Defining a Holistic Data Center Security Management Framework and Designing an Evaluation Tool

Mikko Helin

2021 Laurea

Laurea University of Applied Sciences

Defining a Holistic Data Center Security Management Framework and Designing an Evaluation Tool

Mikko Helin
Security Management
Master's Thesis
June, 2021

Laurea University of Applied Sciences **Abstract**

Degree Programme in Security Management

Master of Business Administration

Mikko Helin

Defining a Holistic Data Center Security Management Framework and Designing an Evaluation Tool

Year 2021 Number of pages 77

Data centers are defined as part of critical information infrastructure in many countries and organizations. The importance of protecting and securing these information processing facilities has increased since information technology is embedded in almost every part of modern societies, businesses, and people's lives worldwide. To be able to protect data centers and their operation against various types of unwanted events, a holistic viewpoint for data center security management is needed. So far, no generally accepted data center security management framework or model has been published even though several information security management and data center management standards and frameworks are available.

The purpose of this thesis study was to define a general holistic data center security management framework and to develop a tool for evaluating data center security management for an anonymous target organization. Developing the evaluation tool also enabled testing and verifying the framework within the scope of this study. Theoretical framework of this thesis study consisted of corporate security frameworks and standards but information security management and data center industry standards and frameworks were also included.

This thesis study was a constructive research project and research-based development processes were followed. The usability of the evaluation tool was verified through a heuristic evaluation process, which formed the research method base of this thesis study. Three domain experts were included in the heuristic evaluation process and as a result, 24 different types of usability problems were found and 15 different types of comments received regarding general acceptability and usefulness of the evaluation tool.

The results of this thesis study suggested that the general holistic data center security management framework and the evaluation tool could be applied in actual use cases. Both the framework and the tool were found as applicable and useful for the target organization. The basic structure of the framework was accepted to represent general data center security management holistically.

The results presented in this thesis could benefit further research on data center security management by providing a holistic framework to start with. The results and the framework may also be utilized outside the academic research community by those creating similar evaluation tools or by adopting the holistic data center security management framework to actual data center management use cases. Further research topics on data center security management were identified throughout the course of this thesis study.

Keywords: data center, security management, evaluation

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuusjohtaminen

Tradenomi (Ylempi AMK)

Mikko Helin

Palvelinkeskusten kokonaisvaltaisen turvallisuusjohtamisen määrittely ja arviointityökalun suunnittelu

Vuosi 2021 Sivumäärä 77

Palvelinkeskukset määritellään monissa valtioissa ja organisaatioissa osaksi kriittistä tietoinfrastruktuuria. Tietojenkäsittelyyn tarkoitettujen kiinteistöjen suojaamisen ja turvaamisen merkitys on kasvanut, sillä informaatioteknologia on osana melkein jokaista modernia yhteiskuntaa, yritystä ja ihmisten elämää maailmanlaajuisesti. Palvelinkeskusten ja niiden toimintojen suojaamiseksi erityyppisiä ei-toivottuja tapahtumia vastaan tarvitaan palvelinkeskusten turvallisuusjohtamiseen kokonaisvaltaista näkökulmaa. Toistaiseksi yleisesti hyväksyttyä palvelinkeskusten turvallisuusjohtamisen viitekehystä tai mallia ei ole julkaistu, vaikka käytettävissä on useita tietoturvallisuuden johtamiseen ja palvelinkeskuksiin liittyviä standardeja ja viitekehyksiä.

Tämän opinnäytetyön tarkoituksena oli määritellä yleinen kokonaisvaltainen palvelinkeskusten turvallisuusjohtamisen viitekehys ja kehittää työkalu palvelinkeskusten turvallisuusjohtamisen arvioimiseksi anonyymille kohdeorganisaatiolle. Arviointityökalun kehittäminen mahdollisti myös luodun viitekehyksen testaamisen ja todentamisen tämän tutkimuksen puitteissa. Tämän opinnäytetyön tietopohja koostui yritysturvallisuuden viitekehyksistä ja standardeista, mutta myös tietoturvallisuuden johtamisen sekä palvelinkeskusten standardeja ja viitekehyksiä sisällytettiin tietopohjaan.

Opinnäytetyö toteutettiin tutkimuksellisena kehittämistyönä ja työssä hyödynnettiin konstruktiivisen tutkimuksen prosesseja. Arviointityökalun käytettävyys vahvistettiin heuristisen arvioinnin prosessilla, joka muodosti tämän opinnäytetyön tutkimusmenetelmän perustan. Heuristisen arvioinnin prosessiin osallistui kolme tutkimuskohdetta edustavan toimialan asiantuntijaa ja arvioinnin tuloksena löydettiin 24 erityyppistä käytettävyysongelmaa ja saatiin 15 erityyppistä kommenttia arviointityökalun yleiseen hyväksyttävyyteen ja hyödyllisyyteen liittyen.

Tämän opinnäytetyön tulokset viittaavat siihen, että yleistä kokonaisvaltaista palvelinkeskusten turvallisuusjohtamisen viitekehystä ja arviointityökalua voitaisiin hyödyntää todellisissa käyttötapauksissa. Sekä viitekehys että työkalu todettiin soveltuviksi ja hyödyllisiksi kohdeorganisaatiolle. Viitekehyksen perusrakenteen todettiin edustavan palvelinkeskusten turvallisuusjohtamista kokonaisvaltaisesti.

Opinnäytetyössä esitetyt tulokset voisivat hyödyttää palvelinkeskusten turvallisuusjohtamisen jatkotutkimuksia tarjoamalla kokonaisvaltaisen viitekehyksen tutkimusten alustaksi. Tuloksia ja viitekehystä voidaan hyödyntää myös akateemisen tutkimusyhteisön ulkopuolella niiden toimesta, jotka luovat samanlaisia arviointityökaluja, tai omaksumalla kokonaisvaltaisen palvelinkeskusten turvallisuusjohtamisen viitekehyksen osaksi varsinaisia palvelinkeskusten johtamisen käyttötapauksia. Tämän opinnäytetyön aikana tunnistettiin palvelinkeskusten turvallisuusjohtamiseen liittyviä jatkotutkimuksen aiheita.

Asiasanat: palvelinkeskus, turvallisuusjohtaminen, arviointi

Contents

1 Introduction

Data centers are information processing facilities or premises which form the backbone of information systems in modern societies and businesses, including such concepts as the Internet and the Cloud (Geng 2014, 4). In current digital age, data centers have been defined as part of critical infrastructure in countries and businesses for example during COVID-19 pandemic (Miller 2020; Cybersecurity & Infrastructure Agency 2020). According to a Fortune 100 cybersecurity company Palo Alto Networks (2021), there are more than 7 million data centers worldwide. As technology is embedded in almost every part of societies, businesses, and people's lives worldwide, the importance of managing and assuring secure and reliable data center processes has increased.

Securing facilities and premises used for information processing, such as data centers, in a cyber-physical world can be viewed as a part of information security management (Kegerreis et al. 2015, 107). At the same time, securing data centers can be also viewed as part of corporate security management in organizations (Cabric 2015, 67). There are various information technology industry and information security standards providing a framework for information security management controls including physical security of information processing facilities (Kegerreis et al. 2015, 471). These information technology industry and information security standards are focused on information security management but the framework they provide might not be enough for describing all needed security management aspects for data centers as such. Corporate security management frameworks on the other hand might not provide enough information security management aspects needed for data centers. There are standards and frameworks created within data center industry focusing on data center industry aspects, but again, these might not provide sufficient security management framework presented in information security and corporate security management frameworks (Geng 2014, 4).

The purpose of this thesis study is to define a holistic management framework for securing data centers, which is then used to produce a tool for evaluating data center security management in organizations. The defining viewpoints in this thesis study are corporate security management frameworks but other information security management and data center industry frameworks are also included to design a holistic data center security management framework. Information technology and cyber security of data center production are delimited outside of the scope of this thesis study. As an end product of this thesis study, a tool is produced to be used for performing data center security management evaluations. The usability of the end product is verified through heuristic evaluation process, which forms

the research method base of this thesis study. This thesis study is following a constructive research approach of a research-based development process.

1.1 Motivation for this thesis

Initial thoughts and needs of this thesis study are evolved from the author's observation of the lack of data center security management publications. Prior to and throughout this thesis study process a thorough search has been made to find research, literature, and articles in libraries and on the Internet but no exact data center security management sources were available in public. As described in previous chapter, there are multiple different standards and frameworks available for information security management, data center management and corporate security management, both in public and paid sources. But no public research or literature defining a holistic security management framework for data centers are commonly found even though there are many industry standards for data centers covering this topic, such as ANSI/TIA 942 and EN 50600 (Shapiro 2016).

As information technology is being embedded in all parts of societies and businesses, information security is being embedded also in other aspects of security such as physical security and corporate security management among others. This phenomenon is called security convergence and it is demanding a holistic view on security management in organizations. (Wakefield 2014, 246.) Studying security convergence impact on security management was also one of the main motivations for this thesis study and the reason for selecting corporate security management framework as the defining viewpoint for this study theoretical framework.

Main motivation for this thesis study being focused on data center security management evaluation is finding a practical application after defining the holistic data center security management framework. Practical application for the framework is enabling testing and verifying the framework within the scope of this thesis study. Heuristics is considered and applied in this study to design a user-friendly end product for having any real use case for the product later on.

1.2 Thesis report structure

This thesis study report is following a basic IMRD-structure of a thesis report containing introduction, methods, results, and discussion. References are mentioned among all parts of this report and a complete list of all the references is presented in the very end of this study as scientific writing practices require. (Hirsjärvi et al. 2007, 244, 332.) The references used in

this thesis study provide also further reading recommendations for anyone interested in the topics presented in this study report and hopefully these are found useful.

The following chapter after this introduction is describing the research methods of this thesis study. The key concepts are described in chapter 3. Theoretical framework for defining the holistic data center security management framework is presented in chapter 4 and the evaluation tool created as an end product of this thesis is described in chapter 5. Heuristic evaluation process applied in this thesis study is presented in chapter 6. Results of heuristic evaluation process are presented in chapter 7 and conclusions of this thesis study in chapter 8. Finally, chapter 9 contains reflections and evaluations of this thesis study and some further research needs are also presented.

2 Development methods and research framework

This study is performed as a master's degree thesis of a University of Applied Sciences and the methodological research selections are focused on research-based development methods. The purpose of a research-based development process, according to Ojasalo, Moilanen and Ritalahti is to achieve practical improvements and new solutions while producing new information about a research subject. Research-based development processes are not bound to scientific research traditions but still contain knowledge acquisition and production of new knowledge by systematical, analytical, and critical process. (Ojasalo et al. 2014, 18, 22.) Selecting research-based development process as the research method is an obvious choice for thesis author since the objectives of this thesis originate from practical need to define a new framework for holistic data center security management and to develop a user-friendly evaluation tool based on defined framework. Any traditional scientific research method would require existing research data about these research subjects, which does not seem to be publicly available, or would possibly be limited to only some parts of the subjects.

Research-based development process proposed by Ojasalo, Moilanen and Ritalahti is presented in figure 1. Process starts with preliminary identification of development subjects and objectives. Preliminary identification should define whether the development process is problem-based or reform-based. Problem-based development is typically practical problem defined in advance requiring development. Reform-based development is about finding new solutions with multiple new connections or interfaces. Identifying preliminary development objective is followed by preliminary definition of development objective which is revised and specified in further development phases when more knowledge is gathered about development subject. One development objective should be producing new knowledge during the process by for example collecting and analyzing experience-based information. (Ojasalo et al. 2014, 26-27.)

The subject of this thesis study was in very early stage identified as reform-based development project for defining a new holistic data center security management framework by combining multiple existing frameworks. Preliminary objectives were produced by further examination of this thought and any practical use for the definition which could be further studied in the scope of this public thesis.

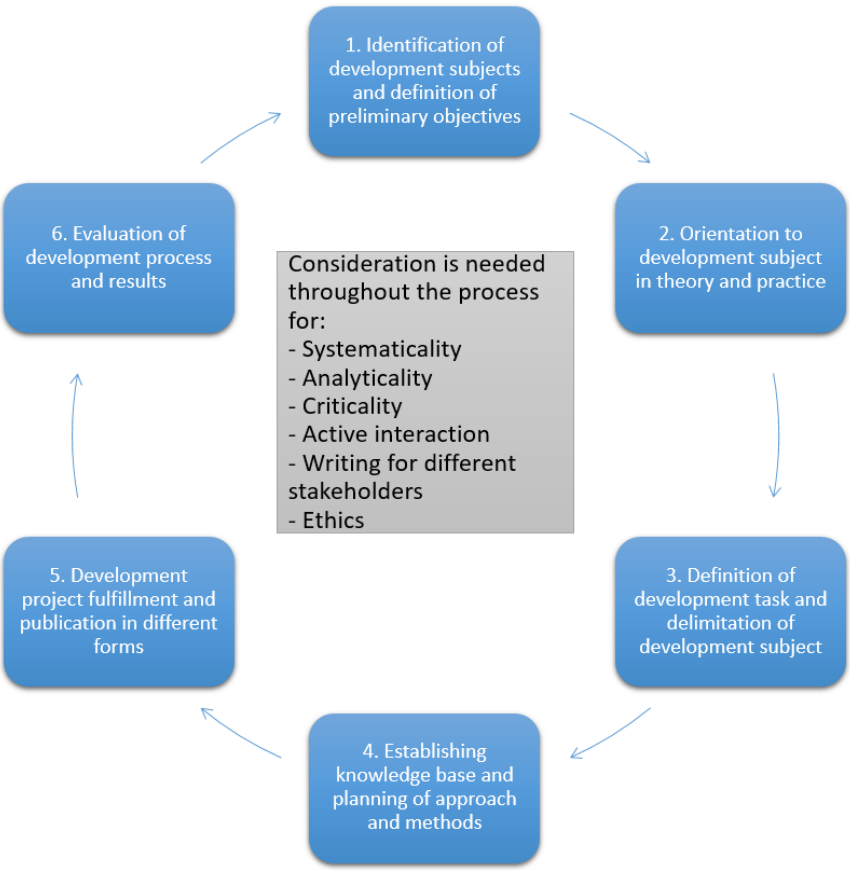

Figure 1: Research-based development process (Ojasalo et al. 2014, 24).

2.1 Information acquisition and source criticism

Second phase of a research-based development process includes information acquisition about development subject and development objectives. A thorough information acquisition should reveal possible existing premises and presumptions. Information acquisition should include different sources of information, both research studies and practical information sources. When development subject is an organization, this second phase of the process should provide information also about the industry in which the organization operates, and the concepts used

in the industry and the organization. Acquired information should be documented for further use in the development process. (Ojasalo et al. 2014, 28-29.)

As the author of this thesis has some experience on the subject industry, this orientation phase in this thesis study was conducted without direct contact to any organization but including a thorough search on multiple different public and paid electronic and printed sources. Search was conducted through Google Search, Google Scholar and Finna.fi search engines. Scientific studies were also searched separately in ResearchGate and Theseus.fi databases. Acquired information was critically reviewed and documented in an online tool called RefWorks provided by ProQuest.

Source criticism is required in any part of modern life and especially in all scientific research processes. Hirsjärvi, Remes and Sajavaara (2008, 109) define source criticism considerations in research to include evaluations on source author's notoriety and prestige, age and origin of the information, credibility and prestige of publisher, truthfulness, and impartiality of the source. Based on preliminary data acquisition phase for example data center industry publications include a lot of commercial articles all of which may not be objective and are not suitable as a source of a scientific research. Some sources utilized in this thesis study are dated back to 1990's and remain still credible and applicable. Source criticism, especially when using Internet search engines, was proven to be more difficult than using search engines meant for scientific research search engines and databases.

2.2 Delimitation of study and research questions

Third phase of research-based development process is about defining development objectives into more specified development tasks. Development tasks can be defined as answers to question of what the purpose or aim of the development process is. Development task can consist of one or more tasks. Rather than being too vague or too broad, development task should be precise and measurable for being able to evaluate how development was succeeded in later stages of the process. Defining development task is not considered the same as defining research question. (Ojasalo et al. 2014, 32-33.) Hirsjärvi, Remes and Sajavaara mention that in qualitative research it is not always required to define a research problem or question when there is a development task, but in traditional research a research problem or question is defined. When defining research problems and questions, usually a main problem is defined first and then sub-problems for it. (Hirsjärvi et al. 2008, 122.)

Defining development tasks and possible research problems or questions require usually, and in this thesis study, a delimitation of the research subject and objectives. In research, important at this stage is to define what exactly one wants to know or what is wanted to

point out by the research data. Quantitative research usually requires very strict measurable delimitation, but qualitative research delimitation can be and usually is adjusted throughout information acquisition. (Hirsjärvi, Remes, etc. 2008, 81-82, 87.)

In this thesis study the first decision regarding delimitation of the research subject based on just preliminary information acquisition is the definition of data center security management. Key concepts are defined further in chapter 3 but based on the results of the number of sources found related to cyber security and information security, data center security management is usually defined as part of information security management. This viewpoint is based on the purpose of data centers being information processing facilities or premises. However, this thesis study is not focused on information security or cyber security management, so the information processing systems, networks and the data produced in data centers are not considered to be in the scope of this thesis study. This decision will delimit research questions, problems, and development tasks to be focused on securing data center facilities and holistic security management processes.

Another delimitation need based on preliminary information acquisition is specifying the possible corporate security and information security management frameworks applied in further part of this thesis study as theoretical framework. There are hundreds of different information security management frameworks, standards, regulations, and guidelines available depending on region and specific industry (Kegerreis et al. 2020, 471). In this thesis the study subject is delimited to Europe so mainly European but also international information security management and corporate security management frameworks are taken into consideration. This regional limitation has an impact on definitions of the key concepts.

Third delimitation need arisen from preliminary information acquisition is regarding evaluation of the defined framework and creating a tool for the evaluation. There are international and local certifications available for information security management systems and data center facilities. This thesis study is not intended to focus on such certifications nor to compete with any existing security management standard. The purpose of this thesis study is to define and provide a holistic data center security management framework and a user-friendly tool to evaluate usability of the applied framework. The need for such tool is commissioned by this thesis study target organization in order to be able to review holistic security management controls in data centers and to find possible vulnerabilities and objects of improvement. To keep this evaluation process as user-friendly as possible, rather than following a defined management system audit process a much simpler informal audit process is needed to apply for the tool.

Through these initial delimitations of this thesis study, two main development tasks are defined:

1. Defining and designing a holistic data center security management framework for European region.
2. Producing a user-friendly tool for evaluating data center security management through the framework.

From traditional research point of view, these development tasks are changed into following research problems or questions and sub-questions:

- What does a holistic data center security management framework consist of in European region?
    a. Can this framework be applied in evaluations?
    b. Does corporate security management framework bring added value for existing data center management and information security management frameworks?
- What does a user-friendly, holistic data center security management evaluation tool consist of?
    a. How can heuristics and heuristic evaluations be applied in production of an evaluation tool?
    b. Does heuristics and heuristic evaluations bring added value for producing such tool?

These research questions and sub-questions are used in later chapters of this thesis report for measuring and assessing the success of study results.

2.3 Research methods and theoretical framework

After defining development tasks and delimitating development subject, the fourth phase of a research-based development process is to establish theoretical framework and to plan approach and methods for the development. Purpose of establishing theoretical framework in research-based development process is to collect all essential information needed for the development including theoretical framework, theoretical models and research results regarding the development subject and objectives. Mind map and concept map are commonly used tools for defining concepts that form the theoretical framework and models. (Ojasalo et al. 2014, 34.) The key concepts used in this thesis study are presented and defined in chapter 3 and theoretical framework in chapter 4.

For being a research-based development process, some research methodology must be included. However, prior to selecting research methods, an approach for development method needs to be defined. As this thesis study is meant to define a new framework and to

produce an evaluation tool as an end product, a constructive research approach is applied. Objective of constructive research is usually to produce a theoretically justified solution for a practical problem and to produce new knowledge. (Ojasalo et al. 2014, 65-66.) Constructive research process resembles the research-based development process but has specific phases and specific objectives in each phase. Constructive research process is presented in figure 2.

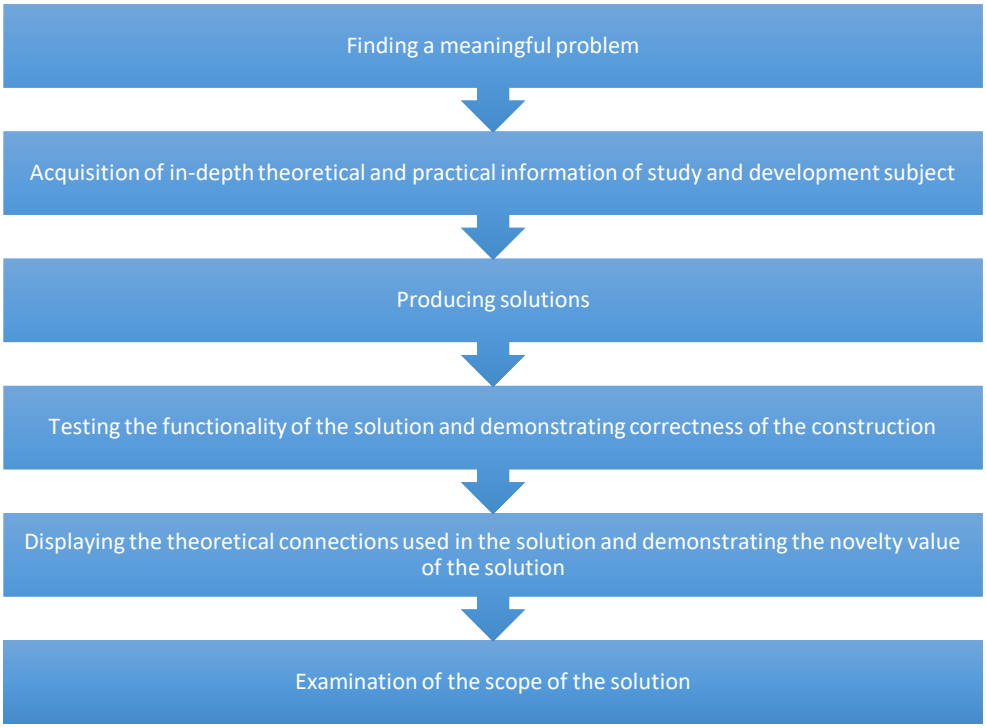

Figure 2: Constructive research process (Ojasalo et al. 2014, 67 according to Kasanen et al. 1991, 301-329).

In the context of this thesis study, first two phases of constructive research process include the same phases as research-based development process phases 1-3 by identifying the problem and acquiring information about the development subject. Phase 3 in constructive research process is including production of the solution and phase 4 testing the produced solution functionality for demonstrating its correctness. Phase 5 contains demonstrating that there is a connection to theories in the solution and that it is bringing a novelty value. Last phase of constructive research process is about examination of other possible use cases for the solution outside research subject such as in another organization. (Ojasalo et al. 2014, 65, 67-68 according to Kasanen et al. 1991, 301-329.) In this thesis study the solution for development tasks are both the framework for holistic data center security management and the evaluation tool. The test of functionality and correctness of the evaluation tool and the novelty value demonstration is included in heuristic evaluation.

Ojasalo, Moilanen and Ritalahti have mentioned that proving the functionality by practical testing is sometimes missing in constructive thesis research reports due to differences in research and research subject organization schedules (Ojasalo et al. 2014, 68). This is the case also in this thesis report as this study scope is delimited. Further testing, demonstration and examination of the solution and its functionality, correctness, novelty value and scope would require another research project outside the resources reserved for this thesis project.

Development method selection for a constructive research vary and multiple different methods are recommended to be used. Traditionally research methodology is divided into quantitative and qualitative methods. Qualitative research methods usually aim to describe real world phenomenon in a comprehensive manner. (Ojasalo et al. 2014, 68, 104.) Qualitative research prefers collecting research data from persons with methods such as interviews, participatory observations, and discursive analysis of documentation. Research subject in qualitative research is selected for the pre-defined purpose of research instead of having a random sample. Research plan may change during a qualitative research process. (Hirsjärvi et al. 2007, 157, 160-161.)

Selection of this thesis study research methods emerged from discourse between the thesis author and the thesis supervisor. It was clear from the beginning of this thesis process that qualitative methodology was to be used but instead of traditional interviews there was a need of ensuring the usability of the defined framework and the end product. Heuristic evaluation was selected to be used as the research method.

Heuristic evaluation is, as described by Nielsen "… a systematic inspection of a user interface design for usability" (1993, 115 according to Mack and Nielsen 1993; Nielsen and Mack 1994). Heuristic evaluation is also called as expert evaluation (Korvenranta 2005, 113). Aim of a heuristic evaluation process is to have persons called "evaluators" to examine an interface, in this thesis study the evaluation tool, to find possible usability problems through an iterative process in parallel with pre-defined usability principles called "heuristics" (Nielsen 1993, 155). This heuristic evaluation method and the process concluded as part of this thesis study is described further in chapter 6.

2.4 Development project publication and evaluation

Fifth phase of a research-based development process is fulfilling the development project and publishing report or multiple reports regarding the development. Again, when comparing to traditional scientific research the publication in research-based development process is not necessarily intended for the scientific community but the communities which may benefit from the results of the development. Publications of a development process include both

written and oral reports and presentations. The final development project report is one part of written publication where results are shared but usually results are also shared during different phases of the development process. (Ojasalo et al. 2014, 46-47.) Hirsjärvi, Remes and Sajavaara (2007, 29-30) remind that writing publications to different target groups or communities require different approach in writing of the publication. This thesis study report is intended to provide new knowledge and new applications by defining the holistic data center security management framework. Main target group could be then data center industry community and security management professionals of different organizations who would have some basic understanding of data center security or security management concepts.

Final and sixth phase of research-based development process is evaluation of the development process and the results although evaluation is part of each development process phase. Final evaluation of success of the development process is typically aimed for the input to the development process, change achieved by or during the development process and the final output of the process. Success evaluation criteria used in research-based development processes are for example relevance, simplicity, usability, applicability, repeatability, and neutrality. Ojasalo, Moilanen and Ritalahti also highlight the importance ethical viewpoints within the development process. (Ojasalo et al. 2014, 47-48.) These examples could all be applied for this thesis study as success criteria, but clear objectives set already for this development process are concerning relevance, applicability, repeatability and especially usability. Evaluation of this thesis study process and reflections are described in chapter 9.

3 Key concepts

By defining key concepts used within this thesis study, further delimitation of the research subject is provided. The key concepts are generated from research subject and objectives. These definitions are used systematically and appropriately throughout this thesis report but are by no means only possible correct definitions when used in other contexts.

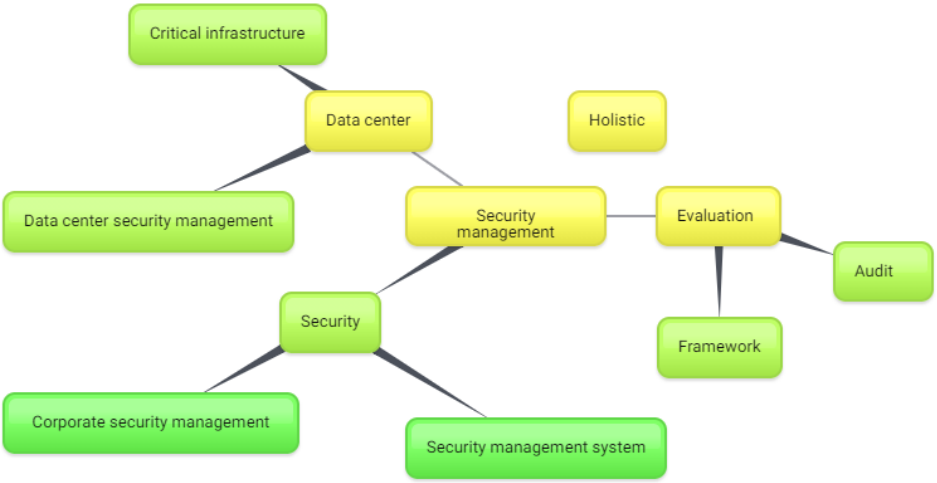

Figure 3: Mind map of key concepts used in this thesis study.

3.1 Data center

Geng (2014, 4) defines a data center simply as an information processing facility but referrers also to such terms as data hall, data warehouse, computer room, server room, hosting facility and co-location. Kegerreis, Schiller, Davis and Wrozek (2020, 107) define data center being a facility "designed to house an organization's critical systems, which comprise computer hardware, operating systems, and applications". Cambridge dictionary refers data center, or data centre as written in the UK, also as a building for "many powerful computers and the systems to keep them running" (Cambridge University Press 2021a). In contrast to the aforementioned, a global research and advisory company Gartner has defined data center as "the department… that houses and maintains back-end IT systems and data store… in one physical place…" (Gartner, Inc. 2021). The difference between these two types of definitions distinguishes clearly; while one definition is regarding data center as a facility for information processing, other regards data center as a collection of information processing systems located in a facility.

In the context of this thesis study, data center is regarded as a facility designed to host information processing systems. This delimits the research subject and objectives to be focused on facilities used for information processing rather than the information processing systems as such. The definition of data center includes supporting infrastructures and facilities for the information processing such as power distribution and required environmental controls.

Data centers can be categorized in many ways. For example, Geng (2014, 4) has categorized data centers by their typical sizes and estimated server volumes, ranging from 19 m^2 and from 1 to 2 server contained server closets to over 465 m^2 and from 800 to over 2000 server contained enterprise-class data centers. A US based Telecommunications Industry Associations standard TIA-942 categorizes data centers according to their usage. According to this, data center can be a privately operated enterprise data centers or publicly used internet data centers, co-location data centers or other service provider data centers. Privately operated enterprise data center refers to a data center operated by a corporation, institution, or agency for their own use. Internet data center refers to a data center operated by "telephone service providers, unregulated competitive service providers and related commercial operators". (ANSI/TIA-942-4 2012, 16.)

Geng also regards the categorization of data center type by the owner of data center and service model, either as in-house data center, hosting data center or co-location data center. Geng defines in-house data centers similarly as previously mentioned privately operated enterprise data centers; "built, owned and operated by the organization itself" (Geng 2014, 47). Hosting and co-location data centers are regarded as business models of data center service providers. These traditionally differ so that hosting data centers provide the data center facility and information processing equipment while co-location data centers, also known as wholesale data centers, provide shared data center facilities for one or multiple different customers and their information processing equipment. (Geng 2014, 47-48.)

As the objective of this thesis study is to define a holistic data center security management framework, the focus in this study is in data center categories defined in this chapter as enterprise-class data centers, hosting data centers and co-location data centers. Delimiting single data closets and rooms will allow review of multiple security management domains.

While information processing systems and the data within data centers are delimited as out of scope of this thesis study, they are however the reason data centers exist and why data centers require security management. To understand protected assets, a brief review of information processing systems as well as basic design principles of support systems and processes in data centers are provided in this chapter.

The size and contents of data centers differ as well as their design. Data center can consist of one or more buildings or it can be a part of a building. Information processing equipment within a data center are usually located in one or more computer room spaces. These information processing equipment can be divided into data processing, data storage and telecommunication equipment and components (SFS EN 50600-1, 9, 14.) Data processing equipment can be referred as servers, data storage equipment as storage equipment and telecommunication equipment as network equipment including cabling infrastructure for

these equipment (Geng 2014, 4; SFS EN 50600-1, 14). Another way for categorizing information processing equipment is defining these as different hardware platforms, such as network and server appliances, blade servers, large-frame processing arrays, large-frame disk arrays and rack-mounted disk arrays. These different hardware platforms are usually mounted in server cabinets except those large-frame platforms which do not fit into standard size cabinets, such as mainframes, supercomputing systems, and tape libraries. In co-location data centers these different hardware platforms and their components can typically be placed to a customer dedicated cage or cabinet within a computer room. Computer rooms also include pathways for power distribution and network cabling either overhead or underfloor, which usually requires a raised floor system within computer room. (Geng 2014, 166-167, 169-170, 177.)

Other data center non-IT infrastructure supporting systems are usually recommended to be located outside computer rooms. These can be located either in separate rooms, different floors or even different buildings and can be dedicated only for the data center purposes or they can support data center as part of infrastructure of a whole building. Supporting infrastructure for data centers include power distribution systems, uninterruptible power supplies (UPS), cooling systems and other environmental control systems for the computer rooms. (Geng 2014, 3-4, 170.) Supporting functions and spaces for data centers include also entrance for data center network cabling and related equipment, entrances for personnel, visitors and outside vendors, control rooms for security, facility and network, workspaces, and offices for data center support staff, loading docks and staging, storage, repair, testing as well as holding or burn-in spaces. Following figure 4 presents an example of a typical schematic diagram of premises containing a data center as presented in EN 50600-1 standard.

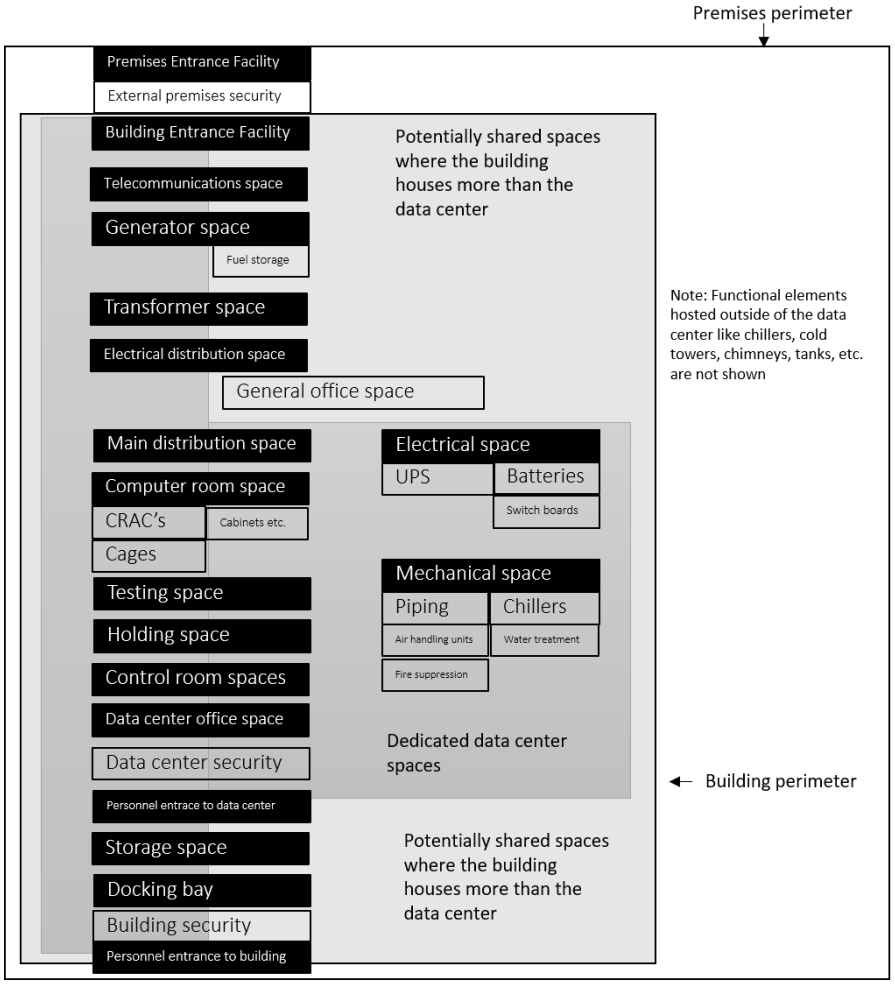

Figure 4: Typical data center premises diagram (SFS EN 50600-1 2012, 16).

Data centers are usually classified based on infrastructure security and availability, which is referring to fault tolerance or redundancy. Most common international data center classification systems are Uptime Institute's tier certification program and Telecommunications Industry Association's tier classification presented in standard TIA-942-A. Similar availability classification and a security classification is also provided in European standard family EN 50600 and international standard family ISO/IEC TS 22237. Principles in these classification systems are similar; the higher the tier class is, between 1 and 4 while 4 being the highest, the more reliable data center infrastructure is. This principle is also followed in other international, regional, and national data center classification systems. (Geng 2014, 9.) EN 50600 and ISO/IEC TS 22237 also include classification systems specifically for data center physical security and energy efficiency enablement (SFS EN 50600-1 2012, 17-21; ISO/IEC TS 22237 2018, 11-15). Usually higher the tier class is, the higher are also initial investments and operating costs for data center. (Geng 2014, 9.) These data center design and classification models are described further within this thesis study in later chapters regarding data center security management frameworks.

Operating a data center requires support personnel, for example a data center manager, a data center facility manager, data center facility engineers and technicians, a data center shipping and receiving clerk, data center security and network operations control personnel. Although this thesis study is not focused on information processing systems, it is worthwhile to mention that the personnel working with the information processing systems can usually work in other locations with remote access and do not necessarily have to be located within the same building as the data center. (Geng 2014, 180.) Even though there has been discussion about so called "lights-out data center" concept which refers to a data center where no personnel are needed, usually information processing systems do need maintenance and replacements for their physical hardware within data centers. Also, security and data center infrastructure personnel are recommended to be located at data center premises, depending on operational requirements and needs. (Judge 2021.)

3.2 Holistic security management

Another important delimitation of this thesis study is related to the definition of holistic security management. Starting with the word security, it is usually defined as "freedom from risk or danger" (Halibozek & Kovacich 2017, 48). In the Nordic languages such as Finnish and Swedish the equivalent terms for security, in Finnish "turvallisuus" and in Swedish "säkerhet", include both definitions of security and safety combined in one word. According to the Finnish Terminology Centre TSK, security usually refers to freedom of intentional dangers and safety to freedom of accidents. (Sanastokeskus TSK 2017, 16.) In this thesis study security is defined as referred by Halibozek and Kovacich (2017, 48) in the context of corporate security "as a process for protecting the business enterprise" from both security and safety perspective. Brooks and Corkill define corporate security "as security that seeks to achieve corporate organizational goals" while also being "embedded in the organization itself" (Brooks & Corkill 2014, 2, 218). Security management is defined by International Organization for Standardization as a management system for security in organizations "to establish policy and objectives and to achieve those objectives" (SFS EN ISO 19011 2012, 17).

Merriam-Webster dictionary defines holism as a method concerning "wholes" or complete systems (Merriam-Webster 2021). A holistic view of data center security management is considering data center security management aspects as a whole and not just for example physical security management of data center facility infrastructure or information security management of information processing systems within data center. Concept of comprehensive security would be referring to similar viewpoint, but comprehensive security is usually used for defining governmental and societal security (Sanastokeskus TSK 2017, 16).

Another concept related to holistic security is converged security which is mentioned also in the first chapter of this thesis report. Security convergence in corporations is not meaning only convergence of physical security, information security and cybersecurity technology but also including risk and threat convergence, functional convergence, vendor convergence, community convergence and educational convergence. For example, risk and functional convergence in corporate security domain refers such risks being included into corporate security which traditionally has been part of corporate risk management function. An example of vendor convergence is a physical security service provider offering information security services, or vice versa, an information security service company providing physical security such as access control services or products. (Wakefield 2014, 246.)

Incorporating all vital elements and aspects of a company and security into security management system is also supported in other corporate security management literature. Cabric (2015, 64) refers to human, physical, technical and information elements as well as procedures, communication, and control. A concept of asset protection is commonly used for example by ASIS International. Asset protection refers to securing and protecting organizations tangible, intangible and mixed assets from all hazards. Protected assets include people, properties, information, reputation, market shares, capital assets and so forth. (ASIS International 2012, 64-65.) Integrated security management and asset protection viewpoints are reviewed further in next chapters of this thesis study report as these are contributing to the holistic data center security management framework.

3.3 Evaluation of a framework

Using the word framework in this thesis study provides yet another delimitation of the study subject and objectives. Framework refers to “a system of rules, ideas or beliefs that is used to plan or decide something” (Cambridge University Press 2021b). The purpose of this thesis study is not to provide a fully defined holistic data center security management system but rather to provide an example of one attempt to define a holistic data center security management concept. If such a management system standard would be created it should include, as referred by International Organization of Standardization (2021) “requirements or guidance to help organizations to achieve specific objectives… across all economic sectors, various types and sizes of organizations and diverse geographical, cultural and social conditions”. This thesis study report does not provide requirements for data centers or guidance for all organizations.

A management system standard can be formally assessed for conformity, or audited, either by an organization itself, organizations users or purchasers or by independent third parties (International Organization of Standardization 2021a). Kegerreis, Schiller and Davis have

defined the differences of a formal and an organizations internal informal audit. According to this definition, formal audits are “performed in a disciplined and thorough manner”, “thoroughly documented and tested, including taking representative samples of data” for presenting any conclusions of the audit (Kegerreis et al. 2020, 12). Formal audit process of a management system usually commits to follow formal auditing guidelines, such as standard EN ISO 19011. This guideline for auditing management systems includes requirements for auditing principles, management of an audit program, performing an audit as well as competence and evaluation of auditors themselves (EN ISO 19011 2012, 3). Organizations internal informal audits can follow more flexible, lighter and less time and resource consuming procedures while holding on to a principle where auditors are not executing controls by themselves. Informal audits can also achieve similar goals as formal audits, such as uncovering possible major risks and promoting internal controls while providing advisory or consultancy to auditees. Kegerreis, Schiller and Davis recommend some basic steps for an informal audit as summarized in figure 5. (Kegerreis et al. 2020, 8-9, 12-13.)

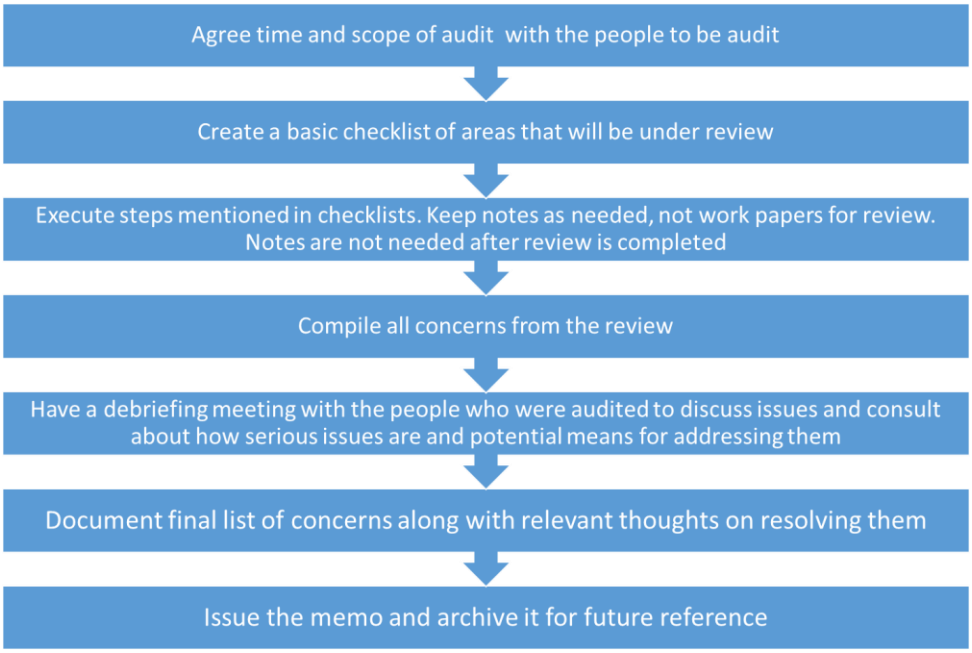

Figure 5: Summary of an informal audit process (Kegerreis et al. 2020, 13-14).

These informal audit process basic steps summarized in figure 5 are fairly self-explanatory and as Kegerreis, Schiller and Davis state ”overly simplistic”; the purpose of this simple process is to “avoid overengineering the process” (Kegerreis et al. 2020, 14). These steps are addressed further in chapter 5 with description of design and production of the holistic data center security management evaluation tool. The reason for using the word evaluation instead of informal audit process is the ambition of the tool to provide as much as value as possible for any possible use case of the tool, both for internal and external use cases for the thesis subject organization. Evaluation is defined by Cambridge Dictionary as “the process of

judging something's quality, importance, or value, or a report that includes this information" (Cambridge University Press 2021c). In the context of this thesis study, evaluation is defined correspondingly as the process and reporting of judging the quality, importance, and value of data center security management while revealing possible topics requiring development.

4 Theoretical framework for a Holistic Data Center Security Management Framework

One of the initial research problems of this thesis study and hypothesis is that a common data center security management framework is yet to be defined. A variety of different security management frameworks do exist as well as data center industry specific frameworks. This thesis study compiles these different frameworks to define a holistic data center security management framework. This chapter includes a review of different selected frameworks from global and European regional aspects. National frameworks are generally delimited from this thesis study to keep the focus of the study in general on global and regional levels. Only exception for this delimitation is considered in the review of corporate security frameworks and the reasoning for this is presented in chapter 4.1.

A common acknowledged principle in corporate security frameworks is that there is no one single correct framework suited for all regions, industries, or businesses. Security management models of different industrial sectors vary due to for example business models and risks. Such differences in security management models can be found for example when comparing health care and telecommunications industries. Both industries share common security management topics such as securing information assets but for example workplace violence is probably not as high prioritized issue in security management within telecommunications when it may be in healthcare industry. (ASIS 2012, 74.) Different industrial sectors may also include sector specific security management regulations on topics which do not occur in any other industrial sectors such as aviation security. Brooks and Corkill define this sector or industry specific area of security management as industrial security. (Brooks & Corkill 2014, 225.)

Cabric also recognizes the need of defining industry specific security management but also presents a company specific approach for defining an integrated industry and company security model. This includes scope of company's services, type and value of company's products, different processes, size and location of company's business, strategy, and brand, just to mention few considerations. (Cabric 2015, 59.) Halibozek and Kovacich for example include protection of governmental assets and even state secrets within corporate security management in all industries and companies doing business with nation-state actors such as

government agencies but also because nation-state security events may impact on different companies in local or global markets. Halibozek and Kovacich mention that almost all nation-state actors have national security programs to protect for example nationally critical information and products. (Halibozek & Kovacich 2017, 339, 341-342.) Another research question could be what kind of value these industry specific security management models may bring for different companies and organizations, but this is not explored further in this thesis study.

When considering data center industry specific security management models, Geng mentions that data center operations adhere to international standards as presented in table 1.

Standard name	**Standard number/series**
Quality management	ISO 9000
Environmental management	ISO 14000
Occupational Health and Safety management	OHSAS 18001
Social responsibility	ISO 26000
Information security management	ISO 27001
Energy management	ISO 50001
Sustainable events	ISO 20121

Table 1: International standards applicable for data center operations (Geng 2014, 11).

Confederation of Finnish Industries have also referred to ISO standards applicable for corporate security. These are presented in table 2.

Standard name	**Standard number/series**
Quality management	ISO 9000
Risk management	ISO 31000, 31010
Supply chain security	ISO 28000
Continuity management	ISO 22301
Environmental management	ISO 14000
Energy management	ISO 50001
Asset management	ISO 55000
Occupational Health and Safety management	OHSAS 18001
Social responsibility	ISO 26000
Energy management	ISO 50001

Table 2: International standards applicable for corporate security according to Confederation of Finnish Industries (EK 2016, 14).

Similarities of standards listed in tables 1 and 2, while referring to different use cases, implicates that these management system standards are meant for general use purposes and are applicable in different settings. A holistic data center security management framework should include compliance to these international management system standards as they are

referred in both data center related sources and security management related sources. Although reaching compliance and utilizing these standards does not necessarily require formal external audit or certification, external audit can provide additional assurance of having effective controls in use and also provide visibility of possible gaps in data center security management (Kegerreis et al. 2020, 104).

As mentioned in the first chapter of this thesis report, data centers are regarded as critical infrastructure for societies and businesses. Critical infrastructure in societies can be defined as functions that are vital or essential to society's economics, social well-being, security, or safety. Disruption in critical infrastructure can therefore have severe impacts on societies. (OECD 2019.) In private organizations critical infrastructure can be defined in similar manner as infrastructure or resources supporting critical business operations. Any disruption in organizations critical infrastructure could have severe impact on business. (Information Security Forum 2008, 3, 7.) Critical information infrastructure is defined as "the information systems and networks… of other critical infrastructures…" in societies and businesses (OECD 2019a, 9). However, critical infrastructure and critical information infrastructure protection frameworks are not included as sources of this thesis study as the preliminary information acquisition process revealed that these include such processes and principles that are included within corporate security, information security and data center frameworks. Therefore, critical infrastructure and critical information infrastructure protection frameworks would not bring any additional value to this study.

For example, critical infrastructure protection framework recommendations of Information Security Forum include risk assessment processes and increasing resiliency of the critical information infrastructure. This recommendation does highlight the importance of protection of such information systems and equipment that are used in factories and production plants, for example process control systems or supervisory control and data acquisition systems known also as SCADA. (Information Security Forum 2008, 29.) OECD report from 2019 recommend national critical information infrastructure frameworks and policies to be further defined and improved to include such processes as public-private co-operation and holistic approach for national digital security risk management (OECD 2019a, 14-15). Based on these international recommendations such co-operation with governmental parties should be included in a holistic data center security management framework. In the context of this thesis study these recommendations for critical infrastructure protection reveal that there is a need for defining a holistic data center security management framework and a tool for supporting data center industry to improve the protection of data centers in a holistic manner.

Following sub-chapters include short reviews of corporate security frameworks, information security frameworks and data center industry frameworks. Each sub-chapter contains both

global and EU regional frameworks. Last sub-chapter compiles these frameworks into one holistic data center security management framework.

4.1 Corporate security frameworks

No internationally standardized corporate security framework was found during this thesis study. One working group in International Organization for Standardization is developing a standard for protective security ISO/CD 22340 which is named as “Guidelines for establishing an enterprise protective security architecture and management framework” (ISO/TC 292 Online 2021). As this standard has not been published yet, this thesis study is not taking this standard into further consideration. Instead, two proposed frameworks are included. These are the integrated corporate security framework proposed by Brooks and the corporate security model proposed by Confederation of Finnish Industries. Although these both frameworks differ from their structure and purpose, they may complete each other.

These two frameworks share common basic principle of providing structured overview of different domains or themes of corporate security. Corporate security model of the Confederation of Finnish Industries includes further examples of more detailed contents for each domain while Brooks’ integrated corporate security framework is describing security domains only in general level. The integrated corporate security framework can be considered as a global framework whereas the corporate security model is representing a national framework. No European regional corporate security framework sources were found during initial information acquisition of this thesis study.

Integrated framework of corporate security

Integrated framework of corporate security is a result of David Brooks in his study of defining corporate security body of knowledge. Brooks produced this integrated framework by reviewing existing frameworks to develop the integrated framework and then by testing it through psychometric multidimensional scaling knowledge mapping. Brooks resulted in his study to define a two-layered integrated framework of corporate security consisting of 13 different operational knowledge categories or functions. Level one functions represent the core categories and level two allied or supporting disciplines. These functions may be overlapping as they are not defined as strictly hierarchical. Framework also includes three levels of governance: operational, management (or tactical) and strategical. (Brooks 2012, 2-4, 6, 10, 12.)

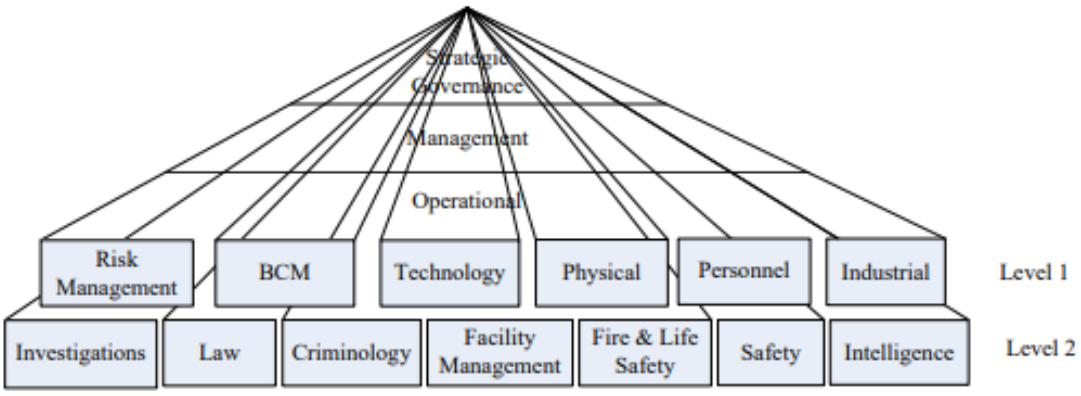

Figure 6: Integrated framework of corporate security (Brooks 2012, 10).

Integrated framework of corporate security does not provide much further explanation of the contents of these different functions. For example, technology function is compiled from information technology, computing, and security technology such as IT networks, access control and intrusion detection systems. Business continuity management or BCM consists of crisis management, emergency management and business recovery. (Brooks 2012, 6, 9-10.)

Corporate security model

Corporate security model published by the Confederation of Finnish Industries is created within businesses to outline and review a corporation's security framework. Corporate security model is created for companies and organizations of different sizes and it is made to be applicable for also international operating environment. The model consists of nine different sections or functions which may be overlapping as presented in figure 7. All sections may not be equally significant for all companies and therefore organizations should define their key sections or functions and the necessary measures within based on local settings, legislation, and risks. (EK 2016, 2-4.)

In the center of the model is the proposed aim and value of corporate security as providing business continuity, security, and compliance. The different security functions are impacted by security management and security culture of the company as well as company's risk framework and overall strategy. Model also includes principles of continuous development by PDCA-cycle while referring to continuous planning, execution, evaluation, and development of corporate security functions. (EK 2016, 4.)

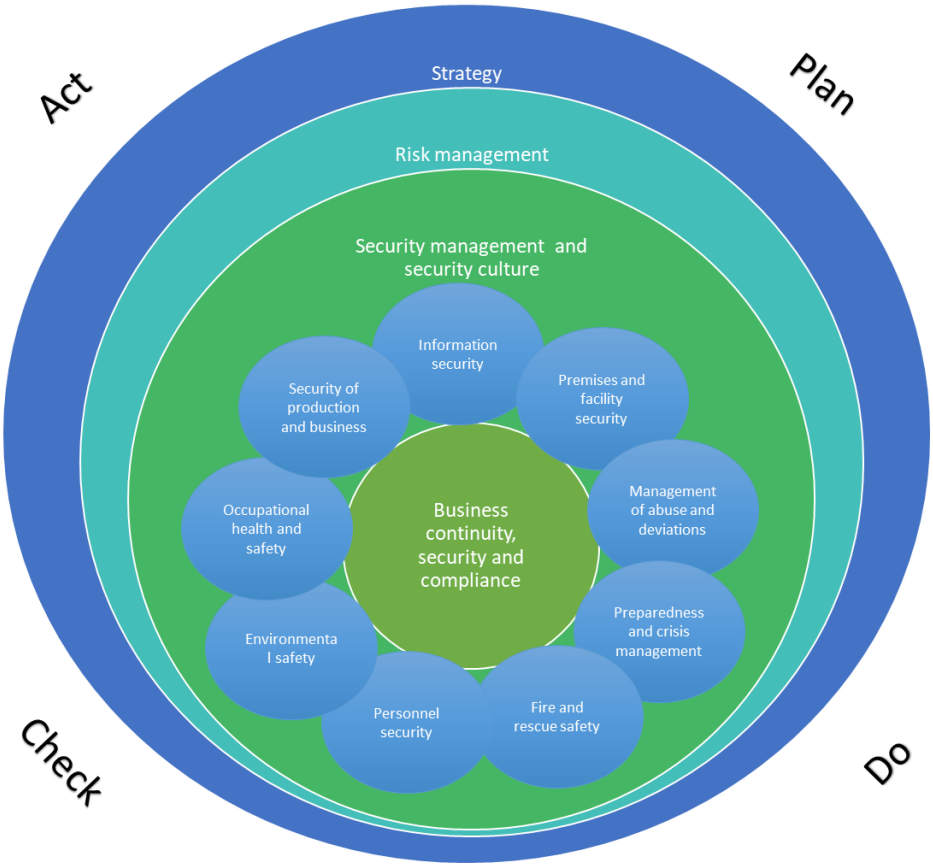

Figure 7: Corporate security model by Confederation of Finnish Industries (EK 2016, 4).

Corporate security model is also presented in a matrix where different functions cross each other and through security management, communications, audit, and development functions as well as co-operation with stakeholders (EK 2016, 5). Model includes examples of the contents of each sector or function with descriptions of the main policies, processes, and procedures. For example, information security is described to consist of securing confidentiality, availability, and integrity of information assets with six main processes: evaluation of the importance of information, classification and processing of information, administrative information security, privacy and protection of privacy, technical information security, securing continuity of systems and processes. Each process is provided with examples of sub-processes or procedures such as under information classification and processing following three procedures are mentioned: classification methods, processing instructions and building of classification system. (EK 2016, 10.)

Both the integrated framework of corporate security and the corporate security models share similar but not identical functions of sectors of security management. Although corporate security model provides more of the contents of these different functions, they are just examples. One clear area corporate security model is missing compared to integrated framework of corporate security is intelligence. Brook's integrated framework of corporate

security is based on his research which is including ASIS International body of knowledge security model which itself includes function or sector of competitive intelligence. Based on this security model and expert discussions Brooks has defined this as security intelligence but does not provide further definitions for it in his publication. (Brooks 2012, 6, 10.) Integrated framework of corporate security includes different levels of governance and divides core security functions from supporting functions whereas corporate security model does not divide security functions. Integrated framework of corporate security is not explained in Brooks' study any further to include security culture or continuous development whereas corporate security model includes these principles.

ASIS International, formerly known as American Society for Industrial Security, highlights three basic underlying principles which should be found in all asset protection strategies or as considered in this thesis, corporate security models or frameworks. These are the concepts of the five avenues to address risk, balancing security, and legal consideration, and the five D's. Five avenues to address risk refers to risk management principles or strategies of avoiding, transferring, spreading, reducing, and accepting risks. Balancing security and legal considerations refer to relying on legal measures such as patents or trademarks to instead of taking additional security measures to protect the assets or vice versa. Usually both security and legal measures are needed in a balanced manner instead of selecting just one of the mentioned considerations as the only measure. The five D's refers to methods of protecting the assets with security approach of deterring, denying, detecting, delaying, and destroying any adversaries or perpetrators threatening the protected assets. (ASIS International 2012, 70.) Some of these principles can be included both in the integrated framework of corporate security and in the corporate security model. For example, five avenues of risk and the balancing security and legal considerations can be included but the five D's is perhaps not applicable for all functions such as safety related functions. These three underlying principles could however be included in relevant parts of a corporate security framework.

Halibozek and Kovacich have also defined some primary corporate security functions as part of corporate asset protection program which can be considered as similar security areas of functions as defined in the integrated framework of corporate security and the corporate security model. These functions include administrative security, physical security, personnel security, security education awareness and training program, fire protection, contingency planning, investigations, government security, information security, executive protection, and event security. (Halibozek & Kovacich 2017, 163-164.) Cabric has defined 10 core security elements of corporate security as mentioned in table 3.

Core Security Elements of Corporate Security
Physical and technical security of people, processes, products, and assets
Safeguarding the reputation of the company and the brands
Information security
Security governance
Crime prevention and detection
Anti-fraud
Investigations
Nonfinancial risk management
Business continuity management and disaster recovery

Table 3: Core security elements of corporate security (Cabric 2015, 23)

Halibozek and Kovacich and Cabric all provide further definitions of these functions as well as principles and best practices to be included within corporate security or asset protection program. The functions or elements of corporate security management listed can again be interpreted to be included to the integrated framework of corporate security and to the corporate security model. The consistency of different functions included to corporate security framework within these reviewed models and frameworks imply that there are common security functions which are and perhaps should be included in a holistic data center security management framework. These reviewed models and frameworks do not provide exact description for the contents of security functions. When comparing to standardized management systems, corporate security framework should include policies, principles, and procedures. The corporate security model gives some examples of all these management system criteria.

Applying these reviewed corporate security frameworks directly to data center security management does require further review of industry specific security issues and ultimately company specific definitions for creating a fully functioning company specific security management model. This thesis study does not however include company specific definitions but instead focuses on defining data center industry specific framework. Industry specific review continues in next sub-chapters.

4.2 Information security management frameworks

As information processing facilities, data centers are naturally considered to be in the interest from information security point of view. All corporate security frameworks and models reviewed in last chapter suggest information security as one of the core sectors or functions of corporate security, although Brooks' integrated framework of corporate security considers information security being part of technology function (Brooks 2012, 10). Information security especially in data centers can be defined as part of the industry specific area of security management.

Information security is usually defined as protecting the confidentiality, integrity, and availability of information in all possible forms such as written, spoken, or electronic. This definition of confidentiality, integrity and availability is also often abbreviated as the CIA-triad. Another way of defining information security could be a condition where information security risks are managed. (Sanastokeskus TSK 2017, 10.) With these definitions it is understandable why securing data centers can be included as part of information security function. Although data centers provide physical information security measures for information processing systems within data center, the information processing systems used to operate data centers should also be in the scope of information security function in corporate security framework.

Information security frameworks vary by region and industry and there are several global information security management standards in use such as before mentioned ISO 27001 (Kegerreis et al. 2020, 462). Information security is also highly regulated sector of corporate security so there are multiple local and regional frameworks and regulations. As an example of global information security management framework this chapter includes a short review of international ISO 27001 standard. Rather than reviewing of any national industrial security program operating manuals this thesis study contains as an example of a regional information security management framework in Europe a short review of the European Union Council decision on the security rules for protecting EU classified information. This latter review relates to what Halibozek and Kovacich refer in their proposed asset protection program as part of information security function for governmental security (Halibozek & Kovacich 2017, 339, 357).

ISO 27001

International Organization for Standardization first published ISO 27001 information security management standard during 2005 based on previous ISO 17799 standard, which in turn was based on British Standard 7799 (Kegerreis et al. 2020, 462). According to a survey done 2017 there are over 39 000 organizations with ISO 27001 certification and almost 37 percent of these organizations are from Europe (Kegerreis et al. 2020, 464). ISO 27001 is part of ISO 27000 standard family which includes standards for information security management system (ISMS) requirements, certification body requirements and additional requirement frameworks for industry sector specific implementation of information security management systems (ISO/IEC 27000 2018, 18). ISO 27000 standard family does not include any data center industry specific implementation guideline but for example ISO/IEC 27009 standard includes general requirements for any specific industry sector implementation. Also, ISO/IEC 27011 standard includes guidelines for implementing information security controls for telecommunications

organizations and ISO/IEC 27017 includes guidelines for cloud services. (ISO/IEC 27000 2018, 20, 23.) These industry sector specific guidelines could be applied in data centers hosting such services, but they are not in the scope of this thesis study.

What ISO 27001 standard contains is requirements for establishing and implementing, maintaining, and continuously improving information security management systems. Standard includes requirements for defining the context and scope of ISMS, requirements for leadership commitment, policy and organization of ISMS, requirements for planning, supporting and operating ISMS processes. Standard also includes requirements for evaluating performance evaluation of ISMS and requirements for improvement activities of ISMS. ISO 27001 standard includes annex describing ISMS controls and control objectives in detail. (ISO/IEC 27001 2013, 1-10.) Control is defined in ISO 27000 as a measure aiming to modify risk, including processes, policies, devices, practices, and other possible actions (ISO/IEC 27000 2018, 3). Headlines of controls described in ISO 27001 annex A are listed in table 4.

ISO 27001 control headlines
Information security policies
Organization of information security
Human resource security
Asset management
Access control
Cryptography
Physical and environmental security
Operations security
Communications security
System acquisition, development, and maintenance
Supplier relationships
Information security incident management
Information security aspects of business continuity management
Compliance

Table 4: Headlines of ISO 27001:2013 controls (ISO/IEC 27001 2013, 10-21).

On top of example objectives, each control headline includes one or more sub-controls with further description of the requirements for a process related to each control (ISO/IEC 27001 2013, 10-22). When comparing these controls to security functions presented in the integrated framework of corporate security and corporate security model, some similarities and overlapping functions can be found. For example, overlapping control headlines and functions could be personnel and human resources security, incident management and investigations, business continuity and physical security. The difference of these may be that information security management system could be focused on these functions mainly from information security point of view when corporate security frameworks or models would consider these functions from overall corporate security point of view. However, ISO 27001

standard provides detailed requirements and guideline for the controls or functions whereas integrated framework of corporate security and corporate security model lacs detailed control or process descriptions. ISO 27001 can therefore be considered as complementing a holistic data center security management framework.

EU Council decision on the security rules for protecting EU classified information

Council of the European Union has published a decision on protecting EU classified information during 2013 “in order for the (EU) Council to be able to work in all areas which require the use of EU classified information” or EUCI (Council of the European Union 2020). The decision contains “basic principles and minimum standards” for “a comprehensive security system to protect” EUCI (Council of the European Union 2020). The principles and standards described in the decision is required to be applied for EU Council, its General Secretariat, and all respected European Union member states when handling EUCI. The rules contain measures or controls for personnel security, physical security, management, and assurance of EUCI, protection of EUCI handled in communication and information systems, industrial security, and the process of exchanging EUCI with any third states or international organizations. Each above-mentioned article of the decision describing principles for each sector or function of security management include also further description of the minimum standards or requirements for the detailed processes of these functions in separate annexes. (Council of the European Union 2013.) For example, protection of EUCI handled in communication and information systems (CIS) principles and minimum standards defined in EU Council decision annex IV contain topics or headlines listed in table 5.

EUCI information assurance CIS principles
Security risk management
Security throughout the CIS life cycle
Best practices
Defence in depth
Principle of minimality and least privilege
Information assurance awareness
Evaluation and approval of IT-security products
Transmission within Secured and Administrative Areas
Secure interconnection of CIS
Computer storage media
Emergency circumstances

Table 5: Information assurance principles in protection of EUCI handled in CIS (Council of the European Union 2013, 27-30).

Although this EU Council decision is regarded as regulatory framework just for protecting European Union Classified Information, it could be regarded as comprehensive security system or framework also in corporations in such industries where EUCI is handled. Again, similarities can be found when comparing EU Council security rules with both the integrated framework of corporate security and the corporate security model. For example, physical security and personnel security functions can all be found within these frameworks as well as in ISO 27001 standard. Based on this short review and comparison, embedding this EU Council decision principles into a holistic data center security management framework can provide additional value even if ISO 27001 compliant information security management system is in use but mainly if the subject organization is included in handling of EUCI. This thesis study considers both ISO 27001 and EU Council decision on the security rules for protecting EU classified information to be included in the holistic data center security management framework just to have an example on how these different frameworks could complement each other and the corporate security frameworks. Further review and comparison to define the differences and value of these information security management frameworks would require further research outside this thesis study.

4.3 Data center frameworks

This chapter includes short reviews of such frameworks and standards that are used within data center industry. Reviews include overall descriptions of the frameworks and standards but also possible security management related contents within these. Compared to reviews in previous chapters, the frameworks and standards presented in this chapter are not focused on security management nor any specific sector or function of security management. The frameworks and standards presented are mainly focused on data center reliability and redundancy which can be interpret as part of availability in the information security CIA-triad.

International data center industry standards reviewed in this chapter are the Uptime Institute's Tier standard and Telecommunication Industry Association's ANSI/TIA-942 standard. Regional European standard selected for this review is EN 50600 standard by European Committee for Electrotechnical Standardization. Another regional data center framework in Europe, the European Union Code of Conduct for Data Centres Energy Efficiency, was reviewed and included as source of this thesis study but delimited out of this study as this framework is heavily focused in energy efficiency and not complementing other frameworks from security management point of view (European Commission 2021).

Tier standard

Uptime institute, a private advisory company based in US, has created the Tier Classification System and published it in mid-1990's for owners and operators of data centers to evaluate data center performance or uptime of data center infrastructure. Tier standards are divided between topology standard for design and construction of Tier classified data centers and operational sustainability standard for Tier classified data centers. (Stansberry 2021; Uptime Institute 2021.) Tier standards are globally popular in data center industry, either used as a guideline or as a certification. There are more than 1700 certifications in over 98 countries issued by Uptime Institute for Tier standards in different kind of data centers. In European region there are about 300 Tier standard certifications in data centers. (Uptime Institute 2021a.) Tier standards do not include specific guidelines on how to implement the topology or operations. The Tier Classification System is based on four performance level requirements presented in Tier Standard Topology as described in figure 8.

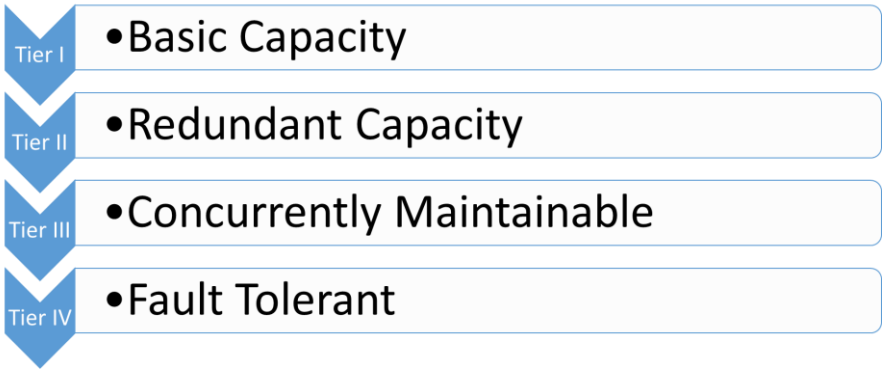

Figure 8: Tier Classification System (Stansberry 2021).

Each of the four data center infrastructure performance level represent the result of the topology selected. Each higher performance level or Tier includes the performance characteristics of the lower levels. Tier 1 includes basic dedicated data center infrastructure such as uninterruptible power supply or UPS, cooling system and an engine generator enough for the IT capacity needed. Tier 2 has the same infrastructure and more than Tier 1 but also with the difference of having redundant components which activate in case of any component failures. Tier 3 concurrently maintainable refers to a data center infrastructure which does not require a shutdown in case any components are replaced or maintained so that it would impact IT production. Tier 4 includes all previous features but is also fault tolerant for example if there are any failures in infrastructure distribution paths, such as power feed or cooling. Also, in Tier 4 performance level there are several independent and physically isolated data center infrastructure systems. The physical isolation of data center infrastructure systems and components refer to also fire compartmentalization. (Uptime Institute 2021b; Stansberry 2021.)

Data center operational effectiveness is standardized by Tier Standard Operational Sustainability. Compared to topology standard, operational sustainability includes three performance levels: bronze, silver, and gold. These three levels can be reached within all four Tier topology levels, so they are not bound to each other. Each level of operational sustainability covers five categories of data center operations as presented in table 6. Basic principle in bronze level is that there is room for improvement although the bronze certification is achieved. Silver level refers to operational sustainability being close to fully compliant but there is still some room for improvement. Gold level would mean that data center is managed and operated with its full potential. (McClary 2017; Uptime Institute 2021c.)

Key operational behaviors
Planning, coordination, and management
Staffing and organization
Training
Operating conditions

Table 6: Key behaviors of the operational sustainability certification (Uptime Institute 2021c).

Tier Standard for Operational Sustainability includes management guidelines and management requirement for data centers in different Tier levels. These do contain for example policies, principles, and processes for the five categories, just as any management system framework. Operational sustainability is including considerations related to security management frameworks, such as natural and man-made risks related to data center location, data center staffing and organization, data center premises design characteristics. (Datacenter Dynamics 2010.) While Tier Standard Topology does not include much security management related domains, the Tier Standard for Operational Sustainability does. These considerations should be included in a holistic data center security management framework as they represent industry specific best practices, but alone they may not provide full picture of data center industry specific security functions.

ANSI/TIA-942

Telecommunications Industry Association or TIA, a non-profit corporation based in US, has published Telecommunications Infrastructure Standard for Data Centers ANSI/TIA-942. This standard describes minimum requirements of data center architecture and topology but also provides a four-level rating in similar manner as Tier Standard referred in figure 8. (TIA 2021; TIA 2021a.) ANSI/TIA-942 can be used as a guideline but conformity can also be audited and

certified for different rating levels. There are over 140 ANSI/TIA-942 certified data centers globally of which 15 are located in European region. (TIA 2021b.)

A revision of the standard from 2012 named as ANSI/TIA-942-A contains the requirements of data center building design, cabling system infrastructure, telecommunication spaces design and topology, cabling systems and pathways and redundancy considerations. This standard includes also informative guidelines as annexes for previously mentioned considerations but also for data center location selection and design examples. (ANSI/TIA-942-A 2012, 7-12.) Design and topology requirements for computer rooms include security and safety considerations such as location, structures, access control, lightning, signage, fire protection, water infiltration prevention, seismic and vibration protection (ANSI/TIA-942-A 2012, 39-43). Also, as an example of security and safety considerations in the standard, cabling pathway requirements include security requirements and cabling requirements include fire safety or fire-rating requirements. (ANSI/TIA-942-A 2012, 56, 58.) The infrastructure guidelines in annex F, which is not considered to be part of the standard and certifications, include four level Tier classification for not only data center infrastructural systems such as cooling and power distribution but also for example architectural and structural considerations. Also, multiple physical security considerations are included such as layered perimeter protection, access control, entries, and emergency exit. (ANSI/TIA-942-A 2012, 84, 90-95.) Latest revision of ANSI/TIA-942 was published 2017 as ANSI/TIA-942-B and while the security considerations did not change much, a reference to ANSI/TIA-5017 was added which contains physical security considerations for telecommunication cabling pathways and spaces (Jew 2017, 27, 37).

ANSI/TIA-942 standard does not include data center operations or management requirements as such within the standard. However, the guidelines for Tier ratings in annex F as well as the design and topology requirements suggest some recommendations for data center security management. For example, the guideline for architectural Tier classification set requirements on the level of protection against man-made and natural intentional and accidental events to be “additional minimal protections” or “specific and in some cases redundant protection against such events” (ANSI/TIA-942-A 2012, 84). More precise controls are defined in the same annex as guidelines, for example physical security staffing requirements vary from having no requirement in Tier 1 level to having 24/7 basis security staffing in data center with spare personnel for different tasks in Tier 4 level (ANSI/TIA-942-A 2012, 93). These guidelines in the annexes can be considered as best practices for data center industry security functions but as the guidelines are not exactly part of the ANSI/TIA-942 standard or certifications the guidelines may not be generally implemented and thus these controls may not be commonly applied. A holistic data center security management framework should still include similar classification with these best practices.

EN 50600

European Committee for Electrotechnical Standardization has created EN 50600 series of European standards for data centers as requirements and recommendations. EN 50600 is not available to use as certification in the way that previously presented Uptime Institute's Tier standards and ANSI/TIA-942 are, but EN 50600 can be used in third party audits to assess conformity towards the requirements set in EN 50600 (Future-tech 2020). Therefore, there is no reliable data publicly available regarding prevalence of the use of EN 50600 standard within data center industry. However, some evidence of the prevalence of EN 50600 is provided by International Organization of Standardization creating an international data center standard family ISO 22237 based on EN 50600. ISO 22237 follows the same standard structure as EN 50600 and many of the standards within ISO 22237 standard family are not published during this thesis study timeline. Although EN 50600 is a European standard it is applicable globally. (Elliot 2020.)

EN 50600 standard series consists of multiple data center standards ranging from data center building constructions to energy reuse and management. EN 50600 series standards publicly available during this thesis study are presented in table 7.

EN 50600 standards
EN 50600-1:2019 Part 1: General concepts
EN 50600-2-1:2019 Part 2-1: Building construction
EN 50600-2-2:2019 Part 2-2: Power supply and distribution
EN 50600-2-3:2019 Part 2-3: Environmental control
EN 50600-2-4:2015 Part 2-4 : Telecommunications cabling infrastructure
EN 50600-2-5:2021 Part 2-5: Security systems
CLC/TS 50600-2-10:2021 Part 2-10: Earthquake risk and impact analysis
EN 50600-3-1:2016 Part 3-1: Management and operational information
EN 50600-4-1:2016 Part 4-1: Overview of and general requirements for key performance indicator
EN 50600-4-2:2016/A:2019 Part 4-2: Power usage effectiveness
EN 50600-4-3:2016/A:2019 Part 4-3: Renewable energy factor
EN 50600-4-6:2020 Part 4-6: Energy reuse factor
EN 50600-4-7:2020 Part 4-7: Cooling efficiency ratio
CLC/TR 50600-99-1:2020 Part 99-1: Recommended practices for energy management
CLC/TR 50600-99-2:2019 Part 99-2: Recommended practices for environmental sustainability
CLC/TR 50600-99-3:2018 Part 99-3: Guidance to the application of EN 50600 series

Table 7: EN 50600 standard series standard titles (CENELEC 2021).

EN 50600 standard series provides a broad guideline for both data center commission and operation. Like Tier Standards and ANSI/TIA-942, EN 50600 series include classification system for data center infrastructure but the classification system is divided between availability,

security or protection and energy efficiency enablement classes. Each of these three features consists of four classes which complement each other. Different classes of the three features can be combined so that classification levels can have different combinations. Classification system in EN 50600 is focused on defining requirements and recommendations for data center building construction, power distribution, environmental controls, telecommunication cabling infrastructure and security systems. Classification system also requires a risk analysis which is described in detail in the standard series. Security or protection classification is further divided into four protection subjects including protection against unauthorized access, protection against internal fire, protection against other internal events, and protection against environmental events. Each protection subject has four level of basic protection measures which include such as building construction, protection systems and organizational measures. Further measures for the protection classes are described in relevant EN 50600 standards, for example location and construction specifications in EN 50600-2-1, environmental specifications in EN 50600-2-2, security and protection system specifications in EN 50600-2-5. (SFS EN 50600-1 2012, 17, 19-20.)

EN 50600-3-1 standard includes requirements and recommendations for data center management and operation processes. The aim for the standard and the processes described is to support data center management with resilience, availability, risk management, risk mitigation, capacity planning, security, and energy efficiency on desired and expected level. Data center management processes within EN 50600-3-1 are divided as presented in figure 9. (SFS EN 50600-3-1 2016, 6, 8.)

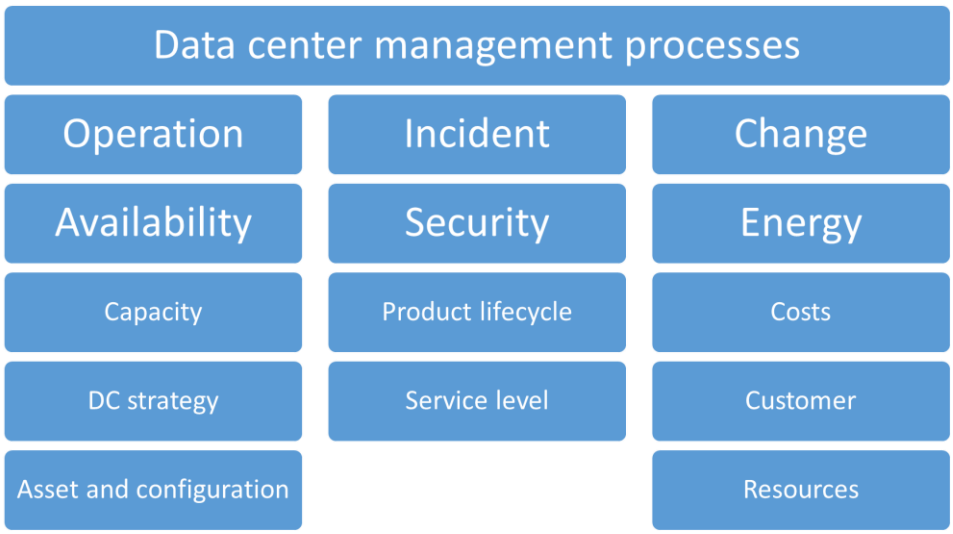

Figure 9: Data center management processes overview according to EN 50600-3-1 (SFS EN 50600-3-1 2016, 8).

The data center management processes defined in EN 50600-3-1 standard include both general process descriptions and acceptance tests for establishing the processes. The

standard also includes informative guidelines as annexes describing process prioritizations, maturity levels of the management processes and normative management process for security systems. (SFS EN 50600-3-1 2016, 2-3.) Security management process includes establishing policies and sub-processes for “monitoring, analysis, reporting and improvement” of data center security (SFS EN 50600-3-1 2016, 26-27). Security management is also including access control related processes and threat and vulnerability assessments (SFS EN 50600-3-1 2016, 26-27). EN 50600-3-1 standard includes also informative guideline for data center security systems and processes such as managing access to data center premises, guarding of data center premises as well as guidance for processes such as visitors and deliveries. Also, processes related to fire suppression systems are included in the guidelines. (SFS EN 50600-3-1 2016, 42-46.)

By comparing the data center frameworks and standards reviewed within this chapter, EN 50600 standard series seems to include the most holistic data center security management process contents. The Tier Standard for Topology does not include much data center security management requirements or guidelines for either design or processes, but the Tier Standard for Operational Sustainability does include such risk and security-based considerations as data center location, building features, data center site policies, organization, training and planning for emergencies, documentation, and access management. ANSI/TIA-942 includes quite detailed requirements and recommendations for data center design with security, safety and risk-based considerations which may result in additional recommendations for data center security management processes. Combining these reviewed data center industry frameworks gives one example on data center industry specific security functions and processes which aim to support and protect data center premises and production.

4.4 Holistic data center security management framework

Geng has mentioned that the design of a data center should be beyond requirements of building codes and standards to protect both data center properties and components against natural disasters and for example terrorist attacks. As an example, Geng mentions that building codes are generally concerning life safety of occupants but not the properties. (Geng 2014, 12.) A recent example of this consideration is a fire of a data center in France which destroyed one data center and damaged others in a campus area consisting of multiple data centers. Uptime Institute gave a comment after this fire and referred to fire system requirements in Tiers to be limited only in fire compartmentalization requirements in Tier 4 as fire safety systems are usually controlled by local building or life and safety codes. (Lawrence 2021.)

Another recent example of considering data center design and management beyond requirements is the COVID-19 pandemic which has required such measures also in data centers that may have not been prepared for before. For example, in lockdown situations supporting facilities for data center personnel to shelter within data center premises for long periods of time such as days or weeks may have been needed in some locations (Korolov 2020). These examples demonstrate that Geng's consideration is valid and that a holistic viewpoint for data center security management is needed to be able to protect or prepare data centers against different kind of unwanted events. No one single existing framework or standard may be enough to reach this goal, although within data center industry the EN 50600 standard family does seem to have the most holistic viewpoint on protection of data centers compared to other industry frameworks. However, even EN 50600 is missing such security management considerations that are included in the corporate security model and the integrated framework of corporate security.

Integrating the previously reviewed data center industry frameworks with information security and corporate security frameworks results in one example of a holistic data center security management framework. These frameworks included and reviewed in this thesis study represent both internationally and locally in European region accepted and used frameworks. There are however multiple other frameworks available internationally and locally. Different results may be reached by altering the frameworks selected for the holistic data center security management framework for example in different regions or industry sectors.

Integration of the previously reviewed frameworks is done by defining different functions of data center security management and the sub-processes within each function. Each function and sub-process contains controls as defined in reviewed frameworks and for this reason they are not described in detail within this thesis study report. Short descriptions of the contents of each data center security management functions are provided in following sub-chapters. Holistic data center security management framework model is presented in figure 10.

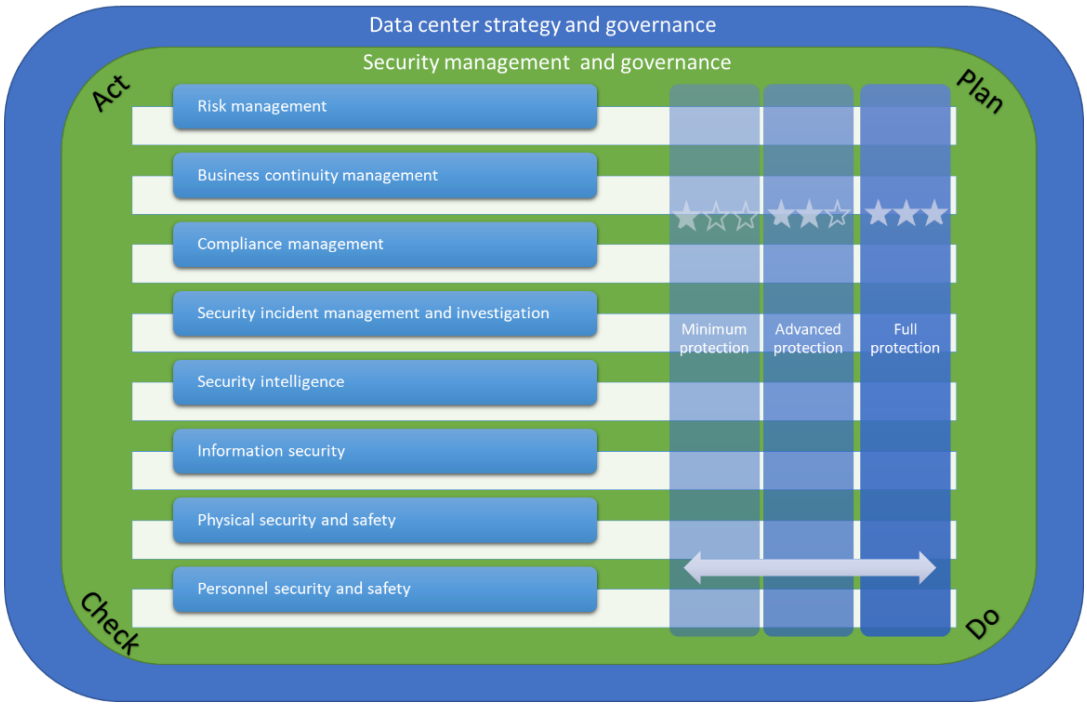

Figure 10: Holistic data center security management framework model.

The model presented in figure 10 is largely based on the corporate security model by Confederation of Finnish Industries and Brooks' integrated security framework of corporate security. One function missing from this model when comparing to the corporate security model is environmental safety. It is not supported to be included in security management processes by other corporate security frameworks or any other frameworks reviewed in previous chapters, except for chemical or hazardous material incident and risk part which is included in this model as part of physical security and safety. Otherwise, the main functions of this model are supported by the definitions of Cabric as well as Halibozek and Kovacich. This further integrated model aims to present data center security and safety functions in a holistic manner but not to provide full taxonomy of all possible security management functions and controls in detail. To support and assure the quality of this framework and all of the processes, so-called Deming cycle or PDCA cycle is implemented and included in all of the functions presented in the model.

The management strategy and governance model of a data center defines data center security management governance. Data center security management consists of governance framework which is implemented through 8 functions consisting of risk management, business continuity management, compliance management, security incident management and investigation, security intelligence, information security, physical security and safety, and personnel security and safety. All security management functions are further classified to have three different levels of controls and protection measures. Instead of presenting four classification levels as in ANSI/TIA-942 and EN 50600, this holistic data center security

management framework model considers only three levels of classification to simplify the approach in further evaluations as this model is intended for larger enterprise-scale data centers requiring higher level of basic security measures. Classification levels are named as minimum protection level, advanced protection level and full protection level. As this framework model is not intended for certification, controls and protection measures in different classification levels could be mixed and used in parallel.

Each function represents set of principles, processes and controls related to a specific sector of security management. Data center security management and governance includes central governance of all data center security management functions by establishing and coordinating all different security functions and the related policies, principles, and processes. Cabric (2015, 76-77) has suggested security governance to also include all rules, standards, guidelines, and instructions and that there are various governance models to select from. Halibozek and Kovacich (2017, 166-167) point out that all the plans, policies and procedures in corporate security context should be established, implemented, maintained, or reviewed at least annually, and applied to not just security department but to the whole organization in the scope. Through this type of governance data center security management would be established in strategical, tactical, and operational levels as suggested also by Brooks' integrated framework of corporate security. Such governance complies with data center industry standards such as EN 50600-3-1 as according to this standard data center should have documented policies and procedures which should be also monitored, analyzed, reported, and improved (SFS EN 50600-3-1 2016, 26). In this framework data center security management and governance also includes management and governance of supplier and supply chain security processes. Each security management function described in next sub-chapters provides means and processes for mitigating risks related to suppliers and supply chains.

4.4.1 Risk management

Risk management function in this framework includes non-financial risk management processes to assess and analyze threats, vulnerabilities and risks which could compromise any data center security management functions. Although this data center security management framework is intended to have a holistic approach, risk management of other data center management functions than security management are delimited as out of scope of this framework model. This approach is supported by corporate security frameworks as well as data center industry and information security standards. For example, risks related directly to change management or financial risks without any impact to security management are not considered to be part of this framework model. Many of the corporate security, information security and data center industry frameworks mentioned in previous chapters refer to ISO

31000 and ISO 31010 risk management standards as guidelines for risk management processes. However, all these frameworks have further considerations to include in risk management processes. For example, insurance policies are covered thoroughly in corporate security frameworks but not considered in information security and data center industry frameworks. The risk management function in this holistic data center security management framework is therefore overlapping with all the other functions individually by setting the basic principles and processes according to ISO 31000 and ISO 31010 standards.

4.4.2 Business continuity management

Business continuity management function of this holistic data center security management framework combines business continuity management, crisis management and emergency management. All previously reviewed frameworks recognize the need for business continuity management processes, and many refer again to international standards such as ISO 22301. Business continuity management consists of such sub-processes as business impact analysis, establishing and implementing business continuity strategies and procedures, exercises, and testing (SFS EN ISO 22301 2014, 15-19). Crisis and emergency management processes are well defined in corporate security frameworks and the different frameworks complement each other. For example, the corporate security model by Confederation of Finnish Industries defines processes of preparing to national emergencies as part of emergency management or emergency preparedness function along with crisis management and continuity planning (EK 2016, 12). The EU Council decision on the security rules for protecting EU classified information also refers to emergency circumstances but defines them as conflicts and war situations (Council of the European Union 2013, 30). Emergency response is also considered in data center industry frameworks, for example as operation of data center infrastructure in emergency situations (ANSI/TIA-942-A 2012, 99; SFS EN 50600-2-5 2016, 20). ANSI/TIA-942 framework considers emergency operation training in its classification system only in the highest requirement class but as part of the training program requirements. For that reason, this holistic data center security management framework would include same topic as part of later described personnel security and safety function and not business continuity function. The business continuity function within this holistic data center security management framework consists of multiple processes and sub-processes which all aim to secure the continuity of data center as a whole.

4.4.3 Compliance management

Compliance management function in this framework is including identification, evaluation and monitoring compliance and conformance of data center security management functions with applicable legal, regulatory, and contractual requirements, industry best practices and data center organizations own policies. Compliance management function also contains functions which Halibozek and Kovacich have defined as government security whether data center is used for governmental purposes or not, as even privately owned data centers are in many countries considered as critical infrastructure. Evaluation and monitoring of the requirements, best practices and policies includes for example audits and management reviews. All frameworks reviewed in previous chapters include guidance for processes of managing regulatory and standardized security requirements, but in general they are not included in classification systems. This holistic data center security management framework however does contain classification of compliance management processes in the three protection levels to support improvement activities towards better management of security compliance. Minimum protection level includes identification, evaluation, and monitoring of compliance towards legal and contractual requirements whereas advanced protection level also includes industry best practices, other regulatory requirements and organizations own policies. Full protection level contains also governmental security functions and certifications or conformity assessments towards for example standards and frameworks mentioned in this thesis report.

4.4.4 Security incident management and investigation

Security incident management and investigation function is combining incident management processes from information security and data center industry frameworks but also non-financial internal investigation processes. Security investigations and interviews related to personnel security clearance or background screening are considered as part of personnel security and not as part of this investigative function. Financial audit is delimited from this function. Security incident management processes covered in this holistic data center security management framework include such sub-processes which are referred in standards EN 50600-3-1, ISO 22301 and ISO 27000 standard family. These include for example security and safety incident reporting, response, warning and communication, collection of evidence and other forensic activities, recovery of normal operation and learning from incidents. These are further combined with internal investigation processes such as conducting interviews, sealing of incident or crime scenes and cooperation with law enforcement. So-called whistleblowing function and processes are included also in this security incident and investigation function. None of the classification systems in data center industry frameworks reviewed in previous

chapters include classification of incident management processes. Again, this holistic data center security management framework does however contain some classification of security incident and investigation processes to support improvement possibilities. Both minimum protection level and advanced protection level include the security incident and investigation processes described above. Full protection level contains certifications or conformity assessments towards security incident management standard ISO 27035 and whistleblowing management standard ISO 37002 which is not published yet during writing of this thesis study report (International Organization of Standardization 2021b; ISO/TC 309 2021).

4.4.5 Security intelligence

Security intelligence function emerges from Brooks' integrated framework of corporate security and is also supported by other corporate security frameworks such as proposed by Cabric. Intelligence function in Brooks' model refers to competitive intelligence while Cabric refers to security threat and business information collection and processing (Brooks 2012, 6; Cabric 2015, 71). Intelligence functions are not considered in other frameworks reviewed in previous chapters although continuous awareness of threats and vulnerabilities are considered both in corporate and information security frameworks. The purpose of including security intelligence function as part of holistic data center security management framework is to provide support to all data center security management functions with relevant, timely and useful information for new and reoccurring threats, risks, and events. Competitive or business intelligence is not included in this framework as it is not considered in any other frameworks reviewed in this thesis study.

Cabric includes various information sources to information collection process such as global and national information sources as well as official and unofficial sources within the organization (Cabric 2015, 71-73). Data center operational information is also considered as information source in this holistic data center security management framework. EN 50600-3-1 standard refers to collecting information related to data center operation and security management such as data center deliveries and visitors as well as different type of alarms and records in technical security and safety systems (SFS EN 50600-3-1 2016, 11, 15). Data center strategic and operational information can also relate for example to security and safety of data center location. Information processing includes reporting of upcoming threats, risks, and events to organizations management with threat or risk mitigation proposals on regular basis and whenever needed (Cabric 2015, 76).

As the security intelligence function and processes described are not considered in any reviewed data center industry classification systems, the minimum protection level of this holistic data center security management framework is not including such function. Advanced

and full protection levels include security intelligence function as proposed. The sources selected for this thesis study are not covering security intelligence processes extensively, which could imply that it is not usually included in data center security management processes and it would require further research.

4.4.6 Information security

Information security function in this framework is referring to securing information processing functions within data center as well as securing information processing systems used to operate data center such as security systems, computerized maintenance management systems (CMMS), data center infrastructure management (DCiM) systems, building management systems (BMS) and other supervisory control and data acquisition (SCADA) systems (Geng 2014, 11). Of the information security frameworks reviewed in previous chapters ISO 27001 standard provides processes included in this information security function. Some of the processes included in ISO 27001 standard are included in other data center security management functions such as human resource security, physical and environmental security, security incident management, business continuity and compliance management.

Privacy related processes are not included in this holistic data center security management framework as protection of personal information can be considered as part of protection processes of all information, although there are specific considerations and regulations such as GDPR impacting the processes. In European region, GDPR may be applied to data center management processes as personal information is very likely handled, but it can be argued whether it should be managed as part of data center security management processes or not. Some of the frameworks reviewed during this thesis study included privacy protection related processes and some did not. Delimiting privacy processes from this holistic data center security management framework is done mainly to delimit thesis study further.

Frameworks reviewed in previous chapters do not include information security in their classification systems. As information security is considered to be vital part of data center industry, the minimum protection level includes information security management system processes described in ISO 27001 standard. Advanced protection level and full protection level include certification of ISO 27001.

4.4.7 Physical security and safety

All corporate security, data center industry and information security frameworks reviewed in previous chapter include various physical security and safety requirements and

considerations. Data center industry frameworks reviewed provide detailed design guidelines and requirements whereas corporate security frameworks include general guidance but for also such security functions that are not found in data center industry frameworks. Information security frameworks include some general requirements for physical security design and management. Physical security function in this holistic data center security management framework combines processes for protecting data center premises and physical assets, including physical IT assets such as IT devices and cabling, from various external and internal physical threats and hazards. Also, processes such as logistics security, security and safety of events are included in physical security function. Processes related to electrical safety, data center power and cooling distribution, personnel safety and security are not included in this function. Power and cooling distribution are not considered to be a part of data center security management processes and as electrical safety is a crucial part of managing any electricity distribution systems, electrical safety is also delimited from this physical security and safety function. Personnel security and safety is separated as an individual security management function.

Protection of data center premises include sub-processes related to location selection and monitoring, which is supported by security intelligence function. Other data center premises protection sub-processes are for example design and managing of the physical construction of data center facilities, zones, and technical security and safety systems. Access management and control are one of the main sub-processes related to protection of both data center premises and assets. Fire protection systems and fire safety processes are also included as well as protection systems and processes against other environmental threats within and outside data center premises, such as electromagnetic interference, vibration, flooding, gaseous substances, chemical spills and accidents, and dust. Emerging from information security frameworks are processes for physical IT equipment such as transferring, removing and disposal of physical IT assets. Physical security personnel considerations and processes are also part of physical security and safety function.

Logistics security processes in this holistic data center security management framework include sub-processes related to protecting transportations and controlling all deliveries and dispatches in data center premises. Processes for protecting and controlling data center premises used for logistics are also included such as parking areas, loading bays and storages.

Event security and safety is not included in information security or data center industry frameworks, but all reviewed corporate security frameworks supported the idea to include this as part of this holistic data center security management framework. Event security and safety processes include similar and perhaps somewhat overlapping functions and processes as data center security management such as physical security and safety, information security, personnel and executive security and safety, and contingency planning. From this thesis

author's opinion, when considering the criticality of data centers to businesses and societies as well as related safety and security risks, data centers should not be generally used as venues for events. If special events are however held in data center locations, this physical security and safety function would be providing supporting processes.

Physical security and safety processes are considered in all the classification systems included in data center industry frameworks reviewed in previous chapters with somewhat differing requirements and guidelines. The classification used in this physical security and safety function is created by mapping and combining Tier Standard Operational Sustainability, ANSI/TIA-942 and EN 50600-2-5 standards. The four-level classification is replaced with three-level classification by removing lowest class named usually as Tier 1, as the level of security and safety requirements is usually not meant for enterprise-level data center applications. Minimal protection class in this holistic data center security management framework includes additionally all the physical security and safety process requirements and considerations mentioned in reviewed information security frameworks. Transportation security and safety as well as event security and safety related processes are included only in full protection as described in reviewed corporate security frameworks although there are also related standards available, for example Transportation Asset Protection Association standards for facility, trucking, and parking (TAPA 2021).

4.4.8 Personnel security and safety

Personnel security and safety function in this holistic data center security management framework is combining multiple distinguished security and safety management functions related to personnel and visitors. However, resourcing personnel to data center security management, and leading or managing personnel are not considered as part of personnel security and safety function but part of general data center human resource and personnel management processes. Personnel security and safety function in this framework includes processes for human resource security, handling and managing of visitors, occupational health and safety, travel and expatriate security and safety, executive protection, and education, awareness and training programs related to all security management functions.

Human resource security processes are included in all previously reviewed frameworks. These include sub-processes related to employment lifecycle such as pre-employment screening or investigation, security and confidentiality agreements, personnel security searches, drug testing, disciplinary processes in case of security breaches and protecting organization's interest during employment terminations and changes. Also, managing and handling of visitors are included in all frameworks and especially data center industry frameworks contain detailed requirements and guidelines for visitor processes. Workplace violence prevention is

also considered in reviewed corporate security frameworks to be part of human resource security.

Occupational health and safety processes are generally excluded in previously reviewed information security, data center industry and corporate security frameworks. The Corporate security model by Confederation of Finnish Industries and Brooks' integrate framework of corporate security are the only frameworks reviewed which include life safety and occupational health and safety as part of security management. These two are considered to describe most holistic models for security management compared to all other selected frameworks. For that reason, this holistic data center security management framework contains also occupational health and safety processes as part of personnel security and safety function. Occupational health and safety is highly regulated area in European region and processes may vary depending on local legislation, but some common processes can be established by implementing for example ISO 45001 standard compliant occupational health and safety management system. This includes for example identification and mitigation of occupational health and safety hazards with such control as elimination, reorganization or replacement of processes, administrative controls and use of personal protective equipment. Occupational health and safety processes are not limited only to organization's own personnel but also contractors and outsourced functions and processes. (SFS ISO 45001 2018, 19, 25-26.) The COVID-19 pandemic has increased the importance of identifying and mitigating health and safety hazards in workplaces and brought new processes for infectious diseases mitigation also to data centers. These processes are also highly dependent on local regulations but as an example of common processes, ISO 45005 has been established and published during 2020 as general guidelines for safe working practices in workplaces (ISO/PAS 45005 2020).

Travel and expatriate security and safety processes are included in all corporate security frameworks reviewed in previous chapters. Processes related to travel and expatriate security and safety may be overlapping with other security functions in this holistic data center security management framework, such as risk management, business continuity planning, information security and security intelligence. However, travel and expatriate security and safety processes require considerations for all the travel and living arrangements of employees and even their families. Sub-processes related to travel and expatriate security and safety include for example risk assessments, travel and accommodation clearances, emergency, and evacuation planning. (Cabric 2015, 172, 175-178.)

Executive protection processes are as well included in all reviewed corporate security frameworks. Halibozek and Kovacich (2017, 375) describe executive protection as "application of protective measures to reduce the risk to executives and avoid threats" and that it contains proactive efforts. Executive protection processes include similar sub-processes as travel and expatriate security and safety, for example risk and threat assessment

and various protection measures overlapping with other security management functions, but also for outside work environments such as travelling and home. Halibozek and Kovacich mention that usually executive protection is not needed full-time which is also supported in corporate security model by Confederation of Finnish Industries (Halibozek & Kovacich 2017, 382; EK 2016, 6). Data center industry and information security frameworks selected for the reviews did not include executive protection processes at all. However uncommon executive protection would be in data center industry, this holistic data center security management framework includes executive protection in personnel security and safety function to provide support and example of such processes if these are needed.

Security and safety education, awareness and training processes include and combine these processes from all the security management functions in this framework. Reviewed information security and data center industry frameworks include requirements and guidelines for the contents of relevant awareness educations, trainings and updates or refreshers regarding policies and procedures related to security management functions. These include for example information security, business continuity, risk management, incident management, physical and personnel security and safety. Education, awareness, and training processes include also planning and performing exercises and tests related to all security management functions. Awareness and training sub-processes can be defined for example by the audience or targets such as executive management, middle management, first-line supervisors, individual employees, new employees, and non-employees such as supplier personnel, customers, and visitors (ASIS International 2012, 291-293).

Classification systems in the frameworks reviewed in previous chapters do not generally include these processes related to personnel security and safety function. Tier Standard for Operational Sustainability includes staff and vendor training program in the classification covering required policies, processes, procedures, and rules. This is used as a basis for security and safety education, awareness, and training classification in this holistic data center security management framework. Processes related to human resource security and handling and managing of visitors are included in most of the reviewed frameworks and for this reason these are included in minimum protection level of this framework classification. Occupational health and safety related processes are included also in this classification so that compliance towards local occupational health and safety regulations are placed in minimum protection level. Advanced protection level includes additional conformity to ISO 45001 standard and full protection level includes ISO 45001 certification as well as conformity to ISO 45005 standard during COVID-19 pandemic. Minimum protection level includes also processes related to travel and expatriate security and safety as these are usually included as part of occupational health and safety regulations. Executive protection processes are included in full protection level as it is not commonly applied in data center industry frameworks but may provide additional guidance if these processes are needed.

Personnel security and safety function in this holistic data center security management framework contains such processes which could be divided as separate and individual functions of data center security management. However, all the functions in this framework as presented in figure 10 are supposed to present different security management processes in general level. Many of the processes as described in this chapter are and may be overlapping. Applying the processes may not require separation of all the functions and processes as described but it may be beneficial when evaluating data center security management through this framework. Next chapters of this thesis study report include an example of practical application of the framework as an evaluation tool as well as reviews of the framework along with the evaluation tool.

5 Design of a holistic data center security management evaluation tool

This thesis study does not include an actual experiment or testing for implementing of holistic data center security management framework established and described in previous chapter. Instead, to test the established framework to prove its validity for different practical use cases, an evaluation tool is designed based on the framework. Furthermore, to support the usability of the evaluation tool for practical use cases, principles of usability heuristics are incorporated in the design of the tool. The evaluation tool itself is not tested as part of this thesis study but the validity is assessed through heuristic evaluation method. This chapter includes description how the holistic data center security management evaluation tool is designed and created together with usability heuristic principles. The evaluation tool is designed and created for the use of the target organization of this thesis study and thus is not published as a part of this thesis study report. Heuristic evaluation processes of the tool as well as the findings from heuristic evaluations are described in the latter chapters of this thesis study report.

5.1 Holistic data center security management evaluation tool

The purpose of the holistic data center security management framework is not to support compliance to any referred standards or frameworks but to support a holistic way of establishing, maintaining, and developing data center security management by providing references and considerations to be included. As the holistic data center security management framework is not designed or intended as a complete management system standard with specific controls, it should not be used as a way of verifying conformity to any of the frameworks which it is based on. Instead, it could be used as a reference to develop data center security management in a holistic manner.

The evaluation tool created as part of this thesis study is designed to describe, support, and follow a simple informal audit process as presented by Kegerreis, Schiller and Davis. Some common audit principles are however applied and supported even within this evaluation tool, such as integrity, fair presentation, due professional care, confidentiality and at least on some level independence and evidence-based approach as described in management system audit standard SFS-EN ISO 19011 (2011, 19). Audit team members and audit team leader should be appointed before audit and they should have competence as well as resources to complete the audit on time as agreed. The audit should be well planned and prepared with additional considerations instead of just agreeing audit scope and time with the auditees as suggested in the informal audit process. Confidentiality and information security requirements for the audit and audit documentation should be identified and agreed. Also, other possible security, health and safety and language requirements are needed to be agreed depending on if the audit is completed on-site at data center location or in a remote location without visiting data center at all. (SFS-EN ISO 19011, 31, 33, 79.) Evaluation should include some level of reviewing evidence or sampling to confirm and validate the information or data in the scope of the evaluation. For the evaluation to be practical and usable to be implemented, it would not be feasible to review all available data but some samples representing total population of data. Sampling should be based on auditor's judgement by referring to for example findings in any possible previous audits or evaluations and previously identified risks or areas of improvement (SFS-EN ISO 19011, 83).

These above-mentioned considerations are included in the evaluation tool. The tool is designed and created as an Excel spreadsheet so that these preparative considerations are documented in the tool. The tool also contains template for documenting the evaluation findings. A separate tab is included for summary of evaluation progress, findings, and results. The holistic data center security management framework is used in the evaluation tool as a basic checklist with descriptions of all the security management functions, processes, sub-processes and classifications as presented in chapter 4. Each data center security management function is separated in their own tabs. The evaluation tool does not contain complete lists of all controls related to the framework. Various security management standards are included as a reference in many parts of the tool, but all controls are not rewritten or copied into the tool as it may be restricted for some of the standards referred in previous chapters.

5.2 Usability heuristic principles

The holistic data center security management framework and the tool created for the evaluation are both aimed to be used by data center and security management professionals.

The design and creation of the evaluation tool includes applying usability heuristic principles for supporting a good user experience to make it compelling and viable for these different users. Usability heuristics referred in this thesis study are associated with usability engineering of computer systems for good user interfaces as defined by Jacob Nielsen. Nielsen suggests usability, as part of computer system design, as part of a broader definition of system acceptability which also includes such categories as social acceptability, cost, compatibility, reliability, and usefulness. System acceptability refers to fulfilling the needs and requirements of all the users and stakeholders related to the computer system. (Nielsen 1993, 16, 24.) This broader definition of system acceptability is considered in next chapter as part of heuristic evaluation of the evaluation tool.

The usability heuristics defined by Nielsen includes 10 principles which are meant to be followed in design of all user interfaces. Principles are summarized and presented in figure 11. These principles are used also in the heuristic evaluation process of the evaluation tool described in next chapter.

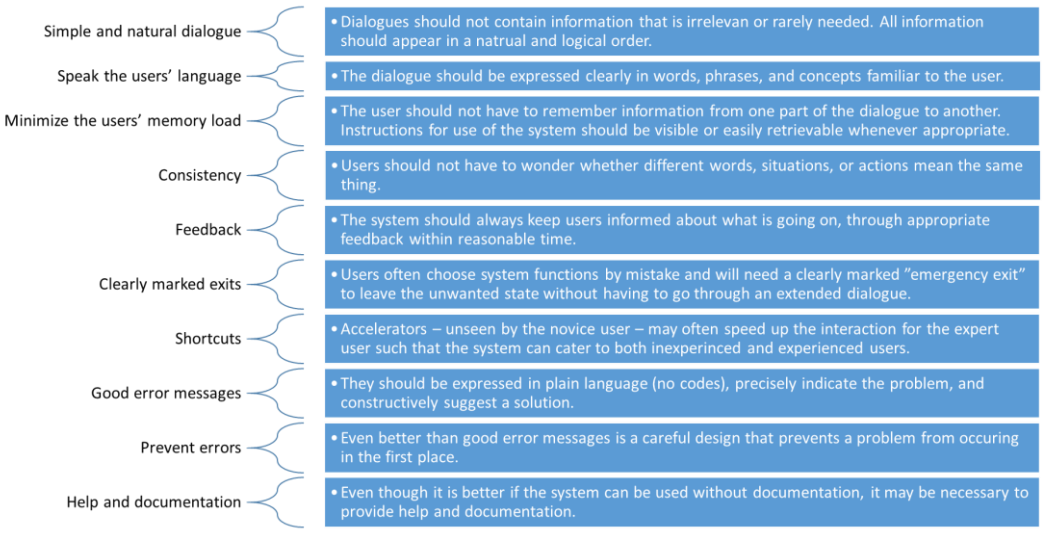

Figure 11: Usability heuristic principles as described by Molich and Nielsen 1993 (Nielsen 1993, 20).

Applying these usability heuristic principles in the evaluation tool for holistic data center security management is simple since user interface in this tool is basic Microsoft Excel spreadsheet. Usability heuristic principles are still considered in most part of design and creation of the tool. The dialogue in the tool is following natural and logical appearance order; first tab contains template for preparatory planning, second tab includes summary and information regarding progress of evaluation process, and all the rest of the tabs are each representing individual security management function and a checklist for the named function.

Navigating between the tabs is minimized as each data center security management function should be evaluated individually without a need to visit the other tabs. The language used in the tool is English and terminology referring much to security management terminology as the users of the tool should have some basic understanding of this area. Abbreviations are avoided as much as possible and when used, the meaning is defined also in plain text.

One of the main reasons for using Excel spreadsheet as software for the tool is the popularity of the software and ease of use, but also the possibility to include vast amount of data and variables. This allows including all needed information within the tool such as guidance for different fields while minimizing the need for the users of the tool to guess or remember what each field is meant for. Consistency is built into the tool so that all tabs containing data center security management checklists are utilizing exactly similar design and functionalities. Only feedback provided by the tool is the progress and results of the evaluation process which is presented and visualized in a separate tab. The evaluation tool itself does not contain any specific exits, shortcuts, or error messages except what the spreadsheet software provides for the user as default. The tool does however contain recommendation to save the document in each tab before closing the spreadsheet. To prevent user from altering the template and the functions built in, spreadsheet is locked so that user can only add, change, and delete certain fields. Help texts are included in the tool as guidance for the user but no other documentation such as manual is created for the evaluation tool in the scope of this thesis study.

Applying these usability heuristic principles presented in figure 11 into the evaluation tool does not alone provide sufficient assurance that the users of the tool find it as user-friendly. Usability engineering lifecycle as described by Nielsen also includes other processes, for example identifying, analyzing, and evaluating users, setting usability goals, and different design phases such as prototyping. Testing of the prototype or multiple prototypes is also included as well as collecting feedback from users. Heuristic evaluation is used as part of initial testing of the design, even before creating prototypes. (Nielsen 1993, 71, 91-92.) If the research objective of this thesis study would be just to produce an evaluation tool based on any existing framework, perhaps whole range of usability engineering lifecycle processes could have been applied. However, usability engineering lifecycle processes are otherwise not applied in this thesis study, but heuristic evaluation is used as described in next chapters.

6 Heuristic evaluation

Nielsen has defined heuristic evaluation as “discount usability engineering” (1993, 160). This refers to the possibility of heuristic evaluation method to be used to find cost-efficiently usability problems which may prove to be more expensive to be found later by other methods

during usability engineering lifecycle. Nielsen does not guarantee that by using heuristic evaluation method all possible usability problems can be found in an interface. (Nielsen 1993, 160.)

General idea of heuristic evaluation is to have a small group of people called “evaluators” to systematically inspect a user interface to find usability problems according to defined usability principles or heuristics. As each evaluator may find different usability problems, it is recommended to use at least three to five evaluators. Number of evaluators can be more, depending on the importance of usability of the interface. However, the expertise of the evaluators is what benefits more than just the number of evaluators, especially when cost-benefit ratio of heuristic evaluation process is compared to for example other usability testing methods. (Nielsen 1993, 155-156, 161.)

Heuristic evaluation method has received some criticism. The method is intended to generate a list of usability problems, but it is not intended to provide a systematic way to solve them. However, evaluators may come up with solutions to the problems they have found, especially when using expert evaluators problems and solutions related to other acceptability features may be brought up. It would be disadvantageous to disregard these just because heuristic evaluation process defined by Nielsen is not focused on such findings. (Korvenranta 2005, 120-122.)

This criticism is noted in design and implementation of the heuristic evaluation processes used in this thesis study. Following chapters include a description of the heuristic evaluation process as used in this thesis study, and a description of principles used in selection of expert evaluators.

6.1 Participant selection for heuristic evaluation

There are many benefits of using experienced evaluators in heuristic evaluation process and one major benefit is the problem finding efficiency. According to results of a case study by Nielsen, evaluators with expertise on usability engineering could find as much as 1.8 times more usability problems in an interface compared to evaluators with no usability engineering expertise or “novices”. When the evaluator has both usability engineering and domain specific expertise related to the evaluated system, the “double expert” could find 2.7 times more usability problems compared to novices, and 1.5 times more than usability engineering experts. If usability engineering experts are not available, Nielsen recommends using technical writers who would be experienced on creating instructions for users. (Nielsen 1993, 161-162.)

As the heuristic evaluation method is used in this thesis study to collect findings related to both usability problems and general acceptability, only domain experts from thesis study target organization with experience on similar evaluation tools were invited to evaluation sessions. The evaluators were selected based on their expertise in data center management domain and corporate security management domain. The number of evaluators were kept on minimum three persons as resources for the evaluations were limited.

The evaluators did have experience on using and creating similar interfaces as this holistic data center security management evaluation tool. But based on Nielsen's classification, the evaluators would have been classified as usability "novices" since no specific usability engineering experience was identified. Finding "double specialists" with both usability engineering experience and domain experience, in this case data center, corporate security or information security management experience proved to be impossible in the time frame and resources available for this thesis study. The most optimal "double specialist" for these evaluation sessions would have had holistic data center security management experience as well as usability engineering experience, but since the holistic data center security management framework is only defined in this thesis study, "double specialists" were not available.

Two of the three evaluators selected and invited to evaluation sessions had between 10 to 20 years of experience in data center management, including data center security, information security, certification, auditing, and other compliance management topics. One of the three evaluators had experience on corporate security and physical security domain for between 3 to 10 years. As the evaluation sessions were anonymized, the evaluators are referred in following chapters as E1, E2 and E3.

6.2 Heuristic evaluation process

Performing heuristic evaluation is, in its simplicity, done by having each selected evaluator inspecting the interface independently and "trying come up with an opinion" about the usability of the interface (Nielsen 1993, 157). Evaluators should not communicate with each other before all findings are aggregated to ensure that the findings are also independent of each other (Nielsen 1993, 159).

Heuristic evaluation is usually done within one-hour or two-hour evaluation session for each evaluator. If needed, the sessions can be repeated multiple times. Evaluators can complete the evaluation session alone, which means that the findings are also documented and reported by the evaluators themselves. Another solution to report findings is to include an observer into each evaluation session to record evaluator's findings. Observer is not intended

to interpret any of the evaluator's actions but can provide hints and assistance on using the interface so that the evaluation can proceed on time. Observer can also interact with the evaluator by providing answers to evaluator's questions regarding the interface or even the contents. Evaluator should however be allowed to face and comment usability problems. Observer should not prevent or discourage the evaluator from getting into trouble with usage of the interface. (Nielsen 1993, 157-158.)

The evaluator is not supposed to use the system as such but to test different dialogue elements found in the interface. Evaluators should decide how they wish to proceed with the testing and observer should not interfere or guide the evaluator in the testing procedures. Throughout testing of the various elements found in the interface, evaluators should compare their user experience towards the heuristic principles defined in beforehand by the organizer of heuristic evaluation sessions. The interface inspection should be done several times, at least twice, by the evaluator during the evaluation session. First inspection is intended to provide the evaluator with an overview of the interface and its functionalities, while second inspection is allowing further testing of specific elements. (Nielsen 1993, 157-158.)

Nielsen suggests having a debriefing session with all evaluators together after all evaluation sessions are held. Debriefing session can be used for brainstorming to find solutions to the found usability problems and to possibly re-design the interface. Debriefing session is however presented by Nielsen as an extension to heuristic evaluation process. (Nielsen 1993, 160.)

The heuristic evaluation process used in this thesis study followed similar process as defined by Nielsen. A selected group of expert evaluators were invited individually to evaluation sessions lasting one hour to inspect the interface of the holistic data center security management evaluation tool. Evaluators were requested not to communicate with each other regarding the evaluation sessions before results were published. Author of this thesis participated evaluation sessions as an observer to document the evaluation session and followed similar principles of refraining from interfering the inspection procedures as defined by Nielsen. Usability heuristic principles used in these evaluation sessions were the same as defined in figure 11 of this thesis study report. Debriefing session was not held as part of this thesis study as the further design phases were delimited from the research.

The evaluators received a manuscript of the evaluation session including short description of the purpose of thesis study, evaluator expertise related background questions, general guidance for heuristic evaluation and the usability heuristics to be used during the session. Manuscript of the evaluation session is found in appendix 1 of this thesis study report. In order to save time for the evaluation session, the evaluation tool itself was also provided in beforehand to the evaluators. This was intended as a possibility of having the first round of evaluation to be completed before the actual evaluation session. Intention was also to give

evaluators a possibility to familiarize themselves with the actual content of the interface to be able to assess general acceptability and usefulness of the evaluation tool and the holistic data center security management framework.

Nielsen defines usefulness as a practical acceptability attribute answering to question if the system, not just the interface, “can be used to achieve… desired goal” (Nielsen 1993, 24). Other general acceptability attributes could include social acceptability and practical acceptability such as cost and reliability. General acceptability and usefulness were however not defined further as part of this evaluation. The purpose of including these acceptability attributes as part of evaluation sessions was to collect general acceptability findings related to the tool and the frameworks from expert evaluators.

The heuristic evaluation sessions were held during May 2021. Each evaluation session lasted about 40 to 60 minutes. The sessions were held remotely in a video call using Microsoft Teams communication platform and recorded so that evaluators were presenting their screen in real-time as they inspected the interface. Transcriptions of the discussions between the evaluators and the observer were also recorded to assist with the collection of the findings. All usability problems found by the evaluators and the comments regarding general acceptability and usefulness of the tool and the framework were further transcribed based on beforementioned Teams -recordings. The findings and the comments from all the evaluators were then structured according to their equivalence and labelled with a short description summarizing the contents of the findings and the comments.

7 Results of heuristic evaluations

As a result of the three heuristic evaluation sessions, a total of 24 different types of usability problems were identified in the holistic data center security management evaluation tool. In addition to identifying usability problems, 15 different types of comments were recorded regarding the general acceptance and usefulness of the tool and the framework which the tool is based on. Figure 12 summarizes the number of findings from each evaluator and the number of aggregated findings. These numbers are reviewed further in following sub-chapters.

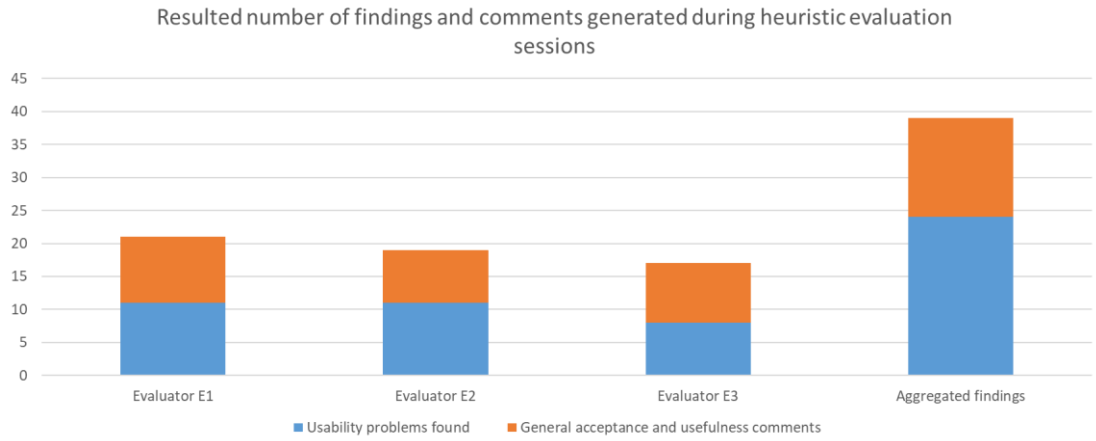

Figure 12: Number of findings and comments generated during heuristic evaluation sessions.

The usability problems found in the interface of the tool included some problems and limitations in the Excel -tool but also the functionalities built in the interface, user instructions and ambiguity of the contents describing evaluation checklists. The comments related to the general acceptability and usefulness of the tool and the framework included recommendations to add some features in the tool which the evaluators considered important. The comments included also praise related to the usefulness of both the tool and the framework. The results are presented in more detail in the following sub-chapters.

Some of the usability problems found by the evaluators and the comments related to general acceptability and usefulness of the tool and the framework were general in nature and some were related to the organization which the evaluators represented. As the evaluation sessions were anonymous, these organization related findings and comments are not described in this public thesis report.

7.1 Usability problems of the evaluation tool

All evaluators found similar as well as differing usability problems during heuristic evaluation sessions. E1 and E2 found both 11 usability problems and E3 found 8 usability problems. After further analysis, 24 different usability problems were identified in total. Although heuristic evaluation according to Nielsen includes defining only usability problems, the evaluators provided solution proposals for 12 of the problems they found. The solution proposals are not included in this public thesis study report but found problems are summarized in this chapter.

Most common problem found and commented by all the three evaluators was related to a problem when moving between rows in the Excel-spreadsheet checklists during evaluation when cells were filled with text. This made evaluators to jump over some rows and miss items in the checklists. This made it also difficult for evaluators to enlarge the size of the texts in checklists to be able to read the texts. As this problem reoccurred in all the different data center security management functions checklists, one of the evaluators mentioned the problem to be “really annoying”. The problem was known for the evaluators and it was mentioned to be “an issue within Excel itself”.

Other common problems found by at least two evaluators were related to spreadsheet cell formatting and ambiguity of the terms used in checklists. The cells which users were supposed to write observations and notes from each checklist were not formatted in beforehand to match rest of the document formatting such as aligning and wrap the text in similar manner. This was noted to make some of the texts to disappear and as one evaluator commented “it’s something that makes it irritating when it (text) ends down and you are reading from up”.

Ambiguity of the terms and concepts used was experienced in many parts of the evaluation tool and the checklists. References in the checklists to organization’s management was felt unclear as organizations usually have many levels of management. Documenting preparative considerations for the evaluation were not understood. Especially the purpose for fields created for documenting preparatory considerations related to security and safety raised questions about what should be recorded there.

Remaining 21 identified usability problems were found by the evaluators individually. These problems could be divided in three categories based on the type of the findings which are related to designed functionalities in the spreadsheets, formatting of the texts and spreadsheets, and descriptions or contents of the checklists. Seven usability problems found were related to functionalities or functions built into the tool. For example, observations were counted and presented as part of the statistics progress and result summary tab. One evaluator found that when writing multiple observations related to one item within the checklist, it was counted only as one observation making the statistics incorrect. One of the evaluators found that evaluator notes were not presented in any of the progress and result summary tab, even if the notes would be considered as vital information for the evaluation.

Five of the remaining problems were about spreadsheet formatting. For example, headlines of columns in checklists were not locked so evaluator was not able to see purpose of the cells. One evaluator wanted to understand how evaluation statistics for progress and results were generated from the checklists, but it was not described in the tool. Last remaining nine usability findings were related to the actual content of the checklists. The purpose of

referring to international standards and frameworks were not clearly understood by the evaluators in different parts of the checklists. As the exact parts or chapters of the standards or frameworks related to each evaluated item were not described in the checklists, the basis where each item originates was considered confusing. Also, the protection level evaluation was found to be unclear and subjective regardless of the guiding descriptions in the checklists.

Many of the usability problems may be fairly easily fixed by adjusting the evaluation tool. These kinds of results were expected as Nielsen also has mentioned many usability problems to "have fairly obvious fixes as soon as they have been identified" (Nielsen 1993, 159). As some of the usability problems found are related to the restrictions of the Excel spreadsheet - tool used, fixing such problems may require re-design or consideration for using another software for the tool interface.

7.2 General acceptability and usefulness of the evaluation tool and the framework

Heuristic evaluation sessions included collecting comments and findings from the evaluators related to general acceptability and usefulness of the evaluation tool and the holistic data center security management framework. This part of the evaluation sessions was not strictly following the heuristic evaluation process defined by Nielsen but provided important feedback for developing the evaluation tool further and for verifying validity of the framework, as the evaluators represented both data center and corporate security management domain expertise. General acceptability and usefulness were not defined further in this thesis study nor to the evaluators, but the comments were considering validity and usefulness of the tool in general and from the evaluators point of view. The comments were generated during the evaluation sessions as natural feedback continuum to the usability problem findings.

Evaluator E1 gave 10 comments, E2 gave 8 comments and E3 gave 9 comments. In total 15 different types of comments were aggregated from these. However, five of the comments were identified in later analysis to be related to further development suggestions for the evaluation tool itself. The rest 10 comments were considering general feedback about usefulness and acceptability of the tool and the framework.

All three evaluators found the progress and result summary tab as useful and good to have to follow evaluation progress, observations, and results of evaluated protection class. The systematic structure of the evaluation tool was also considered as a good feature to have. A comment from one evaluator to the systematic structure was that it is "a structured way of doing work that can potentially be very confusing if you don't have a structured or systematic

approach to it". This comment can be considered to be related both to the evaluation tool and the framework which the tool is based on. Another evaluator commented to the systematic structure by stating that it is useful when the requirements or desired protection level changes over time: "The structure stays the same and it's just a different version of the evaluation deck and dependent on the level".

The resulted overview of holistic data center security management when using the evaluation tool was praised by two of the evaluators. One evaluator commented that the tool "will help… to have control over where one stands in different areas" while referring to evaluating all security management functions defined in the framework. Another evaluator referred that when using the evaluation tool regularly, such an overview is generated also regularly. Features that were considered also as good in the tool related to for example having a possibility to document preparatory information, and overall consistency throughout the tool. One comment was related to questioning why environmental management standard ISO 14001 was referred in the evaluation tool checklists when the evaluation headline was data center security management.

The evaluators comments related to developing the evaluation tool further included recommendations to have such features as ability to include multiple data center evaluations in one result and progress report. This was raised by two of the evaluators. Also, further adaptation and tailoring for individual organizations, or part of organizations, was suggested by one of the evaluators: "I would have no problem using it as it is, but I would prefer having it tailored to … avoid unnecessary confusion or disagreements on the findings". One evaluator would have liked to add comparison of observations to evaluated items in the result summary. One evaluator also would have liked to include in the evaluation checklists a documentation review to be completed before going into the data center security management evaluation session.

Two of the evaluators commented general usefulness of the tool and emphasized the benefit of the tool and the framework being based on existing recognized standards and frameworks. One of the evaluators commented that using the tool and the framework would be "a much better starting point than starting with a blank paper and just creating something from your own mind because this is based on something with background and knowledge". Another similar supporting comment from one of the evaluators was that "this type of setup allows process information a lot easier based on specific points in standards". One of the evaluators also considered the costs related point of view in general acceptance of the evaluation tool by stating that "most of this stuff you need to invent yourself or you need to buy something that is so expensive that it is not worth it. So doing this in Excel that is quite inexpensive is really good".

Even though not all results from the heuristic evaluation sessions could be published as part of this thesis report, these mentioned results represent well the non-public findings and comments that were related more to the organizations which the evaluators represented. Conclusions drawn from the results of the heuristic evaluations presented are included in the next chapter.

8 Conclusions

As the main development tasks of this thesis study, a holistic data center security management framework was defined and designed, and a user-friendly tool was produced for evaluating data center security management through the framework. This chapter contains conclusions related to these development tasks based on the results of the heuristic evaluations. The results suggest that the framework and the evaluation tool could be applied in actual use cases as such and with further development.

The focus of the evaluation sessions was on the interface of the evaluation tool but based on the comments on the evaluation tool contents, some conclusions can be drawn regarding the framework which the tool is based on. The comments collected during heuristic evaluation sessions suggest that a systematic structure covering different data center security management domains was found as beneficial. Combining this framework with existing international or regional standards and frameworks as reference was found to bring additional value. Although the entire content of the tool was not evaluated in detail as part of the heuristic evaluation sessions, the basic structure of the framework was accepted to represent data center security management holistically. The framework was applicable as a checklist for the evaluation tool.

Based on extensive information acquisition throughout this thesis study, this type of holistic data center security management framework has not been defined before in a public research paper. Although the framework designed in this thesis study is largely based on corporate security management frameworks, the evaluators saw there is a demand for defining such a holistic data center security management framework. One of the evaluators summarized this when referring to the tool: “Usually this doesn’t exist, and it is something that is invented (as) new everywhere. It depends on what kind of knowledge and understanding anybody in organization have to deep dive into these kinds of areas. If this tool would be available for others, that would help because it’s a starting point.”

The usability, general acceptability and usefulness of the evaluation tool were verified during heuristic evaluation sessions. Based on the comments from the evaluators, the tool was found as useful and applicable for evaluating data center security management holistically. The

evaluation tool was considered to bring additional value to organizations by generating an overview of the data center security management with possible findings for areas of development.

The evaluation tool was designed as a compromise between informal audit process as defined by Kegerreis, Schiller and Davis, and formal audit process as defined in standard ISO 19011. Based on heuristic evaluation results, heuristic principles were successfully applied as design guideline for the tool. Although usability problems were found and further development needs were recommended, the tool was thought to be user-friendly when considering the cost-effectiveness of the Excel-spreadsheet used as an interface. One evaluator however suggested to consider another interface for the tool.

When considering creating other possible applications for the holistic data center security management framework in the future, heuristic principles and heuristic evaluation could be utilized. However, when evaluating acceptability attributes other than usability, heuristic evaluation may not be the best method to follow as it is intended for finding usability problems. Furthermore, as heuristic evaluation is considered as one method in usability engineering lifecycle toolbox, other methods and processes should be included in the whole design process.

9 Reflections

The two main development tasks set for this research-based development process were achieved. A holistic data center security management framework was defined and designed based on multiple existing corporate security, information security and data center industry standards and frameworks. An evaluation tool for data centers security management was created for an organization based on this framework and usability problems were found enabling further development of the tool. Heuristic evaluation method was utilized to validate the usability, acceptability, and usefulness of both the framework and the tool by domain expert evaluators. Based on experience on this thesis study, heuristic evaluation was an effective method for generating usability problem findings, but the method as defined by Nielsen is not useful for evaluating other acceptability attributes as it is not intended for such a purpose. However, after adjusting heuristic evaluation session contents to include feedback related to other acceptability attributes, the comments received from evaluators during the evaluation sessions was that both the framework and the tool were found as very useful for the target organizations and others as well. The framework and the tool will be utilized by the target organization after further usability development and tailoring.

Data center security management was identified early on as a difficult research topic due to the lack of available research publications. Information security management related sources were identified also early on not being able to provide a holistic framework for data center security management. Many of the data center related sources included either technical requirements of data center design or requirements for operating or managing a data center but not both. Corporate security related sources provided a good general framework to apply, but data center specific considerations were missing. Both the framework and the tool were results of combinations of these different aspects.

Another difficulty related to the research topic besides lack of publications was finding a way of approaching such sensitive and confidential research subject in a public thesis. The main goal for this thesis study was to define the holistic data center security management framework, and to test and evaluate its validity. A case study of a single data center operator or a survey for multiple data center operators would have perhaps provided more reliable results. However, preliminary planning of this thesis study revealed that finding research subjects would have been difficult due to the confidentiality surrounding data center security topics, or such research setting would have required resources which the thesis author did not have available. The research setting selected for this thesis study allowed to maximize anonymity and connection to any existing data center environment, operator or organization even though a target organization was involved.

Ensuring confidentiality and anonymity were considered as vital part of this thesis study, especially regarding heuristic evaluation sessions and using source material. Ojasalo, Moilanen and Ritalahti (2014, 48) have emphasized the importance of ensuring anonymity of all individuals in any development or research target group to obtain true and fair responses. The evaluators involved in the heuristic evaluation sessions were assured and ensured to have full anonymity and only relevant background information was included in this thesis report to provide verification of the evaluator's expertise. Many of the international and regional standards utilized throughout this thesis study are from paid sources and the possibility to present their contents are restricted to a certain level. Special consideration for copyright rules was taken during writing of this thesis report to not to violate any rules set by the publishers of these standards. Citations to all source materials and publications utilized in this thesis reports were considered also as important, not only to respect copyrights and research ethics but also to provide further reading recommendations to all readers of this report.

The results presented in this thesis report could benefit further research on data center security management by providing a holistic framework to start with. The results and framework presented in this thesis study report may also be utilized outside academic research community as such by creating similar evaluation tools or by adopting the holistic data center security management framework to actual data center management use cases.

However, this thesis study includes multiple delimitations which have affected the results. Although validity and reliability of the framework and the tool were tested through heuristic evaluation, further research would be needed to verify the results in other context such as geographical locations other than European region. Some further research topics were identified throughout the course of this thesis study and these are explored in sub-chapter 9.1.

9.1 Further research needs

This thesis study included multiple delimitations which set the course of the research as well as impacted on the results. Delimitations also raised multiple questions which could be interesting to study further. As a lack of publications and research regarding data center security management was noted during this thesis study, there is still much to research on the topic. Securing and protecting data centers is a topical research topic, which implicates that there could be also a need for further research on the topic.

Security convergence phenomenon was identified in many of security management source literature reviewed during this thesis study. Security convergence itself is not regarded as novelty but utilizing holistic viewpoint in security management to tackle the challenges related to the phenomenon was not identified in other than corporate security related literature. Security convergence in corporate security management would be very topical research topic, not only from an obvious cyber security point of view but considering the whole range of security convergence as suggested by Wakefield (2014, 246).

The holistic data center security management framework and model defined and designed in this thesis study was largely based on the Corporate security model by Confederation of Finnish Industries and Brooks' integrated framework of corporate security. Although the application was now data center security management, this combined model could perhaps be utilized also in a context other than data centers. As mentioned in chapter 2.3, further testing of the model and framework and its correctness and novelty value would require another research project. One angle to examine this could be considering similar research as conducted by Brooks and study the common body of knowledge required for the holistic data center security management. This would be very beneficial research topic especially for data center industry, where shortage of skilled specialist staff has been identified already as a global problem (Ascierto 2021).

Although one of the identified difficulties of this thesis study was the lack of relevant publications, it should be noted that due to the thesis authors' limited resources and capabilities as well as delimitation choices made, only source material available in English

and Finnish languages were acquired and utilized. However, publications could be available in other languages and including these could provide different results. This similar problem would have occurred if only sources available in English would have been utilized as the Confederation of Finnish Industries has not provided an English version of their publication on the Corporate security model. It would be beneficial for researchers and security management professionals if this model would be available also in English. Same would be applied for any other existing local corporate security models which are not published in English.

During writing of this thesis study report, one international standard for protective security ISO/CD 22340 “Guidelines for establishing an enterprise protective security architecture and management framework” was being prepared. The exact contents of the standard were not available for the thesis author but according to article by ISO/TC 292 working group 6 preparing the standard, this would provide “overarching principles -based architecture”, which could be a standardized solution equivalent to the framework defined in this thesis study (ISO/TC 292 Online 2021). This would have been valuable source for this thesis study, and it may provide further research study topics and applications in the future once the standard is published. Another viewpoint to consider in further studies could be, as mentioned in chapter 4 of this thesis report, to consider what kind of value these frameworks could bring to corporate security management and organizations overall.

Security intelligence function in the holistic data center security management was introduced only shortly in chapter 4.4 as the resources used in this thesis study regarding this topic were limited. The frameworks and standards as well as literature sources reviewed in this thesis study did not provide much information regarding security intelligence as part of security management. This may suggest that security intelligence is not either generally accepted as part of security management, or that the topic has not been addressed in such sources because of its novelty. In any case, further research would be required to fully identify and define proper sub-processes for security intelligence as part of holistic data center security management framework.

Finally, as security management in data centers seems to be a less researched topic, it could provide multiple opportunities for further research. Just to name few examples of the current challenges and trends in data center industry are the current COVID-19 pandemic and the post-pandemic challenges, increasing sustainability requirements, edge computing, and changing energy storage related challenges such as those related to lithium-ion batteries (Miller 2021). These current and also future challenges in data center industry could benefit from additional research-based knowledge and application of holistic security management. Hopefully this thesis study has been able to provide inspiration for further research on these topics.

References

Printed

ANSI/TIA-942-A. 2012. Telecommunications Infrastructure Standard for Data Centers. TIA 942-A. Arlington: Telecommunications Industry Association.

ASIS International. 2012. Protection of Assets: Security Management. Alexandria, VA: ASIS International.

Brooks, D. J. & Corkill, J. 2014 Corporate Security and the Stratum of Security Management. Edited by Walby, K. & Lippert, R. K. 2014. Corporate Security in the 21st Century: Theory and Practice in International Perspective. Basingstoke: Palgrave Macmillan.

Cabric, M. 2015. Corporate Security Management: Challenges, Risks and Strategies. Oxford: Butteworth-Heinemann.

Geng, H. 2014. Data Center Handbook. New Jersey: Wiley.

Halibozek, E. P. & Kovacich, G. L., 2017. The Manager's Handbook for Corporate Security: Establishing and Managing a Successful Assets Protection Program. Second Edition. Cambridge, MA: Elsevier.

Hirsjärvi, S., Remes, P. & Sajavaara. 2007. Tutki ja kirjoita. Helsinki: Tammi.

Information Security Forum. 2008. Securing Critical Infrastructure. Workshop Report.

ISO/IEC 27001. 2013. Information technology. Security techniques. Information security management system. Requirements. Geneva: International Organization for Standardization.

Kegerreis, M., Schiller, M., Davis, C. & Wrozek, B. 2020. IT auditing: Using controls to protect information assets. Third edition. New York: McGraw-Hill Education.

Korvenranta. H. 2005. Asiantuntija-arvioinnit. Edited by Aula, A., Ovaska, S. & Majaranta, P. 2005. Käytettävyystutkimuksen menetelmät. Tampere: Tampereen Yliopisto.

Nielsen, J. 1993. Usability engineering. Boston: AP Professional.

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaa. 3. uud. p. Helsinki: Sanoma Pro.

Sanastokeskus TSK. 2017. Vocabulary of Comprehensive Security. Second Edition. Helsinki: Sanastokeskus TSK ry.

SFS EN ISO 19011. 2012. Johtamisjärjestelmän auditointiohjeet: Standardi. Guidelines for auditing management systems. Second Edition. Helsinki: Suomen standardoimisliitto SFS.

SFS EN ISO 22301. 2014. Societal security. Business continuity management systems. Requirements. Helsinki: Suomen standardoimisliitto SFS.

SFS ISO 45001. 2018. Occupational health and safety management systems. Requirement with guidance for use. Helsinki: Suomen standardoimisliitto SFS.

SFS EN 50600-1. 2012. Information Technology: Data Centre Facilities and Infrastructures. Part 1. General concepts. Helsinki: Suomen standardoimisliitto SFS.

SFS EN 50600-2-5. 2016 Information Technology: Data Centre Facilities and Infrastructures. Part 2-5: Security systems. Helsinki: Suomen standardoimisliitto SFS.

SFS EN 50600-3-1.2016. Information Technology: Data Centre Facilities and Infrastructures. Part 3-1: Management and Operational Information. Helsinki: Suomen standardoimisliitto SFS.

Wakefield, A. 2014. Corporate Security and Enterprise Risk Management. Edited by Walby, K. & Lippert, R. K. 2014. Corporate Security in the 21st Century: Theory and Practice in International Perspective. Basingstoke: Palgrave Macmillan.

Electronic

Ascierto, R. 2021. Data center staff shortages don’t need to be a crisis. Uptime Institute Journal. Retrieved May 24, 2021 from https://journal.uptimeinstitute.com/data-center-staff-shortages-dont-need-to-be-a-crisis/

Brooks, D. 2012. Corporate Security: Using knowledge construction to define a practicing body of knowledge. Retrieved March 25, 2021 from https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1504&context=ecuworks2012

Cambridge University Press. 2021a. Meaning of data centre in English. Retrieved March 3, 2021 from https://dictionary.cambridge.org/dictionary/english/data-centre

Cambridge University Press. 2. 2021b. Meaning of framework in English. Business English. Retrieved March 15, 2021 from https://dictionary.cambridge.org/dictionary/english/framework

Cambridge University Press. 2021c. Meaning of evaluation in English. Business English. Retrieved March 17, 2021 from https://dictionary.cambridge.org/dictionary/english/evaluation

CENELEC. 2021. CLC/TC 215 Working documents. CLC/TC 215 Electrotechnical aspects of telecommunication equipment. European committee for electrotechnical standardization. Retrieved April 9, 2021 from https://www.cenelec.eu/dyn/www/f?p=104:30:1761946254531301::::FSP_ORG_ID,FSP_LANG_ID:1258297,25

Council of the European Union. 2013. Council decision on the security rules for protecting EU classified information. Decisions. 2013/488/EU. Retrieved April 3, 2021 from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0488&from=EN

Council of the European Union. 2020. Protection of European Union classified information EUCI. Information assurance. General Secretariat. Retrieved April 3, 2021 from https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/

Cybersecurity & Infrastructure Security Agency, 2020. Advisory memorandum on ensuring essential critical infrastructure workers ability to work during the COVID-19 response. Guidance on the Essential Critical Infrastructure Workforce. Retrieved February 20, 2021 from https://www.cisa.gov/sites/default/files/publications/Version_4.0_CISA_Guidance_on_Essential_Critical_Infrastructure_Workers_FINAL%20AUG%2018v3.pdf

Datacenter Dynamics. 2010. Uptime Institute’s Operational Sustainability standard is here. Retrieved April 8, 2021 from https://www.datacenterdynamics.com/en/news/uptime-institutes-operational-sustainability-standard-is-here/

Elinkeinoelämän keskusliitto EK. 2016. Elinkeinoelämän yritysturvallisuusmalli. Retrieved March 25, 2021 from https://ek.fi/wp-content/uploads/yritysturvallisuus_2016.pdf

Elliot, B. 2020. Explaining the new family of ISO Data Centre Standards. Techerati. Retrieved April 9, 2021 from https://www.techerati.com/features-hub/opinions/explaining-the-new-family-of-iso-data-centre-standards/

European Commission. 2021. Data Centres Code of Conduct. Joint Research Centre. European Energy Efficiency Platform E3P. Retrieved April 8, 2021 from https://e3p.jrc.ec.europa.eu/communities/data-centres-code-conduct

Future-tech. 2020. Use of the EN 50600 standard for assessment or "certification". Retrieved April 9, 2021 from https://www.future-tech.co.uk/use-of-the-en-50600-standard-for-assessment-or-certification/

Gartner, Inc. 2021. Gartner Glossary: Data Center. Retrieved March 3, 2021 from https://www.gartner.com/en/information-technology/glossary/data-center

International Organization of Standardization. 2021. Management System Standards. Retrieved March 15, 2021 from https://www.iso.org/management-system-standards.html

International Organization of Standardization. 2021a. Glossary. Conformity assessment. Retrieved March 15, 2021 from https://www.iso.org/glossary.html

International Organization of Standardization. 2021b. Standards by ISO/IEC JTC 1/SC 27. Retrieved April 29, 2021 from https://www.iso.org/committee/45306/x/catalogue/p/1/u/0/w/0/d/0

ISO/IEC 27000. 2018. Information technology. Security techniques. Information security management systems. Overview and vocabulary. Retrieved April 2, 2021 from https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

ISO/PAS 45005. 2020. Occupational health and safety management. General guidelines for safe working during the COVID-19 pandemic. Retrieved April 30, 2021 from https://www.iso.org/standard/64286.html

ISO/TC 292 Online. 2021. Projects. ISO 22340 Security and resilience - Protective security - Guidelines for security architecture, framework and controls. Retrieved March 26, 2021 from https://www.isotc292online.org/projects/iso-22340/

ISO/TC 309. 2021. Projects. ISO 37002 Whistleblowing management systems – Guidelines. Retrieved April 29, 2021 from https://committee.iso.org/sites/tc309/home/projects/ongoing/ongoing-2.html

Jew, J. 2017. Data Center Standards: How TIA-942 and BICSO-002 Work Together. 201 BICSI fall conference and exhibition. Retrieved April 8, 2021 from https://www.bicsi.org/docs/default-source/conference-presentations/2017-fall/data-center-standards.pdf?sfvrsn=367f9892_2

Judge, P. 2021. What is a lights out data center? Data Center Dynamics. Facilities Management. Retrieved March 8, 2021 from https://www.datacenterdynamics.com/en/analysis/what-lights-out-data-center/

Korolov, M. 2020. Data Center Operators Cut Onsite Staff and Visitors, Postpone Projects. Data Center Knowledge. Retrieved April 8, 2021 from https://www.datacenterknowledge.com/uptime/data-center-operators-cut-onsite-staff-and-visitors-postpone-projects

Lawrence, A. 2021. Learning from the OVHcloud data center fire. Uptime Institute Journal. Retrieved April 8, 2021 from https://journal.uptimeinstitute.com/learning-from-the-ovhcloud-data-center-fire/

McClary, R. 2017. Uptime Institute's Tier Ratings Explained. Data Center Frontier. Retrieved April 8, 2021 from https://datacenterfrontier.com/uptime-institute-tier-rating-explained/

Merriam-Webster. 2021. Merriam-Webster.com Dictionary. Holism. Retrieved March 15, 2021 from https://www.merriam-webster.com/dictionary/holism

Miller, R. 2020. Investors see Data Centers as Critical Infrastructure for the New Economy. Data Center Frontier. Retrieved February 20, 2021, from https://datacenterfrontier.com/investors-see-data-centers-as-critical-infrastructure-for-the-new-economy/

Miller, R. 2021. The Eight Trends That Will Shape the Data Center Industry in 2021. Retrieved May 24, 2021 from https://datacenterfrontier.com/eight-trends-that-will-shape-the-data-center-industry-in-2021/

OECD. 2019. State of play in the governance of critical infrastructure resilience. Good Governance for Critical Infrastructure Resilience. OECD Reviews of Risk Management Policies. Retrieved March 5, 2021 from https://www.oecd-ilibrary.org/sites/02f0e5a0-en/1/2/3/index.html?itemId=/content/publication/02f0e5a0-en&_csp_=eb11192b2c569d5c3d1424677826106a&itemIGO=oecd&itemContentType=book

OECD. 2019a. Policies for the protection of critical information infrastructure. Ten years later. OECD Digital Economy Papers. No 275. Retrieved March 5, 2021 from https://www.oecd-ilibrary.org/docserver/efb55c54-en.pdf?expires=1616704328&id=id&accname=guest&checksum=F53746BE7DC5FFAB9A6D17300E9D3DA3

Palo Alto Networks. 2021. What is a Data Center? Retrieved February 21, 2021 from https://www.paloaltonetworks.com/cyberpedia/what-is-a-data-center

Shapiro, S. 2016. Data Center Design: Which Standards to Follow? Data Center Knowledge. Retrieved February 21, 2021 from https://www.datacenterknowledge.com/archives/2016/01/06/data-center-design-which-standards-to-follow

Stansberry, M. 2021. Explaining the Uptime Institute's Tier Classification System. April 2021 Update. Uptime Institute. Retrieved April 7, 2021 from https://journal.uptimeinstitute.com/explaining-uptime-institutes-tier-classification-system/

TAPA. 2021. Standards and certifications. Transported Asset Protection Association. Retrieved April 30, 2021 from https://tapaemea.jdi.nl/standards-certifications

TIA – Telecommunications Industry Association. 2021. About. Retrieved April 9, 2021 from https://tiaonline.org/about/

TIA – Telecommunications Industry Association. 2021a. The leading global data center standard. Retrieved April 9, 2021 from https://tiaonline.org/products-and-services/tia942certification/ansi-tia-942-standard/

TIA – Telecommunications Industry Association. 2021b. TIA-942 Certified data centers. Retrieved April 9, 2021 from https://tiaonline.org/942-datacenters/?fwp_regions=western-europe&fwp_sort=title_asc

Uptime Institute. 2021. About Uptime Institute. Retrieved April 7, 2021 from https://uptimeinstitute.com/about-ui

Uptime Institute. 2021a. Uptime Issued Awards. Retrieved April 7, 2021 from https://uptimeinstitute.com/tier-certification/tier-certification-list

Uptime Institute. 2021b. Tier Classification System. Tier Certification. Retrieved April 8, 2021 from https://uptimeinstitute.com/tiers

Uptime Institute. 2021c. Tier Certification Operational Sustainability. Tier Certification. Retrieved April 8, 2021 from https://uptimeinstitute.com/tier-certification/operations

Figures

Tables

Appendices

Appendix 1: Heuristic evaluation manuscript

HEURISTIC EVALUATION SESSION MANUSCRIPT

Observer presentation

- Mikko Helin, Master's thesis researcher, Laurea University of Applied Sciences, Degree Programme in Security Management, Master of Business Administration
- Thesis main development tasks 1. *Defining and designing a holistic data center security management framework for European region. 2. Producing a user-friendly tool for evaluating data center security management through the framework.*
- Evaluation session is anonymous, lasting 1 hour
- Aim of this evaluation session is to find usability problems and to evaluate general acceptability and usefulness of the tool and the framework

Evaluator presentation

Domain expertise background

- Work experience in data centers, information security, or corporate security domain?
- Work experience in usability engineering?
- Work experience in years?

Heuristic evaluation

Evaluator is asked to go through the interface of the tool several times and to inspect the dialogue elements and to compare those to usability elements listed below and provide feedback based on these.

- Simple and natural dialogue
- Speak the users' language
- Minimize the users' memory load
- Consistency
- Feedback
- Clearly marked exits
- Shortcuts
- Good error messages
- Prevent errors
- Help and documentation

Found usability problems during this evaluation session are documented by observer in a simple table:

Problem 1.	
Problem 2	
Etc.	

General acceptability and usefulness of the tool and the framework

Comments and opinions from Evaluator related to general acceptability and usefulness of the tool and the framework.