Developing camera surveillance

Tuomas Tähkä

2020 Laurea

Laurea University of Applied Sciences

Developing camera surveillance

Tuomas Tähkä
Safety, Security and
Risk Management
Bachelor's Thesis
January 2021

Laurea University of Applied Sciences **Abstract**

Safety, Security and Risk Management

Bachelor's Degree

Tuomas Tähkä

Developing camera surveillance

Year 2020 Number of pages 55

The purpose of this functional thesis is to demonstrate how a camera surveillance plan was produced for the case company and what kind of benefits does it provide if this plan is implemented as part of the security processes. This thesis is most useful for the case company and the professionals working in administrational and operational security. In addition to the case company professionals, methods are applicable in other camera surveillance related development projects. For the use of other professionals, a checklist tool has been provided in the thesis as well.

The development task of the thesis was to examine the current state of the case company camera surveillance system and after that deliver development ideas on how to utilize the case company camera surveillance system more efficiently in the future. The case company personnel also wanted documentation that delivers justification for the use of camera surveillance in the building.

The theoretical framework of the thesis composes of camera surveillance, physical security, risk management, and business continuity related literature including ISO standards and professional handbooks. Methods of the thesis are level of security assessment, risk assessment, defense-in-depth assessment, K method test, and business impact analysis. These methods provided results, which enabled the formation of a camera surveillance strategy. This strategy is written as a camera surveillance plan, which is the product of this thesis.

The final product will deliver an efficient camera surveillance strategy that the case company can utilize as such. The product also demonstrates key risks that might affect the camera surveillance system itself making the whole system more resilient. When the camera surveillance plan is used, the case company can ensure the level of surveillance quality, resilience, and efficiency of the monitoring conducted with building cameras. The introduction of the product is left out of the scope due to confidentiality reasons.

Keywords: camera surveillance, CCTV plan, physical security, business continuity

Laurea-ammattikorkeakoulu **Tiivistelmä**

Safety, Security and Risk Management

Bachelor's Degree

Tuomas Tähkä

Kameravalvonnan kehittäminen

Vuosi 2020 Sivumäärä 55

Tämän opinnäytetyön tarkoituksena on esitellä miten kameravalvontasuunnitelma tuotettiin case-yritykselle, sekä minkälaisia hyötyjä tämän suunnitelman käytöstä syntyy, jos se otetaan käyttöön osana päivittäistä turvallisuustoimintaa. Tämä opinnäytetyö on tuotettu case-yrityksen turvallisuushenkilöstön käyttöön, mutta metodit sekä lopputuote ovat sopivia muihin kehitysprojekteihin, jotka liittyvät kameravalvontaan. Muiden kehitysprojektien käyttöön on luotu tarkastuslista, joka jaetaan osana tätä opinnäytetyötä.

Opinnäytetyön kehitystehtävänä oli tuottaa nykytila-analyysi case-yrityksen kameravalvontajärjestelmän nykytilasta sekä tämän analyysin pohjalta tuottaa kehitysideoita, joita voidaan käyttää tulevaisuudessa kameravalvontajärjestelmän tehokkuuden varmistamiseksi. Tämän lisäksi case-yrityksen henkilöstö halusi dokumentaation, joka oikeuttaa kameravalvonnan käytön case -yrityksen rakennuksessa.

Opinnäytetyön teoreettinen viitekehys koostuu kameravalvontaan-, fyysiseen turvallisuuteen-, riskienhallintaan- ja jatkuvuudenhallintaan liittyvästä kirjallisuudesta johon muun muassa kuuluvat ISO-standardit sekä ammatilliset käsikirjat. Opinnäytetyön metodit ovat: turvallisuustason arviointi, riskien arviointi, defense-in-depth -arviointi, K menetelmä ja kohdistuvien vaikutusten arviointi. Nämä metodit tuottivat tuloksia, jotka mahdollistivat kameravalvontastrategian synnyn. Tämä strategia kirjoitettiin auki kameravalvontasuunnitelmaksi, joka on tämän opinnäytetyön lopputuote.

Lopputuote mahdollistaa tehokkaan kameravalvontastrategian käyttöönoton sellaisenaan minkä lisäksi lopputuote myös havainnollistaa pääriskit, jotka saattavat vaikuttaa kameravalvontajärjestelmän toiminnallisuuteen, mikä mahdollistaa kestävämmän kameravalvontajärjestelmän. Kun kameravalvontasuunnitelmaa käytetään, case-yritys voi varmistaa valvonnan tason, kestävyyden ja tehokkuuden valvonnassa, joka toteutetaan kiinteistön kameravalvontajärjestelmällä. Luottamuksellisista syistä lopputuotteen esittely on jätetty opinnäytetyön skaalan ulkopuolelle.

Avainsanat: kameravalvonta, kameravalvontasuunnitelma, fyysinen turvallisuus, jatkuvuudenhallinta

Table of Contents

1 Introduction

The purpose of this functional thesis is to introduce how a camera surveillance plan was produced for the case company and what kind of benefits does it provide if this plan is implemented as part of the security processes. The thesis also introduces a checklist tool that can be used in other camera surveillance projects. The thesis composes of theoretical background, methods used to produce this plan, results, and conclusion. In the theoretical background, the basic functionality and the main implication of camera surveillance are introduced for the reader. This section also elaborates on main functions related to security operations involved with camera surveillance as well as the theory behind methods used in this thesis work. The method section of this thesis presents how methods were utilized in the case company building and the implementation of these methods is displayed in chronological order. The results section of the thesis introduces the camera surveillance plan itself and findings that were made after the methods had been performed. The last part of the thesis, the conclusion, handles the writer's own conclusions regarding the work that was carried out.

One key factor realized in the early stages of information searching was realizing that the security related literature is lacking with instructions about how to produce a camera surveillance plan. Because of this lack of information, it is valuable to demonstrate the methods that were tested during the production of the plan as well as present the findings that were made after the methods had been tested in a real-life business environment. Providing this information in the thesis is not only useful for the case company but for professionals working in the security field. Besides introducing the method process and the results, thesis also introduces a tool called checklist that can be used in other environments and camera surveillance projects. The methods of the thesis delivered results that enabled a strategy and this strategy was formed into a plan. The development goal of this thesis is to develop the case company camera surveillance system, introduce methods and results of this development assignment and introduce a checklist tool which can be used in other related projects. The thesis also aims to provide benefits of why a camera surveillance plan should be produced.

1.1 The case company

The case company itself is a global organization that operates in the IT-sector and the headquarter for operations conducted in Finland is a large office building that hosts over 1000 employees daily. The headquarters has over 60 surveillance cameras placed inside and outside of the building. Most of the cameras are in the first-floor interior area and the outside exterior area of the building. The second most surveilled area with the cameras is the basement lev-

els. The rest of the cameras are located at the outside visitor parking area and the public areas on the upper floors. The main influencing factor for camera surveillance system in the building is that the case company's security related policies and standards required "positive identification of all visitors and members entering the facility". Because of these policies and standards, every entry made to the building was monitored with a surveillance camera. The case company uses camera surveillance as part of their overall facility security processes. Camera surveillance is utilized in the protection of assets, property and staff, surveillance of critical areas and entry points as well as enhancing the investigations after a possible crime or adverse event has occurred.

The initial demand for this thesis was realized during an internship that was carried out in the case company headquarter at the start of the year 2020. The case company security team wanted to review and update their current physical security systems of the building and decided to offer this development project for safety, security, and risk management student. The assignments concerning the internship were the formulation of a current state assessment and development of the camera surveillance, access control, and alarm intrusion detection systems of the building. During the current state assessment, strengths, weaknesses, and areas of development of the security systems were discovered. After the development areas were introduced to the case company security team, both the case company supervisor and the writer of this thesis realized that, a separate camera surveillance related thesis project could be carried out to bring additional value to the case company physical security operations. Besides additional value, the case company security team realized that they were lacking a plan that delivered justification for the use of camera surveillance in the building. Because of these factors, it was decided that the goal of the thesis is going to be a production of a camera surveillance plan that introduces strategy and guidelines related to the building's camera surveillance operations. After this decision, the internship was solely concentrated on other areas of physical security, and the camera surveillance development tasks were produced separately as a thesis work.

2 Theoretical background

This section of the thesis composes from theoretical background that introduces relevant literature that effects the camera surveillance and theory behind methods that were utilized in the thesis work. This section also introduces the basic functionality and features of a camera surveillance system, including different ways how surveillance is performed, how data is transmitted between a camera and a monitor screen, as well as what kind of recorders are suitable for different usage. According to authors Estelle Phillips and Derek S. Pugh (2010), the relating activity behind theoretical understanding is to demonstrate that the writer has a professional command of the background theory (Phillips, Pugh, 2010. 65). This professional

command was established by reading security related literature in the early stages of the thesis. The primary stress was targeted to camera surveillance and to business functions that either use camera surveillance directly or introduce methods that were utilized to test and develop camera surveillance in the case company building.

2.1 Business continuity

Business continuity management and business continuity planning are a part of a business that is in charge of planning and preparing an organization for a disaster. The focus of this practice is to recover from a disaster and maintain operations during a disaster. Author Stuart Hotchkiss (2010) states that the essence of good continuity is that everything is planned to the smallest detail so that there is no need to think when something goes wrong. Key parts in operations are to maintain business running at a service level that customers accept as well as emphasizing the functionality of IT procedures during a disaster (Hotchkiss 2010). Authors Wei Ning Zechariah Wong and Jianping Shi (2013) also handle the fundamentals of business continuity by stating that business continuity management is a versatile discipline and this discipline is about the management of threats and their impacts to critical operations. According to the authors, this discipline "improves the organization's capacity to withstand the impact of an incident that may otherwise jeopardize its ability to achieve its objectives" (Wong & Shi 2014, 6). With profound and comprehensive business continuity planning, organizations can establish leverage that will increase their likelihood of survival during disasters.

ISO 22301 standard provides a framework for the business continuity management system which is a key part of business continuity management. Factors and actions included in the scope of the business continuity management system, according to the standard (2012), include ensuring that organizations establish parts of the organization and requirements of BCM while considering the organization's goals, mission, internal and external obligations as well as legal and regulatory responsibilities. Organizations shall also identify products, services, and all related activities and interested parties, such as customers and stakeholders while ensuring the scope of the system. When the scope is defined the organization documents and explains exclusions (ISO 22301 2012, 10). The business continuity management system also has a policy, which is established by top management. Executing this according to the standard means (2012) that the policy is appropriate to the purpose of the organization and that it provides a framework for setting objectives to the business continuity. The policy should also satisfy the continual improvement of the BCMS and be available for interested parties as documented information (ISO 22301 2012, 11). In addition to the ISO standard, Author Tony Drewitt also states (2013) that "essentially, the policy is both a commitment to doing things, and a mandate to execute the tasks necessary to doing those things; in this case, the development and maintenance of a BCMS" (Drewitt 2013, 23).

The key component of business continuity is the business impact analysis - BIA. Authors Andrew Hiles and Kristen Noakes-Fry introduce the business impact analysis. According to the authors (2015), implementing a BIA is necessary for effective business continuity management. It will also work as a justification for the chosen business continuity strategy (Hiles & Noakes-Fry 2015, 149). Authors John Rittinghouse and James G. Ransome specify the BIA procedure as a "process of identifying the critical business functions and the losses and effects if these functions are not available" (Rittinghouse & Ransome 2011, 140). Authors Andrew Hiles and Kristen Noakes-Fry (2015) also introduces that the BIA process includes the preliminary assessment of required resources for recovery, providing input to the risk assessment and raising awareness of the business continuity. Conducting the business impact analysis, an organization will gain new undiscovered information relating to the business risks and has a documented pre-planned guideline that will allow more resilient activity (Hiles & Noakes-Fry 2015, 150-151). In the essence of a business impact analysis is identifying critical functions and services and a time window in which recovery must take place. Authors Andrew Hiles and Kristen Noakes-Fry (2015) state that the business impact analysis will help an organization to identify areas that are critical to achieving their mission, set a risk appetite of the organization, define the timeframe in which recovery has to take place, and identification of vital documents and other material that is needed during a disaster. Risk assessment is closely involved with the BIA and typical risk areas of this practice are, for instance, health, life, safety, financial, quality, compliance, and legal requirement-related risks (Hiles & Noakes-Fry 2015, 150-151).

Business continuity is a vital part of business operations no matter what industry is dealt with. At the start of the year 2020, word-wide pandemic Covid-19 virus was discovered and within months the virus has spread all around the world with its aggressive ability to transmit from person to person. This pandemic increases the meaning of business continuity and incident management for organizations and puts organizations and government's business continuity management into a test. In the ISACA blog post, author Susan Snedaker (2020) states that until recently few people outside of governmental agencies have seriously planned for a pandemic even though it is a line item in a business continuity checklist. According to her, it is important to look at the organization holistically to understand how the pandemic could impact company revenues, customers, and employees. With proper planning and scenario testing, a company can be better prepared to survive a global pandemic (Snedaker 2020).

According to author Abdullah Al hour (2012) physical security is highly linked with business continuity management by its comprehensive coverage and focus. A well-delivered physical security is effective in minimizing disasters caused by humans as its relevant controls are related to people-related threats. If this type of threat occurs, physical security contributes to the detection, controlling, and recovery phases. Because of this function, physical security is

one of the building blocks in the information security program that covers areas where technology, or logical, security falls short (Hour 2012, 165).

2.2 Physical security

Physical security in its fundamental purpose is set out to protect tangible assets of organizations and entities. Author Abdullah Al hour (2012) states that for an organization to properly operate and achieve its strategic goals, there must be a controlled environment with specific conditions no matter what industry the organization is operating (Hour 2012, 160). Dictionary of military and associated terms that sets the standard for US military and associated terminology to encompass the joint activity of the armed forces of the United States define physical security as the "part of security that is concerned with physical measurements designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material and documents; and to safeguard them against espionage, sabotage, damage and theft (Dictionary of military and associated terms 2017, 168). In the book, Effective physical security author Lawrence Fennelly (2012) says that in the battle against criminal activities "our resourcefulness in designing and developing more and better methods of protecting our life, property, and livelihood has been unbounded" (Fennelly 2012, 77). However, there is not a system that is 100 percent defeat-proof. If a system is designed to eliminate most threats, it will still have its weak links. If a system cannot fully protect assets, its minimum offer for protection must be the delay of the threat temporarily to the point at which the threat can be defeated (Fennelly 2012, 77).

Environmental design is an important part of physical security. The practice of crime prevention through environmental design (CPETD) is an agenda that is set out to manipulate the surroundings of buildings and neighborhoods to increase the level of security. The book Crime prevention through environmental design by authors Timothy Crowe and Lawrence Fennelly set out fundamentals and benefits when effective CPETD is executed as part of the operations. According to the authors (2013), CPETD is focused on "reducing the propensity of the physical environment to support criminal behavior" (Crowe & Fennelly 2013, 25). Author Rachel Armitage supports this statement by stating that "CPTED measures also often incorporate specific standards of physical security (including doors, windows, locks, glass) to increase the time and effort required to successfully break and enter into a building" (Armitage 2016, 3). Authors Timothy Crowe and Lawrence Fennelly (2013) also add that in this practice term, "design" includes physical, social, management, and law enforcement directives that aim to affect the behavior of people when people interact with the environment. Because of this behavior, CPETD program tries to prevent certain crimes within a specific environment by manipulating factors that are closely related to the environment itself. CPETD strategies include three overlapping factors; these are natural access control, natural surveillance, and territorial surveillance (Crowe & Fennelly 2013, 27-28).

According to author Abdullah Al hour (2012), an important part of physical security is a companywide, solid and clear physical security policy. The effective policy determines the scope, activities, and controls that the organization is using in their physical security and it should be integrated as part of other organization programs such as business continuity plan and information security. To determine accountability, the physical security policy should also cover the ownership of the overall physical security discipline and the owners of substantial activities (Hour 2012, 165-166). Implementing a physical security policy is an important part of security operations since it works, as a justification for chosen strategy as well as it is an effective tool that can develop the security culture of the organization.

Physical security activities include many different functions and categories. These activities, according to author Abdullah Al hour (2012), are introduced in the table below:

Function	**Barriers/systems included in the function**
Perimeter protection	Walls, fences, gates and guards
Access control	Keys, locks, ID cards, badges, mantraps and automatic access control
Internal premises protection and security	Confidential spaces inside the facility such as, data center and executive office, that must be protected with walls, access control, and doors
Surveillance and monitoring	Includes security systems like, camera surveillance and movement detection sensors. These systems produce vital data for the professional in charge of physical security.
Guards	Guards are utilized along with physical and technological setup being one the most major element of physical security.
Alarm systems	An element that works closely with surveillance and monitoring. Alarms notify and communicate events within the zone of surveillance allowing necessary actions to be taken.

Fire suppression system	System that automatically or manually suppress fire by reducing oxygen levels or burning temperatures

Table 1: Physical security activities and functions according to Abdullah Al hour

These activities don't work independently. They are used together as an integrated totality whose sole purpose is to prevent unwanted access, improper use, and minimizing threats to the lowest possible level (Hour 2012, 166-171).

Author John Kingsley-Hefty highlights the importance of understanding security goals and assessing the needs of your business in his book Physical security strategy and process playbook. The author states (2013) that before the assessment of a security system can start, a person in charge of the security system delivery must know related security goals. If security goals are not understood, a person in charge will not be able to implement a cost-effective system (Kingsley-Hefty 2013, 1-2). In addition to understanding the goals of the physical security system, author Lawrence Fennelly describes important approaches for physical security. According to author (2012) before implementing a security system, it is necessary to build a security plan that in its basic sense is a "description of the protection system and its components" (Lawrence 2012, 88). Author John Kingsley-Hefty also adds that establishing an overall assessment of the security issues relating to business operations is efficiently achieved with security assessment that, according to the author, is the first step in assessing the needs of the business (Kingsley-Hefty 2013, 1-2).

Camera surveillance is an essential and useful tool in the physical security function of a company. Authors Paul Baker and Daniel Benny (2016) state that "there are few subjects that dominate publications, education sessions, negotiations, and actual deployments as much as video surveillance does in the physical security industry" (Baker & Benny 2016, 123). The market today offers many different ways of how this surveillance can be carried out and the technology in the camera surveillance system has advanced a lot from its earlier days. The following section introduces the basic functionality of a camera surveillance system as well as different camera types and forms of surveillance.

2.3 CCTV system functionality

Camera surveillance is a popular physical security tool that is widely used for many different motives. The main implication is involved when a person or an entity is trying to protect and surveil their property. These motives, for example, are monitoring of ongoing production in industry, ensuring the health and safety of employees, protection of business assets, and protection of personal property. In its basic functionality, a camera surveillance system includes

a set of cameras, a monitor screen, and a person who is watching the footage transmitted from the camera lens to a monitor screen. With this function, the camera surveillance system enables remote surveillance of a designed area where the owner or operator of the system can deliver a service where different events can be surveilled either in real-time or captured for later use. Without camera surveillance, surveilling a big area with one or few persons would not be possible which enables a cost-effective surveillance solution for the security operations of different businesses.

CCTV (Closed-circuit television) is a highly popular form of surveillance carried out with multiple cameras that are connected to a recorder via cables. The recorder transforms camera footage into an examinable form, which is by then monitored with a computer screen. CCTV is usually utilized in business properties and in challenging process industry facilities. In addition, acquiring a CCTV system for personal use, for instance, cottage area or home apartment has increased a lot in recent years. The purpose of camera surveillance is to monitor the designed area and to gather footage for investigation. CCTV is also a tool for preventing crimes and property damages as it works as an effective deterrent.

2.3.1 Forms of surveillance

Footage achieved with CCTV is monitored with security guards working in a control room or monitoring via mobile phone application is also an option nowadays. The form of surveillance is chosen based on the necessity of surveillance. Forms of surveillance are divided into four different types: active monitoring, sporadically active monitoring, passive monitoring, and remote monitoring. The center of operations with active monitoring is the control room, which receives footage of camera surveillance and other alarm signals. The security guard is the most favorable choice to perform active monitoring. Daily operations for this type of security guard are to watch screens that broadcast CCTV footage and announce events detected in the designed surveillance area. Sporadically active monitoring is carried out by momentary monitoring of the CCTV footage usually activated because of stimulus, such as an alarm. This is usually utilized in small stores and gas stations by placing the monitor in the near presence of a cash register. Passive monitoring doesn’t need a control room at all. The main point of passive monitoring is to gather and examine footage that was recorded in the recorder afterward. It is also possible to have remote access to the recorder with an internet connection. This allows recorded footage to be examined from a private workstation. Remote monitoring is utilized in cases where a company decides to outsource its camera surveillance. Service is produced with a secured internet connection that connects the client and service provider. Alongside surveilling, the outsourced party also performs alarm monitoring and camera footage checkups (Kameravalvontaopas 2010, 39).

2.3.2 Technical features

Camera types in the market offer a lot of different options for a specific need. Choosing a certain type of camera always depends on the use and purpose of the camera. Usually, a functional camera composes of a power supply, optic, body, and pedestal. Nowadays the market for camera technology provides mostly cameras that provide color high definition footage, as well as buyer can choose from cameras that are solely designed for night or day surveillance. Options in the market include stationary indoor and outdoor bullet cameras, stationary dome cameras, PTZ – Pan Tilt Zoom - cameras, megapixel cameras, and other camera types, such as, EX-cameras designed for volatile areas, EMP-cameras protected by electromagnetic pulses, heat cameras, and spy cameras - cameras that are masked as something else than a camera. (Kameravalvontaopas 2010, 17).

Mostly used camera types in many industries are DOME-cameras, which allow the 360-degree field of footage with their ability to remotely adjust the direction of the optic, bullet-cameras, which are cost-effective, reliable and able to cover long distances. IP-cameras also have been witnessed in modern facilities due to their high-quality footage, network data transforming abilities, and software that can be updated frequently. This feature allows IP-cameras to have specific smart abilities like scanning license plates of cars, identifying persons, or alert when the camera detects a disturbance in the surveilled area (businesswatchgroup 2019).

2.3.3 Data transmission

Video footage data transferring is achieved by using two different options, analogical and digital form. In analogical data transfer, cameras CCD image sensor transfers the light that reflects on the surface of the sensor with an electrical signal. This signal moves forward for transfer where it is recorded. In digital data transfer, the IP cameras CMOS image sensor forms a picture from pixels. The difference from analogical data transfer with the cable to digital transfer is that the IP camera transforms the picture information to digital bits. These bits move via a data network to a network video recorder that stores the footage (Kameravalvontaopas 2010, 20).

CCTV technology handbook by the U.S Department of homeland security (2013) describes general data transmissions of CCTV. According to the publication, “CCTV transmission system is an important component that sends and receives video signals between the cameras, the processing system, and the monitoring system”. Criteria that effects in choosing the correct video transmission are the distance between cameras, monitor, and storage system. Options for video transmission are wired and wireless transmission, analogical and digital. In a wired transmission system, there exist three different options: Coaxial cable, fiber optic cables, and

UTP cables. A telephone network is also an option for wired transmission, however considering cybersecurity vulnerability threats, utilization of a telephone network is not advisable. In the wireless system, there exist four different options: Laser-, IR-, radiofrequency- and microwave transmission. According to the CCTV technology handbook, advantages in choosing wireless transmission are easy installation, lack of cabling requirements, and assured mobility. Disadvantages of a wireless system are the need for a dedicated frequency to transmit signals, signal interruptions, and signal interference (CCTV technology handbook 2013, 36-41).

2.3.4 Recorder features

Today markets offer three types of recorders: DVR (Digital video recorder), NVR (Network video recorder), or hybrid DVR. Choosing a video recorder is based on the camera type utilized in the facility. Analogical data transfer can only record footage with DVR. Features with this option are that the footage can be collected, reclaimed, and examined in the later stages since the recorder retains every single picture captured in the DVR. Additional features like movement sensing can be added to the system with specific software. The benefits of utilizing analogic technology are that their data protection related risks are much more minor since data transfer is not performed with the network connection. Other benefits are their overall performance such as reliability, vision during the night, and smaller expenses in the acquiring and maintenance phases. The negative side of analogical video surveillance is the quality of the footage. (Kameravalvontaopas 2010, 22)

According to author Nathan Dinning (2018), the digital form of recording technology has surpassed analogical form during the last ten years and many of the CCTV vendors invest in modern innovations for digital cameras. The analogical camera can produce HD, high definition, image which is suitable for many industries, but digital cameras can record 4k footage which gives them a lot of advantage on what comes to the quality of footage (Dinning 2018). NVR can only accept digitally transferred footage and that is why it is only used when IP cameras are utilized in a target facility. NVR technology enables a lot more features comparing to analogical technology due to its network quality. Besides previously mentioned features, register plate scanning and person identification, IP cameras can also be connected to smartphones.

Hybrid DVR combines both recorder features as it allows the recorder to accept both analogical data transformation as well as digital transformation. This is a suitable option for a client when they want to add IP cameras into already existing analogical CCTV system. Utilizing a hybrid DVR can enable many savings when a client wants to add newer technology cameras and does not want to lose already existing cameras in the system (Kameravalvontaopas 2010, 25). This will also enable more dynamic CCTV systems since it allows the implementation of modern technology camera features in the possible future CCTV system updates.

2.4 Legislation

Legislation regarding the CCTV restricts and provides practices that the owner of the CCTV must follow when CCTV is implemented to surveil a building. From a legislation point of view, video surveillance gathers image registry of individual persons and the main characteristics are related to where the video footage is gathered and how, where the footage is retained, how the recorded footage is handled, and who can access the surveillance camera footage. Besides previously mentioned functions the purpose for video footage retained must be justified.

Act on the protection of privacy in working life protects employees and their rights on CCTV related matters. The owner or subscriber of the CCTV must ensure that recordings of surveillance are used only for the purpose for which the surveillance was carried out. Employees are informed of when the camera surveillance will begin, how it will be implemented, how and in what situations any recordings would be used. Prominent notification of the camera surveillance and its method of implementation is displayed in the areas in which the cameras are located. The owner also must ensure that recordings are destroyed as soon as they are no longer necessary for achieving the purpose of the camera surveillance, and no longer than one year after the end of the recording (Act on the protection of privacy in working life 347/2019).

General data protection regulation also affects the operating of CCTV in a building. The owner of the CCTV must ensure that on the request of the person, the person has the right to gain access to the information related to his or her data, rectify mistakes or inaccuracies, and be forgotten when information is no longer needed. The owner must also ensure that person can obtain information on how their data is being handled and who can access the surveillance camera image (General data protection regulation 2016/679).

In addition to previously dealt legislations, the criminal code of Finland describes, that CCTV system should be planned in a manner where it does not gather footage that violates a person's privacy. Places related to this are toilets, dressing rooms, and particular employee or employees working desks. This function can only deviate if the nature of the work can cause an immediate threat to a particular employees' health or the employee has expressed a self-imposed need for a camera surveillance (Criminal code of Finland 531/2000). The criminal code of Finland does not require the previously mentioned actions but criminalizes the function if these rules are violated.

In the thesis work, legislation related actions were part of the CCTV plan produced for the case company. The legislation part of the plan described what kind of measures need to be taken into account for the case company to fulfill legislation related requirements. In addi-

tion, a video surveillance personal data register was produced during thesis project. This register was placed in the reception services that was the main operator of the CCTV system. This register is handed to every person who has an inquiry related to cameras that are recording footage in the public areas nearby the building. The register itself, described contact information, what kind of personal data was collected, how the data is handed over, the responsibilities of participants and rights of the person whose data is collected.

2.5 K method

K method is introduced by Finance Finland. The method is produced for the use of a person who is in charge of planning and acquisition of a camera surveillance system into a certain building. The person can also be a vendor of the system or owner of the camera surveillance system that is used in the building. The appropriate expedient is achieved when guidelines of the method are utilized during system planning, installation, monitoring, and maintenance phases. The method is also useful when it is used in assessing the quality of the footage, which is the main implementation of the K method during this thesis project. According to the camera surveillance-planning guide of Finance Finland, camera surveillance is a tool widely utilized by companies and properties, which produces continual footage-based information of properties areas and target that is placed into a particular space. The camera surveillance system in this context means a system that can record live footage, which enables active real-time surveillance of the designed area. The meaning of camera surveillance, according to the camera surveillance-planning guide, is to generate a stimulus that allows appropriate actions to be initiated that prevents or mitigates damages targeted to personnel or fortune assets (Kameravalvonnan suunnitteluohje 2017, 4-5).

An important part of camera surveillance is the planning and design of the field of footage of every single camera. In camera surveillance, every camera should have a designed target or goal that is under surveillance. This target can for instance be surveillance of a certain door, fence, area or camera can be installed to identify persons entering a certain building. K method provides a testing tool that defines the quality of footage obtained with a surveillance camera. In this test, the executor places a test board in front of a camera. The test board has three different qualities that represent a target for the tested camera. After the test, the executor can see results from a screenshot captured from the precise moment when the board was held in front of the surveillance camera. According to the camera surveillance planning guide, the goal of camera surveillance is the detailed data gained from a target that has been surveilled. The requirements in the test board are K120, which is used for the individualization of the target of the footage. K50, which is used for recognition of a target surveilled, and K10, which is used for the detection of a surveilled target (Kameravalvonnan suunnitteluohje 2017, 5).

The K120 requirement means that the target of the surveillance takes 120% of the screen that is used for receiving footage that cameras provide and that the person monitoring this footage can identify the target that has been recorded. Because of this, K120 is the most suitable requirement for a surveillance camera which goal is to identify a person entering a building. In addition, cameras that can record K120 footage are suitable for scanning register plates of cars and they can be utilized as a support function for access control. K50 requirement is most suitable for recognizing persons and, for instance, cars. In person recognition, this data can mostly be utilized when the record is used to determine if the person in the field of footage is a boy or girl, young or old e.g. Cameras designed to produce K50 footage are placed in a manner where the target takes 50% of the screen that receives the recorded footage. This type of camera can surveil a greater area than K120, but it cannot retain identifying data of persons or cars. Data utilized from K50 cameras mostly composes of detection of events happening in the perimeter or some other bigger area of surveillance.

Requirements in K10 quality is that the target takes 10% of the screen used in monitoring. K10 requirements are most suitable for recording events of a big area and detecting, for instance, is there a large mass of people or just a small group in the designed surveillance area (kameravalvonnan suunnitteluohje 2017, 6-9). The placing of cameras is the key factor when the quality and target of footage is determined. For example, decreasing the height of a camera can bring K120 qualities into a camera that earlier was used to surveil with quality that is natural for K50 camera. Paying attention to the placement, height and the target of each camera is a vital part of succeeding in camera surveillance related design and development tasks. The figure below elaborates on the target of surveillance cameras by utilizing the K method. The first screen on the left represents the K120 target of footage. The middle screen is an example of a designed K50 field of footage and the screen on the right is utilized for the K10 target of footage. Target on the screen is a person that is 160-180 centimeters tall.

Figure 1: Target of footage by K method, 2017

The test board that is used in the K method camera test helps owners and main operators of camera surveillance systems identify cameras' abilities and find deficiencies. The test board has black and white lines side by side that are placed horizontally and vertically. A camera that is designed to establish K120 surveillance footage must show visibly every horizontal and

vertical line in the K120 part of the test board. The K120 part horizontal and vertical lines are placed more frequently and thicker than lines in K50 and K10. The frequency and thickness of the lines in the board establish the result of the cameras' abilities. Figure 2 and 3 demonstrate the test board that is used in the K method test and in this thesis project work.

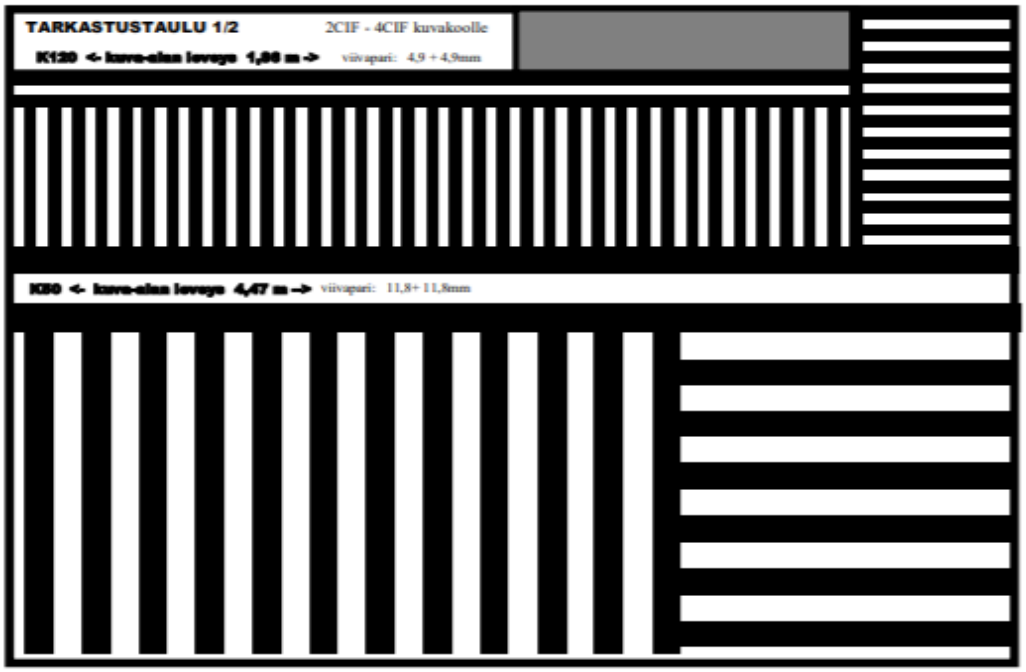

Figure 2: K method test board (K120, K50), 2017

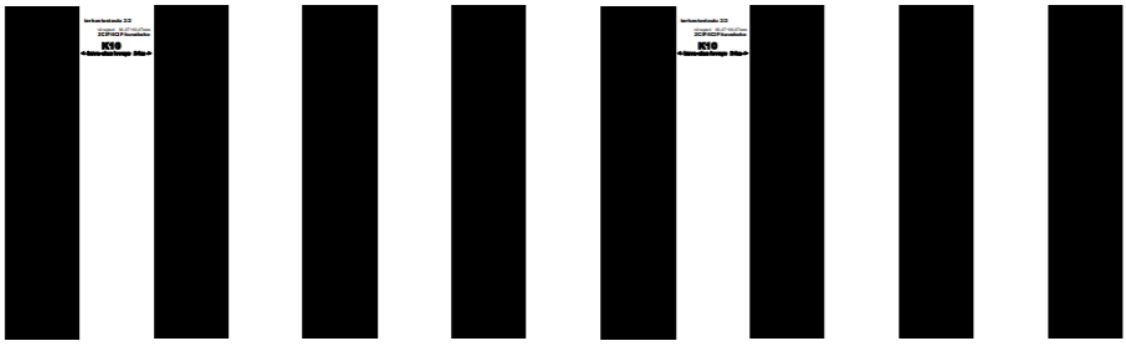

Figure 3: K method test board (K10), 2017

Camera surveillance planning guide by Finance Finland provides accurate printing and execution guides. After the test board is printed, it can be utilized for a camera quality test. An accepted result shown in the screenshot from camera surveillance footage must visibly show every line seen in the figure. The failed result does not show either vertical or horizontal lines and the screenshot shows blurred pixels. The requirement is that both vertical and horizontal lines can be witnessed in the test result. If the camera, for instance, does not clearly demonstrate lines in the K120 part but the abilities of this camera show K50 lines, then this

particular camera is classified as a K50 camera (Kameravalvonnan suunnitteluohje 2017, 34-35). If this cameras' goal is to identify persons entering a building, then the owner of this camera must find ways to upgrade qualities in this camera. This can be carried out by decreasing the height where the camera is placed, or the owner can also consider buying a new camera system that delivers the required quality.

An alternative testing tool for surveillance camera quality is a test chart provided by ViDi labs, a company based in Australia. In their product, a person carrying out quality tests places a test chart in front of the camera covering 100% of the field of footage. Then the testing area is illuminated with LED lamps to a required LUX level. When the environment is organized, a video recording is performed. Image must be captured from this recording and exported to a ViDi lab software that analyses image and obtains the results as graphs and plots that are sent to the customer. ViDi labs test chart is suitable for high- and ultra-high definition cameras to cameras featuring lower megapixels and is produced based on the recommendations of IEC 62676-2 standard (ViDi Labs HD/UHD test chart v.5.x Product manual 2019). Both methods have similarities in the way of running the test since both are done by utilizing a test board and capturing an image from recording. K method was suitable for this thesis work since all the cameras in the building were analogical with low megapixel quality. ViDi lab test is more comprehensive and suitable for high definition surveillance cameras.

2.6 Level of security

For choosing appropriate methods, tools and effective resource allocating it is reasonable to determine the level of security. Determine the level of security is introduced in the book Effective physical security by author Lawrence Fennelly. In this practice (2012), levels are divided into five different levels from minimum to maximum. Physical barriers, such as fences, camera surveillance, alarm systems, guards, and other components, and a combination of them together establishes a certain level of security. The minimum-security level includes simple physical barriers and locks in turn maximum-security level includes a sophisticated alarm system and on-response force. A good example of the minimum-security level is an average American home whereas Maximum-security levels are usually found in nuclear facilities, prisons, military bases, and government research sites. (Fennelly 2012, 77-80). According to author (2012), when the assessment and planning of the level of security is conducted, it is important to understand what assets are being protected, does the cost of protection outweigh the possible value gained from protecting, and how important the overall protection is to the company. When suitable solutions have been determined and the security system ensemble has been implemented, an organization can decrease asset-targeted risks to an acceptable level (Fennelly 2012, 81).

A similar methodology is introduced in the book Physical Security Strategy and Process Playbook by author John Kingsley-Hefty (2013). In the book, the author utilizes security zones as a deterrence mechanism where incidents can be avoided by "creating a security zone in which individuals considering a security violation realize that the probability of being detected and identified is far greater than the reward they can expect to gain from the violation" (Kingsley-Hefty 2013, 5). In the authors' method, the most effective security zones have a high identification and probability of detection and a low amount of expected reward while moderately effective zones and ineffective zones can be enhanced by increasing the probability of identifying an unauthorized behavior as well as overall detection or lowering the expected reward from a possible crime (Kingsey-Hefty 2013, 6).

2.7 Risk management

Assessment of risks is essential in camera surveillance related improvement and current state assessment projects. Risk management is a dynamic process that needs to be examined and updated regularly. ISO 31000 (2018) standard describes risk as an "effect of uncertainty on objectives" and risk management as "coordinated activities to direct and control an organization with regard to risk" (ISO 31000, 6). The standard provides a risk management process that can be applied at different levels of an organization. These levels are strategic, operational, program, project, or other activities (ISO 31000, 13).

According to ISO 31000 (2018), risk assessment is an overall process that includes risk identification, risk analysis, risk evaluation, and risk treatment. The purpose of the risk identification phase is to find, recognize, and describe risks that might help or prevent an organization from achieving its objectives. Relevant, appropriate, and up-to-date information is important in identifying risks. Factors that must be considered are, for instance: tangible and intangible sources of risk, causes and events, threats and opportunities, vulnerabilities and capabilities (ISO 31000, 15-16). In addition to ISO standards, author Ariane Chappelle (2019) introduces another approach to risk identification. According to author "risk identification in an organization should take place both top-down, at senior management level, looking at the large expousures and threats to the business, and bottom-up, at business process level, looking at local or specific vulnerabilities or inefficiencies" (Chappelle 2019, 3).

According to ISO 31000 (2018) the risk analysis phase involves a detailed consideration of uncertainties, risk sources, consequences, likelihood, events, scenarios, controls, and their effectiveness. The analysis techniques can be qualitative, quantitative, or a combination of both, depending on the circumstances and intended use. Risk analysis provides input to risk evaluation. This information is utilized in the decision making about whether risk needs to be treated and how, and what is the most appropriate risk treatment strategy and methods (ISO 31000, 16). Author Thomas Wolke (2017) introduces an additional approach to risk analysis by

stating: “risk analysis depends first of all on the risk attitude of the business or the investor. The spectrum ranges from completely risk-averse to totally risk-taking” (Wolke 2017, 74).

The following step according to ISO 31000 standard is the risk evaluation phase. The purpose of risk evaluation is to support decision-making. The outcome of risk evaluation should be recorded, communicated, and then validated at appropriate levels of the organization (ISO 31000, 17). Author Evan Wheeler describes risk evaluation phase by stating that risk evaluation means prioritizing which risks need to be addressed and how. This function determines the proper steps to manage risk by either accepting, mitigating, transferring or avoiding a particular risk (Wheeler 2011, 147-148). The last phase of the process is risk treatment where the actual mitigation, acceptance, transferring and avoidance actions are carried out. According to ISO 3100 standard (2018), the purpose of risk treatment is to select and implement options for addressing risk. This phase includes for instance, formulation and selection of different risk treatment options, implementing the actual risk treatment as well as deciding if the remaining risk is acceptable and if not, taking further treatment (ISO 31000, 17). The whole process of risk management is a comprehensive continual function that includes systematic application of procedures, policies, and practices to actual activities that are, for instance, consultation, communication, treating, and reporting. This process is illustrated in the figure below.

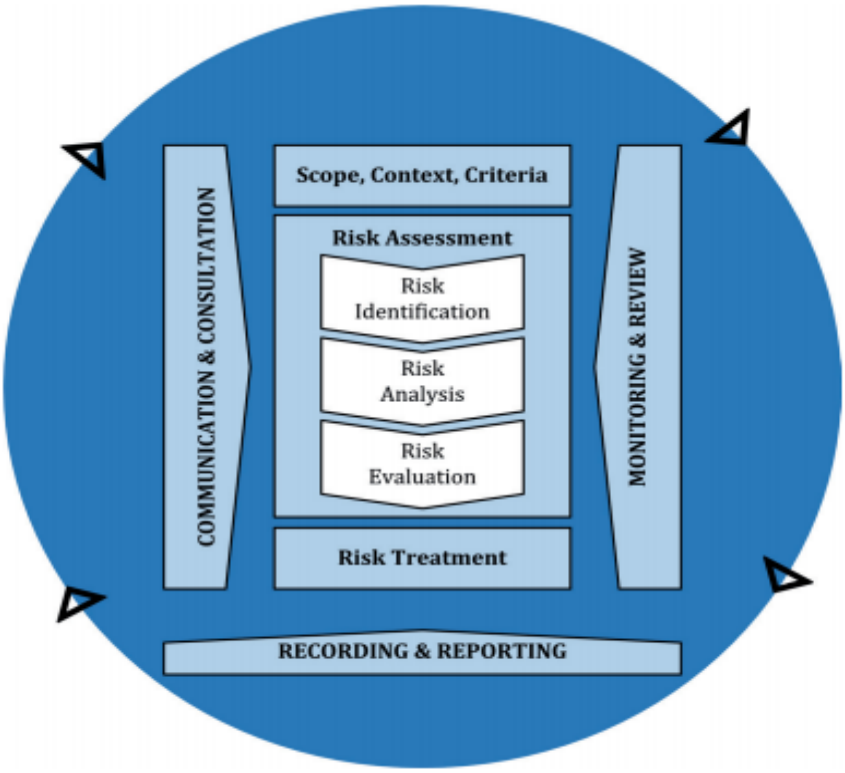

Figure 4: ISO 31000 Risk management process, 2018

Risk management is a practice largely applied in a variety of activity from legal and financial to physical and operational risks. Risks related to camera surveillance are mostly operational risks. In the book Operational Risk Management, authors Ariel Pinto, Raed Jaradet, and Luna Mylene (2015) introduce the foundation for operational risk management. According to authors, operational risk management is related to accidents, hazards, and risks. Accidents are refereed as "events that are not intended to happen", hazards as "objects, actions, processes, or conditions that may contribute toward the occurrence of an accident" and risks as a "future events with undesirable consequences without specific regard to intent, and hence include accidents and non-accidents" (Pinto & Jaradet & Maylene 2015, 3-5). Examples of operational risks are, for instance, theft, vandalism, or abuse. Camera surveillance as treatment can mitigate or remove the likelihood of these risks.

Carrying out risk management, an organization can make many of the processes more efficient, increase the quality of whole operations and make a profit in saved expenses. A good example of successful risk management is introduced in the book Winning with Risk Management by author Russel Walker. In the book, the author uses JPMorgan and the company's success during the 2008 real estate crisis as an example. According to the author (2013), JPMorgan "brilliantly executed a strategy that was rooted in understanding its risk and adapting to the market, as risk metrics and risk information suggested the US real estate market was approaching a downturn". Because of this strategy, not only did JPMorgan successfully survive the real estate crisis but was able to benefit from it. This benefit was realized in terms of risk management when JPMorgan conducted the corporate acquisition of Bear Stearns at 10 dollars a share and purchasing of Washington mutual, which was the largest savings and loan operator in the US. Because of risk-based decision-making culture, JPMorgan was able to examine decisions with long-term goals in mind and turn adversity into fortunate (Walker 2013, 199).

2.8 Defense-in-depth

When assessing spaces inside and outside of a certain building it is advisable to conduct the defense-in-depth assessment. Utilizing defense-in-depth, a person planning physical security into a location, can allocate resources more effectively and find suitable barriers to increase asset protection. In the book, The Complete Guide to Physical Security, author Paul baker and Daniel Benny elaborate the fundamentals behind layer defending. According to authors (2013), the formation of defense-in-depth includes the arrangement of barriers, such as fences, walls, and windows, into layers. The level of security grows progressively as the layers come closer to the center or a specific target, such as the highest protective area. For asset defending, utilizing this method is useful since if one layer fails, another layer might be able to prevent the attack and protect the designed target. Also choosing barriers with strong and

durable materials can improve the level of protection since materials that are hard to penetrate will cause a lot of noise and delay a during possible break-in and by this increase the reaction time for the personnel in charge of security (Baker & benny 2013, 59).

Effective defense-in-depth planning starts from threat analysis of the site. Possible threats in this context include, for instance, vandalism, robbery, terrorism, and kidnapping. This follows designing a system phase that involves choosing suitable equipment and procedures. The fundamentals of this system are the same as they are in any protection method: deter, detect, delay, and respond. The final stage is testing the system, which can be carried out with a penetration test (Baker 2013, 61). The benefits of physical security penetration testing is that person planning or improving security procedures can get accurate results from the efficiency of the defense-in-depth practice (Baker 2013, 71). According to an article post by author Janelle Penny (2018) a physical security penetration test is a comprehensive assessment of all of the physical security measures in a facility. In this test, "inspectors will try to gain access in to critical infrastructure and executive areas by picking locks, hopping fences, piggybacking with credentialed employees or otherwise attempting to gain access to secure areas" (Penny 2018). In the case company environment, the key functions under the inspection of a penetration test is testing how well the reception services detect authorized and unauthorized personnel, do they detect forged access badges as well as are employees of the case company questioning the movement of unfamiliar or suspicious people inside the building.

Author Lawrence Fennelly (2013) addresses technical methods and devices utilized in layer defense in her book Effective Physical Security. According to the author, most usual technical methods to use in a defense-in-depth protection are access control, camera surveillance, and alarm intrusion detection systems (Fennelly 2013). The access control as a layer defense mechanism allows or denies the entries of people trying to enter a building through doors. This function also registers and records every attempt of entries. Camera surveillance in this context records and registers events that are happening in the protected area as well as works as a deterrent for possible criminal behavior. The alarm intrusion detection is a system that alarms when break-in attempt are performed in the protected area. This system also notices sabotage in the areas where components are installed. These components are small devices that are usually installed in windows, doors, or walls of a building and they react to heat, sound or vibration alternations in the area that it is monitoring. Combining these into part of the defense-in-depth strategy will increase the level of asset protection.

A similar methodology is introduced in information security guidelines on business premises produced by the Finnish Ministry of Finance. This guideline relates to information protection and what kind of information is allowed to be handled in a specific area and what kind of control measures need to be taken account in specific control areas. The guideline is mostly tar-

geted to official authorities and spaces they utilize but it is also applicable for public and private operators. In the Ministry of Finances guidelines (2013), spaces are divided into public space, basic level space, increased level space, and highest-level space. Every space in the guideline has its own criteria of information that is allowed to be handled and preserved in this specific area. Information classification is set as ST-I highest secret classification, ST-II high-level classification, ST-III increased level classification, and ST-IV Basic level classification (Toimitilojen tietoturvaohje 2013, 19-23). Utilizing The Ministry of Finance guidelines the defense of a particular target or asset increases as personnel is guided not to handle information in an area where it is not allowed. When information is classified, it is only permitted to be handled or modified in its designed destination resulting in increased information- and asset protection.

3 Methods

This section of the thesis introduces the methods utilized in this functional thesis. Author Maria J. Mayan (2009) states that "a method provides a set of procedures, not prescriptions that outline, for instance, the method's data collection strategies, typical sample size, and analytical strategies" (Mayan 2009, 31). The main value sought from selected methods was to find solutions for a particular problem, which in the case company building meant, a procedure that was not at the desired level or a tool that did not perform desirably. After reading and familiarizing to security fields theory it was decided that the methods described in this section were sufficient and practical to achieve the goals that were set for this thesis. According to author Jorma Kananen (2015), choosing the right method requires that the researcher has a profound understanding of the research problem and choosing the method is the action that provides an answer to the research problem (Kananen 2015, 65). In this thesis, the research problem is not established but the goal is to produce a camera surveillance plan and discover ways on how to develop the current state of the case company camera surveillance system. Understanding this goal was the quality that enabled the guidelines of the thesis production and made the selection of methods phase easier and efficient. In this phase resources were solely targeted on finding methods that ether help to find sufficient ways to assess the building and its critical assets, finding methods that increase the resilience of the camera surveillance system as well as finding methods to test the quality of the surveillance camera footage.

3.1 Functional thesis

This thesis is a functional work that was performed in the case company building. Author Tiina Airaksinen addresses the elements and functions related to the functional thesis. According to her (2009), the thesis is strongly related to writing and writing is an action to make

findings and results visible to you and others. In the functional thesis, the goal is to produce practical guidelines or organize operations as well as rationalize operations and activity. Depending on the field of studies, a functional thesis can, for instance, be instructions, environment program, safety instructions, or crisis communication guidance (Airaksinen 2009). This thesis work is applicable to authors' statements since the product of the thesis is a written camera surveillance plan that introduces guidelines that aims to organize the camera surveillance operations and increase the level of performance of the camera surveillance system of the case company building. Author Tiina Airaksinen (2009) also states that the functional thesis has two parts, a functional part which is production, and documentation of a process (Airaksinen 2009). These parts also fit for the style of this thesis since the methods of the thesis was tested and afterwards analyzed in the case company working environment and then elaborated in this thesis.

In the book Toiminnallinen opinnäytetyö authors Vilkka and Airaksinen (2004) state that functional thesis should be practical and originated from working life. It should prepare the student to be able to participate as a professional in the field of work after graduation, as well as understand the fundamentals of development and research of their field of expertise (2004, 10). The case company ordered this thesis work because their physical security operations were lacking a sufficient camera surveillance system that achieves their global security objectives. Because of this deficiency, this thesis work was originated from real working life that provides practical solutions and guidelines in a form of plan that aims to achieve the security objectives of the case company. In addition, this thesis work was a development assignment that required understanding of the fundamentals of the camera surveillance system, physical security as well as knowledge on how to develop security in a business property. Authors Vilkka and Airaksinen also state (2004) that profound familiarization to the field's literature, researches and electronic sources are an important part of the functional thesis. Utilizing these the student can reflect his or her ideas and produce a solution for a certain problem. The student's ability to utilize theory to solve problems and to produce practical solutions is the goal of every studies conducted. Managing this the student can be part of developing the professional culture of the chosen field (Vilkka & Airaksinen 2004, 41-42). Getting familiar with literature and electronic sources was the first steps of this thesis work. Theory and methods introduced in these sources were tested and results based on these tests were analyzed. How these methods were tested in the case company building is introduced in the following sections of the thesis.

3.2 Method process

The method process of the thesis started from familiarization and checkup of the site. This task was performed with a level of security assessment. After the level of security assessment was carried out, the relevant risks regarding camera surveillance were identified, analyzed,

and treated. In the following phase, the defense-in-depth was performed to identify critical areas in the building. After critical areas had been identified, a camera footage quality test was carried out with the K method test board. The last phase of the method process was the business impact analysis. This phase utilized the results of the K method and defense-in-depth by establishing critical cameras that monitor the building. The following sections of the thesis introduce how these methods were tested in the case company building. The table below demonstrates the process of methods and how they were tested in the case company building in an orderly fashion.

Method	Description
1. Level of security	• Assessment of the case company security level; what characteristics establish the level of security. • Investigation carried out by walking around the building and identifying features introduced in theory.
2. Risk assessment	• Identification of risks related to case company building and camera surveillance system. • Risk analysis and evaluation produced by brainstorming with case company security team while following the guidelines of the case company global risk register template.
3. Defense-in-depth	• Identification of critical areas of the building and assessment of how to protect these areas. • Defense-in-depth: Formation of levels and setting minimum requirements of surveillance in every level.
4. K method	• Printing the K method test boards and testing the cameras that monitor the critical areas of the case company building. • Assessment of camera footage quality and setting up minimum requirement for footage quality.
5. Business impact analysis	• Establishing critical cameras and their minimum accepted downtime. • Setting up a procedure that enables prioritization of cameras in an adverse event.

Table 2: Method process

3.3 Level of security

The first tasks performed in the thesis work was carrying out an investigation of the case company building. To gain an understanding of the current state, the case company building was walked through from the lowest to the highest floor while writing notes during the review. Notes were made to copies of building floor plans by marking every single camera, alarm burglary device, and access control reader to the floor plan copies. A review was also conducted on camera surveillance and access control software's operated in building's reception services. Based on this review the level - introduced in the book Effective physical security by Lawrence Fennely – was formed.

The level of security in the case company was level three, medium security. Characteristics for this level of security are on-site security guards with basic communications, high-security physical barriers at the perimeter, and an advanced remote alarm system. Characteristics related to the lower levels, high-security locks, and simple security lightning e.g. are included in the upper levels of security, since achieving higher levels requires additional features to the already existing security system (Fennelly 2012, 78). Besides previously mentioned, the case company also has barriers suitable for high-security level. Additional barriers were comprehensive closed-circuit television that included multiple surveillance cameras around the perimeter and indoor areas of the building. The case company had also implemented a comprehensive access control system that was operated by on-site guards during weekdays. Guards reported daily safety and security activities to administrative security personnel who worked in the facility services. Mobile guarding services were activated during times when the building was closed. The medium-security level is designed to stall, detect, and evaluate unauthorized external activity and some unauthorized internal activity. These activities could be originated from example, shoplifting to sabotage (Fennelly 2012, 79).

3.4 Risk assessment

The second phase after establishing level of security was the risk assessment. The case company had implemented a global risk register template, which was used during the risk analysis phase of camera surveillance plan production. Case company guidelines included likelihood level, impact level and risk level matrix that was utilized for a risk score. The likelihood of risk described risk probability from slight (1), likely (3) to expected (5), and impact as potential consequences for case company if a risk occurs and what does it mean to business. Impact levels started from no material impact (1), followed by important (3) to critical (5). To achieve a risk score there needs to be an assessment where both likelihood and impact are considered. When the assessment is ready, points are given to both criteria's and these points set a particular risk into a risk matrix. From this procedure risk level is established (Case Company: Risk register template).

Following ISO 3100 standards guidelines and utilizing a case company risk register template enabled the assessment and documentation of risks strictly related to camera surveillance. First, the risk related to camera surveillance were identified and then placed into the risk assessment chart and named by risk ID. Holistic approach was utilized as far as what comes to risk identification that allowed the identification of both tangible and intangible sources of risks, from vandalism to insufficient CCTV user knowledge. According to the book Flood Risk: The Holistic Perspective author Zoran Vojinovic (2015) states that "holistic way of thinking combines qualities and quantities for the purpose of gaining a better understanding of the phenomena under consideration" (2015, 24). Following phase, Risk analysis was conducted by brainstorming with other security team members to increase quality and performance when scores for particular risks were given. According to author Ellen Lupton (2011) "brainstorming and related techniques help designers define problems and come up with initial concepts at the start of the project" (Lupton 2011, 16). In the brainstorming sessions, subjective points were given for the likelihood and impact of each risk identified which lead to establish a risk score. This score enabled to establish risks that were most critical in terms of likelihood and impact. The last phase of risk assessment was risk evaluation and risk treatment. The possible mitigation, avoidance, and control procedures for each risk was written and placed into the risk assessment chart of the camera surveillance plan. These procedures included, for instance, added lightning at the perimeter of the premise, camera circulation carried out daily, updating CCTV system passwords frequently and added camera surveillance signs at the perimeter wall of the building. Production of a camera surveillance plan was one of the risk treatment procedures since the risk assessment chart provides written procedures and actions that will mitigate, avoid, or control a certain risk. In addition, risk treatment has already been established in some of the risks identified since the client has, for instance, added camera surveillance signs at the building perimeter.

All together 14 camera surveillance related risks were identified, assessed, evaluated, treated, documented, and then placed into the camera surveillance plan. Top five risks, written in an orderly fashion, for case company buildings' camera surveillance system was: Insufficient CCTV user knowledge (high), Data leak (moderate), Blanking of camera/cameras (moderate), Crash of CCTV center system (moderate), a darkness that restrains cameras abilities to surveil (moderate). The advantage point of conducted risk assessment is that the case company has written documentation of procedures and development ideas they can utilize as such to increase the level of performance, increase resilience and prepare for risks that might occur during their operations.

Some of the risks were identified during the content analysis phase of the thesis work by reading guidelines and literature that provided lots of useful information related to factors to consider in camera surveillance. Besides analyzing this content, couple of risks were identified during building examinations when the level of security and defense-in-depth analysis

was conducted. Top risk, insufficient CCTV user knowledge, was identified based on the nature of the security guards' work. Risk description for this particular risk is "Due to sudden illness, the permanent guards working in the reception services can't make it to work. Guard who is unfamiliar with the software has to produce the shift" (Case Company, CCTV Plan 2019, 10). The likelihood of this risk is high since it is unlikely that permanent guards are always going to make it to work due to sick leaves and holiday times. The sum from the likelihood score and impact score concluded that this risk level was nine, which placed it in the high-risk category. In the risk treatment, procedures that either mitigates, controls, or enables avoidance of the risk were written. Examples of risk treatment procedures are, "Every single guarding staff gets at least week-term familiarization period where every system operated is instructed profoundly", "reception services own a contact person who can guide in urgent matters" as well as "familiarization card is updated frequently and signed after every section is guided. A guard who has not signed the familiarization card shall never produce shifts in the building" (Case company, CCTV Plan 2020, 10). With these instructions, the case company can mitigate the risk and ensure proper user knowledge at all times during operations.

The second highest risk according to risk level was data leak. This risk was identified in the content analysis where many of the instructions and guidelines included cyber vulnerability related risks. Even though the likelihood of this risk was assessed to be not likely, the impact of the risk is high, making it one of the top risks for the camera surveillance system of the building. The risk description in the risk assessment chart states that risk might realize if "an external person or entity gains access to the building's CCTV and records of footage". Risk treatment for this particular risk included procedures, such as "updating the password of the CCTV software and computer frequently", "Back-up saving for every collected and recorded footage to external flash drive" as well as "camera surveillance is operated with separate, a local computer that is not connected to the internet" (Case company, CCTV Plan 2020, 10).

The third highest risk assessed is the blanking of camera/cameras. This risk had already been realized in the building and because of historical signs; this risk scored a high likelihood level. Risk treatment procedures for this risk are, "preventive maintenance actions every 6 months; Cleaning of dust and updating of components", "camera circulation during every reception shift" as well as "maintenance agreement with the vendor, which includes preventive maintenance and fixed-period upkeep measurements" (Case company, CCTV Plan 2020, 9). Utilizing these risk treatment procedures and control methods, the case company can prepare in advance, increase the quality and efficiency of the whole camera surveillance system, expand the life span of the existing system and increase the level of performance in camera surveillance operations. Documented procedures in camera surveillance plan enable practical instructions that generate more effective and desirable physical security tool for the case company.

3.5 Defense-in-depth

After risk assessment was done, the next phase was to identify critical areas inside the building. The case company utilized its own international defense-in-depth standard that was included in the company's facility related security policies and standards. These documents described similar methodology and practices as in defense-in-depth methods generally. The standard was applicable to all facilities owned or rented by the case company. Areas in the scope were divided by Baseline zone, Limited access security zone, Enhanced security zone, and High-security zone. The lack in the current standard was that camera surveillance was not utilized and included effectively compared to other protection methods. Based on the case company standards and policies the production of separate defense-in-depth maps were produced into the floor plans of the building. In these maps the critical areas inside and outside of the building were assessed. Critical areas - high-security zone, and enhanced security zone - were marked as a red and yellow color. Non- or semi-critical areas - limited access security zone, and baseline zone - were marked as blue and green color. When these zones were established the level of each zone and their capability to stop, stall or surveil a possible intruder was evaluated.

During the level of security analysis, critical areas for client were identified and the actual formation of zones was formed based on defense-in-depth analysis. For instance, a particular basement level was classified as a high-security zone since critical data centers and distribution stations were located there. Hallways connecting and separating the high-security zone were classified as an enhanced security zone. This meant that only authorized personnel were allowed to enter the high-security zone and only employees of the case company were allowed to enter the enhanced security zone. In upper office levels, critically classified data is handled, and this sets out limitations to people who can access this particular area. Based on this assesment, all the office parts of the building were classified as an enhanced security zone. The first floor, where clients and visitors are welcomed, possessed all the classifications of the standard. The perimeter area located outside was classified as a baseline security zone since everyone can access or go through this area. General areas inside the first floor were classified as limited access security zone since persons can access this but they must be a registered visitor or employee of the case company. All the negotiation rooms were classified as enhanced security zones since delegate data is handled in these rooms. The only high-security zone on the first floor was reception services where buildings' security system software was operated. All of these areas were formed during the thesis work and at the later stages the results of this assessment enabled the basis for the new implemented surveillance strategy that was introduced in the camera surveillance plan.

The case company's most critical objectives of protection are the entry points in to the building, staff and visitors of the company, valuable assets placed inside the property, including

art and hardware, information that was handled in negotiation rooms and office levels as well as information that was stored digitally, rising the value of data centers and data transmitting cables located around the building. The data centers not only retained case company's own data, but also critical data of the clients of the company, which meant that data centers were placed in the highest criticality category and surveillance was planned according to the requirements of this category. As part of the overall facility protection, including access control, burglary detection devices, and structural protection, camera surveillance was utilized as a surveillance mechanism that enabled the company security personnel to detect, surveil and store footage of these previously mentioned protective areas and assets more effectively. The lack witnessed in the early stages of the internship, carried out before the thesis, was that these areas were not clearly demonstrated, ranked, and assessed based on their criticality. Due to this lack, some of the areas that were assessed as high security zone, during the thesis, were not protected and surveilled as high security zone requires. For instance, this included data centers where doors were accessible with low level authentication as well as entry points to the enhanced security zones were surveilled with poor surveillance camera footage quality or footage was not produced at all. During the internship, other areas of physical security, including access control and alarm burglary procedures, were handled and improved and in the thesis project camera surveillance was assessed separately based on the assessment of the defense-in-depth.

The defense-in-depth strategy enabled the identification of these previously dealt critical areas and functions and based on this assessment, a minimum requirement was set out to particular space. In terms of the camera surveillance this meant that, for instance, high-security zones were constantly monitored with at least K120 footage quality, which enables more accurate detection and identification of possible risk sources, like burglary. In addition, the original surveillance performed with camera surveillance of the building possessed gaps in the CCTV system design, where a poorly targeted camera, or blanked out camera, didn't produce footage of the critical entry point. Because the building areas were classified and every single camera was designed according to the strategy, the case company can now ensure that these critical areas are surveilled with strategic fashion where a minimum footage quality requirement and minimum accepted downtime (chapter 3.7) were set. The most vital improvement compared to the earlier system is the strategy set out in the camera surveillance plan. With this new strategy, a requirement has been designed for a particular area in terms of surveillance camera quality and target. This strategy includes a precise target and footage quality of each camera, which enables the case company to recognize persons entering, or attempting an entry to a particular protected area. In data centers, this for instance means surveillance of the door of the space in a manner where a person's face can be identified during the attempt of entry. In real time monitoring this development increases the reaction time, since persons can be identified with cameras during a work assignment or a possible break-in event.

The earlier system did not achieve this quality. In other spaces of the property, the main development was related to the main entry points of the building. By setting a requirement through defense-in-depth and demonstrating the critical space, the case company can ensure that all of the entry points and general areas are surveilled with proper devices. Because these requirements were set out in the defense-in-depth assessment, they can be implemented to the whole building by following requirements set in the particular zone.

Defense-in-depth was chosen as one of the strategies since it enabled the assessment of barriers that were used in the building. The negative side regarding the results of defense in depth was that there weren't enough resources to conduct a penetration test. The original plan was to test the defense of the building with a penetration test when a camera surveillance plan was produced. This test would have set the defense into real-life test where weaknesses of the defense would have been easier to notice. The final proposal included multifactor authentication when entering the high-security zone and added authentication tools such as access card readers in high- and enhanced security zones entry points. The camera surveillance plan included strengthening camera surveillance in the areas that were found to be lacking with protection. Practically this meant that every surveillance cameras' precise target as well as the quality of footage requirement was adjusted in a manner that suited the particular security zone in and outside the building. In some areas, added cameras were required to fulfil an effective surveillance. By setting a target and requirement of footage quality for each camera, the quality of defense layers in the building increases as security guards have more time to react and notice unauthorized accesses. With this development, security guards can notice suspicious actions happening on the first defense layer placed at the perimeter and prepare for a possible attempt of unauthorized access. In addition, increasing the camera footage quality enables more enhanced identification of persons entering unauthorized area. This increased surveillance quality will enable more efficient investigation in the face of adversity. By utilizing the developments delivered to the case company, the organization can now decrease the change for a possible break-in or unauthorized access through increased access control and increased quality of surveillance. However, if this break-in were to be happening the case company can retain a precise and accurate data from the adversity which saves resources and increases the efficiency of the investigation.

3.6 K method

The following phase after identifying critical areas and risk sources was testing the quality of footage of surveillance cameras. K method test was found to be suitable for this test since it was provided with profound instructions and it didn't cost anything. In the thesis project, the K method test was carried out to some of the critical cameras at the perimeter as well as in the indoor areas of the building. Testing every single camera was not necessary since every camera in the building was identical and during the project it came apparent that the whole

camera surveillance system is going to be updated to a new modern system. The test was performed during darkness in the morning time and during the daytime when the lightning is more active. An interesting result witnessed was that the cameras' ability to record footage at night was far greater than the recorded footage gathered during the daytime. Some cameras placed at the perimeter were able to fulfill requirements of K50 during the time of darkness but at times of daylight, cameras' abilities decreased to K10. It came apparent during the study of camera functions and content analysis that this is a common quality in old analogic cameras.

K method was suitable for this particular thesis work since case companies own standard required positive identification of all persons entering a case company building. This meant that critical indoor cameras - cameras that monitor main entrances - required qualities that provide K120 quality of the footage; footage where persons face is recognizable. K method test provided neutral results that showed what kind of footage a particular camera was able to produce. Besides utilizing the test board, writer of this thesis also took screen captures from surveillance footage of the moment he was standing in front of the surveillance camera. Using these screen captures together as a result, it could be demonstrated that current surveillance cameras were not able to produce footage required for this building. K method was also suitable since all the cameras in the property were old analogical surveillance cameras that did not have modern surveillance camera qualities. Surveillance cameras produced today are mostly high definition cameras that can produce a quality that is suitable for a variety of companies and users. Testing camera footage quality with the K method is not necessary for cameras' that produce high definition footage but utilizing the K method, as part of the planning phase might be useful. In this type of situation, a person planning the camera surveillance system can use the K method test board to determine the height of a particular camera and length in the field of footage, even though cameras' technological features already produce required footage. Criticism regarding the K method is that it is not suitable for testing cameras that are placed in outdoor areas. According to finance Finland, the K method test is adequate for surveillance cameras that are placed inside a building where circumstances, like lightning or humidity, does not differentiate (Kameravalvontaopas 2010, 30).

K method was also utilized by other means during the thesis work. It came apparent that case company buildings' entrance monitoring cameras were the most critical cameras for the case company. Besides entrance monitoring cameras, other production areas, and hallways that lead to critical rooms, like the data center e.g. were critical for the case company objectives. Carrying out a classification of every camera in the building was one of the developments that were proposed and then later implemented into the camera surveillance plan. The classification of cameras was based on K method results. First, the objective and target of every buildings' camera was established. After this, the K method board was utilized to test

these cameras. Combining these results with case company policies, a table demonstrating every critical, semi-critical, and non-critical cameras of the building was delivered.

3.7 Business impact analysis

Last phase of the methods was classifying cameras and camera impact analysis that was one of the major improvements delivered during the thesis project. The purpose of the camera classification and impact analysis is to demonstrate critical cameras that cannot be out of use during daily operations. With a pre-designed analysis, the case company can prioritize surveillance-related tasks in a case where some of the cameras appear to have dysfunctions as well as increase the overall resilience in adverse events. Since the case company's internal security related policies and standards set requirements regarding the camera surveillance function and some of the cameras had been broken before, it seemed reasonable to formulate business impact analysis and camera classification.

Cameras were classified by utilizing defense-in-depth analysis and K method test that was carried out to some of the cameras while considering the requirements set by the case company's security policies and standards. The policies and standards requires the identification of people entering the building. This meant that all the cameras surveilling entry doors are critical for the case company objectives and therefore classified as critical. The highest classification in this practice was appointed as "K120 EMC" that stands for entrance monitoring camera that should gather surveillance footage with K120 quality. The second-highest classification was "K120". These cameras were surveilling enhanced- and high security-zones inside the building and that is why classified as semi-critical cameras. These particular zones possessed critical data centers and maintenance rooms that required increased surveillance. The zones were produced during the defense-in-depth analysis. Appointing these category cameras as "K120" meant that these cameras should surveil with K120 quality. The last two classifications are "K50" and "K10" and their classification description is: "These category cameras are monitoring limited security zone and perimeter area of the building. They are classified as non-critical cameras."(Case company CCTV Plan 2020, 3). It is not reasonable to suggest that all of the cameras are critical since maintaining high-quality cameras in every corner of the building means unreasonable costs and poor resource investments. In the final draft of the camera surveillance plan, 16 of the buildings' cameras were classified as K120 EMC, 14 cameras as K120, 28 cameras as K50, and 13 cameras as K10 cameras.

Business impact analysis is introduced in the book business continuity management: global best practices by authors Andrew Hiles and Kristen Noakes-Fry. Based on the theory (2015), each camera in the system was placed into a table and this table was placed into the camera surveillance plan. This table works as a procedure that the case company can utilize if the building cameras are compromised. The business impact analysis was also formed to

strengthen the classification of cameras and case company resilience in adverse events. In business impact analysis, allowed camera downtime was listed for different camera classification categories. Accepted downtime was arranged by one day, one week, and one month meaning that some of the cameras cannot be broken for one week without having an impact on case company objectives. Impact severity was displayed by using green, red, and yellow colors. Green color states the impact has no material impact on case company objectives during downtime. Yellow color represents moderate impact and red color materiality reduced the ability to achieve case company objectives. The table below demonstrates the impact analysis that was performed and placed into the camera surveillance plan (Case company, CCTV Plan 2020, 3-4).

Camera classification	1 day	1 week	1 month
K120			
K120 EMC (Entrance Monitoring Cameras)			
K50			
K10			

Table 3: CCTV plan, Business impact analysis (2019)

4 Results

The main result of the thesis is a camera surveillance plan that introduces the surveillance strategy of the case company and a checklist that can be utilized as tool if this plan is performed with same method process at some other site. This section of the thesis covers the benefits of using camera surveillance plan from business perspective as well as in the case company building, how the theory and methods suited this work and what were the most significant findings made during the thesis work. The motive for this plan was to produce a strategy that the case company can utilize when they decide to install a new camera surveillance system into the building. Updating the current system was decided before the thesis even started, and this is the reason why it was a good time to perform a review of the current system. The other motive to produce the plan was to demonstrate justification for the use of camera surveillance in the building. These two motives initiated the birth of a camera surveillance plan and this thesis work.

4.1 How the CCTV plan supports the case company business function

From a business point of view, camera surveillance is acquired for many different reasons but the main idea behind camera surveillance is to surveil and protect the assets of a company

that are worth money either directly or indirectly as well as mitigate the risks that might affect these valuable assets. The case company utilized camera surveillance for these same reasons. The problem realized at the start of the thesis was that the system acquired in the case company building did not perform at a desirable level. This meant that risks, such as theft, sabotage, data loss and malfunctioning of the system were more likely to be happening because the system had serious deficiencies, including poor target of footage for cameras and 16 blanked cameras that did not produce footage at all. Alternatively, from a different perspective, the system did not allow the case company to surveil their critical assets in a manner where the assets were efficiently protected, which also increases the change for a variety of risks. From a business function point of view, the case company was utilizing their CCTV system insufficiently in two different aspects. The first aspect is that, if these risks were not to be noticed and prevented, the case company would possibly lose money directly due to a theft where some tangible or intangible assets, for instance data, is stolen. Losses related to strictly money and data could also happen indirectly when classified data is lost due to theft or data leak. The other downside in the case company's CCTV system was that the system itself costs money while it does not deliver efficient surveillance. Utilizing a system that costs money but does not serve the purposes of the company is a clear indicator of poor use of resources.

The first result of the thesis project was rehabilitating of the cameras that did not produce footage at all. This malfunction was quickly fixed by rebooting the control relay that connected the broken cameras to the system. Because of having these cameras back in the real time surveillance, the case company building does not suffer from blind spots at the building protection, which enables more efficient surveillance and increases the ability to react in adverse events. From a business point of view, the surveillance was rehabilitated to its designed state, which mitigated the risk of losing money or data via theft or unnecessary investment for adding more surveillance equipment to the building while the original cameras were already there. By utilizing the already existing hardware the company was able to save money and extend the life cycle of the current system. In addition, producing a camera surveillance strategy in a form of a plan, where every single camera has a pre-design target, enables the reduction of risks targeted towards the case company. This reduction is simply realized by establishing critical cameras and areas where a camera is surveilling a pre-designed target, which enables more efficient surveillance of a target, which in other words reduces the changes for a risk that might cost money for the case company. The improvement delivered in the case company's building is that the target for cameras was not established in the previous system and now the case company has a goal for the surveillance conducted with camera surveillance.

When assessing the CCTV plan and business function related improvements a couple of examples must be pointed out. The most significant improvement in the plan is that because this

plan was produced free of charge and it can be used as it stands, it enables the case company to avoid using other costly solutions in their upcoming CCTV system updates. Because the original system was going to be updated into a new modern system, the review would have been allocated to a paid consultant or other professional that would have produced the assessment and design for the new system. Utilizing the plan, the case company can now follow the blueprints and instructions introduced in the plan that was performed free of charge. In addition, the original system in the case company did not fulfil the requirements set in the case company's security policies and standards. These frameworks were utilized as a tool for the camera surveillance plan by filling the gaps in the system. Implementing the solutions provided in the new camera surveillance plan, the case company's professionals do not need to utilize other costly solutions to be able to comply with the requirements set by their internal security policies and standards. The other great value in terms of improvements of business was delivered through risk assessment. By identifying, evaluating, treating and introducing key risks regarding the case company CCTV system enables written procedures that can be utilized to increase the level of protection and resilience of the case company CCTV system. By utilizing the risk treatment procedures, the case company can avoid costly threats that might affect the system itself. In addition to the system related risk, the case company can mitigate risks that might for instance threaten the critical data centers in the building. Because of establishing critical areas and a requirement of camera footage quality for this particular area, the case company can decrease the change for a costly event that might damage the companies', and their client's data that is preserved in the data center room. In the end, 14 different risks were identified and analyzed. Based on the strategy implemented in to the camera surveillance plan, a risk treatment was delivered, which decreases the effects these risks might have to functions involved with specific risk and because of this improvement, the case company can leverage savings in terms of money and resources.

4.2 CCTV plan

The final product that was produced for the case company, the camera surveillance plan, is a 26-page document that delivered a camera surveillance strategy for the building. Another key function for this plan was listing all the relevant matters that are related to the buildings camera surveillance system. The contents in the plan are formed in a manner where the last nine sections of the plan composes from floor maps where every single camera and their field and target of footage is demonstrated. The first two pages of the plan presents the plans purpose, scope, policy and legislation, roles and responsibilities, handling of recorded footage as well as maintenance. The following sections introduce the risk management, including risk identification and risk treatment, as well as the impact analysis and camera classification. The plan also lists all relevant stakeholders, including maintenance and the vendor of the camera surveillance system. The whole table of contents of the plan is in the appendices of the thesis (appendix 1 for full table of contents).

Figure below demonstrates the main benefits of the produced camera surveillance plan.

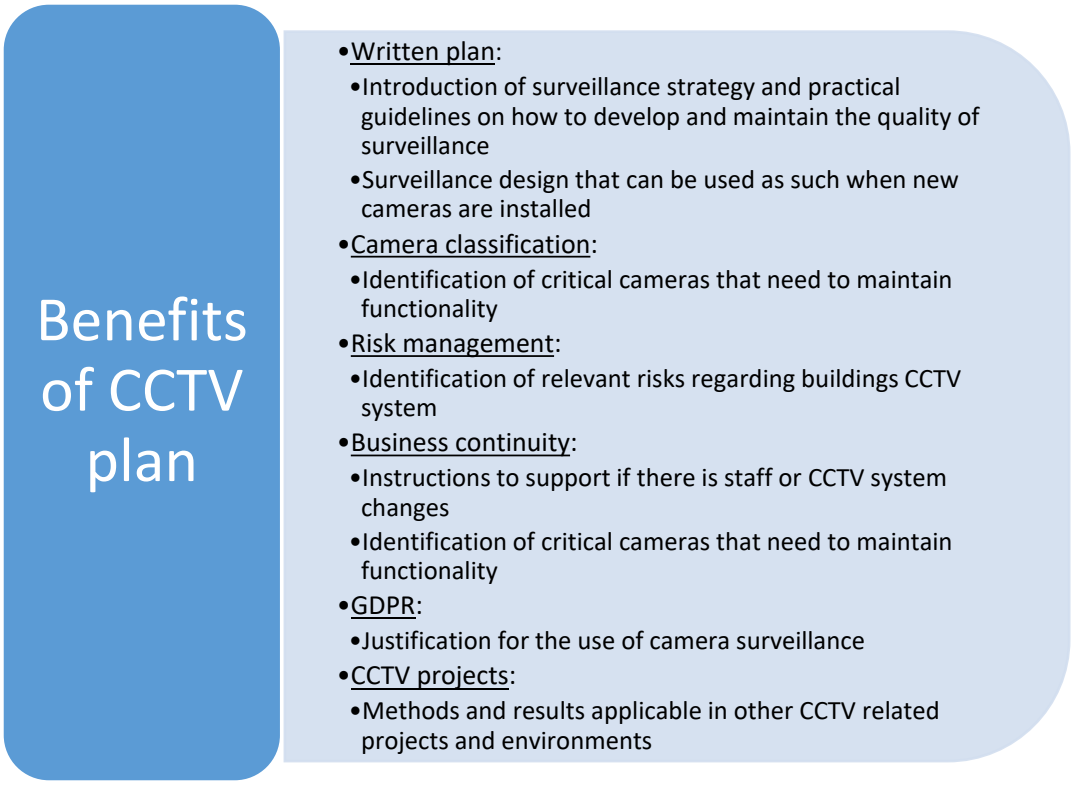

Figure 5: Benefits of CCTV plan

The main benefit of the camera surveillance plan for the case company is that with this plan the security personnel working in the administrational and operational security have a plan that has written procedures on how to develop and maintain the functionality of the current system. In addition, BIA and risk assessment describes critical cameras that need to be prioritized and risks that the company needs to be aware of, which enables more resilient camera surveillance in the building. In addition, the defense-in-depth assessment enabled the identification of critical areas and assets and how to protect them accordingly. Other major usage for this plan is that when the new camera surveillance system is acquired, the case company can set up each camera in a pre-designed manner by following instructions and mapping designed in the camera surveillance plan. This design was established based on the results of the methods, while considering case company security related policies and standards and as a result, this design enables efficient surveillance, which meets the requirements of the case company security objectives.

The justification for the use of camera surveillance is established by clearly demonstrating where each camera is placed and what is the main target of surveillance for a specific camera. According to European Data Protection supervisors follow-up Report to the 2010 EDPS Video-Surveillance Guidelines: “Bodies must establish the legitimate purpose of their VS. In

doing so, they need to be clear, specific and explicit - vague, ambiguous or simply too general descriptions are not sufficient" (follow-up Report to the 2010 EDPS Video-Surveillance Guidelines 2010, 18). Written purposes listed in the plan are protecting assets, property, and people working in the building, prevent crimes targeted to case company assets, and people working in the building as well as investigation after crime or accident. Besides justifying the legitimate purpose of the camera surveillance, the camera surveillance plan also describes the handling of recorded footage in the case company building. This section introduces a description of the recorder device used and the period of how long the video footage is retained.

This plan is mostly useful for the case company since it was produced for the case company environment, but methods are applicable in other environments as well. This thesis demonstrates how the camera surveillance plan was produced for a big office building that has over 60 surveillance cameras and what kind of methods were used to review and develop the current system. Demonstrating the method process in the thesis is beneficial since it provides examples and results for other professionals working in the security field and with this thesis, professionals can consider if these methods are applicable in their environment. In addition to the method process, a camera surveillance plan checklist is also provided in this thesis. This checklist is a valuable tool to be utilized as part of the camera surveillance plan production. This checklist is formed in chronological order where an executor can place marking and comments when a specific method of the process has been carried out. The full checklist is placed in the attachments of the thesis (see attachment 3: Checklist: camera surveillance plan).

Based on the results of the thesis, a camera surveillance plan should be produced if a company wants to ensure continuity and efficiency when guards and other security personnel are replaced as well as if the system is compromised due to a major breakdown or adversity. This plan is also useful if the camera surveillance system is updated to a new system since the plan's camera blueprints demonstrate where a specific camera should be placed and what the target of surveillance for this camera is. Because of these reasons, the camera surveillance plan is not only useful for the case company but also for other companies as well.

4.3 Theory and methods

The theoretical background of this thesis introduces functions and methodology included in the scope of camera surveillance. The goal was to find useful tools that could be tested as they were instructed in the contents. The first literature that was studied was the camera surveillance guide that introduced the basic functionality of a camera surveillance system. This literature did not introduce methods or tools that were used in the thesis but it did provide useful information that generated the base knowledge regarding the camera surveillance

that was an important part of the whole life cycle of the thesis. It also enabled the review of the current system and helped to identify lacks that were in the current case company system. The second theory that was applied in the thesis was the level of security analysis. This assessment is introduced in Lawrence Fennelly's book Effective physical security and the main implication of this theory was to identify characteristics involved in different security solutions, identify the case company's level of security and compare them together. According to the author (2012), categorizing the levels helps to identify lacks within the current system (Fennelly 2012, 77). In this thesis, the most useful method used for identifying the lacks of the system was the defense-in-depth analysis, which is why the result achieved with the level of security assessment was not effective and did not produce meaningful results for the sake of this thesis. It did provide a good knowledge base on the different options and models that exist, which helped to identify the level of the case company system but after all of the methods had been tested, it came apparent that this method could have been omitted.

The theory behind risk assessment is introduced in the ISO 31000 risk management standard. According to the standard (2018), it "can be used throughout the life of the organization and can be applied to any activity" (ISO 31000, 6). This framework provided by the standard is applied in the whole life cycle of the operations of a company but because this thesis was produced as a project work that lasted ten weeks, the continual improvement part of the risk management was not performed. According to ISO 31000 standard (2018), the continually improving part of the framework means that, "the organization should continually improve the suitability, adequacy, and effectiveness of the risk management framework and the way risk management process is integrated" (ISO 31000, 13). This thesis performed the standards risk process by identifying, analyzing, evaluating, and treating the risks related to camera surveillance but continual improvement is the responsibility of the security professionals working in the case company. This method did provide the starting point for the continual improvement of camera surveillance risk management. As a result, this theory was important and suited for the objects of the thesis.

The theory of BIA suited this thesis well and was an important part of the results of the thesis. The BIA analysis theory is introduced by authors Andrew Hiles and Kristen Noakes-fry (2015), and according to the authors, its main implication is related to assessing the financial and non-financial costs of a disaster as well as identifying the vital materials and records necessary for the recovery of continuance (Hiles & Noakes-Fry 2015, 149-151). These assessments were not applied in this thesis since assessing financial costs were not essential to deliver the accepted downtime of the cameras. In addition, the thesis time frame and resources didn't enable the identification of materials and records for recovery. The main usage of BIA was establishing the critical cameras and the time window in which the recovery must take place. The BIA table was formed based on the results of defense-in-depth and K method assessments.

The last two methods and the theory of defense-in-depth and K method were found to be efficient regarding the results of the thesis. Both of them suited this thesis and provided results that allowed the assessment of the camera footage quality and critical areas that need to be protected. Defense-in-depth as a method establishes layers of defense that increase the protection progressively as the layers come closer to the center. In the thesis, there did not exist a specific target that needed protection but because the theory introduced this mindset, it allowed identifying critical assets and areas inside the building. This mindset also helped to identify critical cameras since areas that were classified as high and enhanced security zones required cameras that must be functional all the time. Besides establishing critical areas, defense-in-depth helped to identify lacks in the overall asset protection. K method theory provided practical and cost-effective instructions on how to test the camera footage quality. Negative side about the K method is the lack of sources regarding the test. The document - produced by Finance Finland - that provided instructions about the test had only one version that could be acquired from the internet. Even though this document was located in different service provider's websites, it was always the same document in every location. Additional sources or versions regarding the K method test would have provided more profound instructions that could have been considered during the test that was performed in the thesis work. The best part of the K method guide is that it provides clear instructions on how to print the test board and what kind of distance must be used to get sufficient results. In addition, the instructions are free which made it an effective method for this thesis work. The table below presents the main sources regarding the topic and method utilized in this thesis work.

Topic	Main source	Method/Main implication
Camera surveillance	Kameravalvontaopas (Turva-alan yrittäjät ry. 2010)	• Base knowledge related to camera surveillance that was utilized during the whole file cycle of the thesis.
Level of security	Effective physical security (4th edition) (Lawrence Fennelly 2013)	• Level of security assessment. ○ Identification of the current state and lacks in the system. • Enabled a good knowledge base related to security level assessment.

Risk management	ISO 31000 (SFS-ISO 2018)	• Risk assessment:
		  ○ Risk identification
		  ○ Risk analysis
		  ○ Risk evaluation
		  ○ Risk treatment
		• Starting point for continual improvement.

Business impact analysis	Business Continuity Management: Global Best Practices (Hiles, A. & Noakes-Fry, K. 2015)	• Establishing accepted down time for camera groups.

Defense-in-depth	The complete guide to physical security (Baker, P. R. & Benny, D. J. 2013)	• Identification of:
		  ○ Critical areas and spaces.
		  ○ Critical cameras.
		• Identification of lacks in the current system

K method	Kameravalvonnan suunnitteluohje (Finanssialan keskusliitto 2017)	• Test for the camera footage quality.

Table 4: Theory and methods

4.4 Order of the methods

The order in which these methods were carried out worked well since every step taken did support the following step excluding the level of security assessment. For instance, analyzing critical areas inside the building with defense-in-depth assessment before conducting footage quality tests with the K method enabled the classification of critical cameras. This decision turned out to be efficient since because of the identification of critical areas, only critical cameras were tested, and resources were not wasted. Another great value realized in the thesis was the combination of BIA analysis and the K method test. These two methods had great synergy utilities since the classification of the BIA tables' cameras was based on the K method camera classifications. Because of this synergy, the BIA table not only introduces the minimum downtime of a certain camera group but also introduces the quality of footage of this particular camera group. In addition, getting familiar with the camera surveillance functionality established a knowledge that allowed the assessment of the case company system. This knowledge was crucial in every step and especially important in the risk identification phase. The risk assessment part of the thesis was also efficient during the period it was carried out since it provided many potential risk sources. These sources were considered in the latter stages where, for instance, the quality of the footage was tested.

When assessing the least effective method in terms of the order, it is clear that the level of security assessment was not relevant for this thesis work. In the end, it did not provide sufficient data since the level and characteristics of the case company security system were self-explanatory and were found to be suitable for this particular building. The positive effect it had was that it enabled a good familiarization with the building but this knowledge would have been gained either way during the building reviews and walks. In terms of the order, this thesis would have been more effective if the level of security assessment was skipped and the first step of the thesis would have started from risk assessment. According to author Lawrence Fennelly (2012) "assessing security conditions and planning for appropriate levels of assets, protection begins with the basics: risk management" (Fennelly 2012, 339). In this order, the risk assessment would have taken place at the start and at the end of the method process

where it would have enabled more profound risk identification and risk treatment where possibly more risks would have been identified. The suggested order of the method process is introduced in the attachment 3.

4.5 Findings

Figure below demonstrates the key findings established in the thesis.

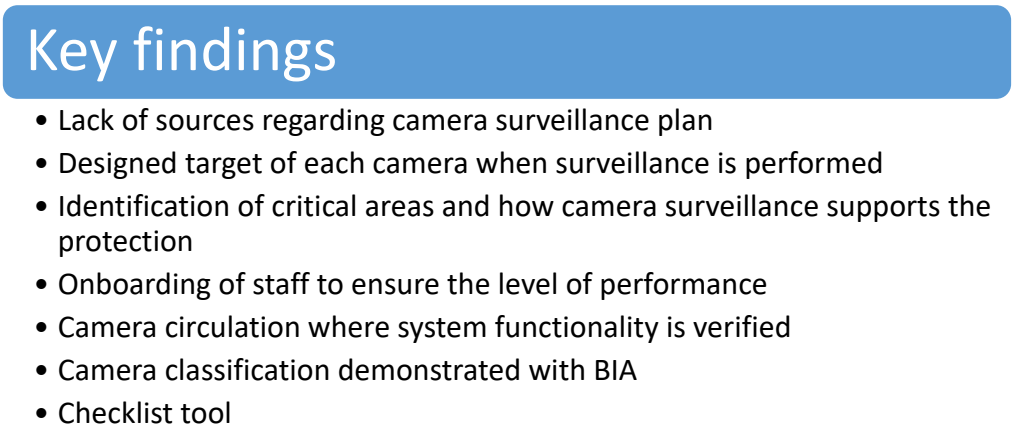

Figure 6: Key findings of the thesis

Many key findings were made during this thesis work but the main ground finding realized in the early stages was that the internet or literature does not provide sufficient instructions on how to produce a camera surveillance plan. The Google searches with “camera surveillance plan” generates instructions on how to set up an efficient camera surveillance system but the guidelines for the plan are lacking with proper sources. This key finding was the main motive for this thesis and the way this thesis is presented. Based on the thesis results, the most important discovery established in the thesis project produced for the case company was the target of a particular camera when it is performing surveillance. Every single camera that is acquired and mounted for surveilling must be planned in a manner where this camera has a pre-designed target that it is surveilling. This reasoning applies in all environments and it must be taken into account in every camera surveillance related plans and projects. In this thesis work, targets for cameras are, for instance, identification of persons entering the building, surveillance of a particular door and entry point, or surveillance of a particular area. With this strategy, camera surveillance can be planned in a reasonable manner where entrances, movement of people, and possible risk sources can be detected. In addition to the camera’s target, another key concept established in the thesis is the identification of critical areas and functions in a company and how camera surveillance system can be planned to increase the protection and surveillance of these matters.

Another key finding in this thesis was related to continuity and quality assurance when camera surveillance is performed. During the risk assessment, it was realized that it is not reasonable to assume that security guards, who operate the camera surveillance system, are going to make it to work every single day. This problem should be dealt by ensuring that every single guard who starts their work in the case company building has a profound and comprehensive onboarding period at the start of the assignments where the camera surveillance system is familiarized. The guideline in the plan regarding this procedure instructs that every single security guard must achieve at least a one-week onboarding period. This one-week onboarding is a requirement that is set for the reception services and if this requirement is not fulfilled then this guard shall not perform shifts in the case company reception services (Case Company, CCTV Plan 2020. 10). With this procedure, the reception services can ensure the quality of surveillance when a permanent security guard cannot make it to work due to illness as well as the continuity of performance is assured when the permanent security guard is leaving the site for good. Besides increasing the amount of onboarding, the camera surveillance plan itself is also a valuable document, which the security guards can utilize in the onboarding and other periods during the service.

Another discovered finding in the thesis was related to a procedure called camera circulation. In the case company CCTV plan, this procedure is instructed as a task where the security guard conducts a checkup of the condition of each camera in the building via footage that is broadcasted into a computer monitor screen (Case company, CCTV Plan 2020, 10). This task should be carried out daily and the key finding with the procedure is ensuring the functionality of each camera surveilling the building with a cost-effective solution. Besides ensuring the functionality, this procedure also increases the effectiveness of surveillance and awareness of the building surroundings. In addition to the security guard related procedures, an essential finding regarding this thesis was the utilization of BIA in the camera surveillance operations. Realizing that it is not reasonable to assume that every single camera in a building is equal when the overall surveillance is at stake in a building that has over 60 surveillance cameras monitoring the building. This means that for effective resource allocating some of the cameras in the building are more important than others due to the location and target they are surveilling. This reasoning can be demonstrated by producing a BIA table, which establishes the most critical cameras to the least critical cameras by categorizing them based on their accepted downtime - a period in which a certain camera must be operational for it to not have negative effects on the case company objectives. The key finding in this was the realization of how well BIA is suitable for a camera surveillance strategy. This procedure might not be suitable in buildings where only a few cameras exist but according to the thesis results, it should be included in the CCTV plan to increase the resilience and continuity of operations. The last finding introduced in the thesis is the tool called checklist that professionals can use around the world when they are developing camera surveillance systems.

5 Conclusion

The main challenge in this thesis is the confidentiality of the camera surveillance plan, which limits the amount of information shared in this thesis work. Without the restrictions, the final product would have been presented in this thesis and all the produced guidelines would be visible. Another key weakness that reader should be aware of is the lack of information and instructions about how to produce a camera surveillance plan. Because of this shortage, the thesis was started with insufficient examples and knowledge about what needs to be included in the plan and what kind of benefits can be established with this plan. Because of this, the plan is solely produced based on thesis writers own subjective opinions and perceiving's. Another strictly thesis results related weakness is the lack of penetration test. According to author William Allsopp (2009) if an organization "wants to ensure the highest form of security in place, penetration testing can help you" (Allsopp 2019, 2). Because of the lack of resources and a thigh schedule, thesis did not have any results on a penetration test. This test would have tested the protection of the building with a real-life simulated attack as well as enabled valuable results where real weaknesses of the protection would have been witnessed.

The key findings of the thesis are the introduction of the method process and the checklist tool, which demonstrates suggestions that should be included to achieve sufficient camera surveillance plan. According to the results and findings, the level of security assessment is not necessary action to take since it doesn't necessarily produce meaningful results. In addition, during the thesis it was witnessed that K method was suitable and effective method to demonstrate the poor quality of footage in the case company camera surveillance system. The criticism regarding K method, in addition to the lack of different sources, is that it is not the most suitable solution for modern high definition cameras, which are mostly used today, since these cameras will achieve a high-level camera footage quality. In addition, thesis results demonstrate that more weight should be targeted on risk assessment to achieve more resilient wholeness of surveillance.

A possible future study or thesis project relating to this subject could be related to the production of international guidelines that could be used to produce a camera surveillance plan. Creating a framework that could possibly work as a standard for the production of this plan would benefit a lot of camera surveillance users in their future camera surveillance development projects. It would also enable a tool where executors - like the writer of this thesis - can save a lot of time when information is searched for this project. Because of this, the thesis can be developed further and used in the future research and development tasks as well as utilized in the development of the new camera surveillance standard.

When looking back at the starting point of this thesis project, the case company CCTV system did not perform sufficiently and did not provide the service it was initially demanded. This

system was acquired to surveil the case company building while fulfilling the requirements that the case company had set in their global security related policies and standards but in the original state, the system did not perform at a level that was required in these frameworks. In addition, the surveillance was performed without any justification and specific strategy-based goals. By identifying these lacks in the system while comparing the situation at its current state the level of performance has increased a lot. With the camera surveillance plan, the case company not only has a strategy-based surveillance function but also a justification for the use of camera surveillance as well as a system that fulfills the requirements set in their own global security related policies and standards.

In the end, the camera surveillance plan did enable some improvements in the case company security processes since the plan introduces a strategy that can be utilized as such, meaning the case company doesn't need to allocate resources on the planning phase of the new camera surveillance system. In addition, the plan enables a practical camera surveillance strategy that increases the quality and resilience of performed surveillance as well as the camera surveillance plan itself created a cost-effective path for the continuous development of the company's camera surveillance. Due to the increased level of security, thesis writer is happy with the product delivered and feels that this product is a useful totality. The case company supervisor who ordered the thesis work also supports this statement. According to the supervisor, the camera surveillance plan is a good quality document that is used on a weekly basis in physical security related operations (See Appendix 2, feedback from client). The competency and knowledge about camera surveillance, physical security and project management of the thesis writer has increased a lot and this gained knowledge and method process can be used in other physical security or camera surveillance related development projects. The goal of the thesis was to develop the case company's camera surveillance system, deliver a justification why a camera surveillance plan should be produced as well as deliver a tool (checklist) which enables other executors to produce a same type of plan. Combining the thesis method process and checklist together, this thesis has the opportunity to work as an excellent foundation for the next executor.

References

Printed

The first printed reference

Phillips, E., Pugh, D. S. & Pugh, D. S. (2010). How to get a PhD: A handbook for students and their supervisors. Maidenhead: McGraw-Hill International (UK) Ltd.

Baker, P. R. & Benny, D. J. (2013). The complete guide to physical security. Boca Raton: CRC Press

Fennelly, L. J. (2013). Effective physical security (4th edition.). Amsterdam: Butterworth-Heinemann

Kingsley-Hefty, J. (2013). Physical Security Strategy and Process Playbook. Oxford: Elsevier

SFS-ISO 31000:2018. Risk management - Guidelines.

Vojinovic, Z. (2015). *Flood Risk: The Holistic Perspective*. IWA Publishing.

Pinto, C. A., Jaradat, R. M. & Magpili, L. M. (2015). *Operational Risk Management*. Momentum Press.

Walker, R. (2013). *Winning With Risk Management*. World Scientific Publishing Co. Pte Ltd.

Chapelle, A. (2019). *Operational Risk Management*. Wiley.

Wolke & Thomas Wolke; De Gruyter Oldenbourg. (2017). *Risk Management*. Oldenbourg: De Gruyter Oldenbourg.

Wheeler, E. (2011). *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*. Burlington: Elsevier Science.

Criminal code of Finland 531/2000.

Act on the protection of privacy in working life 347/2019

General data protection regulation 2016/679

Kananen, J. (2015). Opinnäytetyön kirjoittajan opas: Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Mayan, M. J. (2016). Essentials of Qualitative Inquiry. Milton: Taylor and Francis.

Vilkka, H. & Airaksinen, T. 2004. Toiminnallinen opinnäytetyö. 1.-2. painos. Jyväskylä: Gummerus Kirjapaino.

Wong, W. N. Z. & Shi, J. (2014). Business Continuity Management System: A Complete Guide to Implementing ISO 22301. Kogan Page.

Hour, A. A. (2012). Business Continuity Management: Choosing to Survive. Ely: IT Governance Publishing.

Joint Chiefs of Staff Washington United States. (2017). DOD Dictionary of Military and Associated Terms.

Crowe, T. D. & Fennelly, L. J. (2013). Crime Prevention Through Environmental Design. Butterworth-Heinemann.

Armitage, Rachel (2016) Crime Prevention through Environmental Design. In: Environmental Criminology and Crime Analysis. Crime Science Series. Routledge, Abingdon, UK, pp. 259-285. ISBN 9781138891135

Hotchkiss, S. (2010). Business Continuity Management. British Informatics Society Limited.

SFS-ISO 22301:2012. Business continuity management systems – requirements.

Drewitt, T. (2013). *A Manager's Guide to ISO22301: A practical guide to developing and implementing a business continuity management system*. IT Governance Publishing

Hiles, A. & Noakes-Fry, K. (2015). Business Continuity Management: Global Best Practices. Rothstein Publishing.

Rittinghouse, P. & Ransome, P. (2011). Business Continuity and Disaster Recovery for InfoSec Managers. Burlington: Elsevier Science.

Valtionvarainministeri. (2/2013). Toimitilojen tietoturvaohje. Juvenes Print - Suomen Yliopistopaino Oy

Lupton, E. (2011). *Graphic Design Thinking: Beyond Brainstorming*. Princeton Architectural Press.

Allsopp, W. & Allsopp, W. (2009). *Unauthorised Access: Physical Penetration Testing For IT Security Teams*. Wiley.

Electronic

The first electronic reference

Business watch. 2019. Types of CCTV cameras - The complete guide. https://www.business-watchgroup.co.uk/types-of-cctv-cameras-the-complete-guide/

Nathan Dinning. 2018. HD analog vs. IP cameras: A feature comparison. https://www.march-networks.com/intelligent-ip-video-blog/hd-analog-vs-ip-cameras-a-feature-comparison/

Tiina Airaksinen. 2009. Toiminnallisen opinnäytetyön kirjoittaminen. https://www.slideshare.net/TiinaMarjatta/toiminnallinen-opinnytety-tekstin

Susan Snedaker. 2020. Business continuity – Pandemic preparation.https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2020/business-continuity-pandemic-preparation

Turva-alan yrittäjät ry. 2010. Kameravalvontaopas. http://www.turva-alanyrittajat.fi/doc/kameravalvonta/KAMERAVALVONTAOPAS_2010.pdf

U.S Department of Homeland Security. 2013. CCTV Technology Handbook. https://www.dhs.gov/sites/default/files/publications/CCTV-Tech-HBK_0713-508.pdf

Finanssialan keskusliitto. 2017. Kameravalvonnan suunniteluohje. https://www.finanssiala.fi/vahingontorjunta/dokumentit/Kameravalvonnan_suunnitteluohje_K-menetelma.pdf

ViDi Labs HD/UHD test chart v.5.x Product manual. 2019. https://vidilabs.com/download/vidilabs-test-chart-v.5.x-product-manual%20(1).pdf

Penny, J. (2018). How Safe Is Your Building? *Buildings, 112*(3), p. 6.

European Data Protection Supervisor. Follow-up Report to the 2010 EDPS Video-Surveillance Guidelines. 2010: https://edps.europa.eu/sites/edp/files/publication/12-02-13_report_cctv_en.pdf

Unpublished

The first unpublished reference
Case company: CCTV Plan

Case company: Security policy

Case Company: Risk register template

Figures

Tables

Appendices

Appendix 1: **CCTV Plan table of contents**

Table of contents

Appendix 2: **Feedback from client**

Tuomas produced a clear, practical and useful current state analysis. The quality of the product was above all expectations, as it was very professional and it can be (and has been) utilized as is. During his traineeship, Tuomas was able to clear out underlying issues that had been lying around for too long. When working on the project Tuomas picked up a whole lot of information that he also willingly shared with the team, which brought non-material value. The product is in use weekly, and it is utilized for example this week when negotiating with a camera vendor.

August 28, 2020

Head of Security at Strategic Business Unit of Case Company

Appendices 1: Checklist: Implementing the camera surveillance plan

A camera surveillance checklist that can be utilized as a tool during the production of camera surveillance plan.

Checklist: Implementing the camera surveillance plan				
ID	Procedure/method	Duties	Comments	Status
1	Risk assessment (1)	1. Assessment of risks regarding the building protection 2. Risk analysis and evaluation		☐
2	Defense-in-depth assessment	1. Identification of critical areas 2. Identification of critical assets		☐
3	Target of the camera footage	1. Establish a specific target for each camera in the building		☐
4	K method	1. Test the quality of footage of the cameras with K method test board		☐
5	Camera classification	1. Set up minimum requirement for the quality of footage in critical areas 2. Assessment regarding the cameras ability to fulfil the minimum requirement 3. Establish critical cameras		☐
6	Business impact analysis	1. Establish accepted downtime for each camera or camera groups 2. Set up a procedure that enables corrective actions		☐
7	Assessment of the current state	Does the CCTV system produce footage quality that fulfils the requirements set for critical and other areas?		☐
8	Risk assessment (2)	1. Assessment of risks regarding the building protection 2. Risk analysis and evaluation 3. Risk mitigation 4. Establish a procedure to ensure the continual improvement of risk management		☐
9	Formation of strategy	1. Produce a CCTV strategy based on: • The target of footage • Critical areas • Critical cameras • Accepted downtime • Corrective actions • Preventive and mitigating actions • Continual improvement		☐

10	Formation of the plan	1. Implementation of all of the assessments (ID 1-7) and strategy in to the plan. 2. Identify stakeholders, roles and responsibilities regarding the CCTV system 3. Introduce maintenance related actions, stakeholders and needs of the CCTV system 4. Present: o Handling of footage o Method of surveilling o Justification for surveilling 5. Introduce main legislation and company policy regarding the camera surveillance		☐