jamk

Implementing and Applying ISMS in Organization's Customer Delivery Projects

Development of a Framework for Project's Information Security Tasks

Tiina Leppänen

Master's thesis
May 2021
Technology
Master's Degree Programme in Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Leppänen, Tiina

Implementing and Applying ISMS in Organization's Customer Delivery Projects, Development of a framework for project's information security tasks

Jyväskylä: JAMK University of Applied Sciences, May 2021, 86 pages.

Technology. Master's Degree in Cyber Security. Master's thesis.

Permission for web publication: Yes

Language of publication: English

Abstract

The role of information security and data privacy requirements in IT system development projects is growing as information security awareness and threats are increasing. At the same time information security is seen more as a responsibility of IT system specialists than project management.
The objectives was to investigate in target organization how customer delivery projects could get more force and support from Information Security Management System (ISMS) to project's information security and data privacy tasks. Status of project's information security tasks was investigated in the target organization by surveys. The case study was done in ISO/IEC 9001 certified organization where information security management system (ISMS) was implemented and ISO/IEC 27001 certified.
The results of survey revealed that by sharpening selected processes the utilization of organization's ISMS can be boosted radically. These reforms were identified as good progress in translating security aspects into customer value because instead of focusing only on information security requirements, the project ensured its work process aligned with overall expectations on information security and data privacy by the customer.
Identified development needs of information security task management were key drivers creating framework of information security tasks of customer delivery projects: information security tasks must be launched before customer delivery project starts. As a result, a new project receives information security requirements and risks as input information already in starting phase. It must be noticed that information security tasks are a natural part of project management process and that process can produce data, for example, for auditing.
The developed framework containing information security controls and tasks is reusable and can be implemented as a project's information security task template. The preliminary results of assessment showed that connecting the project process with related processes was especially fruitful. Extending the responsibilities and tasks to surrounding processes (mainly sales and quality) supports a good start and initiation of a project towards secure and agreed outcomes. Applying the framework in different operational environment, in product delivery processes and in continuous services was identified as interesting further development ideas.

Keywords/tags (subjects)

cyber security, information security, data privacy, information security management system, project management, ISMS, ISO/IEC 27000, ISO/IEC 27001, PRINCE2

Miscellaneous (Confidential information)

n/a

jamk

Description

Leppänen, Tiina

Implementing and Applying ISMS in Organization's Customer Delivery Projects, Development of a framework for project's information security tasks

Jyväskylä: Jyväskylän ammattikorkeakoulu. Toukokuu 2021, 86 sivua

Technology. Master's Degree in Cyber Security. Opinnäytetyö YAMK.

Julkaisun kieli: englanti

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

Tietoturva- ja tietosuojavaatimuksien rooli ja merkitys on kasvanut tietojärjestelmien kehittämisprojekteissa erityisesti tietoturvatietoisuuden ja -uhkien lisääntyessä. Samalla tietoturva mielletään edelleen enemmän järjestelmäasiantuntijoiden tehtäväksi kuin projektin hallintatasolle liittyväksi osa-alueeksi. Tavoitteena oli selvittää miten tietoturvan hallintajärjestelmää (ISMS) voitaisiin hyödyntää tiiviimmin osana asiakastoimitusprojektien tietoturva- ja tietosuojatehtävissä kohdeorganisaatiossa. Nykytilanne kartoitettiin analysoimalla laatujärjestelmän mukainen toimintaympäristö tietoturvaprosessien ja -tehtävien osalta sekä haastatteluiden avulla. Tapaustutkimus toteutettiin ISO/IEC 9001 -sertifioidussa organisaatiossa, jossa oli toteutettu ISO/IEC 27001 -sertifioitu ISMS.
Tulokset osoittivat, että tietoturvan hallintajärjestelmä (ISMS) ja asiakastoimitusprojektin tietoturvatehtävät tulisi integroida tiiviimmin niin, että asiakastoimitusprojekti hyödyntää tietoturvan hallintajärjestelmää ja saa tietoturvaan ja tietosuojaan kohdistuvien vaatimusten ja riskien hallinnassa tukea myös muilta prosesseilta (erityisesti myyntiprosessi).
Toimintaympäristön ja kehitystarpeiden pohjalta laaditussa asiakastoimitusprojektien tietoturvatehtävien viitekehyksessä huomioitiin erityisesti se, että tietoturvatehtävien tulee käynnistyä ennen asiakastoimitusprojektin aloittamista, jolloin ne saadaan syötetietoina projekti- ja toimitusprosessille. Kehitystarpeissa korostui myös tietoturvatehtävien sisältyminen projektinhallintaprosessiin, jolloin niistä voidaan tuottaa raportointitietoa mm. auditointia varten.
Laaditun viitekehyksen avulla projektin tietoturvatehtävät ovat koko projektin elinkaaren ajan hallittava ja asiakkaalle lisäarvoa tuottava kokonaisuus, jossa huomioidaan tilaajan asettamien järjestelmävaatimusten lisäksi tavoitteet tietoturvan ja tietosuojan huomioimiselle ja toteutumiselle projektityössä.
Asiakastoimitusprojektin tietoturvatehtävät ovat laajempi kokonaisuus kuin mitä tietojärjestelmän toteutukselle asetetut tietoturvavaatimukset. Viitekehyksen alustava arviointi osoitti, että projektiprosessiin liittyvillä prosesseilla on tärkeä rooli erityisesti tiedon tuottajana ja tukena tietoturva- ja tietosuojavaatimusten toteuttamisessa projektin hallintatasolla.
Viitekehyksen sovittaminen muun tyyppiseen toimintaympäristöön ja jatkokehittäminen esim. tuotetoimitusprojektien ja jatkuvien palveluiden käyttöön huomioitiin mielenkiintoisina kehitysmahdollisuuksina.

Avainsanat (asiasanat)

kyberturvallisuus, tietoturvallisuus, tietosuoja, tietoturvan hallintajärjestelmä, projektin hallinta, ISMS, ISO/IEC 27000, ISO/IEC 27001, PRINCE2

Muut tiedot (salassa pidettävät liitteet)

n/a

Contents

Figures

Tables

Abbreviations

AQAP	Allied Quality Assurance Publication
CIA	Confidentiality, Integrity, Availability
CISO	Chief Information Security Officer
GDPR	General Data Protection Regulation
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
IS	Information Security
Katakri	Finnish National Security Audit Criteria
PRINCE2	Projects IN Controlled Environments, version 2

1 Introduction

Information security's days as just a technology issue are over. Authorities and business leaders are waking citizens and employees up to realize that digitalization and emerging technology means growing requirements on awareness of cyber scams and frauds. This is the trend that was one of the inspirations to this research topic, too. Project's security tasks are not only technical. In this thesis, a framework of project's information security tasks is proposed as a solution and studied along with the research question "How to drive information security into customer delivery projects?".

Information technology (IT) projects are facing constantly more complex requirements and challenges from customers who are renewing their multi-layer technology platforms with high information security demands. Project managers are facing extra burden of staying updated with latest security necessities. Quite often the information security is seen only as a technical issue managed by system specialists in projects. However, it should be one of the core themes included in the stone foot of the project.

"Humans are the primary source and the weakest link of IT projects" (Sangi, Ilkan & Tokgöz 2017, 219). This statement may have "well-worn" stamp on it, but it points to needed security skills and knowledge. Nowadays the success of project is highly dependent on the adoption level of security best practices. Project managers are the glue who should bind together security processes and requirements from both organization's and customer's side. As a result, the information security framework of the project is formulated. Therefore, a project manager is responsible for ensuring that team members are aware of security importance at every phase.

IT companies define their information security landscape in the Information Security Management System (ISMS). ISMSs have been developed and implemented across organizations during recent years. However, the analysis of the implementation maturity and appliance level is a new research area. There is a need of more precise framework how projects should be aware of and comply information security requirements related to both the organization's ISMS and customers' requirements.

The constantly growing requirement level of information security in customer delivery projects puts strong pressure on project management and execution. “Secure and scalable” are the key requirements in ICT business and in digitalization of modern organizations. IT solutions are delivered mainly as service-based solutions and platforms which means that a customer delivery process is a combination of several stakeholders: customer organization, IT system provider and IT service provider. That can be a risk factor for information security of the project: are there possible grey areas which should identified and covered by ISMS. It is vital that information security is in required level in delivery projects: the status is known, and management is transparent.

The focus of this study is to assess and develop how the information security can be driven into customer delivery projects. The ISMS plays an important role as a security framework. According to ISO/IEC 27002:2013, the information security must be integrated into project management processes to identify possible information security risks. Information security goals must be part of project goals and information security risks must be assessed already in the early phase of the project to identify tools needed for management.

This thesis is assigned by IT company (later: target organization) who is providing IT solutions for variety of business and service areas in private, public and third sectors. Target organization’s mission is to proceed modernizing and digitalizing organizations’ processes. Project deliveries are the main offering and one of the business processes. The need for this kind of research work arose during the yearly audit of the ISMS. How could the projects get more force and support from ISMS to project’s information security tasks and then would be utilized in target organization’s customer delivery projects? It became clear that embedding customer delivery projects’ information security tasks into current processes and tools would be a goal worthy of development.

2 Research

This chapter formulates the foundations and the backbone of this study. The research questions define the story line and nature of this work. Construction is directed according to research method and objectives and conducted by ethical principles and data protection. Finally, by searching the related research, a snapshot of existing research focused and finetuned the roadmap of this work.

2.1 Research questions

The main research question that guides this study to achieve its objectives is:

How to drive information security into customer delivery projects?

The fulfillment of objectives is supported and guided with the following sub questions which emphasize the role of organization's ISMS and the customer value to be achieved through the project:

a. How customer delivery projects utilize organization's ISMS?
b. How is the security aspect translated into customer value?
c. What kind of information security controls and tasks should be included in customer delivery projects?

Preliminary study showed that the larger the project, the more information security requirements and aspects should be considered. The industry area of the customer seems to effect on the weight of different requirement areas. Organizations that are in some way responsible for national security assessment, accreditation or guidance clearly place more emphasis on non-functional security requirements than functional, process-oriented requirements.

Preliminary study was executed by evaluating the categories and amount of customer requirements during the past year in information management system product business area of the target organization.

Based on these findings, this study is focused on customer delivery projects that include customer-supplied requirements that guide the implementation of the system to be delivered. The existence of requirements is a measure of the scale of the project.

2.2 Research methods

The objective of this study work was to answer the research questions by developing a model which would support projects' information security tasks. Thereby, *the constructive methodology* was selected as the research method used in this study work. This method is defined as an approach which means "problem solving through the construction of models, diagrams, plans, organizations, etc.", and an example of a construction at its purest is a creation an artificial language (e.g., Morse alphabet or computer languages). (Kasanen, Lukka & Siitonen 1993, 243-264.) Outcomes of this methodology are "innovative constructions" that solve real-world problems and generate contributions to the practice in which it is applied. The key elements of the constructive research method are illustrated in Figure 1. For example, a plan or an information system model is an artefact that is characterized by the fact that they are not discovered but are invented and developed. (Lukka 2003, 83-101.)

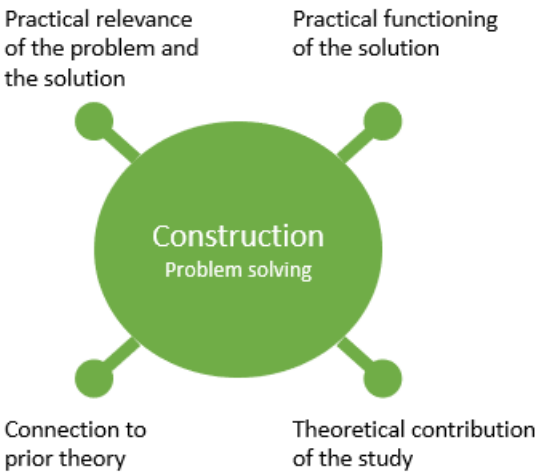

Figure 1. The key elements of the constructive research approach. (Lukka 2003, 246.)

As the construction was done for a case organization, the case study was also applied as a research method. Case study is a research method suitable for understanding and investigating of

complicated issues. Typical for case study method is that it supports a research in a small and specific context. The results of applying the case method are that it is a suitable research method especially for cases where an exhaustive and holistic research is needed. For example, the subjects of study can be a very limited number of individuals. However, case study method has always been criticized of lack of providing results which can be generalized. This can be avoided by using other methods alongside with case study to confirm the reliability of research results. (Zainal 2007, 3-5.)

According to the nature of selected methodologies, this work focuses on real-life challenges that needs to be developed or even solved. The practical need for this work is based on the identified fact that ISMS and information security tasks should be more involved in customer delivery projects. As a result, the aim is to solve identified and further prioritized problems with practical construction. The practicality of the outcomes is ensured by gathering real-life snapshot and development needs in the selected research area. (Kasanen, Lukka & Siitonen 1993, 243-264.)

The most urgent need for this development work raised from the current information security and data privacy checklist which had been created for projects, but its existence, location and content seemed not to be clear. To understand the real-life challenges better, it was decided to gather information about the current state by interviewing key roles related to information security or initiation and management of customer projects. By means of survey research method, the need and relevance of this study was justified by its results. Check & Schutt (2011, 160) defined survey research as "the collection of information from a sample of individuals through their responses to questions". Survey method for obtaining information from individuals and groups has been used for decades. The scale of applied survey can range from free form questions to few individuals to more formal survey which is targeted to many recipients. (Ponto 2015, 168–171.)

There are several potential advantages that may come with constructive methodology. From the researchers' point of view, there is a chance to dig into interesting new research areas based on practical needs. On the other hand, the target organization is expecting to get not only solutions but also new knowledge. It can also be argued that the existing knowledge is tested thoroughly in constructive research process. (Lukka 2003, 83-101.) In this work the status of target organization

is investigated in the light of existing information but from a new perspective. As a result, new knowledge about information security tasks in customer delivery projects is created.

Constructive research method has been criticized about the possible lack of objectivity or non-scientific nature. As Kasanen, Lukka and Siitonen (1993, 243-264) emphasize, by checking the steps of construction, it can be tested, and similar results can be obtained. The objectivity of the outcomes of this work is ensured by producing a construction based on real problem and demonstrating its usability.

It is extremely important in constructive methodology-based research that both participants (target organization and researcher) are committed to the development project. Losing the commitment can arise a risk of failure. (Lukka 2003, 96-98.) The case study part of this research is done in co-operation with Chief Information Security Officer (CISO) of the target organization. He is strongly committed to this work and highly motivated to get practical outcomes to develop existing processes.

2.3 Research objectives

This research is a case study which is focused one organization to gain concrete and in-depth knowledge about stated research questions. The objectives of the thesis are:

- to analyze the awareness of organization's customer delivery projects related to ISMS and
- to design and implement a framework/tool, which defines how information security requirements are included in customer delivery project.

The focus of this study is "the customer delivery project". Wells and Kloppenborg (2015, 1) define *a project* as "a one-time undertaking that will result in a new product, event, or a way of doing things". Typical to a project is, that it has a defined start and finish. Just as any other business, any type of change needs to be guided by effective *project management*. To be precise, the management process of the project, its phases and methods are the main interest when evaluating how information security is involved in project's lifecycle.

As the context of this work is an organization which provides ICT solutions and services for *customers* in variety of industries, there would be no projects without customers and their orders. The expected outcome of the project is defined by the customer and agreed with the project once it starts. The storyline of this study lies strongly on role of information security requirements during the project and their meaning as one creator of expected customer value.

The contents and scope of customer delivery project can vary a lot. For example, it can be a small consultation project to dedicated part of an information management process or customized software delivery including data center services. The *delivery* means the output that is handed over to customer. In this work the precise content of delivery is not significant. However, the main pillars of this study are a *project* which deliveries ICT services to a *customer*. Organization's internal programs and projects (for example, research projects) are not in the scope of this work.

The development or analysis of ISMS related to other organization's processes (for example, IT system development, IT support, IT continuous services or HR) is not in the context of this research. The objective is to focus on IT system delivery project process to limit the scope to be reasonable in given time and resources.

This research will not contain any implementation work other than first draft version of the IS framework. Implementation tool (MS Excel, Azure DevOps, Jira or other) will be decided during research work.

When information security methods, tools and processes are in concern, they are very often seen as IT system and application development related subjects. For example, how to write secure code, what are the known vulnerabilities in certain technology and what is the most appropriate and secure protocol for data transfer, are questions that are not in the scope of this study. As the objectives of this work relate to information security processes related to organization and project management, information system development and implementation processes and security matters are excluded.

2.4 Research ethics

This thesis is aligned with The Ethical Principles for JAMK University of Applied Sciences (JAMK 2018). These principles are defined to promote "*responsible conduct of research*". This means that the research work follows known practices i.e., honesty and accuracy in research work and presentation of results. Methods used in information search and assessment are ethically sustainable. Other research works are respected and referenced in an appropriate manner. (Tutkimuseettinen neuvottelukunta 2012, 5-7.)

The research agreement has been done before starting the thesis and an ethical pre-assessment has been made. The research done by others is considered and respected. The work done by other researchers is duly referred to. This research is planned, carried out and reported in accordance with the requirements for scientific information.

The agreement on Master's Thesis Cooperation was done with representative of the host organization, thesis author and thesis instructor from JAMK. The agreement was signed before this study work started. This is a public thesis, and it does not include commercial or professional secrets of the commissioning party. The contents or outcomes of this work cannot be used in criminal purposes.

Processing of personal data is controlled by The General Data Protection Regulation (GDPR, Regulation (EU) 2016/679). Since information gathering (surveys) was implemented anonymously, no personal data was collected and no information on natural person was needed, used, or collected to complete this work.

Official and licensed Microsoft Office tools were used in creation of this study. All referenced materials (books, articles, etc.) are referred and listed according to the reporting instructions of JAMK.

This thesis becomes public as soon as it is approved. It is stored in common pool of knowledge and published in the open and public Theseus database for universities of applied sciences.

2.5 Related research

This chapter represents research and publications that relate to this work. “ISMS”, “information security”, “data privacy”, “IT project” and “project management” are examples of keywords used in search phrases in reference material searches. The especial interest was to find research or methods that are like the research questions in concern. According to the results of related research, the current limitations was described and the need for new methodology identified. This section is divided into two main themes according to this work: ISMS and customer delivery projects.

2.5.1 The essence of ISMS

Organizations need to systemically ensure the security of stored information by tight regulatory requirements and high customer expectations. To address these challenges, organizations are implementing and maintaining Information Security Management Systems (ISMS). ISMS is a systematic approach consisting of processes and policies to establish, implement, maintain, and continuously improve organization’s information security processes. Recent studies show that the level of content, coverage and status of ISMS depend on the size of organizations. Smaller organizations are gathering forces and requiring support in creating while larger ones have already adopted ISMS and operating with it as part of their processes. (Brunner, Mussmann & Breu 2018, 483-490.) According to Goldes, Schneider, Schweda and Zamani (2017, 1-6) there is no strict standard how to implement ISMS and blueprints are relatively rare.

ENISA reports in their threat landscape report of the year 2020 that cyber-attacks are becoming “more sophisticated, targeted, widespread and undetected” (ENISA 2020). In 2020 the COVID-19 pandemic effected not only health but also cyber security globally. According to F-Secure’s attack landscape report (2020, 3) remote work enlarged the borders of an organization’s network and at the same time the attack surface also. COVID theme was used in several spam and phishing email campaigns targeting organizations and citizens. Changes in threat actors show that they can adapt to new situations by “shifting their operations to target trending topics without losing momentum”.

As the threat and attack landscape reports of the year 2020 show, organizations should ensure they adhere to best practices and recommendations in the continuing process of information security. More professional field of cyber-crime, all-inclusive globalization, and digitalized businesses boost organizations not to allow dust to settle on their Information Management Systems (ISMS). (Goldes et al. 2017, 1-6.)

2.5.2 IT projects and information security

Ali, Soomro and Brohi (2013, 1190-1196) highlight the increased risks of vulnerabilities and threats because of the rapid growth in the networked infrastructure. Organizations are forced to adopt and implement security procedures and standards to keep their information systems safe and sound. As a result of their research "compliance with these security standards ensures that the organizations' information is secured competently and also helps in reducing project failure chances". Payette, Anegbe, Caceres and Muegge (2015, 26-28) motivate their research with a statement that current maturity models used in project management assess quality and practices but do not explicitly consider information security. However, most systems that comprise critical infrastructures are executed as projects using project management practices.

IT project is not complete without IT security. IT firms rely upon project management approach to successfully accomplish their projects and without IT security an IT Project cannot be considered as a complete project. (Sangi, Ilkan & Tokgöz 2017, 219-220.) Pruitt (2013, 1-3) stated that security aspects of the project are usually system developers' and project managers' responsibility. Extra burden is set by the industry of the customer: project managers must be up to date with latest security necessities in projects with public sector.

Year 2013 revision of ISO/IEC 27001:2013 contained completely new thing: security in project management. The implementation of this new control was not clear at first. As Segovia (2015) states, security is usually forgotten in projects and information security should be seen as a process, not as a product. Exceptions are large organizations which have included information security focused risk assessment as one activity in their projects. This is what ISO/IEC 27001:2013 Annex A.6.1.5 requests. Segovia (2015) suggests four key activities which should be integrated into project management activities. First, information security objectives should be included in project objectives. Second and third activities relate to risk management and point out the importance of

assessment's timing and handling of risks. Fourth activity reminds to keep information security policies essential during the project's lifespan. As a result, information security is always a component of project management in the organization. These key activities are depicted in the following figure (Figure 2).

Figure 2. Establishing information security in project management. (Segovia, 2015)

The more project members are aware of the significance and value of the information security, the more reactive and sensitive they are to the potential vulnerability and risks associated with the project's outcomes. As the meaning of organizations' information security rules and regulations increases, also the level of information security awareness will grow. (Raghavan & Zhang 2017, 84-85.)

Secure project management is a combination of project management and security needs. Important is, that project security should be seen wider than just system security. The CIA triad (Confidentiality, Integrity and Availability) must be covered, and security controls (for example, information protection and authenticity) applied to mitigate project risks. (Emory 2004.) Previous studies refer that when security best practices are included in each phases of a project, IT project managers can deliver more secure outcomes in a more secure way. Sangi et al. (2017, 223-224) have presented a framework where information security is integrated in IT project management levels and phases. This framework is presented in Figure 3 and it consists of four levels:

1. CIA Triads: Confidentiality, integrity and availability should be maintained at each level to ensure secure communication and security during the project's lifecycle.

2. Project management phases: These phases are integrated with system development phases (level 3). Execution phase of project management covers both development and implementation phases of system development.
3. System development phases: These phases are integrated with project management phases.
4. Security requirements: These requirements should be accomplished in each phase.

According to this framework Incident handling, Business continuity and Change control plans should be in place to handle any uncertain situation. (Sangi et al. 2017, 223.)

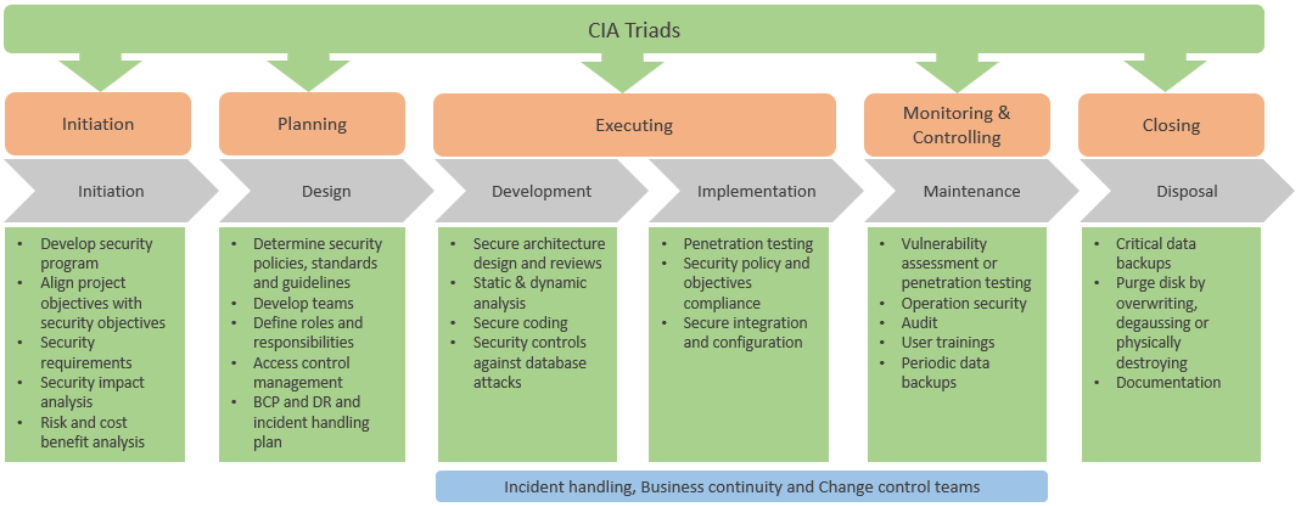

Figure 3. Proposed framework of IT project management security. (Sangi et al. 2017, 224.)

According to Smith (2019) information security should be considered throughout a project's delivery to maximize its profit in long-term. Luckily, project managers can apply information security best practices, he claims. His research includes one example of security incident case where the project was found responsible: project manager was not aware of a risk and used an USB drive containing a virus which then spread rapidly compromising most of the critical systems in the organization.

3 Theory

Information security and data privacy are covered in this research from the customer delivery projects' viewpoint. They are all wide areas in theoretical context. The theories that are most relevant to this research are discussed and evaluated in this frameworks chapter. The main goal is to define key concepts and evaluate relevant theories and models. This part of the study lays the foundations that supports analysis of this work. This frame also justifies the research approach by showing that this work is grounded in established ideas.

3.1 Information security

Information security is a concept that is more and more present in our modern society. In the era of digital information and integrated information systems, methods for protecting and securing digital assets must be versatile and constantly evolving. In general, information security is seen as a key asset of the modern and global business (Andress 2014, 3-6). ISO/IEC 27000:2018 defines information security as "preservation of *confidentiality*, *integrity* and *availability* of information". These three concepts are commonly known as "the CIA triad" and pillars of information security.

Confidentiality means that the information is disclosed to those who are not authorized to access it. Confidentiality must be covered in all stages of information life cycle, for example where stored and transferred. Information must be complete and accurate to preserve its *integrity.* In case of several information versions, the original must be identified, as well as the current one. *Availability* is a property which means that the information is accessible and usable to authorized entity (for example, an individual or a system) when needed. However, this does not mean that information should flow freely. It is also assumed that appropriate security is provided for the information: providing it only to entities with required rights, by appropriate means, and be able to recover it in case of failure. (Harris & Maymi 2016, chapter 2.)

Elements in CIA triad can be used to define security issues according to three aspects it contains. However, those may not be enough, and more dimensions are needed to describe the issue in more detailed level. (Andress 2014, 3-6.) Raggad (2010, 22-24) has presented a so-called security star which enlarges the CIA triad with *authentication* and *non-repudiation* angels. The core anthem of security is also present: *risk*. A risk is an essential factor in driving secure business. Leaders of

business are focused on managing risks, not security. For example, insecure management of information may risk the business, and it may also cause high fees in the name of GDPR.

Another appliance of CIA triad is the Parkerian hexad. It is an extended model of the CIA triad which represents new attributes called *possession or control*, *authenticity*, and *utility*. Possession or control means disposition of the information and related systems and media. That is important because information is very often stored in multiple places containing several versions. Utility means assessing the usefulness of the information taken its format into account (physical/digital). Andress's (2014, 7-8) example of applying Parkerian hexad to transporting encrypted/crypted data tapes could be transferred to present where same information can be sent in different network protocols (encrypted/crypted) via different network security levels (private/public).

Figure 4 presents an illustrated combination of security star and Parkerian hexad. Authentication and authenticity share the same angle but does not mix their original aspect which is defined according to the point of view in case.

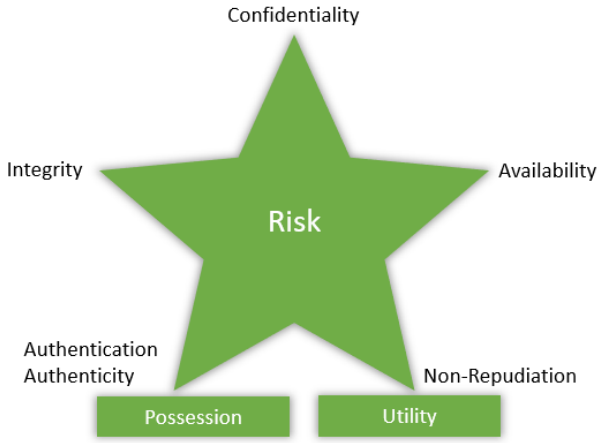

Figure 4. The security star meets the Parkerian hexad.

As Andress (2014, 4) points out, defining insecure is easier than secure. The wider the context, the more there is to secure. As the term "information security" is defined, the context is the information. Nowadays the media is reporting more often about cyber security threats and attacks. What is the difference between "information security" and "cyber security"? Watkins (2013, 18-20) clarifies that cyber security is a term which has emerged along with internet and integrated systems. It covers systems and information across technical domains. According to the glossary of

NIST (2021), the security star is the core of cyber security also, but the coverage is wider than only the information: both electronic and wired communication and related systems and services. Target of a cyber security attack is disrupting enterprise's computing environment or damaging the information.

Although "cyber" refers to both information and communications networks, "information security" cannot be restricted to concern only data in particular system. The era of monolith systems is nearly over and securing information must be a combination of systems, network, processes, and people. These aspects are also included in ISO/IEC 27001:2013 which defines Information Security Management System (ISMS) as a framework to identify, manage and reduce any information security threats in the organization. (Achmadi, Suryanto & Ramli 2018, 149-150.) Development of organization's ISMS is recommended to be done as a project work.

In addition to international and EU level standards and regulations, national public IT procurements contain information security requirements related to national criteria and commonly agreed tools. Katakri is national security auditing criteria which is required especially in cases where classified information is managed (Ministry of Defence 2015, 3-5). Especially in cases, when Katakri is defined as one requirement without applying or specifying it according to the risks and needs of the target system, this requirement must be notified and considered from the beginning of the project.

3.2 Information Security Management System (ISMS)

As there is no place where to hide from information security threats, "manage" and "protect" are the key elements for ensuring business continuity. Modern organization with critical assets relying on information technology requires an Information Security Management System (ISMS) built on three pillars: people, processes, and technology. The main objectives of an ISMS are to secure organization's information and build resilience to information security attacks. As a result, information security costs are more in control and can be reduced. (Dutton 2019.) Considering the three pillars of ISMS, it needs to define how it addresses relationships with staff and customers. They also address that ISMS is "a topic that goes well beyond the remit of the IT department". (Watkins 2013, 18.)

ISO/IEC 27001:2013 standard defines the Information Security Management Systems (ISMS) as “a suite of activities concerning the management of information risks”. ISO/IEC 27001:2013 standard is more a guideline than a must: it does not declare the structure of ISMS.

The ISMS is a framework which is used by the information security management process. As a suite or system, it contains interrelated elements that have dedicated roles which are then synchronized. The goal of the system is to protect the confidentiality, integrity, and availability of information. Figure 5 presents a concept model the elements which ISMS covers. This figure is an adapted version of concept model presented by Dexter (2002) and it addresses elements that are relevant to this study. Primary attention is given to policy and planning. Information security management requires planning for training and directing information security awareness of people. Risk management is managed by policies which are drivers of information security management. (Dexter 2002, 3.)

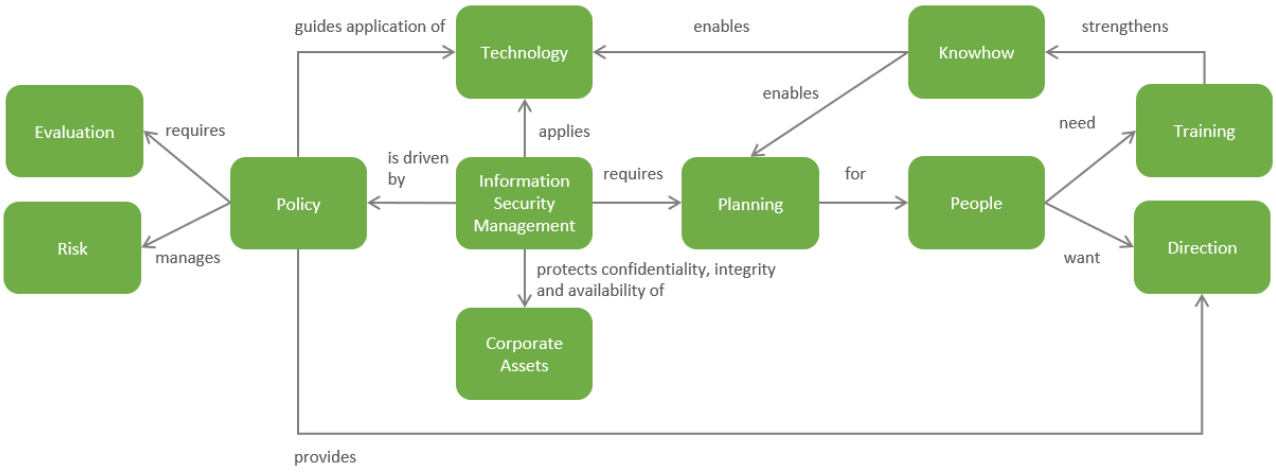

Figure 5. The key elements of information security management process. (Dexter 2002, 3.)

Assessing the efficiency of the security system is a continuous process, and it depends on its components functional properties. Desired security level of ISMS is maintained by periodical auditing and continuous monitoring. (Kiedrowicz & Stanik 2018, 7.)

3.3 ISO/IEC standards: 27000 and 27001

As the importance and complexity of information technology has grown, the urgent need for common practices and standards of information security management has aroused. ISO/IEC 27000 and 27001 are international standards that referred to as “common language of organizations around the world” for information security. The role of these standards is to support and guide the development and maintenance of an ISMS. (Disterer 2013, 92-95.)

Since 2009, ISO 27000 standard has provided an overview and a conceptual foundation for the ISO 27 K family of standards: it defines 46 basic information security terms. The current version of ISO 27000 standard is fifth edition, year 2018. During its timeline, the standard’s core has been the risk management. Companies’ business processes dependent on information processing and integrated IT infrastructures are vulnerable to system failures and disruptions. So, the identified risks are putting pressure on systematic engagement of security policies and practices. (ISO/IEC 27000:2018)

The International Organization for Standardization (ISO) and the International Electro Technical Commission (IEC) published ISO/IEC 27001 Information Security Management System standard in 2013. Its full name is ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements. This standard was created to define a risk management system for controlling information security management.

ISO 20071 standard defines the Information Security Management Systems (ISMS) as a set of activities which relate to the management of information risks. ISO 27001:2013 standard is more a guideline than a must: it does not dictate the structure of ISMS or any information security actions. It is also technology-neutral, and the idea is to focus an organization’s information security roles and responsibilities. Organization’s ISMS determines how the risks are identified and handled. The concrete goal of ISO 27001 compliance is the certification. In addition to good reputation and competitive advantage, that certification is a message to customers and stakeholders about the conscientious and seriousness of information security. However, the certificate is not a guarantee of real security. (Winder 2015, 108.)

ISO/IEC 27001:2013 Annex A lists control objectives and controls to develop and manage the security of information in IT systems. Defined controls describe actions necessary for ensuring that the organization has established a framework that can adequately implement and maintain information security practices within the organization. Control objective A.6.1.5 is especially interesting control from this study work's viewpoint: "Information security shall be addressed in project management, regardless of the type of the project".

3.4 Risk management

The core of information security management is a process where all security risks are accurately identified, assessed, and mitigated according to a risk-driven security program. An effective security management program, on the other hand, requires that organization's assets are valued, and related risks are identified in terms of the vulnerabilities, threats and effects containing evaluation of the consequences if an unexpected incident occurs. (Raggad 2010, 23-25.)

As NIST SP800-30 (2012, 6) defines, "risk is a measure of the extent to which an entity is threatened by a potential circumstance or event and is typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence". Risks that origin from the loss of confidentiality, integrity, or availability of information or information systems are *information security risks*. They may have harmful impact to organization's employees, functions, assets and other actors related to organization. When assessing a risk, it is important to distinguish between its causes and the potential occurrence of the incident that constitutes the risk. An incident is an event that reduces the value of an asset. Whereas an asset is in information security context any data, component, system, or hardware, that supports information-related functions. An asset has value for an organization, company, or unit, which is called a party. The occurrence of a risk is defined and estimated with its likelihood. It means the chance of something to happen. A consequence is the negative impact of an incident. As a result, it causes harm or reduced value of an asset. (Refsdal, Solhaug & Stølen 2015, 33-47.) These risk concepts are illustrated in the following figure (Figure 6).

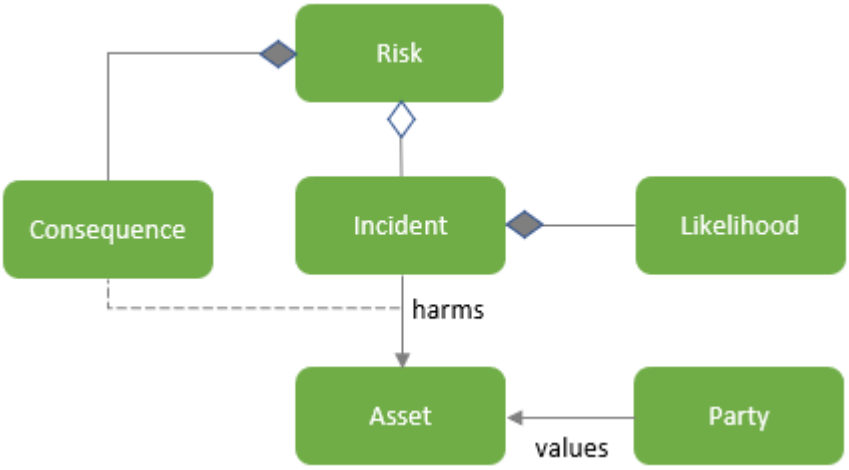

Figure 6. Concept model of a risk. (Refsdal, Solhaug & Stølen 2015, 33.)

Risk management process is an ongoing flow of activities for identifying, analyzing, evaluating, treating, monitoring, and reviewing risks. (ISO/IEC 27000:2018) To achieve effective and efficient risk management procedures, decision makers, stakeholders, and other key personnel must pull in the same direction. This means, that it is crucial to achieve a mutual agreement on and common understanding of how risks are managed in the organization. (Refsdal et al. 2015, 33-47.) The risk management process can be observed and analyzed from several viewpoints and levels. Following figure (Figure 7) illustrates the four top level steps in the risk management process.

Figure 7. Key compoments of risk management process. (NIST 2012, 4-6.)

Before the risks can be assessed in a continuous process, they must be identified. At this phase, all risks that are related to the loss of confidentiality, integrity, and availability of information, should be identified. In addition, the risk owners should be named. (ISO/IEC 27001:2013) The key phase

of risk management process is *risk assessment*. (NIST 2012, 4-6.) Baskerville (1991, 121-130) highlights the difference between risk analysis and risk assessment. The process of identifying risks and related characteristics is risk analysis. When assessing a risk, it is identified, estimated, and prioritized. At this point, an analysis of threat and vulnerability information is required to define the scale of possible impact and its likelihood. To *control a risk* addresses how organization responds to identified and assessed risk. The aim is to define a consistent and organization-wide way how to response to a risk. Risk management process is not ongoing and consistent without risk monitoring and *control review*. The purpose is to address monitoring to evaluate the effectiveness of risk responses ongoing, identify possible changes which are caused by risks and to verify that defined risk response methods are implemented. The analysis of information security requirements which are coming from and traceable to organization's operational environment should be also part of review. (NIST 2012, 4-6.)

3.5 Data privacy

Data privacy governs practices how personal data is *collected, shared, and used*. There is a distinct difference to data security which *protects* data from compromises (attacks) and malicious users. Personal data is all data related to person identified or identifiable. Earlier, laws and regulations concerning personal data were steered nationally. Along with wider freedom of movement and global digitalization, the urge of legislate the processing of personal data became evident at EU level. (Sharma 2019, 2-5.)

The EU General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world, and it governs how organizations process personal data. Preparing for the arrival of GDPR caused massive renovations in organizations' practices and systems related to management of personal data before it replaced the EU Data Protection Directive 1995 and all member state laws based on it. Risk of penalty were notable motivator for putting personal data processing in order: failure to comply with the GDPR may result in significant fines based on company's global turnover. GDPR took effect on 25th of May 2018. It applies to organizations that process or control the processing of EU residents' personal data, wherever the organizations are based. (Regulation (EU) 2016/679)

An ISO/IEC 27001:2013 compatible ISMS provides a strong footstep to cover GDPR requirements. That standard includes controls that are in line with GDPR rules for preventing data breaches and hacks. A personal data breach is defined in GDPR as “a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed”. GDPR’s Article 32 contains the measures that organizations must implement to prevent information security breaches. These are:

- The pseudonymization and encryption of personal data.
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.
- The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident.
- A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

To comply with Article 32, organizations need to identify and mitigate risks that are presented by data processing, “in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed”. (Regulation (EU) 2016/679)

GDPR obliges the organization to take appropriate technical and organizational measures to secure the processing of personal data. Technical means can be, for example, implementing access control, encrypting information with appropriate encryption algorithms and the design and technical implementation of a data anonymization method. Management tools should be implemented as part of the system or application architecture at the earliest possible stage, as they may affect other functions of the system. (VAHTI 2014, 19-21.)

3.6 Katakri

Finnish national security auditing criteria (Katakri) is for the authorities and the business community to harmonize common security procedures and independent monitoring and to improve auditing. Katakri is an auditing tool, which is used in assessing the target organization’s ability to protect an authority’s classified information (national or international). It can also be used to help

companies, organizations and the authorities in other security work and its development. Katakri includes the minimum requirements based on national legislation and international obligations but it does not set any absolute requirements for information security. Katakri contains requirements that are based on the current legislation and the international information security obligations binding in Finland. (Ministry of Defence 2015, 2-4.)

The first Katakri was created by Finnish Governmental program for internal security in 2009. Since then, Katakri has been updated three times, in 2011, 2015 and 2020. Katakri has been accepted as de facto tool which has significant value for the Finland's reputation in information security related questions. The latest version of Katakri aims to comply national legislation renewed in the beginning of 2020. It has been also upgraded according to the latest development steps of digitalization and needed guidance for its appropriate use. (Traficom 2020, 5-7.)

"Katakri audited system" is often one requirement in technical or non-functional requirements in public IT procurements. However, Katakri is not meant to be used in public IT procurements as such. Information security requirements should be defined according to the special needs and risks concerning procurement in case. (Ministry of Defence 2015, 2-4.)

3.7 Project management

In addition to information security, the main topic of this study is a project process and management of information system customer delivery projects. The main concepts of project and project management are defined in this chapter according to the methods that are included in the quality processes of the target organization of this study. The aim of this work is to evaluate, how the used methods identify information security tasks, and if not, how they should be involved in customer delivery projects.

The main goal of a customer delivery project is to bring profit to the organization and its business. This is possible when the following criteria is met: project is finished in time, under budget and within scope. The projects are not in a capsule but operate in the middle of a complex architecture where information systems are integrated, and undoubtedly information security aspects must be put first. In the worst-case scenario when a security risk is materialized, it could be a hazard not

only to the organization or the project but also to the project manager. The reputation knock can take a long time to be fixed. (Smith, 2019.)

Used project management method is PRINCE2 (Projects IN Controlled Environments, version 2). It defines *a project* as "a temporary organization that is created for the purpose of delivering one or more *business products* according to an agreed *business case*." Temporariness separates the project from other business activities. Return for the organization who is the owner of a project is delivered by business products. In the organization context of this study, a business product is an information system which can be tailored, or product/platform based. The heart of the project is a business case, and its key goal is to test the viability of the project. (Hinde 2012, 2-8.)

PRINCE2 defines four main areas of *project management*: plan, delegate, monitor, and control. These areas ensure that the work is co-coordinated and controlled effectively. The goal is to deliver outcomes within agreed constraints, like budget and schedule. (Hinde 2012, 2-8.) PRINCE2 addresses the management of project risks, but not information security. Nonetheless, information security capability could be assessed like any other subjects included in the scope of project management. (Payette, Anegbe, Caceres & Muegge 2015, 26-34.)

An information system project develops and implements an outcome which is based on a need. That need is set by customer in a form of requirements. One of the prerequisites for a successful information system project is good requirements management. Requirements defined by the customer are mainly analyzed, designed, and implemented in the project. The most common reason for project failure is incomplete requirements. However, depending on the quality and unambiguity of requirements, communication and clarification is often needed to ensure common understanding of the needed results. (Hull, Jackson & Dick 2010, 1-10.)

Used projects models in the target organization are Microsoft Sure-Step, Scrum and Waterfall. The model is agreed according to the business case. The Microsoft Sure-Step methodology is an agile implementation model for developing Microsoft Dynamics solutions. (Microsoft 2013). With this agile method customers get better control over the outcomes because development and implementation direction can be quickly changed during sprint cycles. The focus is on delivering the

agreed functionality in iterative sprints which minimizes the risk of resulting to a not needed solution. (Orosz & Orosz 2012, 249–254.) This is also the spirit of Scrum which is a lightweight framework for developing complex solutions in incremental chunks (Scrum 2021). As the trend of software development is to apply agile work methods, the waterfall is a gradually retiring method. Waterfall is a process in a linear sequential flow in which a phase begins only if the previous phase is complete. This model does not support modern and agile development process and it is used only in cases where the customer requires progress in sequential mode.

4 Case study

The case study of this thesis was conducted in the target organization. This organization is providing IT solutions for variety of business and service areas and the project deliveries are the main offering and one of the key business processes. The research questions and related actions of the work process of this study work was defined as shown in Table 1.

Table 1. Actions and collected data related to research questions.

Research question	**Actions and collected data**
How to drive information security into customer delivery projects?	A framework based on organization's ISMS and quality system is developed and tested to assess the results. The main research question is answered with supporting sub-questions.
a) How customer delivery projects utilize organization's ISMS?	Information on current status and especially of the awareness related to ISMS. The results give input to further development by analyzing what are the main reasons if ISMS is not fully utilized.
b) How is the security aspect translated into customer value?	The main target of a customer delivery project is to provide value for the customer with its outcomes. The developed framework concentrates on this aspect from the information security viewpoint. The analysis is done how the related processes communicate with project and delivery process now and what should be developed for the future.
c) What kind of information security controls and tasks should be included in customer delivery projects?	Knowledge of current methods and information security tasks was used as the theory base. How the developed framework should cover and meet the existing requirements and provide support to project management tasks.

In the beginning of this work - and as an inspiration for this work - was a hunch and a perception that information security and privacy tasks should be more preplanned and visible in customer delivery projects. Because in urgent needs, there seemed to be lack of information security support and expertise in some project areas. So, the question was: what the status is and how it should be developed. First, the baseline needed to be defined as a format of current state analysis.

Target organization has been awarded several ISO certificates which cover the company's operational processes. Current quality management system is created based on and certified to ISO 9001:2015 "Quality Management System Certification", ISO 27001:2013 "Information Security Management" and ISO 13485:2016 "Medical Devices". The structure of quality system is created along with the process map of the operational environment. On the top level there are two main process areas: global business processes and support processes.

At first, the process map of the organization was analyzed from the viewpoints of ISMS and projects – in what processes they are defined and what processes are interacting with them. As a result, five processes were selected as a reference for this study work. As the key focus of this study are information security, customer delivery projects and related policies, the following processes was identified as the context of current state analysis:

- business process: projects and deliveries,
- business process: sales,
- support process: security and privacy,
- support process: quality and development and
- support process: risk management.

These processes are interrelated, and they cover the research questions posed in this study. The manuals and other material included in the quality system, were used as reference material in this work (see Figure 8). The quality system was also defining the boundaries for this work: the outcomes must align with existing quality processes and principles.

This research started with a current state analysis to find out how organization's ISMS supports the customer delivery projects, that is, what are the aspects that are expected to be covered. On the other hand, one of the research questions is to explore how customer delivery projects utilize

organization's ISMS, and how it is involved or notified in projects which handle security and privacy requirements. An interesting aspect was also to analyze the awareness of organization's customer delivery projects related to ISMS.

The work process used in this research work is represented in the following figure (Figure 8). The triggers of this work were the practical problems which were formulated as research questions in the beginning. Then, the current state analysis started with an analysis phase and the information gathering was done by interviewing responsible persons of selected roles. Needs for development were defined and prioritized according to result set of interviews. The preliminary development plan was created, and it was used in implementation phase. Finally, the outcome of this development process was assessed by project managers. Related organization's processes, presented in Figure 8, were selected as source and context of this work. Selected resources or outcomes of the related processes are also presented in the figure. They are evaluated as relevant sources for this work. In turn, this research work process produces outcomes to the related processes.

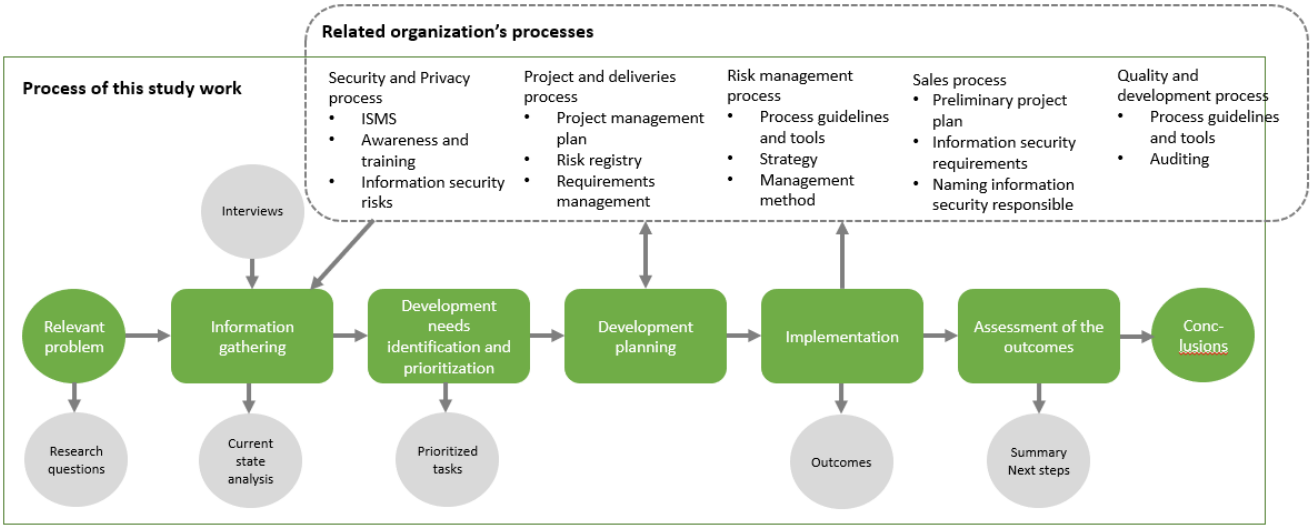

Figure 8. The work process phases, references, inputs and outcomes of this research study.

The process of this work presented in Figure 8 can be mapped to the process of the constructive research method which is used in this study (Kasanen et al. 1993, 246). First, a practically relevant problem which had research potential, was found and research questions were formulated. In the information gathering phase, general understanding of the subjects were obtained, and current

state analysis was made. Then, in the following two development phases, a solution idea was innovated and constructed. The implementation phase included iterative and incremental tasks to demonstrate that the outcomes are aligned with research questions and targets. In that phase, also the connections to related theories and the research value of the outcomes was showed and defined as conclusions of this work. Finally, the assessment of results was done to examine the scope of applicability of the solution, i.e., outcomes of this research work.

4.1 Quality system of the operational environment

The organization's quality system contains process related training materials, templates and documentations which are the tools for all employees. These procedures and tools are the basis for auditable events performed by either external or internal audit teams. The process descriptions of the organization's operational environment are core the content of the quality system. They are grouped into global business processes and supporting processes. Five processes were selected as a reference for this study work. These processes are introduced in Figure 9 and in the following chapters.

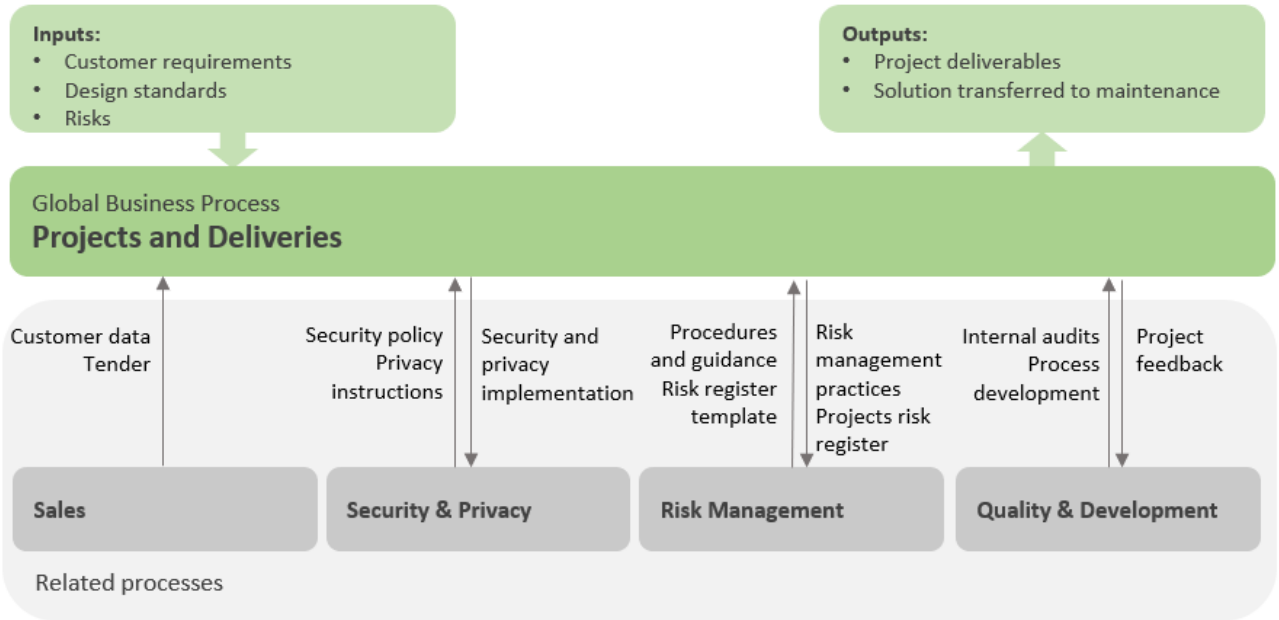

Figure 9. Processes and their interactions relevant for this work.

The current process descriptions included in quality system were used as an information source. The focus is on characteristics, elements, and documentation that are meaningful for the subject of this research. How the selected four related processes are currently connected to project and deliveries process according to quality system, is also an interesting question.

4.1.1 Projects and deliveries

The projects and deliveries process is one of the global business processes and its goals are tightly related to the existence and goals of the core business. The goals of this process are obtained when the outcomes answer the customer's business needs with defined products in the defined time frame and cost.

The project management and delivery is a sub-process of the projects and deliveries process. It is based on the PRINCE2 project management methodology which is adopted to organization's project environment and customized according to project's special features. As a result, this current state analysis is done based on PRINCE2 methodology (Hinde 2012, 2-8) – the processes, tasks, and definitions it contains. The main elements and auditing points (C0-C4) of this sub-process are presented in Figure 10.

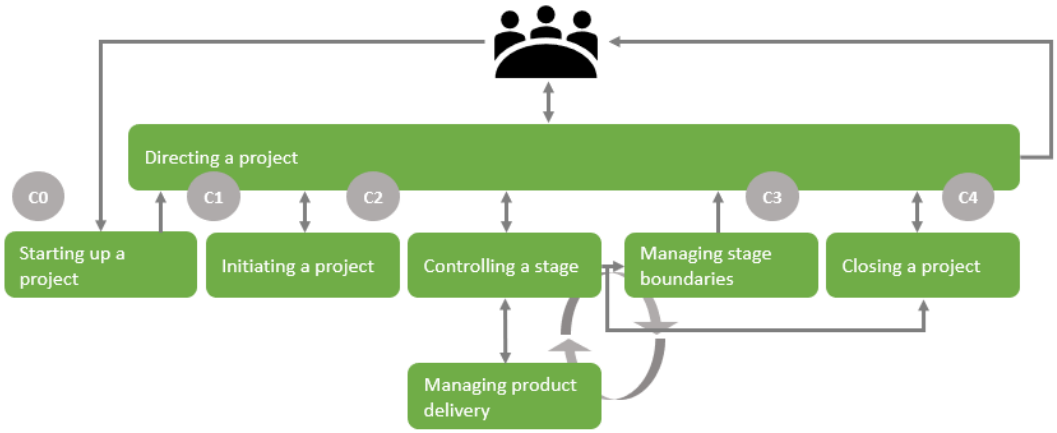

Figure 10. Project management and delivery sub-process and checkpoints.

The sub-processes of project management and delivery are presented in Table 2. The purpose of each sub-process is defined briefly to identify how current definitions possibly reflect to information security and privacy tasks.

Table 2. The sub-processes of project management and delivery.

Sub-process	**Purpose**
Starting up a project	The first check point (C0) includes tasks of sales phase. This sub-process is a transfer from sales to project initialization. Ends with a start stage review audit (C1) which purpose is to check that project starting is done correctly and project manager knows the target, resources and limits. In sales to delivery transfer all relevant information of the project are collected from the sales process for the project team, business management and finance.
Directing a project	To take care of steering the project in such a way that the Business Case is realized.
Initiating a project	To plan the project implementation in such a way that the project will be under control throughout its entire lifecycle and to ensure the validity of the business case in light of more detailed information. How the requirements of the project minimum set are realized is reviewed in the auditing of the project initialization (C2).
Controlling a stage	To concentrate on controlling the delivery stage at hand in such a way that the business case stays valid, the products of the stage are delivered within the agreed upon tolerances, and that risks and problems remain under control.
Managing product delivery	To ensure that the work ordered from the team is agreed upon unambiguously and predictably, the products defined in the work package are delivered within tolerances, and the progress of the work package is reported regularly to the Project Manager.

Sub-process	Purpose
Managing stage boundaries	To ensure that the stage has been delivered as agreed and to plan the next stage of delivery (C3).
Closing a project	To ensure that the project products are approved and has been handed over to the customer, to estimate the project performance compared to the forecasts, to estimate the benefits gained during the project, to produce a plan for reviewing benefits gained after the project, and to ensure the proper follow-up of the remaining problems and risks (C4).

The projects and deliveries process refers to the ISMS. Its role is to assure good security in all functions and thus also in the processes, sub-processes and phases under the projects and deliveries process. Information security is a viewpoint that must be noticed and documented during a project planning and delivery.

During all project stages presented in Table 2 several different types of documentation are created by responsible roles. The project plan is finalized and agreed in the initiation phase and it is the key document during the project lifecycle. When customer requirements usually contain specific information security requirements related to deliverables and outcomes of the project, the project plan defines information security practices and policies which are steering the project management and work. In the project plan, the following information security aspects should be defined:

- Practices related to project material's access management.
- Evaluation of critical information security requirements set to the project and naming security responsible.
- Identification and assessment of information security risks.
- Applying common security frameworks (for example, OWASP top 10) in development work.
- The security and privacy checklist must be filled.

The security and privacy checklist is a kind of embodiment of connection between organization's ISMS and projects, and it should be filled in the beginning of the project. The aim of the checklist is to ensure that information security and data privacy are in the scope on the project and managed in an appropriate way. Its role is also to trigger the security awareness. The checklist is an Excel file, and it is stored in quality manual's support processes' security and privacy category in the intranet. It is also referenced from the project management plan template.

The project manager is the key role of the project. This role is the only one who manages the project and has focus on the project on daily basis. According to PRINCE2, this role can never be shared. Challenging technologies, security threats and digitalization objectives are setting even heavier responsibilities and competence requirements on project managers' shoulders. Managing a project is a combination of a variety of tasks from every possible aspect inside the scope of the project. From the information security point of view, the quality system defines following information security and privacy responsibilities for the project manager:

- Understands and follows security and privacy policies.
- Takes care of that information security viewpoint is noticed during a project planning.
- Utilize the security and privacy checklist.
- Manage personal data during its lifecycle.

According to quality system's process interaction matrix, interrelation between projects and deliveries process and support processes exists by means of:

- security and privacy process: security and privacy implementation in projects and deliveries,
- quality and development process: project satisfaction results and
- risk management process: risk management practices including risk tolerances in euros as part of project delivery, project's risk registers and deviations.

The delivery model of a project can be the Scrum (agile model), based on Microsoft Sure Step (intermediately agile) and, the waterfall (traditional model) or customized delivery model, when the criteria required by the process are fulfilled. Deliveries are classified in four delivery comprehension classes where the criteria is set by the amount of project work (person-days). This study concerns deliveries of standard and complete projects (100 person-days or more).

4.1.2 Sales

The basement and frames of a customer delivery project is built on a sales phase. Before the termination of agreement, sales team gets a lot of information on customer's target state and related requirements.

The sales process is one of the key business processes of this study work. First, it is a phase where security situation assessment is done for the first time. The customer may lay expectations on information classification, handling of personal data and required level of information security awareness before the project starts. The sales responsible must take care of that customer information security requirements are considered when customer information is handled as part of sales process activities. The higher the level or priority of the information security requirements are, the higher is a need to evaluate their impact on coming project's information security resources.

Secondly, the sales process provides vital information as an input to the projects and deliveries process. When information security requirements are already analyzed in the sales phase and transferred to the project, it minimizes the work needed in the project's starting phase. The aim is, that the information security requirements and risks identified in the sales phase would be gathered in such format that they are available for the project without extra effort or risk of them being ignored.

4.1.3 Security and privacy process

The goal of the security and privacy process is to ensure that information security, privacy and data protection are managed on a relevant level according to business needs. Also, cybersecurity and privacy risks are addressed and managed continuously. As expected from a support process, it is closely linked to all other processes described in the organization's process map.

The heart and gold of the security and privacy process is the ISMS. It defines the means of implementing, maintaining, and continually improving the management system in addition to assessing and addressing information security risks. Continuous management is in the responsibility of or-

ganization's CISO together with information security group. In addition to being part of organization's quality system, the ISMS is certified, and it follows the ISO 27001 standard and its requirements.

The ISMS is continually being improved and improvement is steered by information security measurements, internal audit results, identified risks and general information security status. The ISMS is audited regularly by conducting internal information security audits.

Process description of security and privacy process does not contain or directly refer to customer delivery project related roles or tasks. As a support process, it defines roles, responsibilities and procedures that are necessary to facilitate or assist the execution of security and privacy related tasks in projects. According to quality system's process interaction matrix, interrelation between security and privacy and projects and deliveries processes exists by means of security policy and privacy instructions.

4.1.4 Quality and development

The quality and development process has a monitoring role in the organization. Its goal is to offer process documentation for employees and assure that everyday operations are in line with what has been documented. The process is linked the other processes throughout process development and quality and security audits. ISMS internal security audits, process development and management review are done according to quality and development process.

Process description of quality and development process defines project manager as an example of a process owner. As a quality-oriented support process, it defines roles, responsibilities, and procedures for internal quality and security auditing. The main purpose of audits is to observe and handle possible deviations, and to find out how effectively security and quality fulfills the defined objectives. From the information security point of view, finding possible security weakness from audit objectives and an opportunity to develop security are important goals.

According to quality system's process interaction matrix, interrelation between quality and development and projects and deliveries processes exists by means of AQAP (Allied Quality Assurance Publication) instructions, internal audits, and process development.

4.1.5 Risk management

According to target organization´s quality system, the goal of the organization's risk management process is to support the achievement of the company's strategic and operational goals by protecting the company against loss, uncertainty, and lost opportunity. Objective of this process is to make sure that quality management and information security management can achieve desired targets.

The risk management process defines procedures for identifying, assessing and response planning of risks. It also specifies the ways to communicate the status of the risk. Risks related to business environment and stakeholders are documented in risk registers according to this process.

From the customer delivery projects and related information security and privacy risk management's point of view, this supporting process is in an important role. Concrete information security tasks concentrate on the organization's risk registries which are defined in the risk management strategy. Risk registries are managed on several levels of organization and business areas. Hence the focus of this development work is on information security risks and for that reason the information security risk register and project risk register were picked to the context of this study. Their definition and related roles are defined in the risk management process description. The information security risk register is owned by the CISO. The risk register is reviewed annually and when changes are noticed by information security interest group. Complete implementation of the project risk register is required in majority of projects. Project manager is responsible for maintaining project's risk register and communicating project risks within project management team.

According to quality system's process interaction matrix, interrelation between risk management and projects and deliveries processes exists by means of risk management procedures and guidance for risk actions and risk register template.

4.2 ISMS and survey on its utilization in customer delivery projects

The core process of the information security management is assessing and addressing information security risks in the organization. Additionally, information security management must be defined

from the viewpoints of leadership, support, operations, performance evaluations and improvement. According to ISO27001:2013 standard all of this is included in the organization's ISMS and it applies to all employees and subcontractors. This analysis of the current situation begins from the ISMS and its role and content in general and from the information security awareness and customer delivery project's perspective.

To get the best understanding about the status of information security awareness and tasks in customer delivery projects, the information was gathered by interviewing key roles related to information security or initiation and management of customer projects. These roles were: CISO, Quality director, Legal counsel, Project manager and Technical architect. The interviews were conducted in February 2021 in Microsoft Teams meetings. Invitations were sent to 10 persons (representing the named roles).

Totally eight persons attended interviews and all roles were presented. The questionnaire contained 10 unstructured questions which were created in co-operation with CISO by analyzing the current state and related research (see chapter 2.5, "Related research"). Topics of the questionnaire were:

- usability of the information security framework,
- usefulness of the current information security controls,
- overall awareness and level of information security tasks, responsibilities, and results, and
- development needs.

By means of interviews, the need and relevance of this study was justified by its results. The questionnaire is presented in Appendix 1.

4.2.1 ISMS and information security awareness maintenance

The security and privacy is support process which is responsible of information security tasks organization widely. The means of implementing, maintaining, and continually improving the information security are defined in the Information Security Management System (ISMS). It is based on the organization's information security policy and it defines also processes of assessing and addressing information security risks. ISMS complies with the international ISO/IEC 27001:2013

standard. The ISMS is continually maintained and at minimum annually reviewed by top management. The Chief Information Security Officer (CISO) in collaboration with the Information Security Group and process owners are responsible for maintaining ISMS.

As defined in the information security policy, securing business continuity is the key objective of the information security system. Defined information security objectives are in align with security policies. In addition to risk mitigation and incident monitoring, information security awareness and competence are the key objectives. ISMS includes concrete actions how information security awareness of employees is maintained:

- New employees receive introduction, both general and more specific according to their duties. An identified development need is a role-based training.
- Each employee attends a mandatory information security introduction and quiz which offers an introduction to the ISMS (updated yearly).
- Updates to the information security policy and other significant documents shall be communicated to personnel as soon as possible after updates.
- The primary media for communication are the intranet and all-company Teams.

ISMS is audited yearly by conducting both internal and external information security audits. The objective is to determine whether the impact of ISMS is sufficient and to list needed development tasks. Improvement and development needs are actively steered by information security measurements, internal audit results, identified risks and general information security status actively followed by information security group.

Organization's ISMS defines an information security framework and a top-level process with needed roles and responsibilities. "Project management", "project manager" or "project" related roles, tasks and responsibilities are not defined in the process. Though, the responsibility to report on security incident is defined both in project and employee level.

4.2.2 Information security and data privacy in projects

The objective of this study is to develop means how to drive and embed information security into customer delivery projects not only in format of customer requirements but also by utilizing organization's processes and policies. To get to know the role of information security in customer delivery projects in practice, information was gathered by interviewing employees who are responsible of information security, quality and processes, project management and project delivery. The questions (see Appendix 1) were oriented to investigate how the security and privacy aspects are involved in the project work and translated into customer value. If no security tasks were notified, the reason for that was asked. The application and possible impacts of organization's ISMS were also the subject of the interview.

The results of information gathering related to current tasks and procedures are represented in the following tables. Answers given by the interviewees are connected to roles to clarify the practical use or need. Only roles that gave answers are represented in tables.

The aim of the first question was to get a big picture how organization's ISMS is in use in customer delivery projects. The primary interest was to find out if also other parts than the security checklist are utilized from the ISMS. The summary of answers is represented in the following table (Table 3).

Table 3. The role of ISMS in customer delivery projects.

Q1	**How is organization's ISMS connected to and applied in customer delivery projects?**
1.1	Security and Privacy checklist must be filled by the project manager.
1.2	ISMS is part of quality assurance system. Its status is audited and evaluated twice a year.
1.3	Awareness of Security and Privacy Checklist has been a deviation in the auditing report during past years. However, renewal of the task list has improved the situation.
1.4	Not specifically, mainly in the project auditing phase (Security and Privacy checklist).

Q1	How is organization's ISMS connected to and applied in customer delivery projects?
1.5	The source of information security requirements are customers (Act on Information Management and Katakri). Technical architects are responsible of implementing those requirements in project. Information security auditing is done by third party.

The topic in the second question was "information security tasks" and what is their role in projects. It was not clear what these tasks are, and examples were needed. As a result, the answers refer to existing checklist or tasks generated from the customer's information security requirements. So, no additional project management related information security tasks were not identified (see Table 4).

Table 4. Information security tasks included in the projects.

Q2	Are the information security tasks part of the project and how?
2.1	Security and Privacy checklist should be filled in the beginning of the project.
2.2	Typically, by technical architects and customer requirements (for example, code auditing). Information security tasks have impact on system architecture.
2.3	Information security requirements by the customer.
2.4	Product development unit is responsible of implementing security tasks.

Information classification and data privacy is another category in the security and privacy checklist. Proper handling of project data requires classification but no project data classification types were mentioned. According to Smith (2019) example of types could be company data (for example, intellectual property files, system architect diagrams) and customer data (personally identifiable

information). According to given answers (see Table 5), it is obvious that data privacy is the most familiar and actively managed area of information security in project management level.

Table 5. Data privacy as part of project's tasks.

Q3	**How is the data privacy managed in customer delivery projects?**
3.1	Project members are aware of GDPR and requirements of personal data handling
3.2	Data privacy is one of the topics in information security and data privacy task list. The status of these questions is evaluated in project auditing. In addition, projects should notice requirements that origin from project agreement.
3.3	According to non-disclosure agreement and customer requirements, security clearances.
3.4	Data anonymization and audit log requirements in systems.
3.5	Changes in project organization are reported without delay and needed actions are done (for example, user id is passivated/deleted).
3.6	GDPR requirements are part of project's requirement management

Information security methods were understood as tools and procedures used in projects. These origin from the organization's quality process, customer agreements and requirements, and aim is to ensure secure management and distribution of information. Answers are represented in the following table (Table 6).

Table 6. Information security used in project.

Q4	**What information security methods are used in project?**
4.1	Aligned with customer requirements (usually Katakri).

Q4	What information security methods are used in project?
4.2	Project documentation is managed and communicated only in agreed systems according to the content and its classification (for example: Mattermost, Skype, Microsoft Teams).
4.3	Access to project documentation and communication channels is provided only to authorized users (project members).
4.4	Communication channels according to classification of information. Confidential information is sent via secure channels.

Risk management is one of the basic and commonly known tasks of project management. One important aspect of risk assessments is, that the definition of security is aligned between the organization and the customer (Smith, 2019).

However, when risks related to security management were in question, they were not seen as common ones. If the information security threats are not actively assessed, the related risks are not usually involved in the risk registry. Information security risk registry of ISMS was also not mentioned as part of threat or risk management. In practice, the risk registry created and managed by the projects can inherit risks from the organization's information security risks as needed. On the other hand, all identified information security risks must be informed to information security group (see Table 7).

Table 7. Risk management and information security threats.

Q5	Is the information security threats assessment part of project's risk management?
5.1	Risks are managed in project's risk registry.
5.2	Information security threats are not evaluated on project level. When evaluated, they are not put into the risk registry.

Q5	Is the information security threats assessment part of project's risk management?
5.3	Threats are identified according to the security requirements (for example, when implementing eService solution). Threats are evaluated by the customer.

Developing the role and significance of information security in project work requires adequate level of awareness among project group and its stakeholders. The question how the information security awareness is ensured showed that projects rely on training and support provided by the organization (see Table 8). Also, the role of hand-over from sales to project was mentioned. Especially the security awareness related to customer's security needs and requirements should be gathered in the sales phase and further transformed to the project. That would give the security requirement baseline for the project already in the beginning.

Table 8. Information security awareness in project.

Q6	How is the information security awareness ensured in project?
6.1	Project members are familiar with internal information security training.
6.2	During the hand-over from sales to project, the project manager is informed information security requirements notified in sales phase.
6.3	Internal information security training must be passed. Information security responsible evaluates related requirements and their impact on project work.
6.4	A threat analysis related to project's scope was facilitated by CISO when the project started.
6.5	Awareness has been built according to customer requirements/project scope.
6.6	Training/workshop by CISO when the project started.

One of the main objectives of this research is to design and suggest how the information security landscape of customer delivery projects could be developed. Nowadays the subject of information security is condensed from the ISMS's viewpoint in a very limited area: project managers are obligated to fill in the security and privacy checklist. The main issues with the current checklist are unknown existence and poor discoverability. To be able to involve information security more actively in projects, it should be included in project management tools and tasks. As inventing new tools is not a good choice in this case, the current tools were listed, and they are candidates in further development plans. Answers are represented in the following table (Table 9).

Table 9. Systems and tools used in project management.

Q7 **Q8**	**How are the requirements managed in projects?** **What systems or tools are used in project management?**
8.1	Microsoft Sure Step (software process model), Prince 2 (framework, management model)
8.2	Project management plan template, chapter 7: Information security management
8.3	Challenge is to inform about the process and template updates effectively.
8.4	Azure DevOps (customer requirements, releases, sprints), Jira (continued services), MS Project (project schedule), MS Teams, MS Excel

4.3 Summary and analysis of the current state

The organization's operational environment has been audited and certifications cover the operational processes. Acquired certifications prove that organization is managed in compliance with the requirements of the standards. The information management system (ISMS) defines the means of maintaining and continually improving the management system in addition to identifying and assessing information security risks. This is an excellent baseline for further development also in the light of research by al. (2013, 1190-1196) who state that compliance with security standards

ensures that the organizations' information is secured professionally and aids in mitigating project failure chances.

Information security requirements set by the stakeholders are usually based on national and international standards, criteria, and policies. In case of customer delivery projects, the most referenced requirements are, for example, VAHTI-requirements, Katakri- and Pitukri-requirements, SÄHKE2-requirements, and personal data processing agreements in addition to ISO 9001, ISO 13485, and ISO 27001 certificate requirements. These results are consistent with related theory that information security requirements are often stated on high-level (for example, just naming the standard), named standards are not necessarily meant for system requirements as such and they are not customized to suit the subject-matter.

All responses to the questions related to projects' information security status and tasks clarified that the role of information security and privacy is undoubtably important in customer delivery projects. On organization level, information security procedures are certified and maintained accordingly. Hence, it is obvious that information security and privacy procedures and practices are not as uniform as they could be between units and projects. The need is to clarify and inform employees more actively about the information security tasks, especially customer project related ones.

According to the survey results, the utilization rate of ISMS in customer delivery projects is low when measured by filled security and privacy checklist. It does not mean, that information security is not notified in projects. It indicates that the ISMS connection point in projects should be implemented in a different way and format. The control objective A.6.1.5 of ISO/IEC 27001:2013 ("Information security shall be addressed in project management, regardless of the type of the project") needs a control which enables more coherent process and tasks which connect ISMS to the project management.

Focus on a customer delivery project is on customer and customer requirements. The role of information security requirements is getting bigger as technical infrastructures complicate, digitalization needs expand, and cyber security threats must be mitigated. When information security requirements are usually defined as non-functional and technical requirements, they are assigned to

technical architects. The results of the survey show, that information security and privacy tasks are most often handled as technical requirements. When information security is seen mainly as a technical issue, it is not part of the process. According to research results on appliance of 27001, security is usually forgotten in projects and information security is seen as a product (Segovia 2015).

Project manager's role is in central also in case of information security requirements. In addition to customer requirements, the project must follow and fill in the requirements set by the quality system. The momentums of assessment are the closing and the auditing of the project. The price of a success can be high especially in projects where the work mode is more reactive than proactive. During the information gathering the initiation of the project was identified as an important phase for analyzing and acquiring the needed information security awareness and competence. For example, when the project is transferred from sales to project mode, sales should notice information security requirements that origin from project agreement.

When evaluating the status of ISMS utilization in projects, the situation is divided especially from the viewpoint of concrete tools and requirements. The organization's support processes define that the mechanism for information security and privacy assurance is in format of a checklist which is part of project auditing. In addition, the risk registry is expected to be used. On the other hand, customer delivery projects are more oriented to information security requirements that are set by the customer. So, the question for further development is, how the ISMS and related processes would better support and fortify information security in customer delivery projects?

4.4 Development and implementation plan

Management of information security and privacy are often seen as technical tasks. Instead of only programming secure code and implementing secure applications, information security is a topic that is related to all processes of an organization because information owned by organization, organization's partners and customers is the main asset to be protected.

The development and implementation phases of this work is presented in this chapter. After the exploring and analysis of the organization's current state, development plan was created based on

identified and prioritized development ideas. Finally, planned tasks were implemented and demonstrated that the outcomes are aligned with research questions and targets.

4.4.1 Development ideas and needs

The results of the interviews showed that commitment to customer requirements and high quality in customer deliveries are the key objectives for all attendees. The purpose and overall goals of the customer delivery projects are based on a mission to deliver solutions and services with accuracy, quality, and in cost-effective way.

Information gathering questionnaire contained also questions about development needs and ideas - what kind of information security procedures and tasks should be included in customer delivery projects. Questions covered to aspects: information security tasks in customer delivery project and tools supporting management of these tasks. Aligned with the context and subject of this study, questions were planned to gather improvement areas and topics on security and privacy tasks which are executed during project and delivery processes, not technology-oriented or existing and implemented IT system related development needs. The questions of development needs and related answers are presented in the following tables (Table 10 and Table 11).

When asked about the future needs and development ideas related to information security and data privacy, the answers were very practice oriented and sharing a common concern about adequate competence and resources related to information security and privacy. It was said that these needs arise especially in projects where the customer requirements are oversized compared to the scope of the delivery or including management of classified information. When asked about the definition of “oversized requirements”, the interviewees explained that those are requirements which are either on too high level (for example, just naming a standard or a framework) or unanalyzed and unclear (does not match to or clarify the need and how it is related to target state).

Projects are managing risks based on identified threats related to, for example, schedule and resourcing. Traditionally the risks are related to project management aspects more than technology or solution-oriented issues. Development needs for information security and privacy risk management were identified in two main areas:

- Identification of information security threats and including possible risks in project's risk registry.
- Tasks, roles, and responsibilities for identifying information security risks and requirements.

Identification and management of information security and data privacy risks is an ongoing process during the project's lifecycle. However, the information security threats are not a regular topic in risk identification phase unless there are already some security or data privacy related risks identified. Also, requirements that contain high demands for technical infrastructure or solution design may cause threat candidates which may end up in the risk registry.

Nowadays the management of information security and data privacy requirements is not a separate process, but it is one subject area of the entire set of customer requirements. Requirement management and their fulfillment is the key process during the project's lifecycle. According to the results of interviews, the identification phase should be started before the project is initiated. This means, that the hand-over from sales to project should include information security requirements as a standard theme. In practice, as the customer's information security requirements are identified and evaluated during the agreement phase of the project, they should be included in the hand-over phase and be clarified to project manager or project team. In the best-case scenario, a documentation how those requirements are met would be also present.

Currently project's the information security and data privacy tasks are being concretized as a checklist. As supposed, the development needs were mostly oriented on ideas for renewing it or including its content and targets in project and delivery process in a totally new format. The content of the checklist has been updated recently. It contains approximately 30 questions in a structured format (answer options: yes/no/customer/not applicable). Improvement should be done more to the way of expression than to the content. Common opinion among survey attendees was that these questions and tasks are up-to-date and relevant, but their location should be renewed and more substance guidance for filling them is needed.

Cyber and information security awareness of the project team members should be a standard topic in project's agenda according to development needs. The practices and ways of security

training have varied during the times and among projects. Security awareness is a topic that composes of knowledge from several areas (“civic skills”, organization’s security policies and project’s security scope) and appears in individual level. Despite of the fact that security training is not usually in the responsibility of project, it was mentioned as a development need at least from the security related requirements point of view.

The summary of these development needs and ideas related to information security tasks in customer delivery projects is presented in the following table (Table 10).

Table 10. Development ideas related to information security and privacy in projects.

Q9	**What kind of development ideas related to security and privacy task list or information security management there are in customer delivery projects?**
9.1	Information security threats should be assessed and included in the risk registry when risks are identified.
9.2	Customer’s information security requirements should be clarified to project team and needed documentation should be provided how those requirements are met. Development ideas to customer requirements would be a plus.
9.3	Security and privacy checklist should be part of the process, not a separate checklist.
9.4	Security and privacy checklist should be part of sales phase.
9.5	Hand-over from sales to project should include information security requirements as a standard theme.
9.6	Data privacy and GDPR related requirements should be part of project’s requirements and risks from the beginning.
9.7	Information security requirements should be covered in the beginning of the project: what is the scope, inform internal steering group, identifying possible risks and challenges.

Q9	What kind of development ideas related to security and privacy task list or information security management there are in customer delivery projects?
9.8	More guidance and examples are needed.
9.9	Should be useful and supporting, not loosely coupled and extra weight.
9.10	Information security should be a standard topic in the agenda of team meetings, not only in projects.

Tools and systems used in project management and implementation tasks were of interest because one key target for the information security tasks' development is to merge them not only with existing processes but also with used tools. The organization's list of official and supported tools contains several kinds of systems, but the focus of this work was on process and requirement management supporting tools. The results of the survey pointed out that the decision about the supporting tools cannot be made purely in the project. To ensure efficient possible work process in the project, also the tools used by the customer must be considered. This is especially the need in the test phase when there is a need to transfer data between internal systems and customer's systems.

Another requirement for the future tool was a support for monitoring the status of information security tasks. This reporting type of feature would not only serve auditing needs but also support project manager's work. Currently the unit of measurement is the project managers' awareness of the security and privacy checklist. Information security or privacy is not the easiest thing to measure or report in project auditing. Although the impacts can be significant. Information security is one of the support elements which is not noticed until it is broken.

The summary of these development needs and ideas related to tools supporting management of information security tasks is presented in the following table (Table 11).

Table 11. Ideas about supporting tools or systems related to information security tasks.

Q10	What kind of tools or systems are suggested for supporting information security tasks?
10.1	Security and privacy tasks should be integrated into project work.
10.2	Tools should support monitoring the status of information security tasks. Not only for auditing. Dashboard, summary, or status etc. data visualization tool should be available.
10.3	A template for information security and data projection tasks.
10.4	Information security requirements should be evaluated more realistically as part of project work according to the project size.
10.5	More information security resources are needed to support project work.

Several development ideas and needs were identified as a result of information gathering phase. All of them share a common target of being part of existing processes and providing needed support and competence. For acting in a supportive role, the tools and processes used for project work are not always seen as part of the group of critical assets. Hence, information management and communication within the project team are examples of information security components. They are used on organization's internal network and platforms and thought to be private but not necessarily seen valuable to attackers for possible social engineering attacks. This is an example of a threat scenario where "the Achille's heel of cybersecurity is you".

Before creating the development plan, the development needs and ideas were grouped and prioritized. The grouping was done based on items' theme and related project phase.

Table 12. Grouped and prioritized development tasks.

ID	Development theme and tasks
1	Information security and data privacy: Risk management 9.1: Information security threats should be assessed and included in the risk registry when risks are identified. 9.6: Data privacy and GDPR related requirements should be part of project's requirements and risks from the beginning.
2	Information security and data privacy: Requirement management 9.2: Customer's information security requirements should be clarified to project team and needed documentation should be provided how those requirements are met. Development ideas to customer requirements would be a plus. 9.5: Hand-over from sales to project should include information security requirements as a standard theme. 9.6: Data privacy and GDPR related requirements should be part of project's requirements and risks from the beginning. 9.7: Information security requirements should be covered in the beginning of the project: what is the scope, inform internal steering group, identifying possible risks and challenges. 10.4: Information security requirements should be evaluated more realistically as part of project work according to the project size.
3	Information security and data privacy: Information security tasks as part of project management process 9.2: Security and privacy checklist should be part of the process, not a separate checklist. 9.3: Security and privacy checklist should be part of sales phase. 9.9: Should be useful and supporting, not loosely coupled and extra weight.

ID	Development theme and tasks
4	Information security and data privacy: Awareness and support 9.8: More guidance and examples are needed (related to information security and data privacy risks, requirements, and tasks). 9.10: Information security should be a standard topic in the agenda of team meetings, not only in projects. 10.1: Security and privacy tasks should be integrated into project work. 10.2: Tools should support monitoring the status of information security tasks. Not only for auditing. Dashboard, summary or status etc. data visualization tool should be available. 10.3: A template for information security and data projection tasks. 10.5: More information security resources are needed to support project work.

The four development themes presented in Table 12 define the structure of the development plan. In the next phase of this work process, the development plan was created, and development tasks were designed in a detailed level.

In the information gathering phase, tools and software utilized in project management tasks were identified. Those tools were further evaluated in the development planning phase. The aim was to address development efforts into current processes and tools so that information security and data privacy tasks are not a separately managed. In addition to Microsoft Office 365 tools, Azure DevOps and Jira were candidates for supporting tools related to projects' information security task.

4.4.2 Development plan

This study work continued with a planning phase. Status and concerns related to information security and data privacy tasks were systematically identified and analyzed along with the development needs. The results of previous phases provided information to continue exploring solutions to the research questions.

Identified development tasks presented in Table 12, formed the core of the development plan of this work. In addition, common development requirements were formed on the base of current state analysis. These requirements are:

- The development work and its outcomes must be aligned and compatible with organization's quality system.
- The aim is to utilize existing processes and tools, instead of inventing new solutions or creating silos.
- The implemented framework must be suitable for use in different customer projects (regardless of the project outputs).
- The outcomes of the development work must be transparent, traceable, documented and supporting project work during its lifecycle.
- The framework must appropriately be extended to other processes and entities related to the management of project's information security tasks.

These requirements are referring to a "framework". As Sangi et al. (2017, 219-220) recommend, in large and complicated IT projects and implementation of security tasks a framework or a model should be used. It ensures that all information security aspects are covered. So, this planning phase started with designing a proposed framework used as a basis for the development. The first piece and selected approach of the framework was organization's project management method, PRINCE2. The designed framework is presented in the following figure (Figure 11).

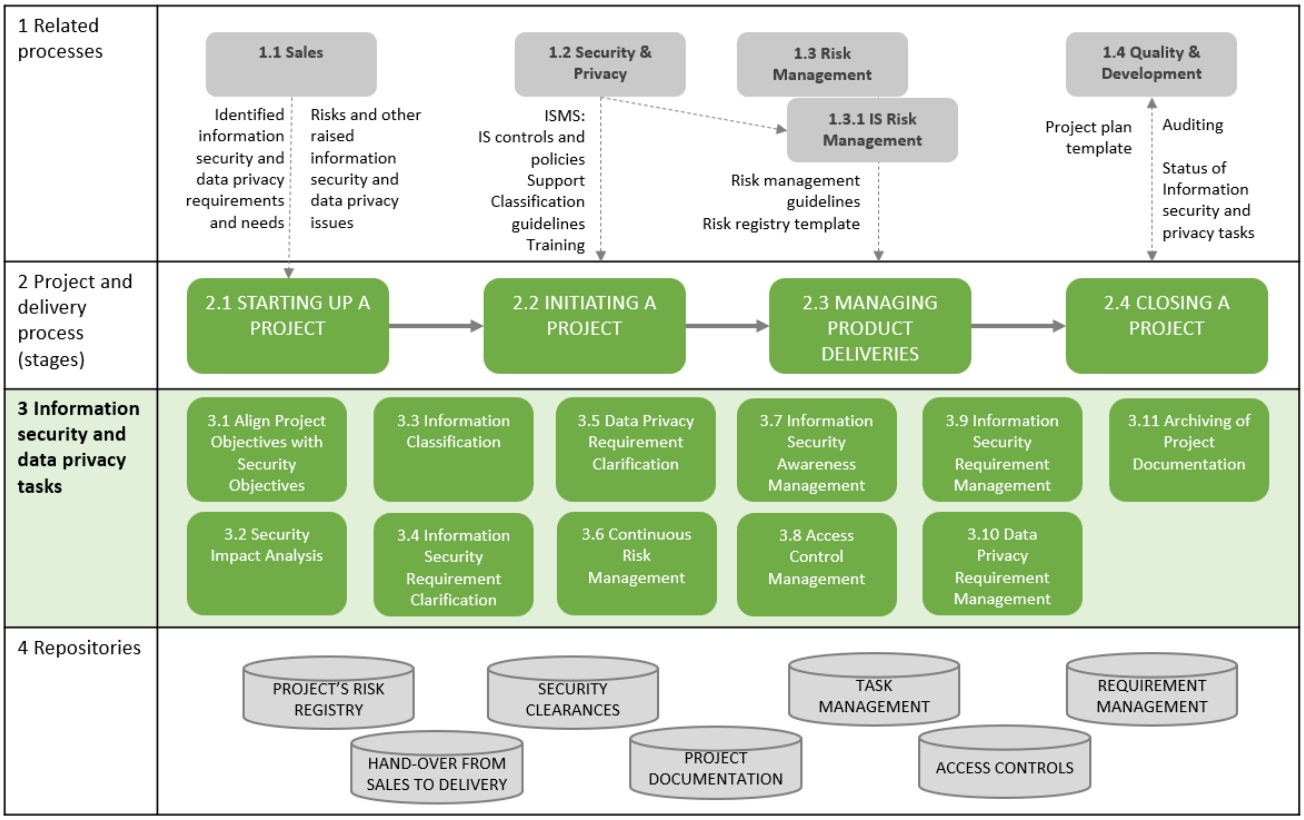

Figure 11. The framework of information security and data privacy tasks in customer delivery projects.

In addition to project's information security and data privacy tasks, related processes, phases, and knowledge pools are presented in the framework. These areas are depicted in four layers which are:

1. related processes,
2. project and delivery process,
3. information security and data privacy tasks and
4. repositories

The first layer, Related processes, contains all processes that were identified as related processes to project and delivery process. The relation is relevant especially from the information security and data privacy viewpoint. These processes can provide input information to project and delivery process, or they can receive information as an output of project and delivery process. The main

information flows are presented in the Figure 11. Information flow, which is connected to the process level and not to a specific task, means that information is utilized as a reference during the lifespan of the project.

The main phases of project and delivery process is presented in the second layer. These phases are applied from the main stages of PRINCE2. In this framework, the upper-level phases were evaluated as adequate. The main idea was to connect project's information security tasks to project's phases in high-level.

The core contribution of this work is defined on the third level of the framework: Information security and data privacy tasks. These tasks were designed as a result of information gathering phase. Total of 11 tasks were defined based on the development needs and ideas which were identified in surveys. Descriptions, related roles, processes, and project's phases, needed input information, related repositories and outcomes of the tasks are presented in more detailed level in this chapter. After a short user story or definition of the task, a summary of task is presented in a table format.

TASK 3.1: Align project objectives with security objectives

Information security objectives and requirements are evaluated in the sales phase when drafting the tender and designing the coming project. Usually, customer has specified certain information security needs and expectations in call for tender. For example, a security clearance may be required for all project members. Those should be identified and aligned with project objectives during sales phase and formulated as input information to the project. These information security and data privacy needs are included in project plan and informed project in hand-over from sales to delivery.

TASK 3.1	**Align project objectives with security objectives**
Description	Creating a project plan where project's objectives are aligned with security objectives. Other notable information security or data privacy needs are documented and handed over to project manager.

TASK 3.1	Align project objectives with security objectives
Roles	Sales team
Related processes	Sales, Security & Privacy, Risk management
Input	Call for tender, Tender
Project's phase	Starting up a project
Outcomes	Project plan is transferred to project as a baseline. Project manager is informed about identified information security and data privacy policy or process requirements provided by the customer. If related risks identified, the first version of project's risk registry is created.
Repositories	Hand-over from sales to delivery, Project documentation (Project plan and requirements), Project's risk registry

TASK 3.2: Security impact analysis

Information security and data privacy targets for project's delivery are specified as part of non-functional requirements by the customer. In addition, a call for tender can state requirements which should be noticed at administrative level of the project. In other words, these requirements may not be part of requirement management process, but they should be identified as project level requirements. Usually, these kinds of requirements relate to security principles and procedures applied in project work or security awareness of project members.

TASK 3.2	Security impact analysis
Description	Analysis of security requirements and security impact on cost and benefit of the project. This analysis is done in starting phase (hand-over from sales to project) and during delivery phase, after approval of requirements (gap analysis).

TASK 3.2	Security impact analysis
Roles	Sales team
Related processes	Sales, Security & Privacy
Input	Call for tender, Tender
Project's phases	Starting up a project
Outcomes	Project gets an analysis of security requirements impacts which should be noticed, for example need for auditing, required information security of data privacy skills, specific requirements for handling of personal data.
Repositories	Hand-over from sales to delivery, Project documentation (requirements), Project's risk registry

Task 3.3: Information classification

Project documentation is one of the main assets to be protected in a customer delivery project. A critical part of information protection is the proper classification of documentation throughout the lifespan of the information. In case of a project, the lifespan of information is longer than the project's timeline. Information is created, stored, copied, handled, transferred, archived, and eventually destroyed according to the information type and related retention rules.

Task 3.3	Information classification
Description	Project documentation is classified according to guidelines defined in the ISMS. Access rules are defined according to project's security requirements and information classification.
Roles	Sales team, Project manager
Related processes	Sales, Security & Privacy

Task 3.3	Information classification
Input	Call for tender, Tender
Project's phases	Starting up a project, Managing product deliveries
Outcomes	Project documentation is classified and managed accordingly.
Repositories	Project documentation

3.4 Information security requirement clarification

Functional and non-functional requirements are the core specification which steers the work of customer delivery project. They are received from the customer in tendering phase. Requirements are in a key role of successful IT project. When requirements are defined properly and they state what is needed (not how), the implementation in project work is straight-forward. Unfortunately, the complete definition of targeted universe precisely is seldomly possible in form of requirements.

From the customer delivery project's viewpoint, it is crucial that information security requirements are identified and analyzed before starting the project. In fact, they are evaluated in tendering phase and the impact on planned project work is estimated. In addition to formal requirement specification, also other documentation included in received tender, can contain information security constraints which are valuable information for the delivery project. In this requirement clarification task, information security requirements are identified to give needed information to the project in hand-over phase. Identification is most important in cases when the customer has not categorized information security requirements in delivered specification.

Task 3.4	Information security requirement clarification
Description	Information security requirements are identified in the sales phase (if not categorized by the customer). They are as input information to project and delivery process and managed in the project according to requirement management process.
Roles	Sales team, Project manager
Related processes	Sales, Security & Privacy
Input	Call for tender, Tender
Project's phase	Starting up a project
Outcomes	Information security requirements are identified from the requirement specification and other documentation included in tender. Project manager receives information on requirements in an overall level and in detailed (requirement) level. The impact on project's management tasks is evaluated by project manager. For example, training needs, new risks arisen from requirements. Requirement specification is imported into requirement management system in starting phase of project. Then analyzed, designed, and implemented during the project work. Technical environment is designed and ordered according to information security requirements.
Repositories	Project's risk registry, Project documentation, Requirement management

TASK 3.5: Data privacy requirement clarification

Data privacy requirements are received from the customer in tendering phase. Like information security requirements, it is crucial that data privacy requirements are identified and analyzed be-

fore starting the project. Data privacy type of requirements can be embedded also in other documentation included in received tender. In this requirement clarification task, data privacy requirements are identified to give needed information to the project in hand-over phase. Identification is most important in cases when the customer has not categorized data privacy requirements in delivered specification.

TASK 3.5	**Data privacy requirement clarification**
Description	Data privacy requirements are identified in the sales phase (if not categorized by the customer). They are input information to project and delivery process and managed in the project according to requirement management process.
Roles	Sales team, Project manager
Related processes	Sales
Input	Request for offer
Project's phases	Starting up a project, Managing product deliveries
Outcomes	Data privacy requirements are identified from the requirement specification and other documentation included in tender. Project manager receives information on requirements in an overall level and in detailed (requirement) level. The impact on project's management tasks is evaluated by project manager. For example, training needs, new risks arisen from requirements. Requirement specification is imported into requirement management system in starting phase of project. Then analyzed, designed, and implemented during the project work.
Repositories	Project's risk registry, Project documentation, Requirement management

TASK 3.6: Continuous risk management

As requirement management, risk management is one of the key tasks of project management. However, more focus should be put on identifying information security and data privacy related risks in starting phase of a project. Continuous risk management was named in this study as one of the customer delivery project's information security tasks because information security and data privacy related risks must be identified as early as sales phase but at the latest in project's starting phase. In an optimal case, the first version of project's risk registry is created already in sales phase containing risks which have been observed during the analysis of documentation received in call for tender.

TASK 3.6	**Continuous risk management**
Description	Information security and data privacy risks identified in sales phase and project's risk registry is created. These risks are analyzed, and they are input information for the project in hand-over phase. Risk management is a continuous process until closing the project.
Roles	Sales team, Project manager
Related processes	Sales, Security & Privacy, Risk management
Input	Identified and analyzed information security and data privacy risks, Project's risk registry (first version)
Project's phases	Starting up a project, Initiating a project, Managing product deliveries, Closing a project
Outcomes	Risks are registered and managed in project's risk registry.
Repositories	Project's risk registry

TASK 3.7: Information security awareness management

Level of information security and data privacy skills varies among project members mainly because of their different roles and required skills. The more technically oriented person, the more information security skills is expected as information security tasks are usually categorized as purely technical tasks. However, in this study the focus is more on administrative information security tasks and awareness. The aim is, that the required minimum level of information security skills is achieved when organization's training is passed and updated when new trainings are available. Other training needs are planned and organized by project manager with the help of CISO. Additional training needs can arise from customer requirements related to, for example, handling of personal data.

TASK 3.7	**Information security awareness management**
Description	Information security and data privacy training is provided company wide. All project members have attended the training. Training is done according to organization's training schedule. If additional information security or data privacy awareness or skills have been required in project's scope, that training is organized by project manager with the help of CISO.
Roles	Sales team, Project manager
Related processes	Sales, Security & Privacy
Input	Organization's information security training
Project's phases	Initiating a project, Managing product deliveries
Outcomes	Project manager informs project members in project's kick off about required training level. Passed organization's information security training of each project member is updated in project's documentation.
Repositories	Project documentation

TASK 3.8: Access control management

Several different types of information systems are utilized during project's lifespan. Project's documentation is often managed in a system or service platform which offers tools for both information and communication management. Usually, these services are created for both internal and external use. More technical and architecture-oriented systems are used in system or product development in several environments. As size of project's system selection arises, the complexity of granted access rights arises. Project manager is responsible to track changes in project team and access rights accordingly. Access to systems must be defined as required by the role and responsibilities of project member.

TASK 3.8	**Access control management**
Description	Access to project's documentation and used systems (collaboration, development environment, customer environment) is granted according to classification of information and project's members' roles.
Roles	Sales team, Project manager
Related processes	Sales, Security & Privacy
Input	Classification and handling of information policies and instruction
Project's phases	Starting up a project, Initiating a project, Managing product deliveries
Outcomes	Access rights are managed in project's documentation. If security clearance is needed, accesses are granted according to the status of them (active member = access rights granted, passive member = no access rights).
Repositories	Security clearances (when required), Access controls, Task management

TASK 3.9: Information security requirement management

Requirement specification is imported into requirement management system in starting phase of project. At this point, all information security requirements have been categorized by the customer and sales team. If any critical or risky ones have been identified, they are tagged. That indicates requirements which must be prioritized, analyzed and actions designed in the early phase of project work. Prioritized information security requirements are usually topics which may require special skills, technical solutions, or larger amount of planning and implementation time.

TASK 3.9	**Information security requirement management**
Description	Information security requirements are imported and managed in the requirements management system. They are tagged, categorized, and prioritized accordingly. Extra attention is paid to top prioritized ones.
Roles	Project manager, CISO, Project team
Related processes	Security & Privacy
Input	Information security requirements
Project's phases	Starting up a project, Initiating a project, Managing product deliveries, Closing a project
Outcomes	Project's information security requirements are assigned to responsible project members. Requirements are managed according to common requirements management process.
Repositories	Requirement management

TASK 3.10: Data privacy requirement management

Requirement specification is imported into requirement management system in starting phase of project. At this point, all data privacy requirements have been categorized by the customer and

sales team. If any critical or risky ones have been identified, they are tagged. That indicates requirements which must be prioritized, analyzed and actions designed in the early phase of project work. Prioritized data privacy requirements are usually topics which may require special skills, technical solutions, or larger amount of planning and implementation time.

TASK 3.10	**Data privacy requirement management**
Description	Data privacy requirements are imported and managed in the requirements management system. They are tagged, categorized, and prioritized accordingly. Extra attention is paid to top prioritized ones.
Roles	Project manager, DPO, Project team
Related processes	Security & Privacy
Input	Information security requirements
Project's phases	Starting up a project, Initiating a project, Managing product deliveries, Closing a project
Outcomes	Project's data privacy requirements are assigned to responsible project members. Requirements are managed according to common requirements management process.
Repositories	Requirement management

TASK 3.11: Archiving of project documentation

As in any other information management process, the lifecycle of project's documentation is planned and managed accordingly. When project is in the closing phase, all it's documentation should be archived, access rights to systems updated accordingly and systems used only during project's lifespan passivated so that no accidental altering of documentation is possible.

TASK 3.11	Archiving of project documentation
Description	After the project is closed, project's documentation is archived according to classification, data privacy, and retention requirements. Access to project's archive is granted accordingly.
Roles	Project manager
Related processes	Security & Privacy, Quality & Development
Input	Retention rules for project documentation
Project's phases	Closing a project
Outcomes	Project is closed, and project's documentation is archived and accessible to appropriate persons.
Repositories	Project documentation, Access controls

Fourth level of the framework presents knowledge pools or repositories which are used by information security and data privacy tasks in the project and delivery process:

- Project's risk registry: A registry which is maintained by the project. Information security risks are registered and managed according to common risk management process (support process).
- Hand-over from sales to delivery: Information which is transferred from sales to customer delivery project by the sales responsible. Project manager is receiving the information in form of project's risk registry (first version), project's profile information (customer, contact information, etc.) and other documentation (for example, presentation).
- Security clearances: When security clearances are required, their status (active or passive) is managed in a database.
- Project documentation: Repository (usually document management system, communication, and collaboration platform) where project's documents are stored. The documentation is created during the project's lifespan from sales to closing the project.

- Access controls: The list of project members who are justified for having access rights on project's documentation and other repositories. If security clearances are required, the access controls are aligned with their status (active members have access).
- Task management: A repository where project's information security and data privacy tasks are defined and managed. In this development work, the recommended system is Azure DevOps or Jira.
- Requirement management: A repository where project's requirements are imported, defined, and managed. Each requirement is categorized and tagged with needed parameters related to information security and data privacy requirements specified by the customer. In this development work, the recommended system is Azure DevOps or Jira.

In the implementation phase, the aim was to utilize existing repositories rather than implement new ones.

5 Results and reliability assessment

Implementation of the development plan and results achieved during this study work are presented in this chapter. The journey of this study began as a mission to find ways how to drive information security into customer delivery projects. Although the baseline was good, the results of this study showed that by sharpening selected processes the utilization of organization's ISMS can be boosted radically. These reforms were identified as good progress in translating security aspects into customer value because instead of focusing only on information security requirements, the project ensured its work process aligned with overall expectations on information security and data privacy by the customer. In addition, the framework containing information security controls and tasks developed in this study work is reusable and can be implemented as a project's information security task template. The developed framework is "art nouveau" in the field of project process and information security tasks. As the related research showed, information security is often a substance matter of only system development and even omitted from the project management process. Extending these responsibilities and tasks to surrounding processes (mainly sales and quality) is beyond status quo.

As described in the previous chapter, defined development tasks start from the tender or sales phase and they cover the project's lifespan until closing the project. Considering the schedule and assigned workload of this study work and duration of a typical customer delivery project, not all tasks could be implemented or assessed in a context of one project.

The results and status of implementation is presented in the following table. When "Project's task" is mentioned in the following table, it refers to a project's task list which is created and managed in project's implementation and development tool. In the context of this work, it means Azure DevOps and existing project template which was extended with information security and data privacy tasks. When a project is started and needed parameters are created in DevOps, also a task list is created. According to current plans, this project template will be implemented also in Jira.

The status of each development task is presented with values: planned, work in progress, implemented and done. "Implemented" indicates that task has been implemented during this study.

When a development task is included in organization's processes related to ISMS and quality system, its status is "Done". Implementation on organization level was not in the scope of this study work.

Table 13. The results and status of implementation of information security tasks.

DEVELOPMENT TASK	IMPLEMENTATION, STATUS
3.1 Align project objectives with security objectives	New fields added in the hand-over from sales to delivery repository: Information security requirements, Data privacy requirements Guidance to create and update project's risk registry when information security risks notified during sales phase. Status: Planned
3.2 Security impact analysis	New field added in the hand-over from sales to delivery repository: Security requirements impact on project's scope Guidance to create and update project's risk registry when impacts are notified during sales phase. Status: Planned
3.3 Information classification	Project's task which contains link to classification and handling of information instructions. Status: Implemented
3.4 Information security requirement clarification	New column added in the requirements analysis "template" which is a set of Excel columns added in customer's requirement specification: Information security requirement, applied when customer has not categorized information security requirements Existing "alert tag" (!) used, when a requirement is analyzed as risky one (for example, extra costs, tricky implementation, etc.) Status: Implemented

DEVELOPMENT TASK	IMPLEMENTATION, STATUS
3.5 Data privacy requirement clarification	New column added in the requirements analysis “template” which is a set of Excel columns added in customer’s requirement specification: Data privacy requirement, applied when customer has not categorized data privacy requirements Existing “alert tag” (!) used, when a requirement is analyzed as risky one (for example, extra costs, tricky implementation, etc.) Status: Implemented
3.6 Continuous risk management	Guidance to create and update project’s risk registry when information security risks notified during sales phase. Status: Planned
3.7 Information security awareness management	Project’s task which contains guidance for project manager to evaluate training needs and keep track on passed trainings, link to organization’s information security training. Status: Implemented
3.8 Access control management	Project’s task which contains link to security clearance repository (when needed) or template of project members and their status. Project’s task which contains a template to manage systems used in project and related access right policies. Status: Work in progress
3.9 Information security requirement management	Categorized information security requirements are imported into requirements management system. The category and alert tag (if needed) added in sales phase are applied in requirements analysis and can be used for searching and filtering. Status: Implemented

DEVELOPMENT TASK	IMPLEMENTATION, STATUS
3.10 Data privacy requirement management	Categorized data privacy requirements are imported into requirements management system. The category and alert tag (if needed) added in sales phase are applied in requirements analysis and can be used for searching and filtering. Status: Implemented
3.11 Archiving of project documentation	Project's task which contains guidance how to passivate and archive project's documentation systems and documents. Tasks contains a link to retention rules. Status: Planned

The presented development plan and results define the answer to the main research question *"how to drive information security into customer delivery projects".* The primary target was to embed information security tasks into existing processes and store related information into existing repositories. Because the biggest drawback in the current state was separate information security tasks, the implementation of each development task was started by analyzing a possibility to extend information created or gathered in current processes. In this sense, the answer to the research question is "by embedding information security tasks and supporting tools not only into project and delivery process, but also into preceding sales process".

This study work was formulated also by the four sub research questions which emphasize the role of organization's ISMS and the customer value to be achieved through the project. *The utilization of ISMS* in customer delivery projects is ensured by using it as a guideline for tasks created in this study work and as a reference in project's information security tasks. When the security is being built into customer delivery project during its lifespan, by specified roles and from different perspectives, *the security aspect is translated into customer value* in a best possible manner. *The planned and implemented information security controls* and tasks included in customer delivery projects were based on requirements set by organization's ISMS and quality system. The information needs of the project were also evaluated and implemented as input information from sales

to the project or as project's tasks. At the same time, *the roles and responsibilities* were defined related to these development tasks.

After, and partly during the implementation phase, was the reliability assessment of the results made. Assessment of the outcomes of this study is especially important because of the applied constructive research method. One of its drawbacks is the lack of objectivity. By evaluating the results, valuable information about the usefulness and effectiveness of the implementation was achieved. As the construction was not completed fully, the assessment is mainly in planning status. Lukka (2003, 83-101) has stated about assessment when applying constructive research method "it is always difficult, if not impossible, to assess the practical adequacy of any new construction prior to its implementation ".

The assessment phase was planned to be executed by using appropriate customer delivery projects as a test case. The assessment concentrated mostly on the start and initiation phases of the customer delivery project because the implementation was done mainly related to those project phases. Information security and data privacy tasks in preceding project phases (managing project deliveries and project closing) focus mainly on the continuous risk management. Because development needs were mostly identified to concern the earlier phases of a customer delivery project, the evaluation of the new project and its first phases was agreed to give enough insight about the results achieved in this study.

The templates and tools implemented for project's information security tasks were used as source material in this assessment. Some areas of assessment were prepared to be done by simulating the end results, if needed. For example, the input that project gets from the sales had to be evaluated based on demo or sample data for scheduling reasons. In other words, information that should have been gathered during tender phase, was created in the hand-over phase from sales to project.

Summary of the evaluation process (phases, main tasks, and outcomes) is presented in the following table (Table 14). This process was applied to implemented development tasks which were in status "Done" (see Table 13).

Table 14. Evaluation plan and process of implemented outcomes.

PHASE	TASKS and OUTCOMES
1 Planning	Discussions with the project managers of the projects which will start soon. Agreement on utilizing project as source material in the evaluation. The evaluators are project manager, project team and CISO.
2 Definition of object and criteria	Questions relate to project's information security and privacy tasks: how they are identified, answered, managed and what is their relevance to the project. Questions relate to thesis work and research questions: How well were the objectives and development task achieved? Which of the actions affected reaching the goals most?
3 Gathering information	The author of the thesis will gather evaluation information. The project will gather and manage information that is on its responsibility. Part of that information can be used in reporting evaluation results.
4 Methods	Evaluation will be done mainly by observing and interviewing.
5 Practices	The outcomes of the thesis work will be used in a most practical manner – in a real project. Evaluation is done during the project work.
6 Conclusions	Evaluation results will be categorized, summarized, and conclusions made. Result categories: what worked fine, what needs development, what is useless, tips for further research.
7 Reporting	Results of the evaluation will be reported in the thesis and in the development project report.

PHASE	TASKS and OUTCOMES
8 Utilizing the information	Results of the evaluation will be informed to the project managers. Probably the results will generate development needs and ideas about further research and development.

Tasks implemented during this study work were related to requirement specification and project's tasks. Assessment of these results was done according to the process defined in previous table. A soon-to-be-starting project was selected and agreed to be used as a test case with project manager. The information of information security and data privacy requirements was gathered from project's source material (as the implementation concerning sales and hand-over phase is not done). The requirements were imported into management system and the project's template (tasks) was initiated for the use of project manager. The usage of requirements and project's tasks were observed during the initiation phase of the project. The project manager was interviewed about the usability and usefulness of task list.

New development ideas were gathered as a result of this reliability assessment. First, the usage of project template must be informed and trained to project managers more actively. Secondly, the task list should be provided as a dashboard to project managers because the list is otherwise difficult to find in a system which contains dozens of projects and hundreds of tasks and requirements. These development tasks will be notified in coming development phases.

6 Discussion and conclusions

The purpose of this study was to sharpen and to unify the management of information security and data privacy tasks in the customer delivery projects. The case organization has been awarded several ISO certificates which cover the company's operational processes. On organization level, information security procedures are certified and maintained accordingly. The situation is aligned with the research results of Brunner & al. (2018, 483-490) that larger organizations have already adopted ISMS and operating with it as a part of their processes. The importance of information security and data privacy is also highly valued and actively communicated among organization. From the organization's operational environment's viewpoint, relevant issues for information security are customer's stricter information security requirements, megatrend and growth in cloud services and privacy value, government's changes in laws and regulations and need for information security skills and competition of it. As the research conducted by Goldes et al. (2017, 1-6) showed, state-of-the-art society boosts organizations actively assess and update their ISMS.

Three different research methodologies were applied during this research. The focus was on a real-world problem with an identified need for a solution (a construction), therefore the constructive method was chosen as the main research method. As the construction was done for a case organization, the case study was also applied as a research method. To understand the real-life challenges better, it was decided to gather information by interviewing key roles related to information security or initiation and management of customer projects. Considering the context of this research, the selected methodologies fit well and supported meeting the research objectives.

Framed according to the research question, the aim of this research was to find *how to drive information security into customer delivery projects*. That topic was focused and supported by the sub-questions:

a. How customer delivery projects utilize organization's ISMS?
b. How is the security aspect translated into customer value?
c. What kind of information security controls and tasks should be included in customer delivery projects?

The research found that embedding information security tasks into project process improved their visibility and importance by helping to notify, perform and manage them along other tasks. The current method had separated information security tasks from the project's context and the customer requirements were notified both technical and product related tasks. This result laid the foundation of developed framework. Segovia's (2015) research suggests key information security activities which should be integrated into project management activities to apply ISO/IEC 27001:2013 efficiently. As a result, in order to provide organization's ISMS more closely to project management process (research sub-question a), the main phases of project process formed the pillars of the framework, phases were fined down into tasks and tasks were linked to ISMS.

As Sangi et. al (2017, 219-220) state, IT project cannot be considered as a complete project without IT security included in project management approach. To ensure that the security aspect is translated into customer value, key activities were integrated into project's information security tasks (research sub-question b). These activities are in line with Segovia's (2015) quadrant. Information security objectives were included in project objectives already in the sales phase. The importance of risk assessment's timing and handling of risks was notified, and risk registry is recommended to be created as early as in the sales phase when information security related risks are identified. Finally, the framework and integrated information security tasks are kept essential during the project's lifespan. As a result, information security is always a component of project management in the organization.

In the developed framework, project's security tasks were defined wider than just system security, also aspects of CIA triad was covered (for example, access rights), and security controls defined (research sub-question c). As Emory (2004) states, secure project management is a combination of project management and security needs.

When the idea and need for this study work were created, they corresponded to expectations of the work topics. After diving into case organization's processes with the research questions, came the first moment of doubt: what is left to study or develop if processes are rolling smoothly and there is no information security deviations on the air. However, when analyzing the results of the surveys, the needs for development became clearer. Information security and data privacy tasks for projects did exist, but they were not caught in project process tight enough. In addition, it was

obvious that information security and privacy procedures and practices were not as uniform as they could be between units and projects. The need was also to clarify and inform employees more actively about the information security tasks, especially customer project related ones.

One of the pain points was to find related research on this area. Although good and interesting research papers were finally found, they were mostly focusing on more technical security areas than administrative ones. Additionally, found references had more limited scope on the research work because the analysis and identification of information security requirements and risks were started along with the project, not earlier. The biggest strength of the framework created in this study is that the identification of information security needs is started in as early phase as in the sales phase. In addition, that these needs are already the key parameters for scale and content of planned project, but security related information is gathered more precisely also for the project's management. It most certainly brings huge benefits for the new project.

The motto of this study was "information security tasks are not technical tasks". As much as we all citizens have been waken up by authorities to be aware of cyber scams and "think before u click", all members of IT project teams do also have a role in information security tasks. Another strength and success of this framework was that administrative information security tasks were put in front. The role of project manager was highlighted when the task responsibilities were defined. Still, the responsibility is more administrative than executive. Information security expertise must be offered by the organization when needed (for example, information security training). Although initial experiences with the application of this framework are promising, it is not ready yet. The implementation of this framework continues in the case organization.

Context of this study work was the customer delivery project from two perspectives. First, it was expected that the scale of project is big or large. That is estimated based on a workload estimate (over 100 days). In addition, behind the workload estimate are requirements set by customer. In this work, the focus was on information security and data privacy requirements. They are received in form of requirement specification but also requirements defined in other documents (for example, call for tender, description of the subject of the procurement) were raised as important in this study. Secondly, this study covered project's lifespan from sales to closing a project. The reason for this cropping was mainly the interest to develop the analysis and management of information

security and data privacy requirements from the early phase of the project. However, information security and data privacy are always present in case of IT project. In the context of this study, after project work is finished, outcomes are accepted by the customer and project is closed, begins the continuous service phase. The information security tasks, and their management in that phase remain an area for further research. Main research question would be how information security and data privacy requirements are maintained and continuously assessed in the constantly changing world of threats and vulnerabilities. Most certainly, the risk management is one of the key areas in that phase, too. On the other hand, customer delivery projects are not always requirement-based, another project type is product-based delivery where instead of implementing secure IT system based on requirements, a secure IT product is delivered. Product-based project and deliveries are also smaller in workload. The management of information security tasks in a product-based project is another subject for further research.

Other interesting areas for developing this framework further are applying this kind of model in a different kind of organization and in technical implementation tasks. The operating environment in the organization of this case is typical for ISO certified IT service providers. However, this framework provides baseline which can be modified to different project management models. For example, for organizations who are utilizing another project management model that PRINCE2. Enlarging the scope of this framework more deeply into information security tasks related to technical implementation phase would mean finetuning the project's tasks with secure coding, auditing, and testing practices.

Finally, I want to quote Smith's (2019) encouraging phrase: "Implementing information security in project management does not have to be hard work". His research was one of the first references I came across when I started this study work. Back then I was skeptical. Right now, I am hopeful that following the resulting framework, the organization is primed with the information and tools for a secure and successful project management implementation.

References

Achmadi, D., Suryanto, Y., & Ramli, K. (2018). On developing information security management system (Isms) framework for iso 27001-based data center. *2018 International Workshop on Big Data and Information Security (IWBIS)*, 149–157. https://doi.org/10.1109/IWBIS.2018.8471700

Ali, S. M., Soomro, T. R., & Brohi, M. N. (2013). Mapping information technology infrastructure library with other information technology standards and best practices. *Journal of Computer Science, 9(9)*, 1190-1196. https://doi.org/10.3844/jcssp.2013.1190.1196

Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice* (Second edition). Syngress.

Baskerville, R. (1991). Risk analysis: an interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems, 1(2)*, 121-130.

Brunner, M., Mussmann A., Breu, R. (2018). Introduction of a Tool-Based Continuous Information Security Management System: An Exploratory Case Study. *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, 483-490. https://doi.org/10.1109/QRS-C.2018.00088

Check J., Schutt R. K. (2011). Research methods in education. *SAGE Publications*, 159–185.

Dexter, J. H. (2002). *The cyber security management system: A conceptual mapping.* Report. SANS Institute.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security, Vol. 4 No. 2*, 92-100. https://doi.org/10.4236/jis.2013.42011

Dutton, J. (2019). *What is an ISMS? 9 reasons why you should implement one*. IT Governance UK Blog. https://www.itgovernance.co.uk/blog/what-is-an-isms-and-9-reasons-why-you-should-implement-one

Emory, D. (2004). The need for secure project management. *ITnews*. https://www.itnews.com.au/feature/the-need-for-secure-project-management-61272

ENISA. (2020). *Enisa threat landscape 2020: Cyber attacks becoming more sophisticated, targeted, widespread and undetected.* https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

F-Secure. (2020). *Attack landscape H12020*. https://blog-assets.f-secure.com/wp-content/uploads/2020/09/17142720/F-Secure-attack-landscape-h12020.pdf

Goldes, S., Schneider, R., Schweda C. M., Zamani, J. (2017). Building a Viable Information Security Management System. 2*017 3rd IEEE International Conference on Cybernetics (CYBCONF), Exeter, 2017,* 1-6. https://doi.org/10.1109/CYBConf.2017.7985763

Graham, N. (2008). *Prince2 for dummies*. ProQuest Ebook Central. https://ebookcentral.proquest.com

Harris, S., Maymi, F. (2016). *CISSP all-in-one exam guide*. McGraw-Hill Education New York, NY, USA, 2016.

Hinde, D. (2012). *Prince2 study guide*. John Wiley & Sons, Ltd.

Hull, E., Jackson, K., & Dick, J. (2010). *Requirements engineering.* ProQuest Ebook Central. https://ebookcentral.proquest.com

ISO/IEC 27000:2018. (2018). International Organization for Standardization. Information technology — Security techniques — Information security management systems — Overview and vocabulary. https://www.iso.org/standard/73906.html

ISO/IEC 27001:2013. (2013). International Organization for Standardization. Information technology - Security Techniques - Information security management systems — Requirements. https://www.iso.org/standard/54534.html

ISO/IEC 27002:2013. (2013). International Organization for Standardization. Information technology — Security techniques — Code of practice for information security controls. https://www.iso.org/standard/54533.html

JAMK. (2018). *Ethical Principles for JAMK University of Applied Sciences*. Approved by the Student Affairs Board on 11 December 2018. https://studyguide.jamk.fi/globalassets/opinto-opas-amk/opiskelu/pedagogiset-ja-eettiset-periaatteet/ethical-principles-11122018.pdf

Kasanen, E., Lukka, K. & Siitonen, A. (1993). The Constructive Approach in Management Accounting Research. J*ournal of Management Accounting Research, 5,* 243-264.

Kiedrowicz, M. & Stanik, J. (2018). Method for assessing efficiency of the information security management system. *MATEC Web of Conferences, vol. 210, 2018*. https://doi.org/10.1051/matecconf/201821004011

Lukka, K. (2003). Case study research in logistics. *Publications of the Turku School of Economics and Business Administration*, 83-101.

Microsoft. (2013). *Dynamics 365. Implementation methodology*. https://docs.microsoft.com/fi-fi/dynamicsax-2012/appuser-itpro/implementation-methodology

Ministry of Defence. (2015). *Katakri. Information security audit tool for authorities.* https://www.defmin.fi/files/3417/Katakri_2015_Information_security_audit_tool_for_authorities_Finland.pdf

NIST. (2012). Guide for conducting risk assessments. *NIST Special Publication (SP) 800-30 Rev. 1. National Institute of Standards and Technology*. https://doi.org/https://doi.org/10.6028/NIST.SP.800-30r1

NIST. (2021). *National Institute of Standards and Technology.* Computer Security Research Center: Glossary. https://csrc.nist.gov/glossary

Orosz, I., & Orosz, T. (2012). Change management and workflow processing using Dynamics AX objects. *2012 IEEE 10th Jubilee International Symposium on Intelligent Systems and Informatics, 249–254*. https://doi.org/10.1109/SISY.2012.6339523

Payette, J., Anegbe, E., Caceres, E., & Muegge, S. (2015). Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects. *Technology Innovation Management Review, 5(6), 26-34*. http://doi.org/10.22215/timreview/904

Ponto, J. (2015). Understanding and evaluating survey research. *Journal of the Advanced Practitioner in Oncology, 6(2), 168–171.*

Pruitt, M. (2013). *Security Best Practices.* https://www.sans.org/reading-room/whitepapers/bestprac/security-practices-project-managers-34257

Raggad, B. G. (2010). *Information security management: Concepts and practice*. CRC Press, 2010.

Raghavan, V., & Zhang, X. (2017). An Integrative Model of Managing Software Security during Information Systems Development. *Journal of International Technology and Information Management. Volume 26. Issue 4.* https://core.ac.uk/download/pdf/153384912.pdf

Refsdal, A. a., Solhaug, B. a. & Stølen, K. a. (2015). *Cyber-Risk Management.* Springer International Publishing.

Regulation (EU) 2016/679. *General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.* European Parliament, Council of the European Union. http://eur-lex.europa.eu/legalcontent/FI/TXT/?uri=CELEX%3A32016R0679

Sangi, S., Ilkan, M., & Tokgöz, H. (2017). Incorporating information security into IT project management (a proposed framework). *Journal of Computing, Communications & Instrumentation Engg. (IJCCIE) Vol. 4, Issue 1.* http://iieng.org/images/proceedings_pdf/112_L_New_formatted.pdf

Scrum. (2021). The 2020 scrum guide. *Scrum guides.* https://scrumguides.org/scrum-guide.html

Segovia, A. J. (2015). How to manage security in project management according to ISO 27001 A.6.1.5. *ISO 27001 & ISO 22301 Blog*. https://advisera.com/27001academy/blog/2015/07/06/how-to-manage-security-in-project-management-according-to-iso-27001-a-6-1-5/

Sharma, S. (2019). *Data privacy and GDPR handbook*. John Wiley & Sons.

Smith, D. (2019). Information Security Best Practices While Managing Projects. SANS Institute. *Information Security Reading Room.* https://www.sans.org/reading-room/whitepapers/bestprac/information-security-practices-managing-projects-38875

Traficom. (2020). Katakri 2020. Tietoturvallisuuden auditointityökalu viranomaisille. *Traficomin julkaisusarja.* https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246

Tutkimuseettinen neuvottelukunta. (2012). Hyvä tieteellinen käytäntö ja sen loukkausepäilyjen käsitteleminen Suomessa. *Tutkimuseettisen neuvottelukunnan ohje 2012.* https://tenk.fi/sites/tenk.fi/files/HTK_ohje_2012.pdf

VAHTI. (2014). Tietoturvallisuuden arviointiohje. Valtiovarainministeriö. *VAHTI-ohjeet, 2/2014.* https://www.suomidigi.fi/sites/default/files/2020-06/VAHTI_2_2014_pdf_0.pdf

Watkins, S. (2013). *An Introduction to Information Security and ISO27001:2013*. A Pocket Guide. Vol. 2nd ed. ITGP.

Wells, K. N. & Kloppenborg, T. J. (2015). *Project management essentials*. First edition. Business Expert Press.

Winder, D. (2015). ISO 27001. *PC Pro 108*. https://search-proquest-com.ezproxy.jyu.fi/magazines/iso-27001/docview/1647262980/se-2?accountid=11774

Zainal, Z. (2007). Case study as a research method. *Jurnal kemanusiaan, 5(1)*. https://core.ac.uk/download/pdf/11784113.pdf

Appendices

Appendix 1. Questionnaire of the current status and development needs

	Usability of the information security framework
Q1	How is organization's information security management system (ISMS) connected to and applied in customer delivery projects?
Q2	Are the information security tasks part of the project and how?
Q3	How is the data privacy managed in customer delivery projects?
	Usefulness of the current information security controls
Q4	What information security methods are used in project?
Q5	Is the information security threats assessment part of project's risk management?
	Overall awareness and level of information security tasks, responsibilities, and results
Q6	How is the information security awareness ensured in project?
	Requirement management methods and used tools
Q7	How are the requirements managed in projects?
Q8	What systems or tools are used in project management?
	Development needs
Q9	What kind of development ideas related to security and privacy task list or information security management there are in customer delivery projects?
Q10	What kind of tools or systems are suggested for supporting information security tasks?