, the objective of the study, the conceptual framework and the co-created recommendations to overcome the weaknesses found in the current state analysis before presenting the initial proposal for the cyber security services

reporting framework. The first and second validation round feedback, comments and discussions generated the Data 3 that was used to adjust the initial proposed framework.

The final validation round happened in one-to-one meeting with the business director of cyber security services of the case company who had initially defined the problem and set the objective for the study and has the ultimate decision power to steer the direction of cyber security services and their deliverables thus ultimately validating the suitability of the final framework for the case company. Feedback from the first and second validation rounds were used to adjust the final version of the proposed framework that is the outcome of this study that was presented for the business director to get it ultimately validated. Based on Data 3, minor adjustments were made to the recommendations and to the final framework.

6.2 Findings of Data collection 3

The Data 3 collection round validated the recommendations and the initial proposal of the framework. There were two minor recommendations to the initial recommendations and the initial proposal. They are presented in table 11 and changes compared to Data 2 stage are in bold.

Table 11. Changes to recommendations compared to Data 2.

#	Recommendation	Description of recommendation
REC3	Cyber security posture / resilience reported through PREVENT, DETECT & RESPOND capabilities in operational level.	The daily operations revolve around the prevent, detect and respond processes that people and technologies produce. When respond activities are low, the focus on reporting shifts to detection of incidents or other proactive aspects of delivering cyber security services. **The prevent and proactive aspect in reporting is scoped to the cyber security services that are provided by service provider.**
REC16	Each customer cyber space is unique. The reporting framework must be standard but needs to able to adapt for each customer environment.	The service provider must be able to adapt to each customer ecosystem. **The cyber security strategy or program or policy which sets the cyber security target is identified along with risk management process that is ran within customer organization with customer processes.** The service provider requires provide input and output to these processes. If service provider is engaged to risk management process this happens through consultancy services and not through managed services.

As can be seen in table 11, only two recommendations received adjustments compared to the initial recommendations that can be found in the section 5.2. Furthermore, the adjustments were minor to the recommendations and the initial framework was adjusted accordingly based on these minor adjustments. The final version of the cyber security services framework can be found in section 6.4.

6.3 Feedback received for the initial recommendations

Since the final workshop in the initial recommendation stage went very well it was agreed that the first internal validation round takes place through materials and individually by each member of the cyber security business team. When the proposal was internally accepted and validated, it was agreed that the mutual workshop between the external key stakeholders and the cyber security business team will be held. The internal validation round was performed as per agreed and the feedback in general was very positive.

6.3.1 Feedback from internal validation rounds

The only validation remark came from the business director who questioned the Prevent metrics part in the operational reporting level. The main concern was that was the responsibility of the cyber security services provider to map all the prevent controls of the customer organisation since there are lot of stakeholders in each customer organisation environment providing some sort of prevention capabilities. The premise for the remark was that the cyber security service provider needs to keep the expectation of customers on a feasible level and cannot include all the prevention capabilities into the cyber security services reporting. The detection capabilities on the other hand are most likely the responsibility of the chosen cyber security services provider.

The remark was dealt through an email distribution that all internal validation stakeholders were part of. It was agreed that cyber security service provider has services that have prevention capabilities, and the reporting framework should be scoped only to provide prevent capability reporting on the services that the cyber security services service provider is delivering to the customer organisation. This adjustment is documented into the recommendation REC3 description to clarify the metrics scope.

Otherwise, the feedback was positive. Here are some comments made by business team members:

> *Very thorough and coherent framework in my honest opinion. I believe we are ready validate this with our key customers. (Business team member 1)*
>
> *The framework fills very well the gap between the strategic and operational levels, but consultative services are still probably needed to complement this. In any case, this is a good and solid foundation to build our future services and reporting. (Business team member 2)*

The business director as well concurred that the remark is dealt with the minor recommendation update and approved that the recommendations and the framework are ready to be validated with the external stakeholders.

6.3.2 Feedback from external and internal validation round

The second validation round was more targeted to get validation from the external key stakeholders. All the internal business team members joined to the validation session to get direct insights from the key customers. All the external stakeholders who participated in the interviews to provide Data 2 were invited to the validation session. Three external stakeholders approved the invitation, one was on vacation during validation session and one external stakeholder would have liked to participate but had already agreed previous engagements for the same time.

The second validation session was held on the 15th of April as a virtual video meeting. One key customer could not make the session, but asked for a new, private session to be organized later. This session is already agreed but is out of the validation of this study. The validation session had two key customers validating the recommendations and the framework. The session was video recorded and field notes were taken during the session as well.

The feedback from the customers was very positive. There was one recommendation from them. One key customer pointed out that the strategical level is missing cyber security strategy element where the cyber security targets are usually set. This was a good point and complements the literature on cyber security management that was introduced in section 4.1.3. This resulted in change to recommendation REC16 description and also to the visual representation of the final framework.

Otherwise, the comments were very positive, and the participants commented that the framework is very thorough. Key customer 2 said after presenting the strategical level:

> *Actually, when I come to think of it, we are following our business and cyber security management as described in strategical level even though we have not used written or visualised process and relationships as described here. (Key customer 2)*

When asking about improvements for the recommendations or framework both customers raised the same question that how the framework can be taken into production and customers would start receiving reports through the presented framework. Both customers stated that the model is valid but were slightly sceptical how this could become into reality but also reminded that this only puts the pressure on the service provider. The business director stated at this point that:

> *When I introduced the problem for this study, the idea for this framework was to have common ground between customers and service provider to have understanding what are the relations and building blocks to have common language regarding situational awareness in the future. We had to have credible framework where we base our reporting, and this was the first step in our improvement process. It is to be seen if we will or implement this identically to framework and now we have a framework to base our development activities and we have made a mental decision to start the next phase in our journey. (Business director)*

The comment was accepted by the external stakeholders and there was encouragement from them to move towards the recommended framework in reporting. One customer was willing to participate in development activities and was eager to receive reports through this model.

For the final discussions the participants were presented set of validation questions to think about the validity of framework. The questions are presented in Appendix 3. All in all, the discussions were very positive, and the customers did not find any showstoppers in the reporting framework and encouraged the case company to move rapidly forward with the development of reporting.

6.3.3 Feedback from the business owner

The final validation was held with the business director on 16 April. The conclusion from the external stakeholder validation session was very positive. There was nothing pointed out by the external stakeholders for being wrong in the framework. A minor modification to the visual representation of the framework was made and this was accepted by the business director. The business director was very happy with the findings, recommendations and the created the framework that was the outcome of this study. When asked if the business problem was solved and was the objective and the outcome of this study fulfilled, he stated the following:

> *I have peer reviewed the thesis chapters one to five and what I understand from research work, the research part in this thesis is outstanding and the framework turned out really great. The tactical level links really nicely as a cause and effect to our and customer activities. (Business director)*

The objective and outcome discussion ended up to a conclusion that the study has fulfilled the initial set objective and the outcome can be used in the case company context. The validation session ended up to a discussion about the next steps how to move forward with the reporting development activities to move towards to a reporting model that the framework suggests.

6.4 Final proposal for the cyber security reporting framework

As the result of the validation stage, two recommendations received minor adjustments that led into the final proposal of the cyber security services reporting framework that is illustrated in figure 35.

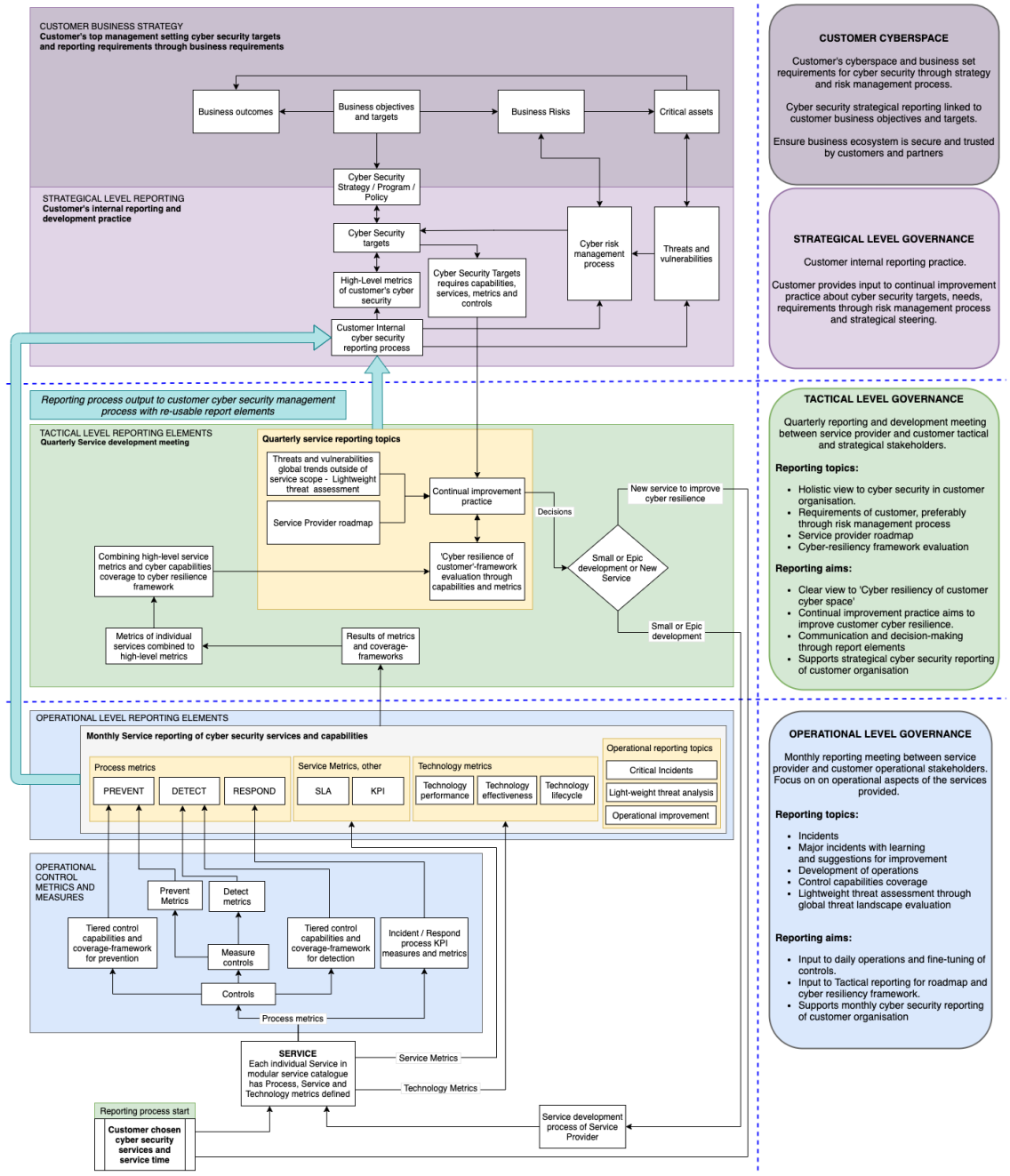


Figure 35. Final proposal for cyber security reporting framework

The only change from the initial proposal framework was to bring a ‘Cyber security strategy / program / policy’ element as part of the strategical level that operates between the business objectives and the cyber security targets.

The validation of the initial recommendations and the framework followed the plan set for validating them. Validation stage did not present any major concerns or implications

to the initial recommendations or the framework and this is most likely due to tight collaboration during the previous co-creation stages. The execution of the validation stage resulted in a validated outcome for this study that enables the case company to develop the cyber security services reporting.

The seventh and final section contains the executive summary of this study along with recommendations for the next steps in order to develop reporting in the case company. The section ends up to the self-evaluation of this study.

7 Conclusions

The seventh section summarizes the study through summary, recommendations for next steps, a self-evaluation of the study and the results before the closing words.

7.1 Executive Summary

The objective of this study was to create a cyber security services reporting framework to enable reporting to cyber security customers that supports the business needs of customers to improve their cyber security posture. The outcome of this study is a reporting framework that enables the case company to start developing and implementing reporting practises to improve the cyber security services and the cyber security posture reporting. The case company has been offering the service since 2015 and was looking to develop and mature the reporting capabilities that previously had been developed and formed organically during the previous years. This had led into a situation that the reporting of each customer deployment was little bit different and focusing mostly on operational and technological aspects of the provided services.

Design research was chosen as research approach method. This enabled using qualitative data gathering methods and the creation of suitable solution as an outcome for the case company and this study. The study comprises four research stages. The study started with current state analysis to find strengths and weaknesses of the current reporting practice. This was followed by literature review where suitable solutions to overcome the weaknesses identified in the previous stage was used to create a conceptual framework based on existing knowledge. The third co-creation stage produced recommendations from the internal and external stakeholders for the initial proposal. The fourth and last stage consists of three validation rounds of the initial proposal where feedback from the internal and external stakeholders was gathered to tweak and generate the final proposal for the cyber security services reporting framework which is the outcome of this study.

In the current state analysis stage data was gathered through interviews, documentation and a workshop to find weaknesses and to find current reporting patterns. The findings consisted of strengths, out of scope findings and weaknesses. The focus in the study then turned to finding improvement ideas for weaknesses. A total of four weaknesses were identified. One of the weaknesses was that there was no reporting framework in

systematic use which made the problem of the study very relevant. The other weaknesses related to the reporting terms and deliverables not being unified and on the other end of the spectrum of weaknesses, lack of customer engagement and lack of linking to the risk management process of customers were identified. These weaknesses set the requirements for the next stage to find improvement ideas from literature to cyber security management, cyber security posture and best practices for reporting of services.

The literature research focused on finding solutions for the weaknesses and topics identified through weaknesses. A structured approach for literature research was generated and followed in this stage. This resulted in the conceptual framework that tackles the identified weaknesses and includes best practises and knowledge for cyber security management in organisations, elements of cyber security posture, how to develop cyber security capabilities in the customer organisation and service provider context and eventually the reporting of cyber security services and capabilities.

The recommendations for the framework were co-created in workshops and interviews. The internal key stakeholders participated in three workshops. A variety of external key stakeholders were interviewed to gain understanding of the cyber security management in the customer organisations along with expectations for cyber security reporting. A total of twenty initial recommendations were identified to overcome the weaknesses. The initial recommendations were used to generate an illustration for the proposal for cyber security reporting framework.

The twenty initial recommendations were divided into four categories based on each weakness. Each recommendation was assigned to a certain weakness that it was providing improvement or guidance how to overcome that weakness. The weakness ‘No reporting framework used or identified’ received seven recommendations. The most important finding and recommendation for this weakness was to divide the reporting framework into operational, tactical and strategical levels. This is slightly different approach compared to the literature where the reporting is focusing on operational and strategical levels, but the literature is mainly written and focusing on cyber security management inside one organisation and not the service provider and customer organisation context. The service provider and customer organisation relationship and responsibilities are researched in this study and the three-level model supports reporting in this context and is a major finding in this study. The three-level model is supported by best practices found

in IT service governance de facto standard ITIL that is guiding and supporting the cyber security services reporting objectives and outcomes.

‘The reporting terms and deliverables not unified’ weakness received five recommendations. The framework does not strictly tell what the exact metrics and measures are to be used but the framework and recommendations support the core foundation of cyber security reporting where metrics are planned first and after them the measures. To ensure the service provider is covering all important service areas, the metrics are divided into process, service and technology metrics and each service is expected to have these pre-planned. The metrics and metrics areas alone are not enough to provide holistic view to cyber security operations development and therefore the framework includes capabilities mapping to the capabilities and controls that the service in question is contributing. Similar pre-planned approach to each service ensures that reporting terms and deliverables are created similarly to all customers and this is the foundation and starting point of the framework.

The identified weakness ‘customers did not have many requirements to push the reporting further and were expecting service provider to develop the reporting alone’ received three recommendations. The most important finding is that reporting is a reciprocal and collaborative process where communication over reporting data is the most important aspect to enable clear view to the current state of cyber security. And when the current state of affairs is known, new targets can be set, and decisions can be made effectively to start the actions or development in order to reach the set targets in the future. To help this reporting process, a common framework to monitor, report and plan the cyber security capabilities is taken into use between the customer organisation and the service provider in the tactical level. This is supported by the ITIL service governance best practices for continual service improvement. All of the aforementioned matters are incorporated to the framework.

The last weakness ‘customer business and risk engagement to services was found to be minimal’ received five recommendations. Each customer is unique regarding their business, operational environment and ecosystem, which set the requirements for the cyber security capabilities. The strategical level of the framework includes the customer processes, relations and responsibilities for effective cyber security target setting and management. The expectation in the framework is that customer organisations are running some sort of risk management processes that includes the cyber risks. The identified

risks need to be managed and the risks set the requirements for capabilities, mitigation and cyber security targets that the service provider is fulfilling through the provided services. The framework does not strictly state how the customer organisations need to manage their cyber security, but the framework has a clear input channel to the service provider reporting process to enable the reciprocal and collaborative services development and steering process mentioned earlier.

The recommendations and the framework were validated in several rounds. The validation included both internal and external validation. After the validation rounds the recommendations and the framework were compiled to their final format and the final validation was done by the business director of the case company who originally introduced and defined the business problem.

The final framework is a comprehensive reporting framework for a service provider to report and improve the cyber security capabilities in customer organisations. The case company management has accepted the framework as the guiding element to plan and develop the reporting practices and deliverables of the cyber security services in the future. The framework enables collaborative and holistic approach to manage and steer the development of cyber security capabilities in all kinds of customer organisations through effective and transparent operational, tactical and strategical reporting.

7.2 Next steps and recommendations toward Implementation

There are certain steps to be considered before starting the implementation of the framework to practice. The first step what the case company needs to do is to set the long-term vision for reporting and all persons working around the services and reporting need to adopt, understand and embrace the framework. This is part of the cyber security services strategy and setting the vision and the objective for reporting requires to answer questions why case company is offering cyber security services reporting to customer organisations, what reporting services and elements are offered to customers and how they will be delivered. This sets the organisational and operational requirements for reporting.

After the strategy definition and implementation phase, the next logical step would be creating a reporting baseline through a current state analysis for the currently delivered services and map the data, measures and metrics to the prevent, detect and respond-

metrics reporting categories in the operational level of reporting. This way a gap analysis against the framework can be made for each service. The gap analysis results in an action or development plan to understand what metrics are missing or need refinement.

At the same time, the external stakeholders meaning customer organisations need to be engaged in developing the metrics. The expectations and requirements for the metrics need to be gathered from the customer organisations to understand the expectations for top management and service provider reporting metrics wise. When the current state is understood, a gap analysis leading to development activities can be generated that supports the selection of frameworks and metrics that need to be developed and especially the measuring methods. The recommended next steps are illustrated as high-level process in figure 36.

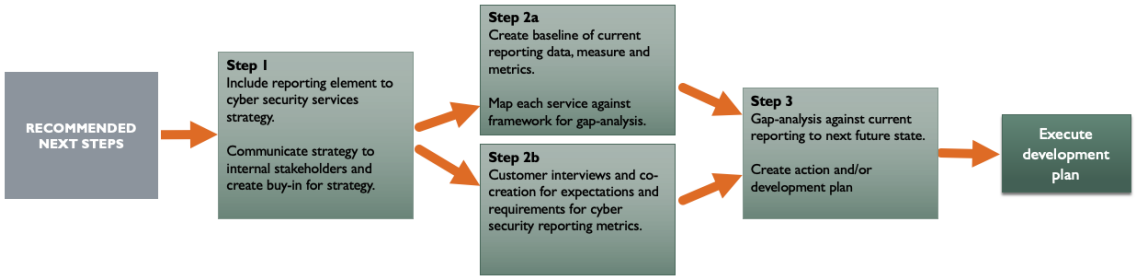


Figure 36. Next steps toward implementation

The next steps have been already discussed with case company top management and the approach has got some traction already but requires more detailed planning and resource allocations.

7.3 Self-evaluation of the study

The initial business problem for this study was raised by the case company who delivers cyber security services for customer organisations, but the reporting of the services was done differently for each customer and the reporting structure was mainly focusing on operative and technological aspects without bringing additional value to customer business needs regarding cyber security. The objective was to create a cyber security services reporting framework to enable reporting of cyber security services to customer organisation that supports the improvement of cyber security posture was based on the

business problem. The outcome of this study is a cyber security services reporting framework that gives tools and means for the case company to resolve the initial business problem. The framework is a comprehensive and robust reporting framework but also describes the main processes of cyber security management, cyber security relations and responsibilities in the service provider and customer organisation context to create common understanding of roles, expectations and responsibilities. Therefore, the result of this study achieves the objective fully.

The author of this study did not work in the cyber security business team when the business problem was identified, and the current state analysis stage was performed. This required author to deep dive into the essence of cyber security before the current state analysis interviews. The other positive aspect of this was that the author was considered neutral, and the information shared by the internal stakeholders was honest and presented the true state of reporting. Even though the initial problem was set by the case company and the identified weaknesses are case company specific, one could argue that the weaknesses are quite general. This is quite true, but the lack of reporting framework not identified or used was taken into consideration when literature reference approach was planned. The problem has been researched quite thoroughly and it has been validated that study enables the development of reporting practises in the future and the customer organisations were eager to receive reports based on the framework. The author joined the cyber security business team during the current state analysis stage.

The quite generic weaknesses were also quite vague from the perspective of the business problem and the objective since the generic weaknesses set new dimensions to the problem and the objective to research and define the cyber security management practices and the relationships between service provider and customer organisation before diving into the reporting of cyber security services. From the perspective of the study there were no so-called text-book solutions available for cyber security reporting in this context and this set a requirement to draw materials from a variety of high-quality sources. Were the right information sources used can always be questioned but to the most relevant areas at least two separate sources covering the area were used to validate the literature. Large and diverse group of external and internal stakeholders with proficient background in cyber security industry participated in the recommendation and framework generation and validation throughout the process to ensure the best possible outcome.

The biggest hardships in the framework generation were, quite understandably, the rather sceptical mindsets of some of the internal stakeholder team due to previous experiences in cyber security management. Many team members have worked for many years in the cyber security industry and have encountered issues in aligning service provider and customer organisation management practices. There were concerns if customer organisations are willing to engage a service provider into the cyber security management processes. The external stakeholder interviews and co-creation sessions have alleviated and showed all team members that cyber security is truly becoming a top management topic in all organisations and the service provider has a role in that process and it was encouraged to improve the reporting practises contributing to the strategical level.

The credibility of the study is evaluated in the following sub-sections. The credibility of the study is done by evaluating the validity and the reliability. When the validity and the reliability are determined the logic and relevance of the study are evaluated. Each of the factors contributing to the credibility are evaluated in their respected sub-sections.

7.3.1 Validity

Kananen (2013) describes the validity as researching the correct things and what measures are used. Saunders et al. (2012) have come to the same conclusion and state that validity refers to the appropriateness of the measures and accuracy of the analysis. (Kananen, 2013; 176 & Saunders et al, 2012; 202)

Shenton (2004) studied trustworthiness in qualitative research projects. The credibility is achieved through many factors, but triangulation contributes to both credibility and confirmability. The triangulation is the use of different methods and different types of informants to receive information of the phenomenon. This contributes to the confirmability that ensures that findings are the experiences and ideas of the informants and alleviates the bias and preferences of researcher. (Shenton, 2004; 63-72)

Saldana et al. (2011) underline that researcher conducts the research with honesty and integrity. The researcher can present these through the descriptions how the research was done and by using transparency to the research. All data collected and analysed are contributing to the research results and there is evidence presented that research was conducted appropriately and valid literature was reviewed and referenced. Saldana

also mentions triangulation and involving participants to observe and review the findings and perspectives about the phenomenon that is researched. (Saldana, 2011; 134-136)

This study has followed the pre-planned research design to solve the initial business to produce the set outcome. The problem and outcome requirements were validated by the business owner before the research began to ensure that correct things were researched. The steps and logic of each data collection round was documented, and the key workshops and interviews have been video recorded to support trustworthiness and credibility. In each data collection round the validity of collected data was triangulated by having diverse group of stakeholders participating to data collection round. Data 1 was collected through three separate internal stakeholder groups. The external stakeholders were utilised in Data 2 and Data 3 collection together with the internal stakeholders to triangulate the data collected in these data collection rounds. The literature references were collected from high-quality sources and to each conceptual framework area several authors and resources were used to ensure literature reference triangulation to improve the credibility and confirmability.

The steps taken in the research have been described throughout the study to underline the honesty, integrity and transparency of the study. The study describes in detail how data was collected, how it contributed to the research and how it was analysed to also support the honesty integrity and transparency.

7.3.2 Reliability

According to Thyer (2009) reliability in qualitative research is also called dependability where researcher attempts to account for changing conditions in the data collection. The data collection must be planned in advance and it must have “audit-trail” of data collection methods and interpretations how dependable it is on the perspective of other collaborators if they could have matched the data as the original researcher. The reliability can be improved by establishing data recording procedures of field notes and cross-checking the data by multiple research participants. (Thyer, 2009; 356-361)

Kananen (2013) also states that the credibility that is the goal for reliability when qualitative research methods are used, can be reached when material and interpretation of it is read by the persons concerned with research results. (Kananen, 2013; 190-191)

Pandey et al. (2014) claim that to ensure rich, robust, comprehensive and well-developed data sources that are credible, a technique call triangulation is used as part of the investigation. In triangulation two or more sources of data are collected through different methods of triangulation that are ‘methods triangulation’, ‘triangulation of sources’, ‘analyst triangulation’ and ‘theory/perspective triangulation’. (Pandey et al., 2014; 5747-5748)

From these explanations we can interpret that reliability is achieved if the study can be replicated and the data collection has been consistent throughout the research. This study has followed these principles. The research design is presented in section 2.2. and the data collection plan and methods together sources have been introduced in chapter 2.3. The data plans of section 2.3 constitute an audit-trail that includes source, context, method, time and data recording method. The data and outcomes were triangulated in both source and analyst triangulation methods and several literature references were utilized to fulfil theory/perspective triangulation method.

The author of this study has delivered materials, results and draft of thesis to several internal stakeholders throughout the research. The thesis sections one to five were peer reviewed during the validation stage by the business director who was initial problem key stakeholder in the case company and has two decades professional experience in the cyber security industry. Neither in the material distribution or in the peer review there were no remarks made about dependability in any form and rather the comments have been positive. This supports the reliability and credibility since other persons have been able to follow the data collection and have interpreted it to be correct.

Triangulation has been used in each stage in this study. Large variety of stakeholders both internal and external have been used to co-create the recommendations and the outcome of this study. The materials have been gathered with several methods such as email conversations, documents, literature, one to one interviews and workshops. All of the methods and sessions encouraged people to ask questions, give feedback and contribute to the research as transparently as possible.

7.3.3 Relevance

Mizzaro (1997) states that relevance is a concept for documentation, information science and information retrieval. Relevance depends on the problem in question that requires obtaining information. The problem and information are then time dependant on a certain

time and what information is already received or if it permits to understand more. Therefore, the relevance in this study is seen as relation between two entities, the problem that is solved and the information that is sought to solve the problem.

The problem of this study was defined by the case company. From this we can conclude that the study is not based on the desires or ambitions of the researcher but a genuine problem that requires solving through obtaining new information since at that point of the time there was no information available in the organisation to solve the problem. The current state analysis revealed that the business problem truly exists since no framework was used or identified. This makes the study problem relevant.

The relevance of the study was ensured throughout the research by involving the internal and external stakeholders to verify the obtained and constructed information. All of the stakeholders that were part of the research are participating actively to the delivery of the services and reporting that enables the improvement of the security posture customer. This ensured the relevancy for both internal and external stakeholders in the data collection and co-creation stages of the framework and also takes into account the time and information relevancy factor.

7.3.4 Logic

Merriam-Webster defines logic as a proper or reasonable way of thinking about something with sound reasoning. Saunders et al. (2012) on the other hand describe a logic as a good theory that can answer questions ‘what’ and ‘how’ but can also explain why the relationship exists. When the relationships are known at this level, it enables that a prediction of new outcomes is possible even if the variables are manipulated. (Merriam-Webster, 2021 & Saunders et al., 2012; 48)

The research design follows the principles that enable the outcome with pre-planned approach and follows clear logic to find the most suitable solution for the problem introduced. The business problem required an outcome that the case company can utilize in the future in their daily operations, and this set requirement to use design research method. This meant that current state of reporting was examined first to understand what areas require improvements. After that, literature was researched to find suitable solutions to improve and build the final framework that was missing from the case company. The conceptual framework provided tools and references to produce recommendations

for the framework in collaboration with the internal and external stakeholders. The co-created framework was then validated by various stakeholders who initially set the recommendations what the framework should include, and result was that they are included in the framework. The logic in the process was to find, what sort of foundation the reporting framework needs to be built on, then the architectural blueprints and materials were sourced to understand how a framework could be built and these were introduced to the key stakeholders. After the initial architectural choices and the building materials were recommended, the framework was co-created. The co-created framework was then evaluated and validated if the framework turned out to be and included every aspect that was suggested by the stakeholders. The execution of the study follows this logic and the research design project plan.

7.4 Closing Words

Cyber security is becoming more and more important to all organisations. It has become evident that many organisations require a skilled cybersecurity partner that connects people, processes and technology into a functional entity. When the service provider operates in accordance with the best processes in the industry, security risks are managed, the use of the services is easy for service consumers and the continuity of the business in customer organisations is secured. The modern approach to cyber security encourages customer organisations and service providers to collaborate and to continually evaluate the current state of cyber security and how it could be improved. The decision making for improvements requires efficient and transparent reporting of cyber security services. The outcome of this study introduces a framework that helps the customer organisations and service providers to collaborate over the needed cyber security capabilities through reporting.

References

Axelos. (2011). *ITIL Service Design.* TSO (The Stationery Office).

Axelos. (2019). *ITIL Foundation, ITIL 4 edition.* TSO (The Stationery Office).

Baimyrzaeva, M. (2018). *Beginners' Guide for Applied Research Process: What Is It, and Why and How to Do It?*, Available from: https://www.ucentralasia.org/Content/Downloads/UCA-IPPA-OP4-Beginners%20Guide%20for%20Applied%20Research%20Process-Eng.pdf (Accessed 31 January 2021)

Bainey, K. (2016). *Integrated IT Performance Management,* CRC Press, Taylor & Francis Group, LLC

Bakshi, S. (2016). *Performance Measurement Metrics for IT Governance,* ISACA JOURNAL VOL 6

Bayuk, J., Healey, J, Rohmeyer P., Sachs, M., Schmidt J., Weiss, J. (2012). *Cyber Security Policy Guidebook.* John Wiley & Son, Inc.

Black, P., Scarfone, K., Murugiah, S. (2008). *CYBER SECURITY METRICS AND MEASURES,* John Wiley & Sons, Inc.

Center of Internet Security (CIS), Cybersecurity threats, alert level information. Available from: https://www.cisecurity.org/cybersecurity-threats/alert-level/ (Accessed February 21 2021)

Center of Internet Security (CIS). (2019). CIS Controls™ V7.1.

Chaplin, M. (2017). *Comments on Draft Update of the Framework for Improving Critical Infrastructure Cybersecurity.* Available from: https://www.nist.gov/system/files/documents/2017/04/20/2017-04-11_-_isf.pdf (Accessed 21 February 2021)

Clement, J. (2020). Statista: *Global digital population as of October 2020*, Available from: https://www.statista.com/statistics/617136/digital-population-worldwide/ (Accessed 14 November 2020)

Feglar, T. (2005). *ITIL Based Service Level Management if SLAs Cover Security,* SYSTEMICS, CYBERNETICS AND INFORMATICS VOLUME 3 - NUMBER 4

Foreman, P. (2009). *Vulnerability Management,* Auerbach Publications

Fourkas, V. (2004). *What is 'cyberspace'?*. Available from: https://www.academia.edu/download/57865756/FourkasV_2004_journal__Media_Develop_what-is-cyberspace.pdf.pdf (Accessed 14 February 2021)

Heyburn, H., Whitehead, A., Zanobetti, L., Shah. J. N., Furnell, S. (2020). *Analysis of the full costs of cyber security breaches,* Ipsos Mori. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/901569/Analysis_of_the_full_cost_of_cyber_security_breaches.pdf (Accessed 4 March 2021)

International Telecommunication Union (ITU-T). (2008). *Recommendation ITU-T X.1055, Risk management and risk profile guidelines for telecommunication organizations.* Available from: https://www.itu.int/rec/T-REC-X.1055-200811-I/en (Accessed February 26 2021)

ITIL Central (2005): History of ITIL. Available from: https://itsm.fwtk.org/History.htm (Accessed November 14 2020)

Jacobs, P., von Solms, S., Grobler, M. (2016). Towards a framework for the development of business cybersecurity capabilities. The Business and Management Review, Volume 7 Number 4, May 2016 51-61

Kananen, J. (2013). Design research (applied action research) as thesis research: A practical guide for thesis research. Jyväskylän Ammattikorkeakoulu JAMK.

Katzan, H. (2012). Cybersecurity Service Model, Journal of Service Science – Fall 2012 Volume 5, Number 2

Khalilian, A., Othman I., Mehrbaksh N. (2017) Integrated feedback control reporting for improving quality of technical service reporting in IT service management, Telematics and Informatics 34 (2017) 1736–1771

Krumay, B., Bernroider, E. (2018) *Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework.* Available from: https://www.researchgate.net/publication/328656212_Evaluation_of_Cybersecurity_Management_Controls_and_Metrics_of_Critical_Infrastructures_A_Literature_Review_Considering_the_NIST_Cybersecurity_Framework_23rd_Nordic_Conference_NordSec_2018_Oslo_Norway (Accessed 2 February 2021)

Limnéll, J., Majewski K., Salminen, M. (2014). Kyberturvallisuus. Docendo

Mattila, J., Ali-Yrkkö, J., Seppälä, T. (2020). *Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät?*. Brief 93. 14.12.2020. ETLA, The Research Institute of the Finnish Economy. Available from: https://www.etla.fi/julkaisut/kyberuhat-yleistyvat-miten-suomen-yritykset-parjaavat/ (Accessed 15 December 2020)

Merriam-Webster, Thesaurus, Logic, noun. Available from: https://www.merriam-webster.com/dictionary/logic (Accessed 12 February 2021)

Meyer, C. (2016). *Talking the Talk: Cybersecurity Metrics for the C-Suite*, Security: Solutions for Enterprise Security Leaders. Aug2016, Vol. 53 Issue 8, p30-32. 3p

The National Institute of Standards and Technology (NIST), (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* Available from: https://doi.org/10.6028/NIST.CSWP.04162018 (Accessed 19 February 2021)

The National Institute of Standards and Technology (NIST), (2015). NIST Special Publication 800-53 Revision 4.

Norman, D. (2021). Teams meeting between study author and ISF. Introduction to ISF and SOGP. (1 March 2021)

Pandey S., Patnaik S. (2014). *Establishing Reliability and validity in qualitative inquiry: A critical examination*. Jharkhand Journal of Development and Management studies XISS, Ranchi, Vol. 12, No. 1, March 2014, pp. 5742-5753

Saldana,J. (2011). *Fundamentals of Qualitative Research*, Oxford University Press, Incorporated, 2011. ProQuest Ebook Central, Available from:

https://ebookcentral.proquest.com/lib/metropolia-ebooks/detail.action?docID=665394 (Accessed 24 January 2021)

Saunders, M., Lewis, P., Thornhill, A. (2009). *Research methods for business students.* 5th ed. Harlow: Pearson Education.

Schatz, D., Bashroush, R. Wall, J. (2017). *"Towards a More Representative Definition of Cyber Security,"* Journal of Digital Forensics, Security and Law: Vol. 12 : No. 2 , Article 8

Shenton, A. (2004). *Strategies for Ensuring Trustworthiness in Qualitative Research Projects*. Education for Information, IOS Press, 22(2), PP. 63-72.

Snyder, D., Mayer, L., Weichenberg, G., Tarraf, D., Fox, B., Hura, M., Genc, S., Welburn, J. (2020). *Measuring Cybersecurity and Cyber Resiliency,* the RAND Corporation

Stallings, W. (2019). *Efficient Cybersecurity,* Pearson education inc.

Standard of Good Practice (SOGP). (2011). *2011 Standard of Good Practice.* Available from: https://www.uninett.no/sites/default/files/webfm/ISF%20Standard%20of%20Good%20Practice%20for%20Information%20Security%202011.pdf (Accessed 21 February 2021)

TAG Cyber. (2020). *2021 SECURITY ANNUAL.* Available from: https://www.tag-cyber.com/downloads/2021_TAG-Cyber_Annual.pdf (Accessed 21 February 2021)

Thyer B. (2009) The handbook of social work research methods, 2nd ed. SAGE.

The Netherlands Organisation for applied scientific research (TNO), (2017). *Library of Cyber Resilience Metrics*. Available from: https://repository.tno.nl/islandora/object/uuid:57da4ef3-7600-479d-954c-e1a4a5122a1e (Accessed 30 January 2021)

Traficom Publications (2020). *Cyber security and the responsibilities of boards.* February 2020. Finnish Transport and Communications Agency Traficom National Cyber security Centre Finland. Available from: https://www.kybertur-vallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_ENG-digi_auk280120.pdf (Accessed 15 December 2020)

Wakaru Oy, (2010). ITIL Foundation version 3 course material – version 2.21

Whitman, M., Mattord, H. (2011). *Roadmap to information security for IT an InfoSec Managers.* Course Technology

QUESTIONS OF CURRENT STATE ANALYSIS

SEMI-STRUCTURED APPROACH – STEERING AVOIDED

- Q1: **Are we using any common framework to report Cyber security services?**
- Q2: **Where is the current report process described?**
- Q3: **Describe how you create the report to you customers and reporting meetings do you participate?**
- Q4: **Do we have reporting requirements from customer? (If yes, where are they stored)**
- Q5: **Is there common report template?**
- Q6: **For whom and what roles do you report to in the customer organisation?**
- Q7: **Do we have clear view what customer is seeking through cyber security services?**
- Q8: **Do we link our reporting to customer acknowledged risks?**
- Q9: **Are we linking the reporting to customer business outcomes?**
- Q10: **How do we report the cyber security posture of the customer?** (Added after 4th interview)
- Q11: **Do we understand the critical assets and data of customer business?**
- Q12: **Do we have clear view what customer is seeking through cyber security services?**
- Q13: **What is good in our current reporting?**
- Q14: **What are the weaknesses and areas where to develop in our reporting?**
- Q15: **Can you name any cyber security reporting frameworks?**
- Q16: **If you would be CEO of a company, what would you ask from your CIO/CISO to be reported to Management Team about the state of Cyber Security?**
- Q17: **Any Other Business? What I did not understand to ask?**

QUESTIONS OF DATA 2 - EXTERNAL STAKEHOLDER INTERVIEWS

SEMI-STRUCTURED – STEERING AVOIDED

- Q1: **Can I record the interview for later transcription? (yes / no)**
- Q2: **Background: What is your role and responsibility regarding cyber security in your organization and can you briefly describe the cyber security governance of your organization?**
- Q3: **Is the cyber security part of your organization strategy?**
- Q4: **Do you have separate cyber security strategy?**
- Q5: **Who is responsible for cyber security targets and objectives in your organization?**
- Q6: **Do you have cyber security policy or program at your company?**
  - **If yes**
    - **Is the policy/program linked to business objectives or strategy of your company?**
    - **Does it state the cyber security objectives and targets?**
    - **Are the certain metrics that you have included to it?**
  - **If no, how do you steer cyber security targets?**
- Q7: **Do you have systematic risk management process in your organization?**
  - **If yes**
    - **How are the cyber risks linked and handled in that process?**
    - **Are you linking threat and vulnerability management process to risk management?**
    - **Would you be willing to include external service provider in risk management process?**
  - **If no, are you planning to have some sort of risk management process?**
- Q8: **Are you using any cyber security framework systematically in your organization such as NIST CSF, SoGP, ISO27000-series or others?**
  - **If yes, how they are used**
  - **If no, have you had plans or are you planning to use?**
- Q9: **How do you identify and prioritize critical assets in your organization?**
- Q10: **What is the cyber security reporting structure in your organization?**
  - **Do you report to top management? If yes, how often?**
  - **What are the questions top management would like to know or receive answer?**
  - **What are the high-level topics or areas of the strategical reporting in your organization?**
  - **Are there certain metrics you are using for reporting?**
- Q11: **Do you see benefit if the service provider and your organization would align cyber security reporting metrics**
  - **If yes, how do you see the metrics between you and service provided could be aligned**
- Q12: **What are they key metrics you are expecting to see in cyber security services in general?**
- Q13: **Would you see benefit that service provider and your organization would follow the development of cyber security in your organization through some cyber security framework that would be agreed upon?**
- Q14: **How can service provider help and contribute to your organization's internal reporting and cyber security governance?**
- Q15: **What are you expecting from service provider from reporting that would enable the cyber security posture improvement in your organization?**
- Q16: **Any other requirements or ideas how the cyber security services reporting could help your organization to improve its cyber security posture?**

VALIDATION QUESTIONS – EXTERNAL VALIDATION

- Are all the relevant reporting elements included to the reporting framework?
- What could be improved in the framework?
- Would this kind of reporting framework bring clarity to the relationship and responsibilities between customer organisation and service provider in cyber security services?
- Could this kind of reporting framework help you reporting the cyber security in your organisation with less burden and/or improved quality?
- Could this kind of reporting framework enable continual cyber security posture improvement in your organisation?
- Could you see this kind of reporting framework could be tested out in Customer organisation and service provider context?
- Any other comments and feedback from the framework?