UNIVERSITY
OF TURKU
Turku School of
Economics

Information Security Requirements for B2B SaaS Providers

Master's thesis

Author:
Tuomas Hyvärinen

Supervisor:
Dr. Sc. Jonna Järveläinen

26.03.2023
Turku

Master's Thesis

Subject: Information Systems Science
Author: Tuomas Hyvärinen
Title: Information security requirements for B2B SaaS providers
Supervisor: Dr. Sc. Jonna Järveläinen
Page count: 64 pages
Date: 26.3.2023

Abstract

To gain a competitive advantage, companies are continuously more willing to collaborate with other companies and share information between them (Karlsson et al. 2015). Outsourcing is a viable option for many companies offering cost savings and improving efficiency, however, it does not come without risks to information security (Khidzir et al. 2010). Due to the current business environment of interorganisational collaboration, new threats are emerging in the space of information security. Collaborating with other companies introduces new threats by creating possibilities for non-compliant behaviour, intrusion, and exposure. (Goodman and Ramer 2014.) Therefore, organisations must now rely on partners to ensure information security is upheld on an interorganisational level (Karlsson et al. 2015).

Within the field of information technology, cloud computing has grown to become one of the most dominant computing paradigms in recent years. According to some estimations, by 2024, more than 45 percent of companies' IT spending will consist of cloud computing solutions. (Gartner, 2019.) The reason for cloud computing's rapid increase in popularity is due to its promise of bringing down costs while delivering the same, and potentially more, functionalities as traditional information technology (Marston et al. 2011). However, information security concerns can be seen as one of the biggest challenges that the cloud computing paradigm must overcome for it to reach its full potential (Tipton et al. 2012).

Therefore, in this increasingly connected and digital business environment, a fundamental challenge for companies is to meet information security requirements (Gordon et al. 2010). Organisations must adhere to both standard and organisation-specific information security guidelines to meet these requirements (Thalmann et al. 2012). Managing security in companies both providing and consuming services is no longer limited to internal services, systems, and infrastructure. Furthermore, companies providing services to other parties must also consider the requirements of their customers. (Currie et al. 2001.)

I am conducting this research for a SaaS company, SoftCo, which operates in the enterprise software industry. The aim of this research was to understand what the most common information security requirements are for SaaS companies by analysing the customer questionnaires regarding information security of the subject organisation SoftCo. These findings are gathered into an artifact which includes the most important information security themes and questions from the analysed companies. This study was conducted as a qualitative study using document analysis to gather the data for identifying the information security themes. Additionally, I have evaluated the produced artifact according to the design science research method process by Peffers et al. (2007) where I compared the information security themes with the ISO/IEC 27001 standard for information security management.

In this study I was able to determine 24 different information security themes that were important to customers of SoftCo and also show which of these themes were of most importance according to the questionnaires. Based on these three themes, I identified three areas of information security which were highlighted in the questionnaires: the shift of administrative control from the customer to the service provider, ensuring business continuity and protection against external threats, and concerns regarding auditability and compliance of the service provided.

TABLE OF CONTENTS

List of figures

List of tables

1 Introduction

1.1 Motivation

The current global business environment is becoming continuously more competitive, and companies do not operate as individual and separate entities anymore. Instead, companies are forming alliances where information is increasingly shared between parties. Often these increased levels of collaboration and integration are enabled by information technology. (Karlsson et al. 2015) Companies have become dependent on information technology and communications networks to operate in a more efficient manner. Outsourcing is a viable option for many companies offering cost savings and improving efficiency, however, it does not come without risks to information security. (Khidzir et al. 2010.)

Due to the current business environment of interorganisational collaboration, new threats are emerging in the space of information security. Collaborating with other companies introduces new threats by creating possibilities for non-compliant behaviour, intrusion, and exposure. While the number of computer networks, people and organisations that have access to data increases, so do the system vulnerabilities which are multiplied through the lengthening of communication lines. (Goodman and Ramer 2014.) Therefore, organisations must now rely on partners to ensure information security is upheld on an interorganisational level (Karlsson et al. 2015). It has even been argued that security breaches in supplier information have the potential to cause more significant harm than other supplier related disruptions (Thomas 2012).

Therefore, in this increasingly connected and digital business environment, a fundamental challenge for companies is to meet information security requirements (Gordon et al. 2010). Organisations must adhere to both standard and organisation-specific information security guidelines to meet these requirements (Thalmann et al. 2012). Managing security in companies both providing and consuming services is no longer limited to internal services, systems, and infrastructure. Furthermore, companies providing services to other parties must also consider the requirements of their customers. (Currie et al. 2001.) Auditing these security processes has also become increasingly important and Kwon et al. (2011) argue that this auditing can be equally as important than making sure of the proper selection and use of security controls. However, in the cross-organisational domain, ensuring and auditing that security requirements are met properly is noticeably more challenging than in internal security related processes. Ensuring that security concerns are met in accordance with customers' requirements is a fundamental part of outsourcing, but it is an expensive process which requires a noticeable amount of manual work to be done. (Thalmann et al 2012.)

I am writing this study for a software company, SoftCo, which provides a analytics cloud service helping its customers analyse their data. Due to the nature of the service, SoftCo handles large amounts of customer data and therefore information security is a crucial topic when targeting new customers. With a large number of customers and subsequently a large amount of security related requirements and requests, it would be beneficial to formulate a single document which contains these information security requirements and questions. When a company is interested in purchasing the services of SoftCo, they send an information security questionnaire prior to any investment. Additionally, during the sales process, there may be communication on the topic of information security through other channels between the sales professionals from SoftCo and the customer's IT and information security personnel. Having a single document which includes the most important information security requirements of customers will allow SoftCo to access this information in one place which consequently could speed up the process of gathering information about the most common information security requirements, in order to answer customers' questions faster and with better consistency.

My own motivation and interest towards this topic comes from my studies and interests related to information security. Also, working for a software as a service (SaaS) company where we handle and manage sensitive customer data, information security is always an important topic that cannot be ignored. This topic also provides a great experience to learn more about information security in cloud computing and specifically in the SaaS field. This will provide me with valuable experience in working on information security topics in a corporate setting before having the possibility to work in an information security capacity full time.

1.2 Research question and expected results

The goal of this study is to understand the information security requirements of customers for SoftCo. The end product of this research study will be a list of the most common information security requirements of customers. Through this, I will attempt to create an understanding of the key areas of information security that SoftCo’s customers are focused on. This will aid the sales department in being aware of these key areas during the sales process and prepare for these questions which will help in communicating the requirements to potential customers.

The main research question, which will work as the base for the proposed list of information security requirements, will therefore be:

> What are most common shared information security requirements for SaaS companies?

With this question I will be able to gather common themes among information security requirements and map them into a list. Other questions I will address in this research study are what are the biggest challenges that companies face in cloud computing, what information security risks are associated with cloud computing, and how companies assess the information security of outsourced IT services.

I expect to find commonalities between companies and their information security requirements from the data analysed in this study. I also expect that the requirements from customer organisations will have a strong focus more on technical components and processes that directly impact the customer’s data. Additionally, I expect that companies will be interested in who has access to their data from SoftCo or SoftCo’s subcontractors. Furthermore, I believe that companies will require information on how this access is managed and tracked.

One possible shortcoming of this analysis is that the results may not be applicable to companies assessing the information security of different kinds of software. SoftCo’s software, is based largely on gathering the customer’s potentially sensitive data and performing analysis and analytics on this data. Due to this reason, customers may have emphasized the importance of access control and authentication more than they would with another software which does not gather the customer’s data in such a scale and detail. The questionnaires in used in this study were also from large international organisations so the results could vary with a pool of questionnaires from smaller sized organisations. Additionally, without conducting interviews with SoftCo’s customers, it is not possible to research the reasoning behind the content of their information security questionnaires. This study will focus more on determining the key areas of information security on a higher level instead of understanding customer specific nuances of information security topics.

2 Cloud computing

Within the field of information technology, cloud computing has grown to become one of the most dominant computing paradigms in recent years. According to some estimations, by 2024, more than 45 percent of companies' IT spending will consist of cloud computing solutions. It has also been estimated that this shift from traditional to cloud solutions might be further accelerated due to the COVID-19 pandemic. (Gartner, 2019.)

Although computing power continues to become increasingly cheaper, the growing complexity of organisations' IT infrastructures and distributed data and software has made computing more expensive than ever before. The reason for cloud computing's rapid increase in popularity is due to its promise of bringing down costs while delivering the same, and potentially more, functionalities as traditional information technology. (Marston et al. 2011.) Also, the ubiquitous, on-demand and scalable nature of cloud computing which provides flexibility is at the core of businesses shifting business processes to the cloud. Cloud computing allows for companies to avoid heavy investments in infrastructure and also frees up resources by moving the management of the technology from the business to the service provider. (Ali et al. 2015.)

2.1 Defining cloud computing

In their definition of cloud computing, Marston et al. (2011) emphasize self-service and on-demand delivery to customers over networks that are not restricted to certain locations or devices. They also mention that the resources used in cloud computing are scalable, shared, promptly available, virtual, and require minimal involvement of the service provider. In addition, the cloud service users pay the fee as an on-going operating expense which reduces the accumulation of capital expenditure.

Iyer et al. (2010) define cloud computing by segmenting companies into four levels based on the provided services: "Infrastructure level, Platform as a service level, Application level, Collaboration level, and Service level". The infrastructure level companies provide computing power to developers and their services provide users a dedicated server with memory. Platform as a service level companies provide more abstraction where developers may build applications in a built environment with its own programming language. This lets developers build applications without having to worry about computer processes. Application-level companies are the most popular in this division and they offer online services such as Google Maps which allows for users to pay flexibly for their usage. The collaboration level is formed by a set of social network applications, such as Facebook and LinkedIn, which aim to boost collaboration and create communities. Finally, service level companies provide consulting and integration services.

NIST has defined cloud computing as “a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” (NIST 2011) The cloud computing model is composed of five essential characteristics, three service models, and four deployment models.” These five essential characteristics are on-demand self-service, resource pooling, broad network access, rapid elasticity, and measured service. The Cloud Security Alliance has also added to this list by introducing multi-tenancy as the sixth characteristic (Ali et al. 2015).

On-demand self-service refers to the ability of a consumer to have access to computing resources based on the current need without having to interact with the cloud provider. Resource pooling refers to the service provider’s ability to use the same pool of resources to serve many customers where both virtual and physical resources are shared based on the customers’ demand. Broad network access refers to the availability of the service on the network and the access via diverse platforms such as mobile phones and computers. Rapid elasticity refers to the ability to scale up and down according to the current demand and the elasticity of resource provisioning. Lastly, measured service refers to the capability of cloud systems to meter the resources being used in order to optimally provision and control resources. (Mell et al. 2011.)

Cloud services can be divided into three service models based on the nature of the service they provide: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Within cloud computing, there are also four different deployment model which vary in terms of ownership and accessibility: public, private, community and hybrid clouds. (Mell et al. 2011.)

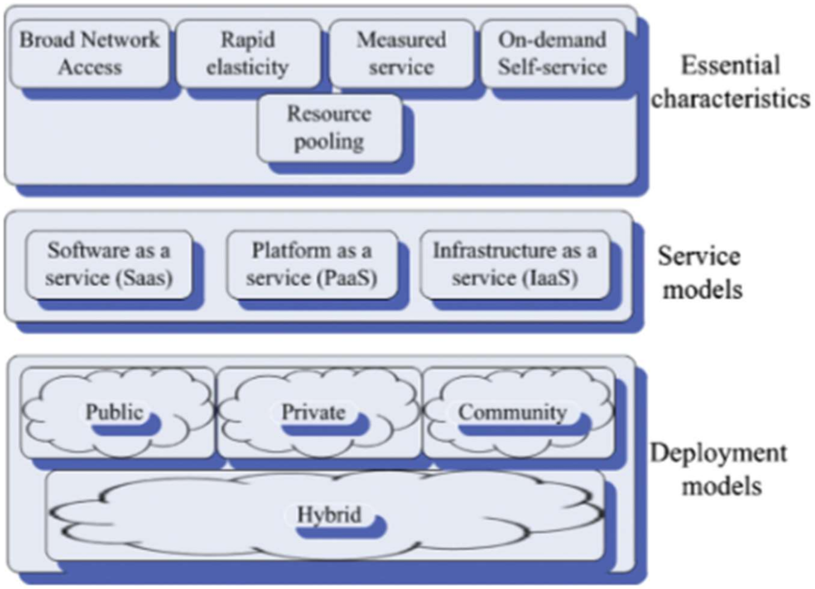

Figure 1 NIST definition for cloud computing (Ali et al. 2015)

The private cloud refers to a model of cloud computing where the cloud is deployed only for a specific user organisation and the resources cannot be utilized by another organisation. This organisation may own and manage the physical infrastructure of the cloud, but equally it can also be owned and managed by a third party which provides the cloud computing services. Additionally, the geographical location of the cloud infrastructure may or may not be located at the organisation's location. Secondly, public clouds are entirely owned by the cloud service provider who are also responsible for the operation of the service. These cloud services are open to anyone who pay for the use. Customers of a public cloud only pay for the services and resources they use in the cloud and the infrastructure is located away from the customers and is managed by the cloud service provider. Community clouds are shared by multiple organisations that generally share a common goal. The management of the cloud and its infrastructure can be the responsibility of any of the organisations using the cloud service or alternatively the management can be overseen by a third-party cloud service provider. Finally, the hybrid cloud, combines the characteristics of any of the prior deployment models and therefore can be seen as a combination of the three. Individual clouds within a hybrid cloud are all unique entities but they share standardized or proprietary technology. (Ali et al. 2015; Sarddar et al. 2019)

As mentioned above, the NIST definition for cloud computing lists IaaS, PaaS and SaaS as the three service models for cloud computing (Mell et al. 2011). IaaS companies provide infrastructure in the form of virtualized computing resources in the cloud. These resources can include for example central processing units, memory, operating systems and application software. IaaS companies therefore virtualize physical resources into resources that customers can use based on demand at different times. One of the core benefits of IaaS is the cost reduction in capital expenditures and allowing users to pay only for the resources they want. IaaS also provides access to enterprise IT grade resources and infrastructure and these resources can be scaled according to the current need of the company. (Rashid et al. 2019; Ali et al. 2015; Alam et al. 2020)

Compared to IaaS, PaaS is more advanced because in the model, the service provider supplies, operates, and maintains the operating system and other computing resources. Other services that PaaS companies provide are application design, development, and hosting. These services may also be accompanied by for example collaboration, database integration, information security and scaling. A large benefit of PaaS is that users do not have to possess their own hardware and software resources and as a consequence do not have to hire experts to manage these resources. Other benefits include scalability and flexibility advantages, and lower upfront investments. A shortcoming of PaaS, however, is the lack of interoperability and portability among service providers. In the PaaS model, users and organisations can deploy their own applications and software on a platform by only paying for access to the platform and its infrastructure. (Rashid et al. 2019; Mell et al. 2011; Ali et al. 2015; Alam et al. 2020)

In the SaaS model, the service is provided through the internet and made visible to the customer as an application interface that users access via a web browser. These applications can also be accessed with different devices with examples of such services being Gmail and Google Docs. In the SaaS model, the customer does not need to purchase licenses or be responsible for the upkeep, upgrading or maintenance of the software. The SaaS model also benefits from scalability and configurability advantages and reduces the need for infrastructure resources. The model also allows for custom offerings of service levels and can have maintenance and support included in the service fee. (Rashid et al. 2019; Mell et al. 2011; Ali et al. 2015; Alam et al. 2020)

2.2 Benefits of cloud computing

As I have previously mentioned, there are multiple reasons why cloud computing has become a prevalent paradigm in computing and multiple benefits can be achieved by companies shifting their IT operations to the cloud. In this chapter I will dive deeper into what the business case is for cloud computing services and what are the core benefits that can be achieved with cloud computing. Then I will provide some shortcomings of cloud computing and look at what obstacles companies face when implementing a new software that is hosted in the cloud.

A key driving factor behind the shift towards cloud computing solutions is related to the cost perspective. Cloud computing software often have minimal up-front which may often deter companies from implementing new IT services. Companies have also found that investments in IT are often underutilised as some corporate servers' have been found to utilize only ten to thirty percent of the computing power available to them. It has also been noted that on average roughly two thirds of the budget IT departments have for staffing, goes towards maintenance and support activities which arise from total ownership of the traditional IT solution. (Marston et al 2011.)

Dikaikos et al. (2009) list three key driving forces for cloud computing: "the ubiquity of broadband and wireless networking, falling storage costs, and progressive improvements in Internet computing software". Cloud services boost IT efficiency by allowing for clients to add more computing power during periods of peak demand and also remove this capacity when and where it is not needed. This will provide customers with more computing power, flexibility, and reduced costs. On the other hand, this allows providers of cloud services to multiplex which will enable them to make larger investments in software and hardware due to higher utilization rates. Service-oriented software, management of large facilities, grid computing technologies, virtualization, and power efficiency can be seen as the foundation for cloud computing services and infrastructures.

There are two major trends in IT that cloud computing addresses, IT efficiency and business agility. IT efficiency is boosted with cloud computing by allowing for a more efficient use of computing power with scalable hardware and software resources which allow for computing power to be used where it is needed. The computing power of cloud services may also be used through the internet in a completely different geographical location to where the computing power and the required electricity is produced. This results in cheaper and possibly greener computing as companies are no longer restricted by their geographical location. Business agility is facilitated through cloud computing as companies may deploy IT rapidly and allocate resources where they are needed. Cloud computing services are also rapidly scalable as computing power can be adjusted according to the current needs of the corporation while also reducing the up-front investments which currently characterize traditional IT setups. Users also gain access to real-time and mobile applications which provide information to changing user requirements. (Marston et al 2011.)

Cloud computing also provides flexibility to employees who are able to join a virtual workspace independent of time and location. Flexibility is further enhanced with the growing number of devices which are connected to the internet, which are able to access the cloud. This allows for flexibility in work practices as data can be accessed from anywhere that has a working internet connection. (Sarddar et al 2019.) This flexibility is also echoed by Aljabre (2012) as cloud applications can be accessed through the internet, cooperation between employees and stakeholders with different operating systems is made possible. Also, having access to documents through the internet further enhances collaboration on shared projects and promotes flexibility on where one must work from.

Cloud computing can be seen to possess five essential advantages: a lower cost of entry, immediate access to hardware resources, less barriers for innovation within IT, the high level of scalability of services, and access to new applications and services. Firstly, cost of entry is lowered for smaller businesses with cloud computing as they gain access to computer-heavy business analytics applications that were previously only available to large corporations. These applications traditionally require large amounts of computing power at relatively short intervals and cloud computing solves this issue with the ability to adjust resources according to the demand. (Marston et al. 2011.) Aljabre (2012) also emphasises the lower cost of entry since Companies do not have to invest in expensive computers with high computing power, as cloud-based applications run in the cloud on the providers servers, not locally in the user’s computer. Because cloud applications are not hosted on the user’s servers, smaller investments are required on the IT infrastructure of an organisation. Organisations can also save money on software investments as with cloud computing, software packages do not need to be purchased for every computer within the organisation. Also, as data is stored in the cloud, less memory storage is needed in users’ computers. (Aljabre 2012.) Secondly, companies can access the cloud service providers hardware resources immediately. Thirdly, cloud technology facilitates more IT innovation by lowering the barrier since less upfront investments are needed. Fourthly, since computing resources are provisioned with software, they can be taken into use very fast which allows companies to scale up or down depending on the current demand. Lastly, cloud computing provides access to new services and applications that were not possible with prior technologies. (Marston et al. 2011.)

2.3 Challenges of cloud computing

Even though there are countless benefits to cloud computing, there are also shortcomings that organisations need to consider. Dikaikos et al. (2009) identified five key challenge areas that cloud computing faces: Software and hardware architecture, data management, cloud interoperability, security and privacy, and service provisioning and cloud economics. Software and hardware architecture is a key challenge since there have been significant changes required to hardware and software in order to facilitate the emergence and increase in popularity of cloud computing. Data management brings challenges to cloud computing as for example data may be stored at untrusted hosts which may cause concerns in data security and privacy. Cloud interoperability has to be developed for example with standards to ensure that cloud services and platforms work as an interoperable network. Service provisioning poses a challenge since providers must be able to correctly estimate the resources needed to meet the demands of each customer according to their service level agreements.

Sarddar et al. (2019) also mention privacy and service level agreements (SLA) and security and data protection, as risks that cloud computing faces while also listing the location of data, and legislation and regulation as risks companies should consider before moving business to the cloud and before selecting a cloud computing technology. Data security and the storage location are critical as storing data at a third-party location poses risks that need to be mitigated with security measures and access controls. The geographical location of the data is also important information as data is often stored outside of the customer organisations local area which means that different legislation might apply to the data.

Companies shifting to the cloud will lose physical proximity to their data and the subsequent control as it is stored in the cloud on the provider’s servers. Larger companies may also have doubts entrusting applications to the cloud that are critical to their mission.

Even though cloud application providers have SLAs in place that promise high levels of service, they can still fall short of the high standards set in place for highly critical applications. Where the shift to cloud computing can be welcomed by IT departments in some companies, in other companies IT departments may reject the change due to fears of change to the IT culture or job security. Concerns may arise about handing operations over to another company which can cause issues if the other company were to experience disruptions or go bankrupt. Another issue is the information security of this outside company as the majority of IT executives and CIOs express concern about the cloud service provider's security. One of the biggest concerns that can deter companies from adopting cloud applications, is the lack of regulation on a local, national, and international level. When it comes to regulation on data privacy and requirements on data access to audit and data location, there can be noticeable differences between different geographical locations in which the company operates in. (Marston et al. 2011.)

3 Information security

As in this study I am researching what the most common information security requirements for companies purchasing SaaS products, I deem it necessary to cover the definition of information security and the different aspects of this field. This will better help understand the requirements set in place by companies for their outsourced IT and the results I get from the content analysis. As determined in the previous chapter, one concern for cloud computing is the information security risks it entails. In this chapter I will dive deeper into what security risks cloud computing contains and how they can possibly be combatted.

3.1 Defining information security

One of the most common definitions for information security comes from the ISO/IEC 27002 (2005) standard, by which the definition for information security is "the preservation of the confidentiality, integrity and availability of information". By this definition, information or data may be stored electronically or on paper either written or printed. It can also be shown via video, through conversation, via post, or electronically by email for example. Therefore, according to the ISO/IEC 27002 standard, information can take on essentially any form, be it physically on paper or conveyed through conversation between colleagues. (Solms et al. 2013)

Whitman and Mattord (2021) have defined information security as "the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information". They also lean on the ISO/IEC 27002 standard when identifying the key characteristics that give value to information within organisations. The same characteristics that can also be found in the ISO/IEC 727002 definition, are the confidentiality, integrity, and availability of information, but Whitman and Mattord do not limit the characteristics to only these three, which are commonly referred to as the CIA definition. This CIA definition has been regarded as the industry standard when discussing information security (Solms et al. 2013). In the ISO/IEC 27002 definition, confidentiality refers to information being unavailable to different parties who do not have the required permission. Integrity refers to the accuracy the information and to how complete the information is. Lastly, availability means that information can be accessed and used when needed by an entity with the proper authorization (Lundgren et al. 2017).

Whitman and Mattord (2021), however, expand on this definition by adding the utility, accuracy, possession and authenticity possession to the characteristics which need protection in information security.

Lundgren et al. (2017) also challenge the concept of the CIA definition, arguing that the characteristics provided in the model are in fact goals, and therefore not intended to be used as a definition for information security. They for example argue that the CIA definition renders secure processes as insecure. For example, a time lock system where the contents which are behind a locked space cannot be accessed by anyone, can be argued as secure, but it does not meet the standards of availability set in place by the CIA definition.

Solms et al. (2013) also deem it necessary to distinguish information security from cybersecurity as these two terms are often used synonymously in information security literature. The International Telecommunications Union (ITU) has defined cybersecurity as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user’s assets.” These assets contain a broad spectrum of resources and systems such as: computers, applications, telecommunication systems, infrastructure, personnel and largely any information which is contained in the cyber environment be it stored or in transmission. According to their definition, the aim of cybersecurity is to ensure the proper attainment and maintenance of the properties of the assets, which combat security risks in their environment. As with many other definitions for cybersecurity and information security, in their definition for cybersecurity, ITU also include the “confidentiality, integrity and availability” as security goals. (ITU 2008)

There is a distinction between information security and cybersecurity, however, there are also commonalities between the two since all security is about protecting assets which are threatened by various vulnerabilities. The risk caused by these vulnerabilities is then mitigated by implementing controls which help in reducing the risk. There is definitely overlap between cybersecurity and information security but perhaps the most distinguishing aspect which separates the two is the assets that are being protected. In information security the protected asset is the information itself and underlying technologies. However, in cybersecurity, the definition of the assets is broader and focuses more on securing anything and anyone within the cyberspace be it individuals or organisations. (Solms et al. 2013.) Furthermore, information security contains the protection of information in all forms whereas cybersecurity focuses on the protection of an organisation's digital assets (Solms et al. 2018)

As the companies that have been included in this study have posed multiple questions to SoftCo pertaining to the security of information for example on paper or transmitted verbally, I argue that information security is the more appropriate term to be used in this study. The use of cybersecurity would limit the scope to only digital assets which would not provide a full picture of the requirements SoftCo's customers have for the protection of their data.

3.1.1 Information security strategy

The role of information within organisations is becoming continuously more critical in the facilitating innovation and providing a competitive edge for organisations that understand this. However, with the development of technology and the usage of information, also comes a wide range of malicious behaviour which risks the security of the information organisations possess. To combat these security risks organisations must formulate and implement information strategies. It can also be argued that even though organisations should use strategies to optimize their resources and direct the actions and efforts that upholding security requires, a single strategy might not be sufficient to succeed in all the different areas of information security in organisations. (Ahmad et al. 2012.) Park et al. (2008) define information security strategies as the process of protecting the information infrastructure of an organisation to ensure the confidentiality, integrity and availability of data in the most optimal and cost-effective manner. This includes decisions on how to best make use of the information security resources and measures in place and coordinating their deployment in a cohesive manner.

Researchers of information security strategies have conceptualised information security in organisations into either a static plan or a dynamic process. The former refers to an artefact which is shared with stakeholders. As an artefact it is central, and it aims to describe how concepts, within the organisation such as goals and policies, are linked together. Where in a static plan, an artefact is shared with stakeholders, in a dynamic process, stakeholders who are concerned about protecting an organisation's information, follow this process. The process-oriented conceptualization emphasizes that the use of a strategy-setting process while ensuring that information security is aligned with the strategy of the organisation. There are differences among researchers who believe information security strategies in organisations to be static plans, and some believe in the dynamic process of information security. Also, some researchers do not find these conceptualizations relevant and therefore do not subscribe to them or describe them in more abstract terms. (Horne et al. 2017.)

Sveen et al. (2009) bring up the distinction between reactive and proactive information security perspectives and strategies. Most of the companies they surveyed had a reactive strategy to security where incidents were fewer and not a top priority until a serious event occurred. One effective proactive strategy is to analyse the potential vulnerabilities before they reveal themselves and cause damage. One form of this proactive analysis on vulnerabilities is called risk assessment where organisations analyse the security controls in place which protect the information and assets of an organisation and calculate the probability that losses could occur to these assets. (Sveen et al. 2009.)

Horne et al. (2017) list four different levels in information security strategies in organisations: “individual level, group level, organisational level, and inter-organisational level”. The individual level looks at how individuals contribute to information security on a strategic level. This is often overlooked, which is surprising since the strength of an information security strategy often depends heavily on the weakest link on the individual level. The group level section looks at groups working together and their dynamics and examines what effect they have on information security from a strategic perspective. The organisational level takes a broader look on information security strategy and this level is the most important one in terms of achieving internal strategic success by providing support to the different strategic elements of information security.

Lastly, the inter-organisational level is where information security related benefits and motives are shared with other organisations that contribute to the strategy. On the inter-organisational level, compliance of organisations is often determined by external auditors. (Banker et al. 2010.)

3.1.2 Information security policy

The information security policy of organisations can be seen as one of the most important documents from a business perspective. Although related to technology, the policy should reflect the organisation and the environment it operates in. It must also consider the business objectives of the organisation. In addition, the information security policy should emphasize the importance of the people within the organisation and ensure that it is understood widely throughout the organisation with managements support. Therefore, it is also crucial for the policy to consider the culture, diversity and geography of the organisation in order to successfully communicate it throughout the organisation. (Layton 2016)

Often organisations rely too heavily on technology-based solutions to uphold information security but with the vulnerability that employees of organisations create, an effective information security policy should also be in place. This policy should include clear instructions for individuals on how information security can be upheld while using information systems in their jobs. (Bulgurcu et al. 2010.)

Organisations ought to use various different controls to ensure success within information security. Moreover, out of these controls, as the information security policy gives direction to the organisation, it can be seen as the most important security control. It defines the commitment and role of management in managing information security and defines what part information security plays in reaching organisational goals. Therefore, an information security policy should clearly describe the need for information security within an organisation and explain the different components it comprises of. (Höne et al. 2002.)

3.2 Information security standards

The importance of information security policies is clear; however, organisations may find it difficult to create them. With many questions regarding policy creation, policy authors often look for outside resources in search for guidance and these resources are often standards. (Höne et al. 2002.) The National Institute of Standards and Technology (NIST) has defined standards to be “a document, established by consensus and approved by a recognized body, that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context". These documents may also provide requirements for a service or process. (Scholl et al. 2008.)

In this study I am researching the most common information security requirements from customers for a cloud service provider SoftCo. SoftCo adheres to certain information security and cloud computing standards and frameworks. The results from this research into the most common information security requirements, will be analysed against the relevant standards and frameworks for this study, namely ISO/IEC 27001.

The ISO/IEC 27000 series focuses on security within information systems management and comprises of four standards: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27006. The main focus in this study is the ISO/IEC 27001 standard, which is internationally recognized and determines requirements on how businesses can implement a certified information security management system (ISMS). ISO/IEC 27001 assists organisations in managing and protecting the information of customers and employees, managing information risks, and protecting and developing the organisations brand. The aim of the standard is for organisations to successfully manage and protect the information of the employees and customers while also managing information risks and protecting their brands. (Taherdoost 2022.)

The ISO/IEC 27001 standard additionally provides a list of 114 controls that are which have the goal or mitigating information security risks (Shojaie 2014). These controls are then divided into security objectives which are further placed under control clauses. These control clauses represent different areas of information security. (Raković 2021.) The 2013 version of the standard contains a total of fourteen control clauses. The previous version which came out in 2005 had only eleven control clauses as cryptography, operations security, and supplier relationships were added to the 2013 version. (Shojaie 2014.) The control clauses are listed in Appendix A of the ISO/IEC 27001 standard:

Information security policy
Information security Organisation
Human resource security
Asset management
Access control
Cryptography
Physical and Environmental safety
Operation security

Communication security
System acquisition, development, and maintenance
Supplier relations
Information security incident management
Information security aspect of business continuity management
Compliance

Firstly, the *Information security policies* control clause contains one security category, *Management direction for information security,* which includes a subset of two controls. This security category supports management in managing information security and providing direction while meeting business requirements and complying with laws and regulations. (Calder 2013.)

The second control clause is Organisation of information security which includes the *Internal organisation* and *Mobile devices and teleworking* security categories. The former refers to implementing frameworks for management to assist in both the implementation of information security within the organisation and also during the operational phase of controlling information security. The latter refers to ensuring the secure use of mobile devices and teleworking. (Calder 2013.)

Thirdly, *Human resource security* contains three security categories which refer to the status of employment: *Prior to employment, During employment,* and T*ermination and change of employment*. The first two categories refer to the process of ensuring that employees and contractors are aware of their responsibilities and are capable of performing their duties. *Termination and change of employment* refers to ensuring that the organisations interests are protected in the case of employment termination. (Calder 2013.)

Fourthly, *Asset management* contains three security categories. *Responsibility for assets,* which refers to the identification of assets within the organisation and the definition of protection responsibilities. *Information classification,* which refers to determining the importance of information to the organisation and ensuring it receives appropriate protection. Lastly *Media handling* refers to the prevention of information on stored media being subject to unauthorized access, modifications, removal, or destruction. (Calder 2013.)

The fifth control clause, *Access control,* contains four security categories. *Business requirements of access control,* which is in place to ensure that access to information and information processing facilities is limited. *User access management,* which combats unauthorized user access to systems and services. *User responsibilities,* which ensures that users are accountable for protecting their authentication information. And lastly, *System and application access control* is in place to combat unauthorized access to systems and applications. (Calder 2013.)

The *Cryptography* control clause contains one security category, *Cryptographic controls.* This category contains controls that are in place to ensure the appropriate use of cryptography with the goals of protecting the confidentiality, authenticity and integrity of data. (Calder 2013.)

Physical and environmental security contains two security categories. Firstly, *Secure areas,* aims to combat unauthorized physical access, interference or damage to the organisation's information assets and processing facilities. Secondly, *Equipment,* aims to ensure that there is no loss, damage or theft of the organisations assets which could cause interruptions to operations. (Calder 2013.)

The eighth control clause, *Operations security*, contains seven security areas. Firstly, *Operational procedures and responsibilities*, ensures that operations of information processing facilities are secure and correct. Secondly, *Protection from malware,* ensures that there are appropriate controls in place to protect against malware. Thirdly, *Backup,* refers to the prevention of data loss. Fourthly, *Logging and monitoring,* contains controls which are in place to record and monitor events and provide evidence. The fifth category, *Control of operational software,* is in place to ensure the integrity of operational software. The sixth category, *Technical vulnerability management,* is in place to prevent that technical vulnerabilities become subject to exploitation. Lastly, *Information systems and audit considerations,* contains controls which ensure that audit activities have minimal effect on operational activities. (Calder 2013.)

Communications security contains two security categories: *Network security management* and *Information transfer.* The former contains controls which aim to protect information in networks and supporting information processing facilities. The latter refers to the security of information being transferred to and from the organisation. (Calder 2013.)

The tenth control clause, *System acquisition, development and maintenance,* contains three security categories. Firstly, *Security requirements of information systems,* ensures the security of information systems during their entire lifecycle. Secondly, *Security in development and support processes,* ensures the design and implementation of information security during the entire development lifecycle of information systems. Lastly, *Test data,* ensures that data used for testing purposes is protected. (Calder 2013.)

The eleventh control clause, *Supplier relations,* contains two security categories: *Information security in supplier relationships* and *Supplier service delivery management.* The former category controls the security of assets which are subject to access by suppliers. The latter, refers to maintaining a certain level of information security which has been agreed with suppliers. (Calder 2013.)

The twelfth control clause, *Information security incident management,* contains one security category, *Management of information security incidents and improvements,* which is in place to ensure the appropriate management of information security incidents which also includes the communication of security events and potential weaknesses. (Calder 2013.)

The thirteenth control clause, *Information security aspects of business continuity management,* contains two security categories. Firstly*, Information security continuity,* which ensures that the continuity of information security is implemented in the business continuity management systems of the organisation. Secondly, *Redundancies,* ensures that information processing facilities are available. (Calder 2013.)

The last control clause is *Compliance* which contains two categories: *Compliance with legal and contractual requirements* and *Information security reviews.* The former ensures that there are controls in place to ensure that the organisation does not breach information security related laws, regulations, or contractual agreements. The latter, ensures that the implementation and operation of information security is compliant with the organisations policies and procedures. (Calder 2013.)

3.3 Information security in cloud computing

In the field of cloud computing, information security concerns are a prevalent topic among researchers and organisations. Alam et al. (2020) remind that information security is an important issue that must be addressed from multiple different perspectives when discussing cloud computing. Concerns regarding security in cloud computing is the biggest obstacle that cloud computing faces. There is a reluctancy to shift from traditional computing methods to cloud computing and transfer digital assets to outside service providers. (Ali et al. 2015.) As this study is focusing on the information security requirements companies have for cloud computing providers, I will dive deeper into what are the major information security risks that companies face when shifting operations to the cloud.

Tipton et al. (2012) also emphasize the importance of security, mentioning that it is one of the major challenges cloud computing must overcome for it to reach its full potential. The security of the cloud must be on par with separate corporate networks for cloud computing to make sense from a business and security perspective. Achieving this level of security is not solely on the responsibility of cloud service customers, but also on the responsibility of cloud service providers. Both must cooperate in order to achieve and maintain the required level of security in the cloud. (Tipton et al 2012.) Even though customers may set in place numerous policies to protect their information when investing in a cloud service, the most common model for security between customer and provider is the shared responsibility model. In this model the responsibility of security and compliance is shared among the customer and the service provider without having a shared database for the security mechanisms in place from both parties. (Brumă 2021.)

Where traditional IT infrastructure allows for an organisation to keep digital assets under its administrative control, cloud computing often requires the transfer of digital assets and information to a third-party service provider. This can cause concerns and doubts among stakeholders of an organisation planning to adopt cloud computing services. There are also concerns regarding the number of users that have no relation to the customer's organisation and are not trusted by the customer. (Ali et al. 2015.) A cloud computing services security is also dependent on the deployment model of the service. For example, in a public cloud where all consumers have access to a software may cause security concerns due to the nature of the access control. Whereas in a private cloud, the service is out of reach from public access, there are less security concerns as it prevents unauthorized access. (Alam 2020.)

Rane (2012) provides a collection of eight high level security concerns for the SaaS deployment model: "the nature of the SaaS deployment model, Data security, Network security, Regulatory compliance, Data segregation, Availability, Backup, Identity management and sign-on process".

Firstly, the decision of what deployment model to use, affects the security risks of the solution. The provider can decide on either deploying the solution through a public cloud public provider which ensures that the necessary information security infrastructure is in place or host the solution themselves which requires them to build the infrastructure and assess the security level. (Rane 2012.) Infrastructure security can be viewed from the perspective of the network, the host, and the application levels. Neither network nor application security issues are necessarily caused by the SaaS model, but these issues are amplified in this service model. (Komperda 2012.) A cause for concern for the security of infrastructure are any security misconfigurations made for the cloud network infrastructure. Customers rely on the security of the providers infrastructure and even a small misconfiguration can compromise the security of the system. One of the most common misconfigurations happens when administrators select a familiar configuration tool to them but one that does not necessarily meet all of the security requirements. (Ali et al. 2015.)

Data security is an important risk since in the SaaS model, off premise storage of the customers' data is used and therefore requires additional security measures from the SaaS provider to ensure that the data is secure and prevent breaches. These additional measures can include strong cryptography and access management processes. (Rane 2012.) One of the major security risks for data security in cloud computing is the lack of adequate encryption methods and capabilities. Also having your data stored in the same location as data from a high threat level customer, may expose you to the same risks from attacks as the high threat level customer. Government agencies may also be able to subpoena customers data from the providers servers without prior notice to the customer. (Komperda 2012.)

Network security is also a risk caused by the transfer of data from the customer's premises to the provider's premises. Since sensitive data is being transmitted over the network, strong encryption techniques are required such as the Transport Layer Security (TLS) (Rane 2012). Communication related issues where data is being transmitted can be divided into external and internal communication. The former refers to communication that happens between the cloud and the customer. As this kind of transmission of information is similar to any other transmission of data through the internet, the security risks are similar to any other traditional IT communication. Countermeasures for these risks include cryptography algorithms, intrusion detection and prevention systems, and digital certificates. Internal communication is communication within the cloud infrastructure which brings risks with shared infrastructure, virtual networks, and security misconfigurations. Due to the resource sharing aspect of cloud computing, also network resources can be share which may expose customers to cross-tenant attacks. (Ali et al. 2015.)

SaaS solutions need to be assessed regularly to ensure compliance with regulations and standards such as ISO-27001. Regulatory compliance is also a prevalent topic in data privacy and how sensitive data should be stored and secured. (Rane 2012.) One concern can be the lack of transparency which can make auditing very challenging for customers. There may also be a lack of proper audit logs provided by the service provider, which can be needed when investigating breaches. (Komperda 2012.) There are many legal issues that may arise due to different jurisdictions and geographical areas with different legislation. Data might be transferred and stored in a different location where different laws apply. Potentially data might be stored in multiple locations which have different laws in place which can bring legal issues for example in cases of investigations where data is being seized. (Ali et al. 2015.)

Data segregation is important due to the multi-tenant characteristic of cloud computing which allows for providers to provision resources to multiple customers from a shared pool. This however also means that additional measures need to be in place to ensure that a single tenant’s data is not accessible by other tenants. (Rane 2012.) As data is segregated in the SaaS model with logical means, not physical, there are relevant concerns regarding data security from customers (Komperda 2012). Resource sharing among customers can also bring security threats to users and the infrastructure due to virtualization. For example, even though virtual machines are separated with a logical isolation, they share physical resources which can expose them to cross VM attacks. (Ali et al. 2015.)

Availability is also crucial for the SaaS model as customers must have access to their data at all times. This requires resilience against hardware and software failures which cause down time and protection against denial-of-service attacks. Availability also means that providers have appropriate plans for business continuity and disaster recovery. (Rane

2012.) However, where data recovery is important for recovering from breaches or disasters, this also poses a threat as attackers may be able to recover sensitive data of previous users. (Ali et al. 2015.)

In case of disasters, backups are crucial for recovering the customer's data which is why data should be regularly backed up with strong encryption methods. (Rane 2012.) This backup data also needs to be guarded against tampering and unauthorized access (Ali et al. 2015). Komperda (2012) also emphasises that cloud service providers do not always provide sufficient storage management protection and disaster recovery processes. Cloud service providers also face issues with improper media sanitization where the destruction of physical media is not done correctly (Ali et al. 2015).

Finally, SaaS providers must support in identity management (IdM) and sign-on processes. Examples of methods used for these processes are Independent IdM Stack, Credential Synchronization, and Federated IdM. (Rane 2012.) Providing adequate identity and access management that meets the business needs of customers, is one of the major challenges that cloud service providers face (Komperda 2012). The issue with access control and identity management in cloud computing is that the resources are in a different from the owner. Also, the customer organisations authorization and authentication methods may not be transferrable as such to the cloud environment. Using separate methods for authentication in the cloud and with internal IT, can cause issues over time through increasing complexity. There is also the possibility of malicious users with for example super user access rights to network components who can potentially launch attacks such as sniffing and spoofing. Additionally, there is the possibility of employees of the SaaS provider acting maliciously which may also pose a security threat to environment. (Ali et al. 2015.)

Ensuring that appropriate information security controls are in place is crucial, but it can also be argued that having the capability to audit the performance of these controls is equally important. (Kwon et al 2011.) ISO has defined the audit as "a systematic and independent examination to determine whether quality activities and related results comply with planned arrangements and whether these arrangements are implemented effectively and are suitable to achieve objectives". (Brumă 2021.) A 2009 study by the European Network and Information Security Agency (ENISA) concluded that loss of governance and compliance risks were among the top ten highest ranking concerns regarding cloud computing. Both of these concerns can be attributed to the lack of auditability of cloud services and providers. (Rasheed 2014.) Indeed, there is a considerable lack of transparency in cloud computing which hinder the possibility of wider cloud service adoption. Not only are security audits necessary but to foster trust between the customer and provider, security transparency is needed. Security transparency refers to the process of making security processes and mechanisms available to the customer for their independent analysis. (Ismalil et al. 2020.) Auditing in the context of cloud computing can be seen as twofold where the first process is ensuring the providers takes appropriate measures to ensure that the data is secure, and the second process is ensuring that the customer has the ability to audit the security controls. (Rasheed 2014.)

The challenge companies face when auditing a cloud service provider is that the most common security model between the customer and provider is a shared responsibility model where the responsibility of the security is shared among both parties. However, both parties having isolated databases for security mechanisms makes auditing challenging as shared databases are uncommon. In addition, the increasing complexity of cloud services brings considerable challenges to auditing as most standards focus on high level topics which are far apart from the low-level logging information within cloud services. (Brumă 2021.)

Rasheed et al. (2014) divide the user requirements for cloud security auditing into two areas, infrastructure auditing needs and data auditing needs. Regarding infrastructure auditing needs, the ISO 27001, and Payment Card Industry Data Security Standard (PCI DSS) standards are the most required and have been largely influential to the development of information security in this field.

The cloud audit can be divided into three different categories: internal audits, cloud provider audits, and public audits. Firstly, internal audits are performed entirely by the customer and no outside resources are used. Secondly, cloud provider audits are performed by the service provider and these reports can certify that the provider is compliant with international standards. Lastly, public audits are performed by independent third parties who audit the security objectively. Deloitte is one of the largest providers of such audits and it uses a framework comprising of nine steps: testing logical and physical security controls; testing IT operations; testing disaster recovery procedures;

testing business continuity; assessing data integrity; assessment of controls over critical system platforms, network and physical components reviewing the IT strategy; reviewing the IT organisation; and reviewing IT processes such as the helpdesk and service management. (Brumă 2021.)

3.4 Risk assessment methods for outsourced IT services

While organisations are attempting to save costs by outsourcing IT services in order to be able to focus on core business activities, there are many potential risks that come with outsourcing. In his study, Khalfan (2004) found that security issues, ability to operate new systems, loss of key IT employees, hidden costs, and inadequate planning and management were identified as key issues in outsourcing IT services. Cayirci et al. (2016) even mention that lacking due diligence is one of the most prominent threats that the cloud computing paradigm faces. Indeed, security issues have been a key issue for outsourcing which can be divided into three dimensions: organisational, legal, and technical dimensions. The organisational dimension refers to policies and procedures which fulfil safety requirements, the legal dimension covers the legal requirements that the organisation and any partners adhere to, and the technical dimension includes the organisation's technical infrastructure and tools for protection of assets. (Nassimbeni 2011.)

Numerous institutes and organisations have developed methods to assess information security risk including the Central Computer Telecommunications Agency's Risk Analysis and Management Method (CRAMM) and the Software Engineering Institute's (SEI) Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). The CRAMM method encompasses five stages: initiation, definition and valuation of assets, threat and vulnerability assessment, risk analysis, and identification and countermeasures. The OCTAVE model has three different stages which include profile development of threats, vulnerability identification, and security strategy and plan development. (Kuzminykh et al. 2021.)

While cloud computing, addresses the needs of lowering costs by resource sharing for example, there are also many risks that come with the technology. Cloud computing is bringing more opportunities, but it is also encouraging organisations to place sensitive data on the internet which causes security concerns. (Akinrolabu et al. 2019.) Risk management refers to the act of mitigating risks to levels which are acceptable to an organisation and is traditionally performed in two phases: “risk assessment and risk treatment” (Bojanc 2013.) Managing these risks requires organisations to perform risk assessments, which is a process including the identification, evaluation and prioritization of risks and is a central part of information security management. Based on the ISO/IEC 27005 standard, risk assessment can be divided to two processes: risk analysis and risk evaluation. The number and severity of risks will depend on the organisation and its predisposition, expertise, and willingness to take on risk. When it comes to cloud computing, risks depend on the deployment model, cloud architecture, level of data sensitivity and existing security controls. (Akinrolabu et al. 2019.) Risk assessment methods can be divided into asset-based methods and scenario-based methods. In asset-based methods, risk is a product of identifying threat in combination with a vulnerability. But with the scenario-based approach in ISO 27001, there is no need to identify each threat and vulnerability but instead, identify and define the risks directly. (Well 2020.)

Although there has been a lot of literature and research on cloud computing risks, no consensus has been yet reached on how to assess the risks of cloud services nor are there any standard measurements. Since there are no standardized cloud computing risk assessment frameworks, the industry continues to use risk frameworks used for traditional IT for these assessments also. This is even though cloud computing risks differ from the traditional IT risks that the current frameworks have been created for. (Akinrolabu et al. 2019.) The current IT risk management and risk assessment standards are from large organisations responsible for standardization such as the International Organisation for Standardization (ISO), the International Electrotechnical Commission (IEC), and the National Institute of Standards and Technology (NIST). These standards are generic and have not been made for cloud computing specifically, although there are some modified versions of these standards which are designed for cloud deployments. ENISA has also produced recommendations and a framework for generic qualitative inductive risk assessment for cloud computing. (Cayirci et al. 2016.)

4 Methodology

4.1 Research method and framework

This research will be conducted as a qualitative study as I will be analysing the content of documents in an attempt to answer the research questions. I have chosen design science research method (DSRM) as the methodology for this study as I will be researching and solving a practical problem within SoftCo. This methodology will also allow me to create a concrete solution, an artifact, to a problem in the form of a list of the most common information security requirements and questions. Design science includes the creation and evaluation of an end product, called an artifact, which has the purpose of solving a problem within an organisation. These artifacts can take on a multitude of different forms and is, in fact, the most important characteristic of design science. These artifacts should be relevant in the solving of the identified issue within the organisation. It is also important that the research is presented to the correct audience which in my case will be the information security and sales professionals within SoftCo's organisation. (Peffers et al. 2007.)

The design science process is an iterative one which consists of six activities: identifying the problem and motivation, defining objectives of the solution, design and development of the artifact, demonstration, evaluation, and communication. In addition, there are four possible "entry points" which can initiate the research: problem centred initiation, objective centred solution, design and development centred initiation, and client/context initiated. (Peffers et al. 2007.)

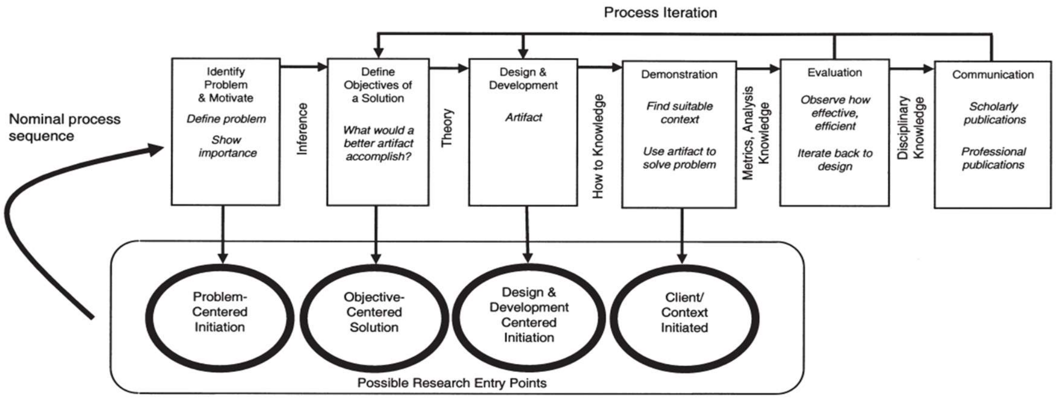
Process Iteration
Nominal process sequence
Identify Problem & Motivate
Define problem
Show importance
Inference
Define Objectives of a Solution
What would a better artifact accomplish?
Theory
Design & Development
Artifact
How to Knowledge
Demonstration
Find suitable context
Use artifact to solve problem
Metrics, Analysis Knowledge
Evaluation
Observe how effective, efficient
Iterate back to design
Disciplinary Knowledge
Communication
Scholarly publications
Professional publications
Problem-Centered Initiation
Objective-Centered Solution
Design & Development Centered Initiation
Client/ Context Initiated
Possible Research Entry Points

Figure 2 Design science process (Peffers et al. 2007)

This study had a problem centred initiation, where the DSRM process started with SoftCo defining the problem to be the absence of a documented overview of SoftCo's customers information security requirements. This causes sales professionals to not have a complete view of what aspects of information security customers value the most. Also, the absence of a single document which outlines the most important information security requirements and questions, leads to employees of SoftCo researching the same questions individually.

The second activity of the process, defining objectives for the solution, requires definition of objectives that provide a solution to the problem defined in the first activity. These objectives can be either quantitative or qualitative. (Peffers et al. 2007.) In this study, the objectives defined were of a qualitative nature. Together with SoftCo, we defined the objectives of the artifact which would solve the problem defined in the first activity. It was defined that the objective would be for sales and other professionals to have the most common information security requirements gathered in one document. This would help in not only understanding the importance of different information security requirements but also serve as a basis for creating an information bank with answers to all of the gathered questions.

Thirdly, I designed and developed the artifact. This activity requires the creation of an artifact which can be "any designed object in which a research contribution is embedded in the design" (Peffers et al. 2008). This included a document analysis, where I analysed the contents of twenty-five information security questionnaires SoftCo has received from customers before they have committed to purchasing a license to SoftCo's software. Analysing these questionnaires gave me an understanding of the most important topics related to information security that companies have prior to an investment in a SaaS product. The developed artifact is a list of the most common information security themes and questions from the analysed companies. The data collection and subsequent artifact development has been described in more detail in the next chapter.

The fourth activity, demonstration, requires demonstration on how the produced artifact has solved a problem in use (Peffers et al. 2007). The artifact produced in this study, is designed to provide information to professionals on a high level of the information security requirements of customers. The aim is that by creating the artifact, SoftCo will get a comprehensive overview on the information security requirements of customers. Additionally, gathering the requirements that customers have through questions asked in the questionnaires, this artifact will also serve as a basis for an information bank after these questions have answers attached to them. In this study I have demonstrated that the artifact indeed fulfils this objective by showcasing the different information security topics from customers and their importance.

The fifth activity of the process is evaluation, where one must evaluate how well the designed artifact solves the problem which has been defined. This evaluation can take any form where the evaluation of success has been supported with empirical evidence or logical proof. (Peffers et al. 2007.) In chapter 5.5 I have compared the findings from the data set and the subsequent themes that emerged against the fourteen control clauses listed in the ISO/IEC 27001 standard. The reason I am using the ISO/IEC 27001 standard, is that this is the most commonly required standard for SoftCo and many questionnaires revolve around this standard. Comparing the findings of this study with the standard not only gives more insight into what topics within the standard are valued but it also provides validity to the produced artifact. By showing that the themes from this study are present in the ISO/IEC 27001 standard, I can demonstrate that the themes are indeed crucial not only according to SoftCo's customers but also the industry in general. Rasheed et al (2014) also mention it to be one of the most influential standards in the field of information security auditing along with the PCI DSS. However, the PCI DSS standard is not relevant due to the absence of payment card information in SoftCo's service. Therefore, by comparing my findings against the fourteen control clauses, I will gain an understanding of if the questionnaires that SoftCo has received are in line with the expectations defined in the ISO/IEC 27001 standard.

The last activity, communication, consists of communicating the identified problem and the designed artifact to a relevant audience. It should also be communicated how important the problem is and how the artifact was designed and how effectively it solves the problem. (Peffers et al. 2007.) Firstly, I have communicated my findings, problem definition and artifact design in this study which will be available for researchers and students to read in the University of Turku. Secondly, these topics have also been communicated to information security and sales professional in SoftCo who can use the information to solve the problem defined in this study and in any future context.

4.2 Data collection and analysis

This study has been conducted as a document study where data is collected through the analysis of documents obtained from SoftCo. These documents consist of questionnaires SoftCo has received from existing and potential customers regarding information security requirements. These customers range from a variety of different industries such as manufacturing, healthcare, software, and consumer goods. I have selected a broad range of different customers to gain an understanding of the customer base in total and not limit the findings to a specific industry. The time when the information security questionnaires were sent to SoftCo ranges from 2017 to 2022. I have been assisted by information security professionals within SoftCo in collecting the relevant documents for this study.

This study could have also been conducted as an interview study which would have allowed a deeper dive into specific customers. However, by analysing documents from customers, I can get a broader understanding of numerous clients. In this study I have not aimed to achieve a deep understanding of individual customers but instead, attempting to understand what the main topics of interest within interorganisational information security for customers are. If I were to interview a select group of customers, there could have been important topics left unmentioned in interviews.

I have conducted the data analysis with a content analysis of the documents. I began this content analysis by going over the collected data and identifying the relevant documents to this study. I have defined documents as relevant if they are extensive enough and cover a broad variety of information security topics. After determining which documents were used in this study, I compared them to each other and combine similar questions to find out the recurrence of these questions. This way I could gather all of the questions into one single document and measure the recurrence of each question. This made analysing the questions and grouping them into themes, easier and more efficient. After this, I coded the questions to higher level themes to determine which themes occur the most across the customers within the data set. This provided me with an understanding of the key areas of focus that companies value when determining the information security level of SaaS providers. I determined these themes after I have gathered the questions from the data set into one file and have analysed them.

5 Results

The data set in this study consisted of twenty-five information security questionnaires sent to SoftCo by customers. An immediate finding from these questionnaires is that almost none of the questions appeared only from a single customer's questionnaire. Instead, there was noticeable repetition and recurrence of questions between the different questionnaires. This allowed me to create themes based on the information security areas of each question.

5.1 Artifact and overview of the results

Based on the analysis of the customer questionnaires, I identified twenty-four themes in which to categorize the questions. These twenty-four themes can be found in Figure 2, where all of the identified themes are listed along with the number of questions allocated to each theme.

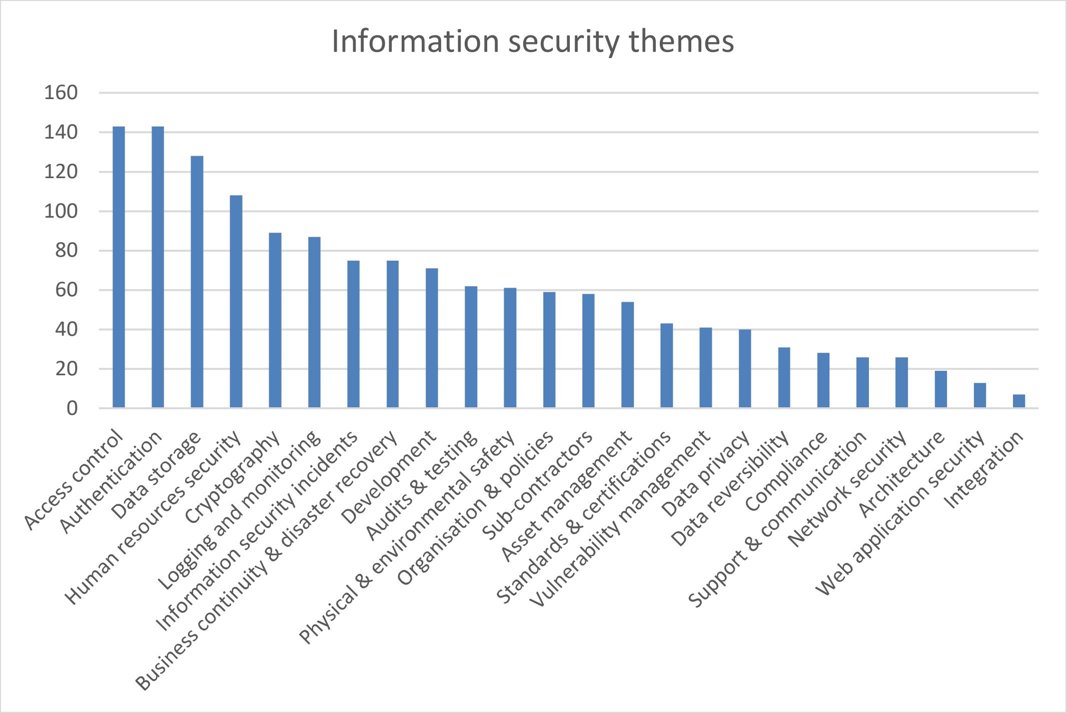

Figure 3 Information security themes from questionnaires

In table 1, I have detailed the most commonly asked questions asked by customers in each information security theme identified in this study. This table serves as the artifact of this study as it details what the most common information security themes are for SoftCo and it also shows what the most commonly asked questions in each theme are.

Table 1 Artifact: Information security themes and questions

Theme	Questions
Authentication	What identification and authentication methods such as single sign on are used? Is there a password policy in place and what are the password requirements? Can the application be accessed remotely e.g., via VPN? Are there controls in place for logon attempt protection? Can each user be uniquely identified?
Access control	Does SoftCo implement privileged access management? What access rights do SoftCo employees have to customer data? Is there a formal access control policy in place? What special access rights do administrators have? Is role provisioning practiced?
Data storage	How often are backups taken and where are they stored? What is the primary data storage location? Does SoftCo have a data retention policy in place? Are customers' data isolated from other customers' data?
Human resources security	What security training do SoftCo employees take and how often? Are background checks performed on SoftCo employees? Do SoftCo employees sign confidentiality clauses in their contracts? Are employee access rights removed upon termination of employment?
Cryptography	What methods are used to encrypt data e.g., TLS or AES? Is data encrypted both in transmission and at rest? How are encryption keys managed?
Logging and monitoring	What logs and audit trails are produced by the system? Can logs be linked to individual users? How long are audit logs retained for? Are security events logged and monitored? Are customer logins monitored?
Business continuity & disaster recovery	Does SoftCo have a disaster recovery plan in place? What is the expected and acceptable downtime of the service? Is there a business continuity management (BCM) clause in place?
Information security incidents	Does SoftCo have an incident response plan in place? What anti-virus and malware products are being used? Is there a intrusion detection and prevention system in place? How many information security incidents have occurred in the past?
Development	Are testing, development and production systems separate? Does SoftCo perform code security reviews? Has SoftCo implemented a patch management program?
Audits & testing	What security and penetration tests are performed and how often? Can these be performed by the customer? How and how often are security audits performed and can the customer perform an audit independently? Does SoftCo have security reports such as SOC1 or SOC2?
Physical & environmental safety	Has SoftCo defined security parameters for critical information and how are they controlled?

	Is physical access to the SoftCo's office restricted and monitored for employees and visitors? What controls are in place to minimize the risk of potential physical and environmental threats, such as fires, floods, and theft? Does SoftCo employ an uninterruptible power supply (UPS)? What controls are in place to ensure security of employee laptops or workstations?
Organisation & policies	How many dedicated information security employees does SoftCo have and what are their responsibilities? Is there a formal risk management and change management program in place? How often are information security policies reviewed and is there an exemption process? Is segregation of employee duties implemented?
Sub-contractors	Are sub-contractors contractually compliant with the same security requirements as SoftCo? Are SoftCo's sub-contractors subject to the same requirements related to information security? Does SoftCo obtain security certifications from third party providers? Will third party providers have access or be provided customer's data?
Asset management	Is there an information classification policy in place? How does SoftCo ensure of the proper deletion and disposal of data both in electronic and physical forms? Does SoftCo use customer data for its own purposes?
Standards & certifications	Does SoftCo have an ISO/IEC 27001 certification? What other certifications does SoftCo have and what regulations does SoftCo comply with?
Vulnerability management	Does SoftCo perform vulnerability scanning and management? What is the remediation process and timeline to fix vulnerabilities?
Data privacy	Does SoftCo store sensitive or personal information? Is SoftCo GDPR compliant or compliant with other data privacy regulations?
Data reversibility	Can data be reversibly transferred back to the customer? Can customer's data be extracted through an Application Programming Interface (API) Is the customer's data provided back to them in an agreed format upon contract termination?
Compliance	What quality guarantees are included in the service level agreement? Does SoftCo guarantee a certain level of data availability in the contract? Does SoftCo and its employees and vendors have a non-disclosure agreement in place?
Support & communication	Are breaches and identified weaknesses communicated to customer? Description of SoftCo's customer support model What is the availability of the helpdesk?
Network security	What controls are in place to ensure network security? Does SoftCo implement network firewall protection? Does SoftCo allow IP whitelisting?
Architecture	Is the service running from a data centre, the cloud, or deployed on-premises only?
Web application security	Does SoftCo implement web application firewalls? Is HTTPS used on web interfaces?
Integration	What configurations are required from the customer to accommodate SoftCo's solution?

Based on the results of the analysis, I have identified three key areas of information security which I will discuss further in the next chapter: shift of administrative control, business continuity and external threats, and auditability and compliance. The division into these three areas came as a result of the literature review and document analysis where I identified these areas to be important concerns for companies contemplating between the shift to cloud computing from traditional IT. One aspects of this shift to cloud computing is the loss of the customers administrative control on the technology and information security. Crucially, companies also want to ensure business continuity and by moving the administrative control to the service provider, they have less visibility on the controls in place to protect their data against external threats which may cause a loss of data and therefore disruptions to operations. Subsequently, since the control shifts from the customer to the service provider, controls must be in place to allow for the auditability of information security and the assurance of the service providers complies with the information security requirements put forth by the customer.

5.2 Shift of administrative control

Where traditional IT infrastructure allows for an organisation to keep digital assets under its administrative control, cloud computing often requires the transfer of digital assets and information to a third-party service provider. This can cause concerns and doubts among stakeholders of an organisation planning to adopt cloud computing services. There are also concerns regarding the number of users that have no relation to the customer's organisation and are not trusted by the customer. (Ali et al. 2015.) Multiple themes found in this study can be interpreted as the customers' attempt to mitigate this concern and control the factors around it. *Authentication* and *Access control* questions which were described in the previous chapter are closely related to this topic as they aim to preserve the confidentiality of the customer's data by ensuring that only authorized personnel have access.

The biggest emphasis related to authentication was on the availability of different authentication methods such as Single sign-on (SSO) and Multi-factor authentication (MFA). It was apparent that customers find it important to have a secure authentication process in place when implementing a new system. The second most frequently asked about topic was the password policy in place which specifies decisions on password policies such as requirements for password complexity, credential sharing and password storage. It was also important for many customers that the system should have the ability to identify users uniquely for access right and auditing purposes. There was also a lot of interest towards the remote access possibilities and if this access is required to have a VPN connection for security. Lastly, it was highlighted that there should be controls in place for logon attempt protection to lock accounts after a certain number of failed attempts and that failed and successful logons should be monitored and logged.

Access control revolved mostly around the access rights and security scopes of users and whether the solution allows for limitation of these rights based on the roles and responsibilities of the user. Apart from only focusing on the capabilities of appropriate access management in the solution, focus was also on the access rights of SoftCo employees and what data they can access. Many customers requested to know if SoftCo has an access control policy in place to address these questions and concerns. Many questions were also related to privileged users and super users who have additional or administrative rights, what these rights are, and how they are monitored and reviewed.

In addition to these themes, questions related to the shifting of information security responsibilities to the provider also occurred in themes such as *Sub-contractors*, *Human resource security*, *Organisation & policies*, *Data storage*, *Cryptography, Asset management* and *Data privacy*.

Both the *Sub-contractors* and *Human resource security* had similarities between them. Both themes contained questions mainly related to understanding who has access to the customer's data outside of the customer's administrative control. In addition to understanding who has access to the data, it was important to understand what access rights these individuals have and what kind of controls are in place to avoid intentional and unintended harmful actions. *Sub-contractors* also included questions related to the compliance of any sub-contractors that SoftCo may have. *Human resource security* contained more detailed questions about how individuals are managed and trained. The most significant topic in this theme had to do with SoftCo employee training and information security awareness. Customers wanted to understand what kind of training employees go through and how often do these trainings take place. Secondly, customers asked frequently if SoftCo performs background checks on its employees prior to employment. It was also important that employee access rights be terminated immediately after their employment with SoftCo ends. Customers also requested information about any confidentiality statements or non-disclosure agreements regarding customer data that employees are made to sign. In addition, customers asked about how compliance with information security policies is enforced and monitored, and if employee logins are monitored.

The *Organisation & policies* theme largely had to do with customers attempting to understand the structure of SoftCo's information security organisation to ensure that there are assigned professionals responsible for information security. In addition, customers inquired about the policies, programs and frameworks in place which promote information security such as the information security policy, formal risk management programs, and IT governance frameworks. *Data storage* and *Cryptography* are both directly related to information being stored outside of the customer organisation's control. *Data storage* was the third most common theme which contained questions regarding the storage of data and its location, how and where data is backed up, and for how long the customers data is stored. The two most commonly asked questions in this theme were related to how customer data is backed up and where the data is stored in terms of physical location. Questions regarding data backups had to with how often data is backed up, are there policies and procedures in place, is backup data stored separately to the main data centre, and how are backups tested and verified. Questions regarding the location of the data storage and main data centre revolved around where customer information resides and what countries are the data centres located in. The third most common topic was the period of time customer data is stored and the retention policy in place for this data. Fourthly, customers wanted to know whether their data was isolated from other customers' data and if SoftCo employed a single-tenant model for data storage and processing. Lastly, questioned the storage of data on removeable media such as flash drives and the security of these devices along with the proper disposal of such data.

Where *Data storage* contains questions inquiring about the security controls to ensure data is stored safely and where the data is stored, *Cryptography* revolved around the secure transmission of data to and from SoftCo. In addition to questions regarding the encryption of data in transit, there were also questions regarding how data is encrypted while at rest when the data is being stored on SoftCo servers. The two most common protocols for securing data with encryption are the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) (Jonsson et al. 2002). Both of these protocols were inquired about and requested that SoftCo use these protocols for data encryption. In addition to inquiring about specific protocols, customers often requested information about any methods and frameworks used for data encryption. Multiple customers also requested information on whether cryptography is used for digital certificate authentication.

Asset management contained mostly questions regarding how the customer's data is deleted and disposed of in a secure and structured manner. The deletion of data concerned both digital data and the physical disposal of external devices containing data and paper documents. The classification of information assets was also inquired about by multiple customers to understand how SoftCo identifies the sensitiveness level of the stored data. Customers were also curious to understand how SoftCo uses customer data and if it is used for any other business cases unrelated to the customer in question. Related to how customer data is handled, classified, and used, is *Data privacy*. This is a clear consequence of transferring data to the cloud service provider as sensitive data of the customer's employees, or their customers may be present in the transferred data. For this reason, the customer must be able to ensure the privacy of the data and that SoftCo is compliant to international data privacy legislation such as GDPR.

5.3 Business continuity and external threats

One clear trend among the questionnaires and subsequent themes was the concern of business continuity, and how the provider prepares and responds to external threats and incidents. As SoftCo stores the customer's sensitive data, it is crucial that this data is protected against both natural disasters and attacks against the provider in order to ensure that the customer's data is available and stored safely, and that the data is not leaked into the possession of a malicious third party. In addition to ensuring that the customers data is safe, the ability of returning the customer's data back from the provider was requested on multiple occasions. Themes where these topics were present were *Business continuity & disaster recovery, Information security incidents, Vulnerability management,* and *Data reversibility*.

The most commonly mentioned question within the *Business continuity & disaster recovery* theme was if SoftCo has a documented and formal disaster recovery plan and if this could be provided to the customer. Formal business continuity plans were also requested and explanations on how SoftCo manages business continuity on the organisational level. There were also multiple inquiries on how and how often SoftCo tests recovery and emergency processes. Another prevalent topic in this theme was the uptime and downtime of the application. Downtime meaning the amount of time when the application is not available to the customer and therefore, they do not have access to their data. Information about downtime statistics was requested along with explanations on what controls are in place to mitigate the downtime and ensure availability of the application and data. Customers also wanted to ensure that SoftCo has insurance in place in the event of a disaster or information security incident.

Information security incidents was an important theme containing the same number of questions as Business continuity and disaster recovery. Questions in this theme had the goal of determining how many information security incidents SoftCo has encountered in the past and what the incident response plan is like. In addition, customers inquired about any possible breaches from outside parties and what controls are in place to protect against any breaches or external threats such as malware and cyber-attacks. Eight customers also wanted to know if SoftCo has intrusion detection systems in place.

Closely related to *Information security incidents* is *Vulnerability management* in which customers' questions were focused on understanding how vulnerability scanning and vulnerability management is performed. It was important for customers that SoftCo actively scans for potential vulnerabilities, documents them, and starts a remediation process to fix the vulnerabilities. It was also important to understand what the timeline is to fix vulnerabilities.

Data storage can also be attributed to the topic of business continuity as it contained questions regarding how and where backups of data are kept. Evidently, this is important when considering for example potential damages to main data centres. Also ensuring that the data centre and back-up data centre are physically separate and have significant distance between them is crucial when protecting against physical threats such as fires, floods, or earthquakes.

Lastly, *Data reversibility* relates to questions regarding the transfer of the customer's data back from SoftCo in the event of contract termination, but this also allows the customer to ensure that data is not only stored in SoftCo's data centre which ensure further data availability in the case of a disaster. In addition to these themes *Organisation & policies* can be linked to the topic of business continuity and external threats as the information security organisation and the employees of SoftCo are responsible for implementing and maintaining proper controls, policies and frameworks to ensure business continuity.

5.4 Auditability and compliance

Ensuring that appropriate information security controls are in place is crucial, but it can also be argued that having the capability to audit the performance of these controls is equally important. (Kwon et al 2011.) It is clear that customers require SoftCo to have adequate security controls in place to ensure the security of its processes and data, it is also apparent that customers value the ability to audit these controls and monitor different processes. It is also important for customers to ensure that SoftCo is compliant with not only the contractual agreement in place, but also that SoftCo adheres to international standards and legislation related to data privacy for example. All themes in this study can be seen as related to compliance with the contract, however, in this chapter the focus is on the controls and processes in place to ensure this compliance not only with the contractual agreement but also with international legislation and regulations. This is represented in such themes as *Logging & monitoring, Audits & testing, Compliance, Support and documentation, Standards and certifications, Data privacy,* and *Development.*

Firstly, *Logging & monitoring* and *Audits & testing* are directly linked to the auditability of information security controls and the security of the application in general. In the *Logging & monitoring* theme, the questions had to do mostly with requests to describe how audit logs are maintained and stored and for how long. Customers wanted to understand what events are logged and stored for them to be traced back and audited at a later time. Also, both customer and SoftCo login monitoring and logging was inquired about in order to monitor who accesses the data. In the *Access control* theme, customers requested that each user be uniquely identifiable, which also has to do with auditability since this way each user can be identified when reviewing audit logs. *Audits & testing* had direct questions related to performing audits and testing. Related to security audits, both customer lead and third-party audits were requested along with the possibility of in person audits on SoftCo's premises. Also questions regarding the reporting of third-party audit results was requested and that audits were carried out according to international standards such as the Statement on Standards for Attestation Engagements 16 (SSAE 16). Customers also frequently requested information regarding the frequency and scope of security tests carried out by SoftCo such as penetration tests, and if the customer would have the right to perform these tests independently.

Standards & certifications have to do with compliance and auditability in the sense that they ensure the customer the SoftCo is compliant with international standards and legislation. The most commonly requested standard that SoftCo be compliant with is the ISO 27001 standard which will be analysed in the next chapter in more detail. Other standards that were requested were the PCI DSS and audit certifications such as SSAE 16 and System and Organisation Controls 1 or 2 (SOC1/SOC2). Multiple customers also inquired about SoftCo's compliance with international data privacy laws such as GDPR which is represented under the *Data Privacy* theme. Additionally in this theme customers wanted to understand in general what sensitive data SoftCo stores, how the sensitive data is identified and processed and if data can be anonymized.

5.5 Comparing results to ISO/IEC 27001

The ISO/IEC 27001 standard, which determines requirements on how businesses can implement a certified information security management system (ISMS) was the most requested standard that customers asked SoftCo to provide a certification for. (Taherdoost 2022.) This standard contains fourteen control clauses which are largely represented in the themes I have identified in the developed artifact. Under each control clause, there are security categories which contain a subset of controls. In its entirety, Annex A contains 114 controls. (Calder 2013.) Understanding the content of the controls sets in ISO/IEC 27001 is relevant to not only understanding what information security requirements customers have for SoftCo but also in understanding how the controls in place correspond to the controls listed in the standard. At least fourteen of the customers analysed in this study inquired about SoftCo's ISO/IEC 27001 certification so it is clear that this is an important topic to customers.

Furthermore, this comparison serves as an evaluation of my findings from this study as is required according to the DSRM process outlined by Peffers et al. (2007). By comparing the identified information security themes with the controls from the ISO/IEC 27001 standard, I am able to show that the identified themes are indeed important to customers as they are also present in the standard. With this comparison I am also able to show that the identified themes are not only present in the questionnaires sent by the customers but are also relevant according to the standard. Although not all of the customers directly asked about a certification for this standard, this comparison also shows that customers had questions relating directly to the control clauses defined in the standard. This further proves to SoftCo that the ISO/IEC 27001 standard certification is crucial to have and for sales professionals to understand.

In the below table, I have compared the themes from the artifact to the control clauses and security objectives from the ISO/IEC 27001 standard. In the first two columns, I have added the control clause and security objectives from the standard. In the third column I have added the corresponding theme from the artifact which includes questions that are directly related to the topics of the control clause and security objective.

Table 2 Information security themes compared to ISO/IEC 27001 control clauses

Control clause: ISO/IEC 27001	**Security objective: ISO/IEC 27001**	**Related themes from artifact**
Information security policies	Management direction for information security	Organisation & policies
Information security organisation	Internal organisation Mobile devices and teleworking	Organisation & policies
Human resource security	Prior to employment During employment Termination and change of employment	Human resources security
Asset management	Responsibility for assets Information classification Media handling	Asset management Data privacy
Access control	Business requirements for access control User access management User responsibilities System and application access control	Access control Authentication
Cryptography	Cryptographic controls	Cryptography
Physical and environmental security	Secure areas Equipment	Physical & environmental security
Operation security	Operational procedures and responsibilities Protection from malware Backup Logging and monitoring Control of operational software Technical vulnerability management Information systems and audit considerations	Data storage Information security incidents Logging & monitoring Vulnerability management
Communication security	Network security management Information transfer	Network security Data reversibility
System acquisition, development, and maintenance	Security requirements for information systems Security in development and support processes	Development

	Test data	
Supplier relations	Information security in supplier relationships Supplier service delivery management	Sub-contractors
Information security incident management	Management of information security incidents and improvements	Information security incidents Support & communication
Information security aspect of business continuity management	Information security continuity Redundancies	Business continuity & disaster recovery
Compliance	Compliance with legal and contractual requirements Information security reviews	Audits & testing Standards & certifications Compliance Data privacy

Firstly, out of the fourteen control clauses, Operations security, and Access control, could be allocated clearly the most questions and themes presented in this study. However, given that these control clauses contain the most security categories, this was not a surprising finding. Operations security contains controls regarding e.g., data backups, change management, separation of environments, protection against malware, logging and monitoring, vulnerability management, and information systems audit considerations. All of these controls were prevalent in the themes found in this study across numerous separate questionnaires. The themes from the artifact that contain these questions on these controls are *Data storage, Information security incidents, Logging & monitoring,* and *Vulnerability management.* Provided that *Authentication* and *Access control* were the two largest themes which I identified in this study, it is not surprising that it is also noticeable when comparing against the control clauses in the ISO/IEC 27001 standard. These two themes had a combined total of 286 questions through all of the questionnaires, which can be allocated to the Access control -control clause. This control clause included controls regarding topics such as access control policy, user access management, user responsibilities, and authentication and log-on methods. As discussed earlier, these topics were very important to customers of SoftCo in ensuring access to only individuals who need it and that there are secure authentication methods.

The remainder of the control clauses were divided more evenly with Human resource security; Information security organisation; System acquisition, development, and maintenance; Cryptography; Asset management; Communications security; Information security aspects of business continuity management; and Physical and environmental security, each containing between 63 to 110 questions.

Human resource security had very similar controls listed in the standard as in the identified theme *Human resources security,* where customers also asked questions related to employee trainings on information security during employment, background checks prior to employment and access right removal upon contract termination. Both Information security organisation and Information security policies contract clauses contained similar topics to the *Organisation & policies* theme where I had combined these to topics to belong under a single theme. There were multiple similarities between the theme and the two contract clauses including topics related to the information security employees of SoftCo, the occurrence of information security policy reviews, and segregation of employee duties. For the System acquisition, development, and maintenance control clause, I was able to identify relevant topics from both *Development* and *Support & communication* themes. Here *Development*, contained topics related to the secure development of the software such as ensuring a secure development environment, protection of test data and implementing secure engineering principles and development policies. The Cryptography control clause contained largely the same as the theme, *Cryptography*, where questions regarding e.g., encryption methods and encryption key management were also listed as controls in the standard. Asset management was also similar to the artifact's theme *Asset management* where both included topics related to information sensitivity classification, ownership and responsibility of assets and media handling. However, I also identified that *Data privacy* contained questions related to SoftCo handling and identifying sensitive information from the customer's data. The communications security control clause contained topics from three different themes: *Network security* and *Data reversibility. Network security* was closely related to the Network security management security objective with similarities in what network controls are in place and the security of network services. *Data reversibility* was in turn closely related to the Information transfer security objective with both containing topics related to the secure transfer of information from SoftCo to the customer. This control clause also contains controls regarding confidentiality or nondisclosure agreements; however, I have included these requirements under the *Human resources security* theme where requirements related to employee contracts are included. The Information security aspects of business continuity management contract clause, contains similar topics to the

Business continuity & disaster recovery theme. Where both covered topics related to the continuity of business operations and information security for example by ensuring the availability of information processing facilities. The Physical and environmental security control clause was closely related to the *Physical & environmental security* theme where I had included customer requirements related to the physical security of SoftCo's offices and protection against environmental threats such as fires and floods. Additionally, both the control clause and the information security theme contained topics related to the security of SoftCo's equipment such as laptops and workstations.

The four smallest control clauses in this study were *Supplier relations, Information security incident management, Compliance,* and *Information security policies,* where each control clause contained less than 50 questions. This result is not entirely surprising as these four control clauses are also relatively small in the ISO/IEC 27001 standard where *Supplier relations* and *Information security policies* contain two security objectives and *Information security incident management* and *Information security policies* only contain 1 security objective each.

From the Supplier relations control clause, I identified similarities with the *Sub-contractors* theme, where questions regarding the information security requirements of sub-contractors and suppliers was also highlighted in the control clause. The Information security incident management contract clause contained same topics as included in the *Information security incidents* and *Support & communication* themes. For *Information security incidents*, the shared topics with the contract clause were related to how SoftCo responds to information security incidents, what procedures are in place and information on past incidents that SoftCo has experienced. In the *Support & communication* theme, I included topics on what topics SoftCo is required to communicate to the customer and these topics included information security incidents which is related to this control clause. The Compliance control clause was related to three of the themes from the artifact: *Compliance, Audits & testing,* and *Standards & certifications.* This control clause contained controls on legislative and contractual requirements, compliance with security policies and standards, and independent reviews of information security. These topics were present in the three themes listed above. In addition, this control clause contains a control on the privacy and protection of personally identifiable information which is related to the *Data privacy* theme where I have included requirements on e.g., GDPR compliance and the handling of personal data.

It was somewhat surprising that control clauses such as Supplier relations and Information security incident management were among the least inquired about control clauses, but the related themes are among the most inquired about. However, upon further examination of the results it is clear that the reason for this is that in the ISO/IEC 27001 standard, these control clauses are indeed more specific and contain less controls. With other control clauses I have found links with multiple different themes which increases the perceived importance of these control clauses such as

I was not able to identify the *Integration* and *Architecture* themes in any of the control clauses in the standard. I would argue that these themes do not indeed contain information security requirements that could be translated to information security controls as these themes contained mostly questions on how the application is deployed and what steps does the customer need to take to accommodate the application. These questions were mainly for the knowledge of the customer's IT department and do not directly translate to any information security requirements. Additionally, I was not able to identify controls on *Web application security*. This was a fairly specific theme and did not contain many questions compared to other themes and is specific to service providers whose application is accessed through the web.

6 Discussion

The questions collected from the questionnaires and the subsequent themes they are categorized under, are in line with what existing literature in this field has found to be the most important topics for organisations. The themes identified in this study and the analysed questionnaires represent the most common concerns that have been raised in literature on the topic of information security in general and also on information security specifically in cloud computing.

6.1 Information security themes and the CIA model

The CIA definition, provided in the ISO/IEC 27002 standard, has been regarded as the industry standard when discussing information security. This definition refers to the process of ensuring the confidentiality, integrity, and accessibility of information. Where this information can take many forms, be it physical, electronical, or transferred through speech. (Solms et al. 2013.) In this definition, confidentiality means that individuals or entities do not have access to information without the required permission. The integrity of information refers to the accuracy and completeness of the information. Lastly, availability mean that the information can be accessed and used when needed by an entity with authorization (Lundgren et al. 2017) Comparing the CIA definition of information security to the findings of this study, it is evident that these three areas of information security are present in the questionnaires.

Firstly, confidentiality is strongly present in the questionnaires and in the themes and can be linked directly or indirectly to most of the largest themes identified in this study. It is evident that confidentiality is an important topic to customers who are planning on storing, transmitting, and processing information outside of the organisation's domain. Two themes, *Access control* and *Authentication* which were the two largest themes in this study can be directly linked to the topic of confidentiality. In both themes, the goal of the customers was to understand how SoftCo ensures that only individuals with permission have access to their data. In *Access control* the emphasis is ensuring that there are controls in place to ensure who can access the data and ensure that these individuals are clearly defined. Questions under *Authentication* on the other hand emphasised how these individuals are authenticated to ensure that these authentication methods provide a secure manner for only defined individuals to access the data. In addition, in *Logging and* *monitoring*, customers wanted to ensure that there are controls in place to log events and monitor who has access and makes changes to the data. This can be used to ensure that indeed only the defined individuals have accessed certain information when auditing this topic. Also, both *Human resource security* and *Sub-contractors* relate to this topic as both themes contained questions regarding who can access the data outside of the customer's organisation and what controls are in place to monitor and secure this access. *Data privacy* is also linked to the confidentiality of data as this theme contained questions regarding how SoftCo protects sensitive information from being access by unauthorized parties. *Information security incidents* and *Vulnerability management* both relate to the confidentiality of data in the sense that these themes contained questions about the controls SoftCo has in place to ensure that outside parties don't get access to the data and that any vulnerabilities which may lead to this, are detected and rectified in an appropriate time frame.

Secondly, where integrity refers to the accuracy and completeness of the information, multiple themes can be linked with this area of information security such as: *Logging and monitoring, Development, Support and documentation,* and *Audits and testing*. Firstly, *Logging and monitoring* is related to the integrity of data as this theme contained questions pertaining to the ability to monitor and trace access and actions by individuals. By ensuring that there is an audit trail to track back with, SoftCo is in a better position to ensure that data has not been for example tampered with. In the *Development* theme, questions relating to the separation of testing and production environments are linked to the integrity of data as with this separation, SoftCo can ensure that any developments or updates which affect the customers data, are first tested in a separate environment from the production environment visible to the customer. This way SoftCo can ensure that data integrity is not compromised due to a faulty or accidental update. Thirdly, *Support and documentation* can be linked with data integrity as this theme contained questions related to the customer support model and helpdesk. This support is crucial to be in place for the customer to be able to contact SoftCo in instances where they detect incorrect data in their environment. The offered support is therefore important in maintaining data integrity. Lastly, *Audits and testing* indirectly affects the integrity of customer data as this theme contained topics related to the controls and processes in place to ensure that the customer can audit SoftCo's processes. By having these auditing processes in place, the customer can ensure independently that data integrity is upheld by SoftCo.

Lastly, availability of data was reflected in the following themes: *Data storage, Business continuity & disaster recovery, Data reversibility,* and *Compliance.* Firstly, since *Data storage* contained questions pertaining to the storage of customer's data and how this data is backed up, this can be linked to the availability of data. Questions regarding how and where data is stored in relation to the customer's location and also to the backup location. By ensuring that the data is stored in a secure and separate location to the backup location, the customer can ensure that they have access to their data in the event of a disaster for example which in turn results in a more assured data availability. Question regarding the location of the data storage were important to customers inquiring about the availability of that data globally in different locations. *Business continuity and disaster recovery* contained questions relating to how SoftCo has prepared for disasters and how it ensures business continuity. This of course relates to data availability as ensuring proper controls are in place to recover from disasters also results in customer's data is not being lost in the event of a disaster. In this theme customers also directly inquired about the uptime levels that SoftCo is promising for the software and therefore for how long the customer can expect to not have access to their data in a given time period. *Data reversibility* related to data availability since this theme contained questions about how SoftCo can transfer the customer's data back to the customer. This can happen in the event of ending the contract or simply if a customer has concerns about having the data only stored on SoftCo's servers. This is one way the customer can ensure that they at least have access to the data if for some reason the data would be lost by SoftCo. The *Compliance* theme contained questions related to service level agreements which are in place to ensure that the agreed levels of uptime are met in accordance with the contractual agreement in place.

6.2 Information security themes and cloud computing

Where it is shown that the questionnaires represented the common findings from academic literature on the subject of information security, the findings are also largely in line with the discussion around information security in cloud computing and the SaaS service model in particular.

NIST (2011) defined five key characteristics of cloud computing: on-demand self-service, resource pooling, broad network access, rapid elasticity, and measured service. In addition, the Cloud Security Alliance has also added multi-tenancy to the list of defining characteristics. (Ali et al. 2015.) Out of these characteristics, broad network access is present also in the discussion surrounding information security in cloud computing, as this broad access to the data also introduces new issues with access control and legislative issues depending on the geographic location of the data and the user. In addition, resource pooling and multi-tenancy, which are great benefits of cloud computing, also introduce some concerns surrounding information security. Since, computing resources are shared among different customers, and the customer's data can be in close physical proximity to other customers' data, there are concerns regarding access control. In addition, having your data stored in the same physical location with another customer who might be subject to a higher risk of attacks, this puts your data in jeopardy also. These issues were addressed by customers especially in the *Data storage* theme where customers wanted to ensure that their data is separated from others'.

Dikaikor et al. (2009) listen security and privacy as one of the five key challenges that cloud computing faces. This notion was also echoed by Ali et al (2015) who emphasized the importance of solving the information security issues related to cloud computing to achieve wider adoption. They also noted that companies can face reluctancy to shift from traditional IT to cloud computing as this requires the transferring of digital assets to outside service providers. This notion is clearly visible in the questionnaires and as discussed under chapter 5.2, can be detected in the themes: *Sub-contractors*, *Human resource security*, *Organisation & policies*, *Data storage*, *Cryptography, Asset management* and *Data privacy*.

Rane (2012) listed eight high level security concerns that the SaaS deployment model faces in regard to information security: the nature of the SaaS deployment model, Data security, Network security, Regulatory compliance, Data segregation, Availability, Backup, Identity management and sign-on process. Each of these highlighted security concerns were addressed in the questionnaires sent to SoftCo and were indeed of high importance to the customers analysed in this study.

Out of these eight security concerns, the deployment model appeared to be of least importance as in this case the deployment model is a private cloud where the service is provided only to a specific customer and other's do not have access to their environment. Data security was raised by customers repeatedly which can be seen in the number of questions under *Information security incidents*, where customers wanted to understand if SoftCo has faced any breaches or incidents in the past and what controls are in place to prevent this in the future. Along with the deployment model concern, network security also was one of the least inquired about out of the twenty-four themes. However, it still emerged as a theme and at least half of the customers had one question related to the network security of SoftCo. Regulatory compliance was raised by multiple customers in this study where customers wanted to understand what regulations and laws SoftCo complies with. These included regulations and laws such as GDPR and other privacy acts from the United States. It was also of importance for the customers to understand where their data is being stored so they know what laws and regulations apply. Data segregation was represented in the *Data storage* theme as customers wanted to ensure that their data was both physically and logically separated from other customers data. Availability was inquired about many times where customers wanted to gain insights into the uptime of the service and also from which countries the data can be accessed. This is also linked with backups which were also highly inquired about by customers. Customers wanted to ensure that their data is backed up securely and separately from the main data storage facility. Ensuring that data is backed up properly customers can also ensure that there won't be long periods of data unavailability. Lastly, Identity management and sign-on process was of perhaps most interest to customers which is represented by the number of questions asked in the *Authentication* theme. Here, customers wanted to ensure that proper authentication and sign-on methods are being used to ensure that only those who should have access to the data can access it and that each user can be identified uniquely.

7 Conclusions

In this study my aim was to understand what the most common information security requirements are for SaaS companies by analysing the customer questionnaires regarding information security of the subject organisation SoftCo. In order to gain a deeper understanding of the topic, I reviewed academic literature from the fields of information security and cloud computing. I gathered a literary review on the topics of information security, cloud computing, and information security in the cloud computing paradigm. In addition, I reviewed how companies assess the information security risks for outsourced IT services such as SaaS services. By gathering this information, I was able to establish a basis for the further analysis on SoftCo's information security requirements. It was also crucial for me in understanding the complex topics which were addressed in the information security questionnaires which were used as the data set for this study.

The main research question of this study was, what are most common shared information security requirements for SaaS companies?

I was able to answer this question by designing and creating an artifact which contained the twenty-four information security themes including the most asked questions from each theme. I created this artifact by analysing the information security questionnaires sent to SoftCo by customers. I performed this document analysis by assigning the questions into twenty-four themes around different information security topics. The artifact demonstrates not only what information security themes are important to customers, but also shows how these themes compare to one another. The largest themes and therefore the four most important topics to customers were: *Authentication, Access control, Data storage,* and *Human resource security.* This was in line with my expectations of customers being especially wary of handing over their data to a third-party software provider whose employees will have access to their data. The findings of the study were also in line with the ISO/IEC 27001 standard which is the most highly requested standard related to information security for SoftCo. Almost all of the control clauses defined in the standard could be identified in the questionnaires and were clearly a point of interest to SoftCo's customers.

One possible shortcoming of this analysis is that the results may not be applicable to companies assessing the information security of different kinds of software. SoftCo's software, is based largely on gathering the customer's potentially sensitive data and performing analysis and analytics on this data. Due to this reason, customers may have emphasized the importance of access control and authentication more than they would with another software which does not gather the customer's data in such a scale and detail. The questionnaires in used in this study were also from large international organisations so the results could vary with a pool of questionnaires from smaller sized organisations.

Further research could be done on this topic by taking a smaller pool of customers and performing qualitative interviews where customers are asked in detail questions about their information security requirements. This would allow for a deeper understanding on the reasoning behind different prioritizations which I have identified in this study. This study could also be replicated with subject organisations operating in different fields as the nature of the provided service can affect the results of the study.

References

Akinrolabu, O. – Nurse, J. – Martin, A. – New, S. (2019) Cyber Risk Assessment in Cloud Provider Environments: Current Models and Future Needs. *Computers & security,* Vol. 87

Alam, T. (2020) Cloud Computing and its role in the Information Technology. *IAIC Transactions on Sustainable Digital Innovation*, Vol. 1(2), 108–115

Ali, M. – Khan, S. – Vasilakos, A. (2015) Security in cloud computing: Opportunities and challenges, Information Sciences, Vol. 305, 357–383

Aljabre, A. (2012) Cloud computing for increased business value. *International Journal of Business and social science*, Vol. 3(1)

Atif, A. – Maynard, S.B. – Park, S. (2014) Information Security Strategies: Towards an Organisational Multi-Strategy Perspective. *Journal of intelligent manufacturing,* Vol. 25(2), 357–370

Banker, R. – Chang, H. – Kao, Y.-C. (2010). Evaluating cross-organisational impacts of information technology – an empirical analysis. *European Journal of Information Systems*, Vol. 19(2), 153-167

Bojanc, R. – Jerman-Blažič, B. (2013) A quantitative model for information-security risk management. *Engineering management journal*, Vol. 25(2), 25-37

Brumă, L.M. (2021) Cloud security audit–issues and challenges. *16th International Conference on Computer Science & Education (ICCSE),* 263-266

Bulgurcu, B. – Hasan, C. – Izak, B. (2010) Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS quarterly,* Vol. 34(3), 523–548

Calder, A. (2013) ISO27001 / ISO27002: a Pocket Guide. Vol. 2, *Ely, Cambridgeshire, United Kingdom: IT Governance Publishing*

Currie, W. – Seltsikas, P. (2001) Exploring the supply-side of IT outsourcing: evaluating the emerging role of application service providers. *European Journal of Information Systems*, Vol. 10, 123-134.

Dikaiakos, M. – Pallis, G. – Katsaros, D. – Mehra, P. Vakali, A. (2009) Cloud Computing: Distributed Internet Computing for IT and Scientific Research. *IEEE internet computing,* Vol. 13(5), 10–13

ENISA (2016), Definition of cybersecurity – gaps and overlaps in standardization, <www.enisa.europa.eu/publications/definition-of-cybersecurity>, accessed 5.8.2022

Gartner (2019) Cloud Shift Impacts All IT Markets <https://www.gartner.com/smarterwithgartner/cloud-shift-impacts-all-it-markets> accessed 24.6.2022

Goodman, S.E. – Ramer, R. (2007) Identify and mitigate the risks of global IT outsourcing. Journal of Global Information Technology Management, Vol. 10(4), 1-6.

Gordon, L. – Loeb, M. – Sohail, T. (2010) Market value of voluntary disclosures concerning information security. MIS Quarterly, Vol. 43(3), 567-594.

Höne, Karin, and J.H.P. Eloff. “Information Security Policy — What Do International Information Security Standards Say?” Computers & security 21.5 (2002): 402–409. Web.

Horne, Craig A., Sean B. Maynard, and Atif Ahmad. “Organisational Information Security Strategy: Review, Discussion and Future Research.” AJIS. Australasian journal of information systems 21 (2017)

International Telecommunications Union (ITU). ITU-TX.1205: series X: data networks, open system communications and security: telecommunication security: overview of cybersecurity 2008.

Ismail, Umar Mukhtar, and Shareeful Islam. “A Unified Framework for Cloud Security Transparency and Audit.” Journal of information security and applications 54 (2020): 102594–. Web.

ISO (2005) ISO/IEC 17799:2005. <https://www.iso.org/standard/39612.html#:~:text=ISO%2FIEC%2017799%3A2005%20establishes,goals%20of%20information%20security%20management>, retrieved 16.4.2022

Iyer, Bala – John C. Henderson. “Preparing for the Future: Understanding the Seven Capabilities of Cloud Computing.” MIS quarterly executive 9.2 (2010): 117–131.

Jonsson, Jakob, and Burton S. Kaliski. “On the Security of RSA Encryption in TLS.” ADVANCES IN CRYPTOLOGY - CRYPTO 2002, PROCEEDINGS 2442 (2002): 127–142. Web.

Karlsson, F. – Kolkowska, E. – Prenkert, F (2015) Inter-organisational information security: a systematic literature review. *Information & Computer Security*, Vol. 24 (5), 418-451.

Khalfan, A. (2004) Information Security Considerations in IS/IT Outsourcing Projects: a Descriptive Case Study of Two Sectors. *International journal of information management* Vol. 24(1), 29–42.

Khidzir, N.Z. – Mohamed, A. – Arshad, N.H. (2010) Information security risk factors: critical threats and vulnerabilities in ICT outsourcing. *2010 International Conference on Information Retrieval & Knowledge Management*, 194-199.

Knapp, J. – Gary, D. – Barner, M. (2011) Key Issues in Data Center Security: An Investigation of Government Audit Reports. *Government information quarterly,* Vol 28(4), 533–541

Kuzminykh, I. – Ghita, B. – Sokolov, V. – Bakhshi, T. (2021) Information Security Risk Assessment. *Encyclopedia*, Vol. 1(3), 602-617.

Kwon, J. – Johnson, E. (2011) The impact of security practices on regulatory compliance and security performance. *International Conference on Information Systems 2011*

Layton, T.P. (2016) Information Security: Design, implementation, measurement, and compliance. *Auerbach Publications*.

Lundgren, B. - Möller, N. (2019) Defining Information Security. *Science and engineering ethics* Vol. 25(2), 419–441

Marston, S. – Li, Z. – Bandyopadhyay, S. – Zhang, J. – Ghalsasi, A. (2011) Cloud computing — The business perspective. *Decision Support Systems*, Vol. 51(1), 176–189

Mell, P. – Grance, T. (2011) The NIST Definition of Cloud Computing, *Recommendations of the National Institute Standards and Technology*

Nassimbeni, G. – Sartor, M. – Dus, D. (2012) Security Risks in Service Offshoring and Outsourcing. *Industrial management and data systems,* Vol. 112(3), 405–440

NIST (2011) The NIST Definition of Cloud Computing, <https://www.nist.gov/publications/nist-definition-cloud-computing> accessed 25.6.2022

Peffers, K. – Tuunanen, T. – Rothenberger, M. – Chatterjee, S. (2014) A design science research methodology for information systems research. *Journal of Management Information Systems,* Vol. 24(3), 45-77

Raković, R. (2021) Project of ISMS Implementation in Organisation — Aspects and Practical Experiences. European project management journal Vol. 11(1), 20–30

Rasheed, H. (2014) Data and Infrastructure Security Auditing in Cloud Computing Environments. *International journal of information management,* Vol. 34(3), 364–368

Rashid, A. – Chaturvedi, A. (2019) Cloud Computing Characteristics and Services: A Brief Review. *International Journal of Computer Sciences and Engineering*, Vol. 7(2)

Sangseo, P. – Ruighaver, T. (2008) Strategic Approach to Information Security in Organisations. *2008 International Conference on Information Science and Security (ICISS 2008). LOS ALAMITOS: IEEE, 2008*, 26–31

Scholl, M. – Stine, K. – Hash, J. – Bowen, P. – Johnson, A. – Smith, C.D. – Steinberg, D. (2008) An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. *NIST Special Publication 800-66 Revision*

Shojaie, B. – Federrath, H. – Saberi, I. (2013) Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A. *Ninth International Conference on Availability, Reliability and Security,* 259-264

Shojaie, B. – Federrath, H. – Saberi, I. (2014) Evaluating the effectiveness of ISO 27001: 2013 based on Annex A. *2014 Ninth International Conference on Availability, Reliability and Security*, *IEEE*, 259-264

Sveen, F.O. - Torres, J.M. – Sarriegi, J.M. (2009) Blind Information Security Strategy. *International journal of critical infrastructure protection* Vol. 2(3), 95–109

Taherdoost, H. (2022) Understanding Cybersecurity Frameworks and Information Security Standards-A Review and Comprehensive Overview. *Electronics (Basel),* Vol. 11(14)

Thalmann, S. – Bachlechner, D. – Maier, R. (2012) Security management in cross-organisational settings: a design science approach. *ICIS 2012*, Vol. 41

Thomas, C. (2012) Practical approaches to supply chain continuity: new challenges and timeless principles. *J. Ross Publishing, Fort Lauderdale, USA*

Tipton, H. – Krause, M. (2012) Information Security Management Handbook*,* Vol. 5, *Boca Raton, Fla: CRC Press*

Tipton, H. – Krause, M. (2012) Information Security Management Handbook. Vol. 6, *Boca Raton: Auerbach Publications*

Von Solms, B. – Von Solms, R. (2018) Cybersecurity and Information Security – What Goes Where? *Information and computer security*, Vol. 26(1)

Von Solms, R. – van Niekerk, J. (2013) From Information Security to Cybersecurity. *Computers & security*, Vol. 38, 97–102

Weil, T. (2020) Risk Assessment Methods for Cloud Computing Platforms. *IT professional* Vol. 22(1), 63–66

Whitman, M.E. – Mattord, H.J. (2013) Management of information security. *Cengage Learning*

Whitman, M.E. – Mattord, H.J. (2021) Principles of information security. *Cengage learning*