UNIVERSITY OF TURKU

Classified Information in Cloud Services

New Era of Cyber Security

Cyber Security
Master's Degree Programme in Information and Communication Technology
Department of Computing, Faculty of Technology
Master of Science in Technology Thesis

Author:
Kris Papaleonidas

Supervisors:
Jouni Isoaho
Antti Hakkala

June 2025

Master of Science in Technology Thesis
Department of Computing, Faculty of Technology
University of Turku

Subject: Cyber Security
Programme: Master's Degree Programme in Information and Communication Technology
Author: Kris Papaleonidas
Title: Classified Information in Cloud Services – New Era of Cyber Security
Number of pages: 55 pages, 16 appendix pages
Date: June 2025

This thesis explores the changes of cyber security in the context of classified information in cloud services. The research investigates the technical, legal, and risk management challenges associated with the adaptation of cloud infrastructure for processing classified information within the government. The focus is on the European Union, with a specific emphasis on Finland.

The motivation for the thesis is motivated by the rapid and recent changes in our society that has re-shaped our way of working. COVID-19 pandemic and geopolitical events such as the war in Ukraine, which have underscored the importance of cyber security measures in government held classified information. Furthermore, these changes have forced governments to restructure on how to handle classified information in a world that is online and fast-paced. Through a combination of literature review, structured surveys, and semi-structured interviews with government officials, the research examines the current state of cyber security and technology, laws on classified information and cyber security, the implementation of cloud services in governments, and the associated risks and benefits.

The main findings show that the use of cloud services has increased significantly in the EU, both among businesses and government actors. This poses unique challenges in the field of cyber security, including ensuring data protection and compliance with national and EU regulations and laws. The study concludes that classified information can be processed securely in a cloud environment, provided that strict cyber security measures are sufficiently considered and implemented. It is important to do a comprehensive assessment and risk management.

Keywords: Cyber Security, Cloud Security, Classified Material, Classified Information, Government, Data Protection, Remote Work, Hybrid Work, COVID-19, Risk Management, National Security, Legal Frameworks

Table of Contents

1 Introduction

"It is not the strongest of the species that survive,
nor the most intelligent,
but the one most responsive to change."
- Charles Darwin

In today's digital age, technology has become an integral part of our daily lives and has brought about many benefits in terms of convenience, communication, and access to information. However, with the increasing dependence on technology an increased need for cyber security has emerged. (Gordon et al., 2015) There are many definitions of "Cyber security", and we will discuss it in different ways and from different angles in this thesis. One of them is defined as the "practice of protecting networks, devices, and sensitive information from unauthorized access, use, disclosure, disruption, modification or destruction." (Bezzi et al., 2012) One thing is sure, as the use of technology continues to evolve and expand, the threat of cyber-attacks also increases.

Cloud infrastructure has become extremely popular and almost necessity amongst businesses. (Wang & Wang, 2020) Businesses seek to reduce their costs across the board and IT costs are not something to overlook. If the business is old, there usually are legacy systems that may be considered to move to cloud. Reasons are cost, scalability, flexible and collaboration capabilities. Same things are sought in government, but it becomes tricky in some aspects – classified information. Businesses can mitigate their exposure to cloud computing risks, when it comes to operational, technology or data and regulatory risks. Governments on the other hand have different kind of problem when dealing with these risks and are greatly exposed in vendor-lock type situation or nation lock. This can be a political issue in some cases, and it needs special attention.

This thesis will explore the current state of cyber security laws and technology used in the cloud infrastructure to process classified information in the European Union with key focus in

Finland. The thesis will focus on the legal, technical, and briefly touch on the political aspects that govern cyber security and processing of classified information in the cloud infrastructure. The thesis will also examine the challenges and risks associated with handling classified information in conventional information systems and cloud-based environments, as well as the impact of remote and hybrid work on cyber security and the role of confidentiality agreements in protecting classified information.

1.1 Motivation

I started my academic path in 2018, with the purpose of acquiring in depth knowledge in the computing field, cyber security, and management. My strength lied in the forensic investigation and security sector of the information and technology world with more than ten years in experience from Finnish law enforcement and countless certifications around the world. At the time of writing Europe's political and economic environment is at somewhat chaos and the very least it's uncertain. In 2019 a contagious disease began to spread which ultimately led to a global pandemic. (*WHO*, 2022b) This virus was called " *Coronavirus disease 2019 or COVID-19* " (*WHO*, 2022a) and it had devasting effect on the population, health and economic sectors. Business had to re-organize the way of business overnight which put huge pressure towards technology and security of it. Remote and hybrid work became the new normal for business and industries alike. Once again, the criminals saw an opportunity like no other and they started exploiting the situation in numerous ways. On one hand a study conducted by Nivette showed that COVID-19 restrictions resulted in larger declines in crime, but the crimes were more of the conventional assault, robbery and burglary. (Nivette, 2021) On the other hand, Interpol, Europol and various news sources indicate that fraud conducted over the internet, selling ads for counterfeit goods and various types of scams are booming. (Silverberg & Smale, 2021) (Knutson, 2020) (Europol, 2021) (Interpol, 2021) Business, governments, and the people have had little time to adapt to the new environment and cybercrime is testing everybody's limits – and not everyone is holding.

While cyber security was put to a test on all fronts by COVID-19, the importance of systems and network security took a major role in business core. After the invasion of the Ukraine on

24 February 2022 by Russia, Europe and the world were plunged into unknow and uncertainty. This time cyber security played a whole different role. There have been previous uses of cyber warfare on a state level, but I believe it never has been anything like this. Mis- and disinformation flooded all social media platforms (Smith, 2022) (Mittal, 2022), and denial-of-service and concentrated malware attacks are constant (Madnick, 2022) (Microsoft, 2022) (Symantec, 2022) (Eset, 2022). Shortly EU responded with help to Ukraine by putting together a Cyber Rapid-Response Team (CRRT) to aid in cyber security issues. (Tidy, 2022) Online seems to be a big part of the war today, and this has governments thinking. What happens if we lose all our network capability? Or if the enemy has access to our classified information? Who can we trust to hold our classified information and not use it against us? Business leaders, and heads of companies began to rethink their companies and government risk management plans, especially the cyber security aspects. And as a consequence, the topic of this thesis suddenly became, a relevant topic.

1.2 Research Questions

In this this we'll examine current situation and future needs of the government for processing classified information. When talking about processing in the thesis, it will mean collection, storage, sorting, analysis and presentation of data. I will evaluate cloud technology benefits and risks that might be related to cloud environment. I will focus on Finnish government, but I will reflect these aspects at the European level. I will try to find risks associated with processing of classified information in the cloud environment and present how these risks can be mitigated through literature, structured and semi-structured surveys that consist of expert and leading specialist interviews.

The research questions in this thesis are:

Research question 1:
What are the associated challenges and key factors for processing classified information in a cloud environment?

Research question 2:
What are the current restrictions or limitations when processing classified information in a cloud environment?

Research question 3:
What are the potential risks associated with processing classified information in a cloud environment, and how can they be mitigated?

Research question 4:
What modifications or improvements are necessary in technology to enable secure processing of classified information in a cloud environment?

Also, a hypothesis is set:

Classified information can be processed in a cloud environment,
if proper cyber security, data protection and risk management has been implemented
and political relations are handled by government officials.

This study consists of seven parts. The introduction outlines the objectives and structure of the thesis and provides motivation for the thesis. In order to test the research questions and hypothesis, a comprehensive and versatile approach is needed. As a first step, we review the literature selected in the literature review, which deepens the discussion and broadens the perspective on the topic under discussion. The selection in the literature review addresses or touches the topics, research questions, or hypothesis that are central to the thesis. By delving into the, we aim to seek practical experiences or case studies from the world and evaluate research questions based on them and thereby enriching our evaluation of the thesis. Additionally, we aim to obtain a broad and comprehensive overview of existing research and

identify gaps in current knowledge base. Ultimately, the literature review aims to form a foundation for our answers to research questions and conclusions.

Chapters 2 to 4 present a literature review, which reviews the most relevant issues for the thesis. We will review the issue from the perspective of cybersecurity, technology, legislation and regulations, and risk management. The chapters examine the handling of classified information in cloud services by examining cybersecurity frameworks and practices, the development of cloud technology, relevant legal frameworks at the Finnish and European levels, and strategies for managing the associated risks. Together, they create a fundamental understanding to answer the research questions and evaluate the hypotheses. The methodology section covers chapters 5 to 6, where we review the topic area through interviews. In addition, we extract the content of the surveys and reflect on their results in the literature. We analyze the collected data and aim to answer the research questions and confirm or refute the hypothesis. We also aim to identify general trends, concerns, and best practices in this field. Chapter 7 discusses the results of the thesis, analyzes the collected data, and answers the research questions and hypotheses based on insights from the literature, surveys, and interviews. Chapter 8 concludes the thesis with a summary of the key results, evaluating the hypothesis, and presenting recommendations for the future development of secure cloud-based processing of classified information.

2 Government Implementation of Cloud Services

The reader is presumed to possess a basic understanding of most of the definitions presented herein. This chapter will delve into the evolution of and into the change of technology in the government. The timeline comparing its state approximately six years ago to present state or from 2019 to 2025. Additionally, an examination of the COVID and other relevant changes in the EU will be examined.

2.1 Overview of Cloud Services

There are several sources for defining cloud computing and origin can be traced back to the idea of utility computing, which was proposed by computer scientist John McCarthy back in 1961. Thomas Erl provides a detailed introduction to the defining cloud computing and he writes that cloud computing represents a specialized iteration of distributed computing, introducing novel utilization models for remotely provisioning scalable and measured resources. (Erl et al., 2013, p. 58) This includes servers, storage, databases, networks, software, analytics and different kinds of intelligence all done over the internet – the cloud. There are three primary types of service layers in cloud computing, with each layer providing specific services tailored to particular market segments.

However, according to the organization's own unique business-and-operational-and-technical requirements, cloud environments can be established according to individual organizations' needs. There are four distinctly different strategies for cloud environment deployment. These include deploying clouds as (1) public clouds, (2) private clouds, (3) hybrid clouds, or (4) multi-clouds. Public clouds are environments whose infrastructure is owned and operated by a third-party provider and offered to multiple organizations or the general public over the internet. (Sehgal & Bhatt, 2018, p. 2-3) The services provided are available to any individual in the public cloud environment, and maintenance and security are cared for by the provider who is responsible for the proper management of such infrastructure. Private clouds are owned and operated by a single organizational entity, primarily for its exclusive use. A private cloud can

reside either on an organization-owned physical site or be managed by a third-party service provider. A hybrid cloud combines public and private clouds, whereby an organization utilizes a public cloud for selected workloads and private cloud for others. Organizations use this combination to take advantage of the scalability and affordability of cloud computing in tandem with governance and quality over sensitive data and applications. While multi-cloud refers to the ascent of services from several cloud providers, in a multi-cloud environment, the organization will leverage resources and services from different cloud providers. This enables some degree of flexibility, letting organizations sidestep vendor lock-in, optimize costs and establish or take advantage of the strengths and capabilities of various vendors according to different workloads or geographic areas. Though it entails intense management and integration challenges. (Sehgal & Bhatt, 2018, 41-44)

LEVEL	DESCIPTION
INFRASTRUCTURE AS A SERVICE - IAAS	Comprises hardware components, such as virtualized servers, storage, network devices, etc. It typically denotes a virtualized environment wherein services facilitate the connectivity and functioning of cloud platforms and applications.
PLATFORM AS A SERVICE - PAAS	Tools for software and product development (e.g., servers for applications, servers for databases, servers for portals, middleware, etc.) that clients lease in order to construct and implement their own applications tailored for their individual needs.
SOFTWARE AS A SERVICE - SAAS	Preconstructed, functionally autonomous, vertically integrated, and widely available to users as services. These encompass email systems, human resource management tools, payroll processors, and various other application processes

Table 2.1 Variants of cloud computing (Mahmood & Hill, 2011, p. 7-9))

Looking at Table 2.1 and comparing it to existing cloud strategies, the following distinction can be made. SaaS applications are ideally suited to public cloud services, where scalability and cost-effectiveness are key objectives. Public clouds can also leverage IaaS and PaaS to avoid the costs associated with on-premises infrastructure, but the organization must rely on the service provider if the information is to be widely utilized. Private clouds, on the other hand, offer better control, making them suitable for the deployment of IaaS and PaaS, as they allow the organization to maintain the infrastructure and manage the development environment

internally. This strategy increases flexibility, optimizes the existing infrastructure, and enables the implementation of broader cybersecurity controls.

In recent years, numerous of vendors providing cloud technology have emerged, each with a unique perspective on the market. Some companies specialize in offering fundamental cloud storage solutions, others concentrate on providing comprehensive workflow management services. Additionally, there are vendors that tailor their offerings to meet the unique needs of specific industries or niche markets with industry specialized solutions. At present, the landscape of cloud services is predominantly shaped by three major industry players: Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure. (Slingerland, 2024) These leading providers have established themselves as pillars in the realm of cloud computing, offering a comprehensive suite of services and solutions tailored to meet the diverse needs of businesses and organizations worldwide. With their extensive global infrastructure, robust security protocols, and innovative technologies, AWS, GCP, and Azure continue to drive the evolution and adoption of cloud computing across various industries and sectors.

2.2 Implementation of Cloud Services in the EU

Shifting government agencies and European businesses to cloud computing is a major focus of the European Union's digital strategy. In the introduction to its digital strategy, the European Commission states, "The European Commission aims to provide European businesses and public authorities with access to secure, sustainable and interoperable cloud infrastructures and services." Increasing access to edge devices is also an important part of this strategy. (EU Commission, 2024) The European Commission is implementing this strategy in a number of ways, including:

> *Infrastructure:* Spending on the Important Project of Common European Interest (IPCEI) that "will federate energy-efficient and trustworthy cloud infrastructures and related services." (EU Commission, 2022a)
>
> *Software:* Promoting, SIMPL, an open-source 'middleware' to enable cloud-to-edge 'federations.' SIMPL is mean to be the main software used by ED-funded data spaces.

Regulatory guidance: The EU planned to set a series of rules and frameworks governing the implementation of data processing services. The guidelines are meant to "provide a single European framework relevant binding and non-binding rules for cloud service users and providers in Europe." (EU Commission, 2024a)

Data regulations: The EU has also passed two regulations related to cloud services. The Data Act aims to make it easier to switch between cloud service providers. (EU Commission, 2022b) A second regulation is aimed at ensuring the free flow of non-personal data. (EU Commission, 2024b)

Data privacy and cyber security: In keeping with another law, the Cyber security Act, the European Union Agency for Cyber security (ENISA) is in the process of developing a cyber security certification program for cloud services that can be used for businesses and public agencies. The program is focused on protecting personal data.

The COVID-19 pandemic has accelerated the adoption of cloud services in both the business and public in Europe. According to the European Data Protection Board (EDPB), "In the public sector, the COVID-19 pandemic has intensified a digital transformation of organisations, with many public sector organisations turning to cloud services." (European Data Protection Board, 2023) In addition to "speed, scalability, agility and cost-effectiveness" cloud computing also offers privacy and security, cyber security, features that are beneficial to governments, even though there are several security, and cyber security issues to be concerned. (Alenizi et al., 2021) These features helped pave the way for the broader adoption of cloud computing during the COVID-19 pandemic, when remote work and other alternatives to the traditional office environment were necessary. (Dwivedi et al., 2020) Cloud computing remains relevant today, particularly as a vehicle for implementing the EU's digital goals, and for the deployment of AI technologies.

In its report, the EDPB identified protection of personal data in keeping with EU regulations as a major challenge during this process, prompting the agency to launch a formal review of member states' use of cloud services. As part of their investigation, the EDPB offered a snapshot of the extent to which cloud services have been implemented throughout EU-member states. In the snapshot approximately 100 public agencies were subject to the review,

highlighting the broad scope of the investigation. One major buyer of cloud computing services was found to have 150 public bodies as clients, which illustrates the extensive network of cloud service utilization in some areas. Also, the number of entities using cloud services, including agencies and information systems, increased by 37% and the utilization of existing capacity for cloud services rose from 54% to 73%. (European Data Protection Board, 2023) This indicates a substantial improvement in the efficiency and effectiveness of cloud service deployment. Furthermore, the EDPB identified government agencies using cloud services spanned various sectors, including health, finance, taxation, education, infrastructure, and justice. The agencies involved in the review represented approximately 20 member states and the cloud service providers involved in this extensive network included major companies such as Microsoft, Amazon, Citrix, IBM, OVH, Fujitsu, Oracle, Adobe, and Google. This diversity in application underscores the versatility and critical importance of cloud services in supporting a wide range of public functions and services. And although the report does not directly mention classified information, it can perhaps be assumed that most of the information, at least cumulatively, meets the criteria for classified information. Nevertheless, it has been decided to move to the cloud, where the risk-benefit ratio is balanced. The involvement of these prominent providers highlights the significant role that leading technology companies play in the provision of cloud services to public agencies within the EU. (European Data Protection Board, 2023)

A survey of 98 government stakeholders revealed that a vast majority – 87 in total – used cloud services or had plans to by the end of 2022, “reflecting the ever-increasing use of CSPs by public authorities.” Most cloud service users, 66 out of the 87, relied on the technology for internal operations like office suites, internal communication and human resources while 48 had integrated cloud services into the delivery of public services, or handling of citizen data. About half of these agencies – 35 – held “regular risks assessments.” (European Data Protection Board, 2023)

2.3 Remote and Hybrid Work

As the COVID-19 pandemic lockdown forced individuals to confine themselves to their residences, what was once deemed unfeasible became achievable. This change happened

overnight, and no one was prepared. Companies and governments had to modify their operations, processes and practices to make remote and hybrid work possible. This meant a very rapid change and adaptation as organizations and governments implement new technologies and strategies to ensure continuity and productivity in the new era. The speed and scale of the changes were unimaginable, highlighting need for resilience in both public and private sectors in the face of global crisis.

Survey done by the Statistics Finland indicate that cloud-based services are on the rise. Their survey conducted in spring 2022 indicate that more than 80% of enterprises used cloud based services. (Statistics Finland, 2022) [1] Furthermore investigation to the statistic the use of security software applications as a cloud computing service was over 70% in large[2], 55% and over in mid-size[3] and small[4] and almost 50% in micro[5] companies. Same can been seen in other countries. In Germany cloud computing has grown from 16% in 2016 to 33% in 2023. (*Statistics Germany*) In Estonia cloud computing has grown from 22% in 2016 to 58% in 2023, with a significant spike in from 33,8% in 2018 to 57,1% in 2020. (*Statistics Estonia*) This highlights a significant an rapid growth in the adoption of cloud computing services among the enterprises around EU. While the surveys do not explicitly outline the reasons behind this rapid growth, one could argue that recent global changes have played a significant role. The COVID-19 pandemic, for instance, forced many organizations to rethink their operational strategies, leading to an accelerated shift towards digital solutions. The need for remote work capabilities, enhanced security, and scalable infrastructure has driven many enterprises to adopt cloud computing as a viable solution.

One clear outcome of this shift is the gradual disappearance of traditional server infrastructure. As cloud computing becomes the new normal, enterprises are moving away from on-premises servers in favor of more flexible and cost-effective cloud solutions. This transition not only offers improved efficiency and scalability but also aligns with the growing demand for digital

[1] Variables:" Use cloud services, % of enterprises"; 2015-2023, Total
[2] 100 or persons
[3] 50 to 99 persons
[4] 20 to 49 persons
[5] 10 to 19 persons

transformation in the modern business landscape. The rise of cloud computing marks a significant evolution in the way enterprises manage their IT infrastructure. The rapid growth observed in recent surveys underscores the importance of cloud services in today's digital age. As traditional servers become a thing of the past, cloud computing stands out as the cornerstone of modern enterprise operations, driving innovation and resilience in an ever-changing global environment.

2.4 Government Digitalization

A 2021 European Commission report states that the COVID-19 pandemic has significantly increased digitalisation in EU member states. "The COVID-19 pandemic has brought turbulence, but also increased resilience and innovation. It has accelerated the digitalisation of the EU economy and society, including the way government services are delivered." (European Commission, 2021)

The EU Member States and around ten other countries (including EU candidate countries and the UK) were ranked according to the maturity of their digitalisation process. The ranking criteria included; (1) user-centricity, (2) transparency, (3) key enabler, and (4) cross-border services. In addition to support these criteria, questions were asked:

1. To what extent are services provided online? How mobile-friendly are they? And what online support and feedback mechanisms are in place?
2. Do public administrations provide clear, openly communicated information about how their services are provided? Are they transparent about decision-making and the design of digital services and the way people's personal data is processed?
3. Which technology enablers support the delivery of e-government services?
4. How easily can foreign citizens access and use online services?

(European Commission, 2021)

Based on these, the report concludes that considerable progress has been made in the digitalisation of public administration services. Although differences or gaps have been observed at different levels of government and across various types of services. The report reveals that 85% of all services provided by public administration organisations are available online. However, some government levels are clearly lagging behind others. When looking at regional and local services, only 74% of services were available digitally, compared to 59% for regional and local services. The same gap is also visible when comparing services for businesses and citizens. The report states that 91% of services for entrepreneurs can be performed digitally. Conversely, only 59% of services for citizens are available online. The disparity in key technologies, such as electronic identification (eID) solutions, is even wider. Electronic identification (eID) solutions are available to entrepreneurs 78% of the time, while citizen services are available 56% of the time. (European Commission. Directorate General for Communications Networks, Content and Technology. et al., 2021)

The report also highlights that entrepreneurs are more likely than citizens to obtain and submit electronic documents. 86% of business-related documents are processed digitally, while only 67% of citizen-related documents. The report cited unemployment services as an example, where eight out of ten registered unemployed people were able to apply for benefits digitally. On the other hand, new businesses were able to obtain or receive a new tax card in 94% of cases, compared to only 81% two years ago. Similarly, registering with their country's social security office was successful digitally in 91% of cases, compared to 81% previously. (European Commission. Directorate General for Communications Networks, Content and Technology. et al., 2021)

While the benchmark does not specifically measure cloud implementation, it is a useful proxy for it, as cloud services are widely considered essential for the effective digitalisation of government services. The average digitalisation rate in the 36 countries studied was 68%. Finland, Sweden and Estonia exceeded the European average of 85%, 92% and 75%, while Germany was slightly behind, at 62%. Overall, Finland and Estonia stand out as the biggest adopters of digitalisation, ranking fourth and second among the countries studied. (European Commission. Directorate General for Communications Networks, Content and Technology. et al., 2021) However, the gap between services for entrepreneurs and citizens, which is 22

percentage points, or one fifth (entrepreneur services 91% vs. citizens services 59%), is striking. This, in my opinion, highlights the need for more inclusive digital strategies that serve the wider population and would promote access to services. Furthermore, the report shows a significant gap in digital readiness and implementation capacity between the state and municipalities, which could be of great importance in the future as digitalisation progresses, both in terms of usability and cybersecurity. These statistics show that while significant progress has been made in the digitalisation of business services, the gap in citizen services still needs to be closed. The report also shows that the COVID-19 pandemic has acted as a catalyst for digital transformation in the EU, significantly contributing to the availability and accessibility of online government services.

2.5 Cloud Services Implementation in the UK Government

The United Kingdom adopted a 'cloud-first' for technology and government services in 2013 and has made significant progress in the ensuing decade. The move to cloud services, in the government, as well as in business, accelerated during the COVID-19 pandemic. (*Government Cloud First Policy*, 2023) Amazon Web Services has a £894 million contract for cloud services with three major government agencies in the UK – Her Majesty's Revenue and Customs (HMRC), the Department for Work and Pensions (DWP), and the Home Office. The three agencies are Amazon's three largest public-sector cloud customers in terms of spending. The DWP planned to operate 70% of its infrastructure out of the public cloud by the end of the 2023-2024 fiscal year. (Computer Weekly, 2024) By 2021, HMRC had "600 services hosted on over 7,000 servers in legacy data centres." By the 2023-2024 fiscal year, the department had moved 372 of 545 critical services to the cloud. That represents a migration of about 70% of services to the cloud. (Butler, 2024) The UK Visas and Immigration, and Immigration Enforcement directorates of the Home Office has adopted cloud technology to streamline the visa application process. By leveraging cloud technology, these agencies have increased the efficiency of their operations, enabling faster processing times and better data management. This technological shift has not only modernized their approach but has also brought significant financial and cyber security benefits. Overall, the agencies have achieved a significant cost saving of 40% or an estimate of 2 million pounds per year, demonstrating the significant savings

and added value that cloud technology can bring to government operations. (*UK Home Office, 2025*)

3 Laws on Cloud Services and Classified Information

This chapter presents an examination of the legal and regulatory frameworks that apply to cyber security and management of classified information in traditional information systems and cloud-based settings. In order for the government to work it needs to have comprehensive security protocols and systems to protect its sensitive material. Classified material is defined by the European Unions classified information (EUCI). EUCI defines that any material that can cause varying degrees of harm to the interest of the EU or any of its states is to be considered classified information. The level of classification can vary, but it is divided into four categories: *RESTRICTED*, *CONFIDENTIAL*, *EU SECRET*, and *EU TOP SECRET*. (European Union, 2013/488/EU) Classified material can be in various forms, including documents, emails, databases, and images, and it is stored in conventional information systems, cloud-services, or hybrid systems. The way to handle this kind of information has to be in compliance with laws, acts, regulations and guidance's to ensure the security and protection of the classified material. (*Council Decision 2013/488/EU on the Security Rules for Protecting EU Classified Information*, 2013)

Laws are the most formal and binding form of legal instrument. They are passed by a legislative body (such as a parliament) and are intended to be binding on all citizens and organizations within a jurisdiction. Laws often carry penalties for non-compliance. (Al-Faham et al., 2019). Acts are similar to laws, but they are typically passed by an executive branch of government (such as a president or prime minister). They are also binding, but they typically focus on specific policy areas or issues. (Al-Faham et al., 2019) Regulations are issued by a government agency or regulatory body and are intended to provide detailed rules and standards for a specific area of policy. They are often used to implement laws and acts, and they typically carry penalties for non-compliance. (Al-Faham et al., 2019) Guidance's are non-binding and provide information and advice on a particular subject. They are often issued by government agencies and are intended to help organizations and individuals understand and comply with laws and regulations. They do not carry penalties for non-compliance, but they can be used as evidence in enforcement actions. (Al-Faham et al., 2019) A rough distinction in the context of cyber security is that laws, acts, and regulations aim to safeguard citizens and organizations from cyber-attacks and to prevent unauthorized access, use, disclosure, disruption, modification, or

destruction of information. Guidance's are intended to help organizations follow the laws, acts, and regulations and to secure their systems and data.

3.1 National Level – Finland, Sweden and Estonia

In the section I'll do a comparative analysis of three key Finnish laws and their equivalents in Sweden and Estonia. I'll focus on Data Protection Act (Tietosuojalaki 1050/2018, 2018), Act on Information Management in Public Administration (Tiedonhallintalaki 906/2019, 2019), and Act on the Openness of Government Activities (Julkisuuslaki 621/1999, 1999). Finland, Sweden, and Estonia have developed comprehensive legal frameworks to ensure the protection of personal data, efficient information management, transparency in government activities, and these laws make the base for the guidelines and recommendations for processing classified information in cloud environments.

All three countries have almost identical data protection laws, which are based on the EU's General Data Protection Regulation (GDPR) and are actually quite similar. The Finnish Data Protection Act aligns with the EU's GDPR, providing a robust framework for the protection of personal data and privacy. (General Data Protection Regulation (GDPR) – Official Legal Text; Tietosuojalaki 1050/2018, 2018) In Sweden, the equivalent law is the Data Protection Act (Dataskyddslagen 2018:218, 2018), which also supplements the GDPR. This act ensures that personal data is processed lawfully, fairly, and transparently, with specific provisions for the rights of data subjects and the obligations of data controllers and processors. Estonia's equivalent is the Personal Data Protection Act (Isikuandmete kaitse seadus 2018, 2018). Similar to Finland and Sweden, this act is designed to comply with the GDPR, ensuring the protection of personal data and the rights of individuals regarding their personal information.

As the Finnish Act on Information Management in Public Administration states:

> "…
>
> 1) ensure the uniform and high-quality management and secure processing of authorities' data in order to implement the principle of openness;
>
> 2) enable the safe and efficient use of authorities' data so that the authority can perform its tasks and provide its services to administrative customers in a productive and high-quality manner, while adhering to good governance;
>
> 3) promote the interoperability of information systems and data resources
>
> …" (Tiedonhallintalaki 906/2019, 2019)

The purpose is to ensure high-quality and secure information, or proper cyber security measures, while also enabling open public administration. Similarly to Finland, Sweden has the Public Access to Information and Secrecy Act (Offentlighets- och sekretesslag 2009:400, 2009). This act governs the management and accessibility of public information, balancing the need for transparency with the protection of classified information. In Estonia, the Public Information Act (Avaliku teabe seadus 2000, 2000) has similar functions, regulating the management and opening of information to the public through the safeguarding of security and integrity in data information. Estonia does not have its own information management law, but the above-mentioned one is equivalent to it. Correspondingly, however, Finland and Sweden have decided to separately enact their own publicity laws: The Finnish Act on the Openness of Government Activities (Julkisuuslaki 621/1999, 1999) and The Sweden's Freedom of the Press Act (Tryckfrihetsförordning 1949:105, 1949). These laws determine what is public and open. In principle, all administrative activities are public, and everyone has the right to obtain information, if they wish, on how public power is used, this also includes data. (Mäenpää, 2020)

While Finland, Sweden, and Estonia have developed their own legal frameworks to address data protection, information management, transparency, and how to handle classified information there are significant similarities due to the influence of EU regulations such as the GDPR. Each country has implemented government openness and as Mäenpää states that the

availability and usability enhances government openness. The importance of openness is also emphasized by the fact that the EU relies on open European government in its operations. (Article 298 of the TFEU) (Mäenpää, 2020) Each country has tailored its laws to fit its national context, but the overarching goals of protecting personal data, ensuring efficient information management, and promoting transparency remain consistent across these nations. Open data is public data that is made freely available; it significantly improves transparency. Public authorities promote this by opening their data interfaces, provided it is not precluded by legitimate options. This is instructed by the Open Data Directive (2019/1024/EU).

3.2 Laws and Technology

One of Lessig's key arguments is that while technology and the internet have made it possible for people and businesses to connect and collaborate on a global scale, this has also led to a number of legal and regulatory challenges. (Lessig, 2000) For example, laws and regulations on cyber security vary greatly from country to country, making it difficult for companies to comply with all the different requirements. Additionally, issues such as intellectual property, privacy, and cyber security are also affected by the global nature of technology and the internet. Lessing argues that in order to effectively address these challenges, it is important to take a holistic approach that takes into account both local laws and global technology. (Lessig, 2000) This means that companies and governments need to be aware of the different laws and regulations that apply in different jurisdictions, and to work together to develop solutions that take into account the unique context and needs of each location. In Lessing’s work, Lessing also emphasizes the importance of international cooperation in addressing cyber security issues, and the need for governments and private sector to work together to develop effective responses to cyber-attacks. Lessing also highlights the importance of balancing security (cyber security) and privacy concerns, and the need to ensure that any measures taken to protect against cyber threats do not unduly infringe on individual rights and freedoms. Overall, Lessing's work highlights the complex and constantly evolving nature of technology law and policy, and the need for an integrated and collaborative approach to addressing the challenges and opportunities presented by global technology and the internet. (Lessig, 2000)

Lawrence Lessig's cyber exploration shows that four puzzles are central in rendering behaviour regulation in cyberspace. Regulability, translation, intellectual property, and privacy are combined, and each field holds different challenges of cyber security and protection of classified information. Regulability resolves the question of whether cyber space can even be regulated. Lessig contends that the so-called "architecture of the internet" (or "code") stands in as a form of regulation just as environmental law does. (Lessig, 2000) This is most relevant of all the puzzles to cyber security because, after all, how do you go about creating and enforcing a sanction to protect against hacking, data breaches, and other forms of cyber espionage? Other forms of cybercrime? The implementation of GDPR within the context of the EU can be seen as informing how legal frameworks have been modulated to control the unique quagmires of cyber space, imposing certain standards for the protection of personal data and privacy. Translation takes place in this context as the embedding of old tort law into all things cyber. Traditional legal principles do not apply directly to cyberspace, therefore necessitating a gentle conceptual push to address the more pressing issues of digital privacy, of data protection, and of cybercrime. All of these types of issues are extant, and once again, these are occurrences in the universe of contemporary cybercrime, where cyber security requires updates for existing laws in cyberspace application. Most people understand that the CFAA originally was enacted in the year of 1986 and has been variously amended in reaction to new intelligences and evidences showing developments in many kinds of cybercrime; this represents an ongoing translation from traditional legal concepts to match the realities of any cyber space context.

3.3 Case Ukraine – Drastic Change in the Digital Field?

Russia's war against Ukraine illustrates how cloud services not only can help ensure the security of classified information, but they can also be vital to their preservation. When Russia invaded Ukraine on Feb. 24, 2022, not only they targeted its land, military units, and physical infrastructure, it also planned to deliver a debilitating strike against the government buildings that housed the servers where classified information was stored. (White, 2022) The missile strike was coordinated with a Russian cyberattack. Both failed – because Ukraine had already moved its classified information (data) out-of-country thanks to cloud storage. As one industry publication noted, "The data which had once singularly been stored on physical servers, had been uploaded to the cloud." (White, 2022) The transition had taken place just a week before

the election and had required a state law prohibiting the use of cloud services be amended by parliament. (Microsoft, 2022)

On the day of the invasion, Ukrainian authorities asked Amazon Web Services for Snowball devices. According to Amazon, Snowballs are “secure, rugged devices” that allow computing and storage capabilities to be used in ‘edge environments’ and facilitate the transfer of data in and out of the Amazon cloud. By July, 10 petabytes of data from the government, along with universities and private companies had been transferred to the cloud. For Ukraine, the benefits of cloud computing and storage extend beyond national security considerations. For example, the cloud also enabled students to complete their annual exams at the end of the school year and ensure property records are not lost. (Amazon) In its report on Ukraine and cloud services, “Defending Ukraine: Early Lessons from the Cyber War,” Microsoft identified a series of lessons from the conflict. A key finding was that states should decentralize their digital operations and data assets across borders to counter physical threats as well as cyber threats. Microsoft highlights in its report that early in the conflict, Russia launched physical attacks (cruise missiles) on data centers aimed at disrupting critical operations. This exposed the weakness of the traditional on-premises servers, where server relies on physical infrastructure to function. Ukraine’s reaction to these risks was to swiftly relocate its digital infrastructure into the cloud, with hosting services distributed all over Europe. This move, despite the ongoing Russian attacks, was strategic in allowing the government to sustain both civilian and military functions. By relocating data stores, including classified information, to the cloud, Ukraine reduced the risk of losing critical data due to physical destruction or local cyberattacks. In contrast to on-premises systems, cloud infrastructure is dynamically scalable and updatable, which was essential to Ukraine. This allowed for operations to be sustained under intense pressure. For Ukraine, this innovative technology was crucial to enabling them to stay connected to vital systems amid relentless threats and assaults. Furthermore, the efficiency of cloud cyber security is further increased by the addition of AI technologies. Microsoft claims that, through their devices and global services, they are able to analyse 24 trillion signals on a daily basis which creates a dataset that allows for faster detection of anomalies. Such ability is especially important in the case of advanced persistent threats (APTs), in which an enemy embeds malicious code to exfiltrate data slowly over extended periods of time. (Microsoft, 2022)

The rapid change in and successful adaptation of cloud services in Ukraine also highlights their role in enabling rapid recovery from cyberattacks. Cloud infrastructure facilitates organizational recovery from an cyberattack and ensures minimal downtime due to off-site backups and distributed systems (Shackelford et al., 2019). This was the case in Ukraine's ability to thwart data wipe malware, which was indented to erase all data. The incident was prevented by cloud-based redundancies, as the Microsoft report reveals (Microsoft, 2022). However, challenges remain. For instance, over-reliance on major cloud-service providers can lead to systemic risks such as single points of failure. Furthermore, smaller countries may struggle to access advanced cloud technologies due to high cost or infrastructure constraints (Kshetri, 2020). These issues and gaps need to be further explored to ensure secure and global adoption of cloud systems.

Another significant advantage of cloud services is the ability to strengthen cyber security against offensive operations done by criminals or hostile nations. Microsoft reports that while some Russian cyberattacks were successful, Ukraine's cloud-based cyber security measures generally exceeded the attacker's capabilities, and the malicious attempts were blocked. The system was combined with endpoint protection, where computer networks are remotely bridged to client devices. This enabled the rapid distribution of cyber security software to devices of all type. Furthermore, this system enabled Ukraine to quickly identify and neutralize malware, limiting the damage caused by wipe attacks. For example, Microsoft describes an incident in Lviv, where a Russian wipe malware attack targeted a company system. Microsoft Defender with Cloud Protection detected and blocked the malware by leveraging artificial intelligence (AI) models that leveraged a wide network of cloud and device interaction signals. This rapid response highlights the ability of cloud ecosystems to process real-time data and adapt to new threats. (Microsoft, 2022)

Ukraine's experience shows that cloud services are revolutionizing cyber security by providing resilience, rapid threat detection, and AI-enhanced defences that are not possible, at least in terms of scalability, in a traditional on-premises environment. As technology and cyberattacks evolve, moving away from on-premises to cloud infrastructure will become increasingly important to protect classified information and maintain business continuity.

4 Digital Security Framework – Cyber Security

Firstly, let us decompose the term “cyber security”. The prefix “Cyber” itself does not mean anything, but rather it’s used as an adjective within the context of a compound word. (*Kyberturvallisuuden Sanasto (TSK 52)*, 2018) (*Cambridge Dictionary*) In Morten’s article titled "What is cyber security?", Morten emphasizes that the term transcends individual cyber security needs. Instead, it delineates the broader requirements of organizations, nations, or the global economy. Subsequently, its interpretation becomes somewhat subjective, varying depending on the perspective of the individual being queried:

Ministry of the Interior – Finland

“Cyber security is one of the targets of national security. The aim is to protect the increasingly digital society and society’s ability to function against hostile cyber attacks and intelligence gathering on information networks.” (*Cyber Security - Ministry of the Interior*, n.d.)

EU cyber security act (*Regulation - 2019/881 - EN - EUR-Lex*, n.d.)

“Cyber security includes the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.”(*Cyber security*, 2023)

Cyber security & Infrastructure Security Agency – CISA

“Cyber security is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.” (*What Is Cyber security?*, 2021)

Microsoft

"Cyber security is a set of processes, best practices, and technology solutions that help protect your critical systems and network from digital attacks." (*What Is Cyber security?*)

Kaspersky

"*Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security."* (*What is Cyber Security?*, 2023)

As we can see the perception of cyber security varies among individuals, encompassing distinct perspectives. For some, it represents an ultimate achievement; for others, it unfolds as an iterative and dynamic process. Simultaneously, certain individuals regard cyber security as a strategic array of technology choices, each contributing to a sophisticated defence strategy. As for me cyber security is not somethings you can achieve, but a collection of technology and practices that are constantly evolving and at the centre lies human.

4.1 Risk Management Relations to Cyber Security

Risk management is a systematic process that involves examining potential threats, determining their reality and impact, and implementing strategies to manage those risks. Numerous studies and sources address cloud security from a various perspective. According to Jansen and Grace, security issues fall into six categories; 1) Trust, 2) Architecture, 3) Identity Management, 4) Software Isolation, 5) Data Protection, and 6) Availability. (Jansen & Grance, 2011) This thesis will focus on trust, data protection, and availability, which are crucial to my opinion when considering the storage of classified information in the cloud. Cloud service providers are usually trusted and this places the in a difficult position, where they are not entirely transparent about their cyber security practices. (Chen et al., 2019)

As discussed, and demonstrated in the previous chapter, the shift to remote and hybrid work is here to stay and has therefore brought new cyber security threats and challenges from a risk management perspective. With employees working from different locations, with the high possibility of using unsecured networks or personal devices with inadequate security features, the attack surface for cybercrime has significantly expanded. Also, the level of competence of each employee contribute to the causes of cyberattack. (Aslan et al., 2023) One of the most prominent threats in remote and hybrid work is traditional phishing emails. Criminals exploit organizations' dependence and reliance on email and other digital communications to trick employees into, among other things, revealing classified organizational information. These phishing attacks have become sophisticated, and with artificial intelligence, their effectiveness continuous to grow. The increase in phishing incidents during the COVID-19 pandemic highlights the need for new, more effective email security measures and employee training to identify and report suspicious emails. The threat is deepened by the use of unsecured networks, as these usually do not meet the organizations' cyber security standards or policies. This poses significant challenges from a risk management perspective. (Bispham et al., 2022)

Phishing attacks have highlighted the shortcomings of weak passwords and poor authentication practices. Employees tend to use simple and reused passwords for multiple accounts, which makes it easier for a criminal or attacker to gain access to systems or into the organization. Solutions such as multi-factor authentication (MFA) have been developed to address these issues, which is commonplace in cloud services. However, MFA is not a permanent solution, but a temporary measure. Additionally, employees are also increasingly aware of technological developments themself, and therefore the use of unauthorized applications and services has increased. For the sake of convenience or ease, employees may bypass or ignore organizations' cyber security policies or guidelines by using unapproved software and thereby creating new cyber security holes.

5 Research Design

5.1 Approach and Data Collection

The research design of this thesis was structured on the utilization of a qualitative methodology, where two types of studies were conducted: structured survey and semi-structured interviews. The exploration and understanding of the complexity of the thesis topic requires in-depth analysis and interpretation, which has been attempted through both a written review, expert semi-structured interviews and structured surveys. This has helped to understand the subject area further and has facilitated the comprehensive investigation of the research questions and hypothesis that were presented at the begin. By employing qualitative methods, the study sought to delve into the underlying meanings inherent in the subject matter, thereby enabling a rich and detailed exploration of the phenomena under scrutiny. Furthermore, I hope that the gathered data and thesis, can serve as valuable resources for future investigations and discussion in the government and education sector.

5.1.1 Semi-Structured Interview – Thematic Interview

The thesis main study was qualitative semi-structured interview or a thematic interview[6]. While the term "thematic interview" is less prevalent in English discourse, the concept aligns closely with what is commonly referred to as a semi-structured interview. In a thematic interview, questions may not be precisely formulated in advance or consistently presented in the same format. Instead, the researcher typically immerses themselves in relevant literature, selects their own perspective and questions, and identifies central themes for the research. Subsequently, the interviewer crafts questions freely around these identified themes. The appeal of thematic interviews lies in granting interviewees the freedom to express themselves, facilitating a more natural dialogue. Analysing thematic interviews is also relatively straightforward, focusing on extracting insights based on the identified themes. (Hirsjärvi & Hurme, 2008)

[6] Finnish: teemahaastattelu.

Thematic interviews took place over video conference sessions spanning from 23.3.2023 to 31.12.2024, with the aim of conducting a total of 20 interviews. This structured timeframe ensured sufficient data collection to explore the research topic thoroughly. By engaging participants through video conferencing, I sought to gather diverse perspectives and insights from different governments bodies. This included the following ministries and their agencies:

- Prime Minister's Office
- Ministry for Foreign Affairs
- Ministry of Justice
- Ministry of the Interior
- Ministry of Defence
- Ministry of Finance
- Ministry of Education and Culture
- Ministry of Agriculture and Forestry
- Ministry of Transport and Communications
- Ministry of Economic Affairs and Employment
- Ministry of Social Affairs and Health
- Ministry of the Environment

This approach was chosen to facilitate a comprehensive understanding of the subject matter, allowing for a nuanced analysis of the gathered data. The target amount of 20 interviews was considered achievable, but adequate to this thesis objectives. Additionally, the objective was to have interviews that included a range of roles and positions within governmental organizations, facilitating a diverse and inclusive perspective. This deliberate approach aimed to capture a broad spectrum of insights and experiences, enriching the depth and comprehensiveness of the research findings. By engaging individuals from different positions within government work, the study sought to incorporate a variety of viewpoints, thereby enhancing the overall richness and validity of the research outcomes. Material, power point, was used to facilitate the interviews (Appendix 4), which contained helper slides on the subject and provided the context for semi-structured interview.

5.1.2 Structured Survey

Structured surveys served as a supplementary approach to data collection within this thesis, enhancing the depth and reliability of the research alongside the thematic interviews. Through the strategic utilization of structured surveys alongside thematic interviews, a more holistic perspective was attained, contributing to a robust and nuanced exploration of the research subject. This dual-method approach not only enriched the data gathered but also ensured triangulation, thereby strengthening the validity of the study's conclusions.

The structured was conducted using Microsoft Forms platform, which was an easy and simple way for data collection. The survey was published to participants between 8.4.2024 to 31.7.2024, allowing a generous timeframe for response to be gathered. The aim was achieving a minimum of 100 answers and preferably over 200 answers for a sufficient range of data. The survey was sent to:

- Prime Minister's Office
- Ministry for Foreign Affairs
- Ministry of Justice
- Ministry of the Interior
- Ministry of Defence
- Ministry of Finance
- Ministry of Education and Culture
- Ministry of Agriculture and Forestry
- Ministry of Transport and Communications
- Ministry of Economic Affairs and Employment
- Ministry of Social Affairs and Health
- Ministry of the Environment

The survey (Appendix 3) was sent via email along with a message (Appendix 2), aimed to inspire and encourage participation for the survey.

5.1.3 Ethical and Security Considerations

As this was a thesis of cyber security and related to classified information, ethical and security considerations were of utmost importance. The thematic interviews were recorded and transcribed to make way for an accurate analysis of data. All interviews received an anonymization so that confidentiality and privacy for the participants were assured. The interviews were conducted on video conference by using the Microsoft Teams or Zoom platforms. This ensured a secure means of discussing and capturing the interview. All recordings were saved to manually managed personal computers and cloud services, all of which had very strong authentication requirements. In terms of data storage, the original recordings were kept containing personal data that would be retained until the completion and acceptance of the thesis. Yet, a date of the 31st of December 2024, was pinpointed for the destruction of any data that contained personal information. Other data storage practices of the thesis conform with the practices of University of Turku in the sense of adhering to the ethical and legal standards regarding data management. All these procedures were presented to the interviewees, who were required to verbally consent to them.

5.2 Additional Analysis Procedures

The methodology included a review of raw data. In this approach, the data was analysed manually to find insights and further to investigate the theme at hand. The analysis was continuously matched against the pre-established aims of the thesis, questions and hypothesis, and a literature offset to ascertain their relevance. Thus, this method allowed for a thorough and objectively analysis of the data, that aligned with both the thesis main questions and hypothesis, but also with boarder academic context. Furthermore, a deep analysis was made to the structured survey dataset, which was conducted by Jyputer Notebook, Python and their standard libriaries.

5.3 Limitations

The limiting factors of this study were the semi-structured interviews and structured survey - the data are simply insufficient. The process of data collection was, frankly, extremely difficult; despite several months of endeavour, the quantity yielded was not nearly to target. Also, conducting thematic interviews also proved troublesome in the process of arranging interviews. Ultimately the timeframe got too wide and any further attempts to gather material was abandoned. The target of 20 interviews was diminished to 6 interviews. Furthermore, there were overall problems regarding the structured survey, which faced limitations in terms of response rate. The Finnish ministries forwarded it to relevant agencies, numbering over 10,000 potential respondents, yet the final count came to around 50 answers. This low response both in thematic interviews and structured survey suggests that it affects the generalizability of findings. Finally, these are limited and focused on a single country - Finland. While decision-making processes appeared to be entirely Finland-centric, this matter would demand further inquiry at the European Union level for comprehensive explanations.

The design of the survey questions was, in my opinion, methodologically sound. Yet this evaluation is subjective by nature. It may also be possible for someone to argue that this approach adds a certain degree of bias, thus affecting the way the questions were weighted and framed. In addition, these surveys were directed more or less to officials and government bodies, so any wider cross-section of perspectives was lost. The treatment and the implication of questions are also looked upon with suspicion and the intended meaning of questions also present challenges. In a structured survey, the high number of questions usually corresponds to very short, predetermined responses, which might lead respondents to misunderstand, misinterpreted, or give incomplete answers. There is also the potential for respondents to embellish their answers, thereby obscuring the true nature of their responses.

6 Analysis of Data and Results

6.1 Semi-Structured Interview – Thematic Interview

A total of six interviews were successfully organized, although the initial goal was significantly higher and extended the time period. All interviews were conducted entirely via Teams and the discussions followed a free-form format – semi-structured. The discussion was supported by a presentation that outlined (Appendix 4) the main features of this thesis and set the context for the discussion. The presentation introduced thesis hypothesis and main questions at the beginning, explaining that the questions or discussions would revolve on this central idea. Following the hypothesis and the initial question, we dived into three themes that reflected the issue on previous literature review material. The interviews were conducted in Finnish with Finnish participants only. No other nationalities were even considered, because of limited recourses. Initially the discussion started on laws and regulations that shape the field and impose restrictions. This provided a foundation for our subject at hand. We then moved on to risk management, focusing on people, contracts and continuity plans etc. In this part we delved into how government manages potential risks and emphasizing the importance of human factors and strategic planning. Finally, we examined the impact of technology on these areas and what the future holds.

The interviewees were experts, specialist or leading experts, all holding a bachelor's degree and most of them had a higher degree (Master's) that was relevant to their position. Each had been in their role or in the government for at least five years, with similar experience in IT field. Each had also spent roughly the same amount of time dealing with cloud technology. Despite the low number of interviews, their extensive experience gave valuable insights into the topics discussed in this thesis. There was a slight uncertainty that could be observed or interpreted by some, possibly due to the evolving and new nature of the field. All interviewees wished to remain anonymous and did not want their names or organizations mentioned. This anonymity was respected throughout the process and all data containing their personal data was removed. Interview requests were sought primarily through personally aquired contacts with the police, ministries and other central agencies, such as the National Cyber Security Centre Finland.

The interviewees highlighted or emphasized that the Finnish legal field is complex and too wide. There are dependencies on different laws and interpretation sometimes requires a trained understanding and interpretation, often in some cases requiring legal consultation. This complexity poses significant challenges in a fast-paced work and cyber space environment where quick, and large scale, decisions are sometimes needed. The interviews also raised the problem that theoretical solutions may not necessarily work at an operational level. Furthermore, sometimes there may be a rush and there is no time to interpret the law but go with the "gut feeling". This causes challenges and highlights the responsibility of an individual civil servant to make informed decisions quickly that can be justify later. If the expert or specialist lacks experience, the decision-making process may be delayed or even stalled due to the fear of the potential consequences. This hesitation can lead to a problematic situation where not making a decision can led to serious consequences that may irreversible and catastrophic.

Regarding the cloud technology, data protection legislation was considered to be highly restrictive and therefore challenging. The interviewees raised a growing concern that future EU laws or directives might impose further restrictions rather than enabling technological progress and advancement. This raised the question by one interviewee that the EU is becoming overly regulatory, potentially falling far behind as the rest of world advances technologically. The balance between regulation and innovation is a critical issue that needs careful consideration and understanding. In addition, the interviewees highlighted the diversity in the interpretation of the law. There had been cases where different agencies and ministries that had issued different or opposite guidelines and regulations based on the same law. This leads to peculiar situation where two different authorities may have different or conflicting opinions on the same issue, raising the question of which interpretation is correct. This diversity of legal interpretation can lead to significant operational challenges, which directly impacts the decision-making process and may lead to serious consequences as stated previous. Also, this confusion can cause inefficiencies, which in turn difficult the implementation of laws consistently and uniformly in the government. How do you resolve these conflicts? Is the only solution to take the matter to court? Is a law effective and understandable if it allows for such broad interpretation? According to interviews, overly broad interpretations lead to inconsistent practices, which eventually become problematic. This inconsistency not only affects the efficiency of the government and public administration but also undermines public trust in the agencies carrying the task. Moreover, resolving these ambiguities or conflicts through the

national or the EU level court are not only costly but time-consuming process that take years. This is impractical in a rapidly changing world and especially in the cyber space and cyber security. The interviews have highlighted a clear need for clarification of the legislation, which minimizes divergent interpretations and narrows the scope of application. In addition, there is a need for improved coordination and communication at ministerial level and between different agencies to ensure a more consistent approach to legal interpretation and implementation at a national level.

In the context of legal framework, overestimation or misassessment of classified information (data) a was highlighted as an issue. One interviewee suggested that various agencies may have or might employ different, varied or inconsistent practices in how information, documents or data is classified. This inconsistency causes distortion, which might impose too tight restrictions and therefore false data. The correct classification of secret information in modern cyber space is crucial. A single piece of falsely classified information may cause significant challenger for an IT specialist, when applying automations or other form of cyber security or overall features in the traditional and cloud environment. However, the responsibility for making corrections lies with the individual government employee who initially labelled the information – or classified the information. A need for standardized approach arose from the interviews to classified information across agencies and ministries to mitigate the risks associated with misclassification of classified information. Standardization could help ensure operational efficiency if sensitive information is adequately protected. Few interviewees saw that the role of cloud technology in this context cannot be overstated, as it offers advanced cyber security tools for managing and securing classified information. Furthermore, as one of the interviewees noted that the IT specialist often have comprehensive view on the whole organization, but they do not own the classified information, and they cannot account for its cumulative effect. A single file itself can have low-level classification (sensitive label), but a thousand such files can collectively pose a higher risk. This raises an important question of whether someone designated individual in the organization should own the entire classified information and oversee it? While overall responsibility generally lies with the management, the reality, as we all in the workforce know, that is not the case. The interviewee also questioned whose interest prevails, when each stakeholder in the organization views the data, problem or the matter from their own perspective and not the whole.

Another major point raised in the interview was the historical use of a concrete red stamp “Classified”, “Secret”, or “Top Secret” in the physical world to indicate that a document should be kept secret (or is classified). In the cyber space, however, this equivalent method needs careful consideration or reevaluation to determine the best approach from cyber security point of view. Is metadata or formatting alone sufficient to mark or indicate a information is classified, or should this be also examined more in-depth? The question arose from the interviewee as to at what level should confidential or classification of information be marked: at the file system, file, or binary level? How do we ensure that a computer does not read it or is not permitted to read such information? Who monitors the actions of the computer or automation to prevent information leaks?

The discussion further delved into the core the core problem of identifying whom do we want to keep the information secret from and why do we do the classification. Practices in the cyber space vary greatly based on the interviews and is supported by my 15 years of experience in the field of government and cyber security. The rapid evolution of the cyber space, technology and new era of cyber security has outpaced the consideration of these issues. Moreover, these have not yet been thoroughly examined under the lenses national or EU law, cyber security or risk management, which are essential for a comprehensive approach.

The focus of risk management as a whole was on people. When transitioning to the cloud, people's skills vary widely on how they can receive and understand it. The interviewees pointed out that, according to their empirical observations and experience, the average age of government officials is well over 45 years. This demographic suggests that a significant portion of the people may not be technically competent or lack technical understanding. This might lead to serious cyber security risks or shortcomings. The shortcomings were considered from the perspective of the basic user, where the likelihood of individual errors is usually high. Depending on the sensitivity level of the classified information, such errors can range from minor to major issues. Also, the interviewees identified a more significant problem with the IT specialist working with “under the hood” who usually has global admin rights that can do anything. Their training and skills were considered to have significant impacts on cyber security

and overall security in both traditional and cloud services. The interviews also revealed that in Finland, civil servants or government employees undergo security clearances to ensure their reliability. However, similar security clearance cannot be performed on cloud service operators due to the global nature of their operations, which are not govern solely by Finnish legislation. This situation raised its own challenges, prompting consideration of whether the position of global market leader should be regulated at EU level. In this way they could, at least in theory, be submitted to the same level of scrutiny and given some kind of security clearance.

Additionally, one interviewee raised the issue of vendor lock, which inevitably arises in a cloud environment. While long-term cooperation may foster a sense of security and trust, there is a question of whether foreign politics will have impact on the market leaders. In a cloud environment, it is an unavoidable reality that risk management is outsourced to a supplier and their actions are trusted. And, in global market with global vendors trust cannot be enforced by national law or contracts, as the law does not apply to a foreign supplier, and the contract can be changed.

Theme	***Sub-Theme***	***Details***
Legal Framework	Complexity	The legal field in Finland is highly complex with dependencies on different laws, making quick and large-scale decisions challenging.
Legal Framework	Data Protection	Data protection legislation is highly restrictive, posing challenges for cloud technology implementation.
Legal Framework	Diversity in Interpretation	There is significant diversity in legal interpretation, leading to inconsistent application and operational challenges.
Legal Framework	Future EU Laws	Concerns that future EU laws may become overly regulatory, hindering technological progress.
Risk Management	People	The focus on people highlights the varying technical competence among government officials, with an average age over 45 years, leading to potential cyber security risks.
Risk Management	Decision Making	The complexity of the legal framework and lack of experience can delay or stall decision-making processes, leading to serious consequences.
Risk Management	Vendor Lock	The issue of vendor lock in a cloud environment is a concern, as foreign politics

		can impact the reliability of cloud service providers.
Cloud Technology	Security	Ensuring the security of cloud services is difficult due to the global nature of cloud service operators and lack of security clearance.
Cloud Technology	Data Classification	Inconsistent data classification practices can lead to operational inefficiencies and security risks.
Cloud Technology	Regulation vs Innovation	The balance between regulation and innovation is critical, with concerns that overly broad interpretations of laws lead to inconsistent practices.

Table 6.1. Key findings from semi-structured interview

6.2 Structured Survey

The majority (over 75%) of respondents possessed higher education qualifications (Master's degree) and predominantly occupied government positions, with few exceptions. This outcome was anticipated, given that the survey was initially directed at ministries and government agencies. However, the evolution and change in remote work practices is particularly noteworthy in this structured survey. Presently, remote work has become a standard practice within government administration, both in ministry and agency level. Survey participants 46% reported engaging in remote work 2-3 days per week, while 54% indicated they did so 4-5 days per week. This shows that presently remote work is the new norm. In stark contrast, prior to the COVID-19 pandemic, the statistics were significantly different: a mere 8% of respondents worked remotely 4-5 days per week, and 23% did so 2-3 days per week. Before the pandemic, remote work was considered an atypical mode of operation, with nearly 70% of respondents indicating they worked remotely at most one day per week. This shift underscores a substantial transformation in work practices within the government administration. A change that has happened overnight.

As stated, the data highlights a broader trend towards the normalization of remote work, which has been accelerated by the COVID-19 pandemic. This trend is not just in Finnish government, but as seen in literature review, in rest of the EU. This shift, which has been rapid, not only reflects changes in technology, where in the EU there is significant uptrend, and work culture but one may also suggests a potential rethinking of how government operations can be conducted efficiently. The increased flexibility in work arrangements could lead to improved work-life balance for employees, potentially enhancing job satisfaction and productivity. Moreover, the widespread adoption of remote work may prompt further investments in digital infrastructure and cyber security to support this new mode of operation, which plays a crucial role. The survey results indicate a significant and lasting impact of the COVID-19 pandemic on work practices within the government administration, marking a departure from traditional work environments and making technology advancements possible.

From my perspective, and the literature review and surveys support it, this shift towards remote work is a fascinating development. It demonstrates how quickly and effectively organizations can adapt to unforeseen circumstances and make rapid changes that were deemed not possible before. The pandemic forced many to rethink traditional work models, and the resulting changes have shown that remote work can be just as productive, if not more so, than conventional office-based work.

I believe this trend will continue to evolve, with more organizations recognizing the benefits of flexible work arrangements and see it as a possibility. This will also open up opportunities for a more inclusive workforce, as remote work can accommodate individuals who may have previously faced barriers to traditional employment. However, it will be crucial to address challenges such as maintaining team cohesion, ensuring cyber security, and providing adequate support for remote workers to sustain this new way of working effectively. Furthermore, this does not remove the "bad apples", and I think old problems in the workforce do still exist. Now, organizations need to come up new ways to manage this.

Respondents were surveyed their opinion on major changes and significant transformations that have occurred in the last five years and what impact they have had on the organization's cyber security. Notable global events, like, COVID-19 pandemic, the threat of war and ongoing war in Ukraine, and joining NATO were perceived as an improving effect on the organization's cyber security. One could assume that organizations (people) have been afraid or the have a sense of vulnerability and therefore compelling organizations to channel additional resources towards enhancing security infrastructure. Interestingly, however, there was also the impact of the increase in remote work and hybrid work, which was seen as mutually weakening the overall security. Nevertheless, this contradiction raises a pertinent question:

> "*Do individuals harbour a lack of confidence in their personal cyber security practices? And thereby placing greater reliance on the collective measures implemented by the organization?"*

This is somewhat troublesome; hence it's the individual that makes the cyber security a whole and at the same time it's the weakest link.

These perspectives underscore a critical discourse in contemporary cyber security strategy, when thinking on classified information. On one hand, the external threats and geopolitical developments have galvanized a concerted effort to fortify security measures in the field. On the other hand, the internal shift towards more flexible work environments has introduced new vulnerabilities, necessitating a re-evaluation of trust and efficacy in both individual and organizational cyber security practices.

The initial adaption of cloud services was largely seen positive by respondents. Approximately 60% of respondents perceived cloud solutions as fundamentally secure and safe in principle, although they recognized that this technology would not solve every problem. When asked about the (cyber)security of information stored in the cloud versus traditional server solutions, nearly 50% of respondents thought that the location of the information was unimportant. This perspective aligns with the broader understanding that I have been applying for years:

> *"Information security or cyber-security is not merely a singular action or technology but a comprehensive lifestyle that must be cultivated and adopted."*

As in per the literature overview on the subject, the past three decades, and particularly in the last five years, there have been substantial advancements in technology and a rapid change in the cyber space. However, in the realm of controls and management related to cyber security or industry regulations and standards, respondents did not perceive a significant advantage in cloud solutions over traditional ones. This can be perhaps a lack of education or familiarity with the new technology, or encapsulated by the adage, "If it ain't broke, why fix it?"

According to the respondents, traditional technological solutions were seen as slightly more outdated. While 54% of respondents believed that cloud solutions are more compatible with industry regulations and standards, 40% felt that traditional solutions are more suitable. Here

too, it can perhaps be interpreted that internationally used standards are better incorporated into cloud solutions, but national-level regulation may be missing. Respondents were also almost unanimous that in the long run, cloud solutions are more cost-effective than traditional solutions. Nearly 70% of respondents answered that the cloud brings cost-effectiveness, while only 20% said that the cloud increases expenses. The survey did not ask the respondents' age, but did consider the length and quality of their working careers. More than 30% of respondents had been in the workforce for over 25 years, which suggests that the adoption of new technology may not yet be fully internalized. Conversely, about 15% of respondents had been in the workforce for less than 10 years, where I assume that they have learned the benefits of the cloud in during their education. Once again, the survey highlighted that the shift towards cloud solutions has been radical, especially in the last five years. The rapid pace of change highlights the rapid and ever-changing development of technology and the need for continuous learning and adaptation. Respondents' views on the compatibility of cloud solutions with industry laws and standards reflect serious shortcomings in the direction towards globalization and harmonization of international standards. The lack of integration of national regulations suggests that work still needs to be done to ensure that cloud solutions meet all requirements.

When asked whether Finnish legislation should be updated in order to meet today's cyber security challenges, the respondents were almost unanimous on the matter. Almost 95% were of the opinion that the legislation is currently insufficient or outdated. The comments highlighted the need for an update, as well as the rapid development of technology as the main problem. As was also evident in the literature review, the development of technology is significantly faster than the development of legislation. Interestingly, the feedback did not reveal or include the position of those who felt that the legislation was sufficient. This might suggest that the respondents felt that the current legislation is still applicable. However, the question arises that if technology or events change radically, should not the change in legislation also be radical? Although legislation should leave some room for interpretation, it cannot be completely open-ended. Half, 50% of respondents felt that Finnish legislation can, at least partially, influence global giants such as Amazon, Apple Google or Microsoft. This is an optimistic and even false view in my opinion, and I personally do not see it as even possible. Although an impact can be made, it is highly likely that Finland, as a small market, will lag behind others. Conversely, 40% strongly believed that Finnish legislation has no impact on the operations of global market leaders.

The respondents were presented with the hypothesis of this study:

Classified information can be processed in cloud environment,
if proper cyber security, data protection and risk management has been implemented
and political relations are handled by government officials.

They were asked to provide their opinions, and the results were as follows:

- 54% of the respondents strongly agreed with the hypothesis,
- 31% partly agreed,
- 8% partly or strongly disagreed.

In other words, the majority did not see a problem with the use of cloud services in terms of classified information. However, the comments provided by the respondents indicated that cloud services are not viewed as fundamentally different from traditional services. It was emphasized that a thorough evaluation of the service provider should always be conducted during the commissioning process, taking into account the overall context – especially cyber security. Cloud services were generally seen as versatile and offering numerous new technological features that could be beneficial in the field of cyber security. Nonetheless, in terms of data protection, it was highlighted that classified information cannot be stored just anywhere in the world and that the matter should be viewed from the EU's perspective.

Opponents or those who disagreed of the hypothesis pointed out that cloud services are relatively new and have not yet been fully defined within existing legislation. This raises the questions once more, that is our legislation enough? In addition, there were also concerns about the reliability of cloud services, with some respondents questioning whether any service can truly be free from interruptions. One of issue that arouse in the comments was the use of the term “proper”, which many respondents felt was too vague and open to broad interpretation. This vagueness could potentially lead to conflicts within the government section. It leaves much to the discretion of individual civil servants, who may interpret the term either broadly or narrowly and lead to unnecessary court cases.

Among those who agreed with the hypothesis, 44% believed that the cyber security of cloud services will improve, and that classified information will remain in better protected that in the traditional systems. Additionally, adapting cloud services 33% of respondents felt that the management of operational continuity and preparedness would improve. Conversely, 29% of respondents felt that it were of the opinion that data protection control will weaken with cloud services. Regarding risk management, 29% also believed that control and management would deteriorate with cloud services. In my opinion and interpretation is that there is not yet sufficient trust in global giants and actors that operate outside the EU in the field of cyber security and classified information. Although in the previous survey question, 53.8% believed that Finnish legislation and 69.3% believed that EU-level legislation can influence global actors.

6.3 Deep Analysis of the Structured Survey

We'll review the structured data in depth and discover new elements and aspects from a technical standpoint. Understanding the dataset's structure, variables and properties of the data is essential for interpreting the results and addressing the research questions regarding the cyber security perceptions and organizational impacts of cloud services. The dataset includes responses from 51 participants, representing different Finnish public sector organizations. The survey was sent to all ministries in Finland, which have forwarded them to their own affiliated agencies, such as EYL centers[7] and Regional State Administrative Agencies[8]. The key variables were education level and working experience, with experience divided into private, municipal and public sectors. In addition to these, the dataset contains a categorical variable of organization type. The dataset was analyzed utilizing Jupyter Notebook with the Python, leveraging standard libraries without modifying or altering the original dataset. All code and procedures are available in the appendix (Appendix 5) for transparency and replication, along with detailed instructions for dataset use. Table 3.1 summarizes the key characteristics of the dataset main features, including sample size, variables, response scales, and limitations. This overview provides the basis for subsequent descriptive and inferential analyses, which aim to

[7] Finnish: Elinkeino-, liikenne- ja ympäristö -keskus (ELY-keskus)
[8] Finnish: Aluehallintovirasto (AVI)

explore how educational level and organizational context shape perceptions of cloud services in the Finnish public sector.

Attribute	Description
Dataset Name	Deep_Analysis_of_Processing-of-classified-information-in-cloud-services.xlsx
Sample Size	51
Key Variables	Education level Organization Experience years Statements: likert Free comments
Response Scale	5-point likert scale: 1 = Strongly disagree/worsens and 5 = Strongly agree/improves
Data Type	Qualitative (likert, categorical) Quantitative (text comments)
Limitations	Overall small sample size Unequal distribution in key variables, e.g. education level

Table 6.3.1 – Dataset attriburtes and their description

The results were divided into three distinct groups: (1) distribution by educational level (Figure 1), (2) total years of work experience (Figure 2) and (3) years of work experience by sector and level of education (Figure 3). These findings demonstrate a skewness, primarily attributed to the small sample sizes of Lower Tertiary[9] and Secondary Education[10] (n=5 each). This highlights the incomplete illustration within these groups. The distribution of respondents across educational level is illustrated by a bar graph (Figure 1), which shows the number of respondents in the three educational categories that were asked. The analysis reveals an uneven distribution, with the majority of respondents having a higher university degree. This imbalance may cause variability into the results and is unlikely to fully represent the broader population. For the purpose of examining work experience, total years were calculated by aggregating each respondent's work experience across the state, municipalities and private sector. The statistical data describing total work experience is presented in Figure 2. A subsequent graph (Figure 3) integrates or merges these two data to provide an overview. However, due to the limited number

[9] Finnish: Keskiaste
[10] Finnish: Alempi korkea-aste

of respondents, it predominantly reflects the work years of those with Higher education, rendering other educational levels less visible. This uneven distribution and the small sample sizes for Lower Tertiary and Secondary Education may constrain the generalizability of the findings, particularly for these underrepresented groups.

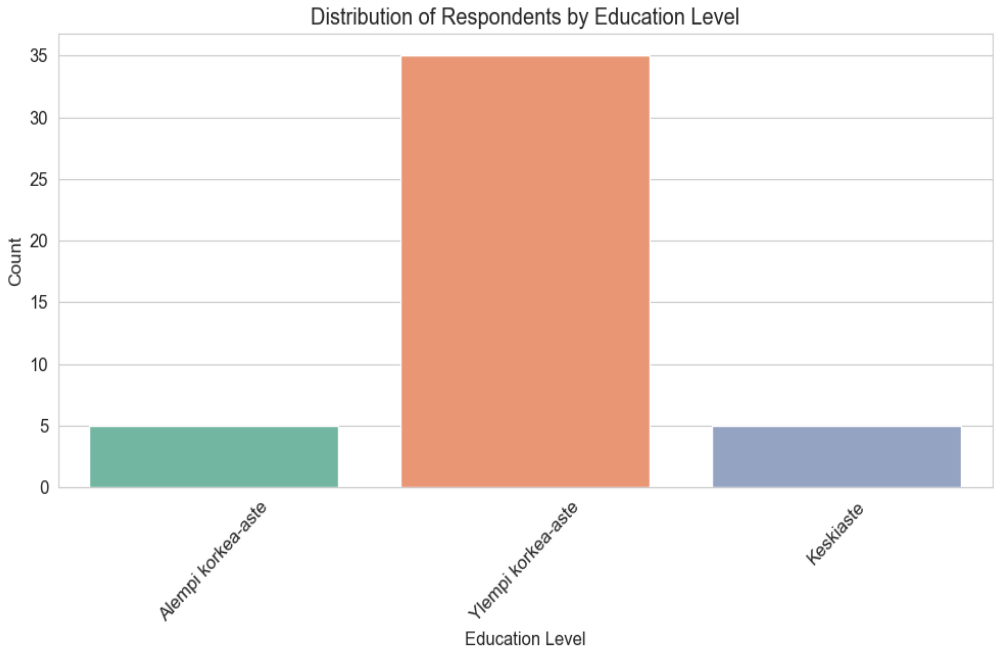

Figure 1 - Distribution of Respondents by Education Level

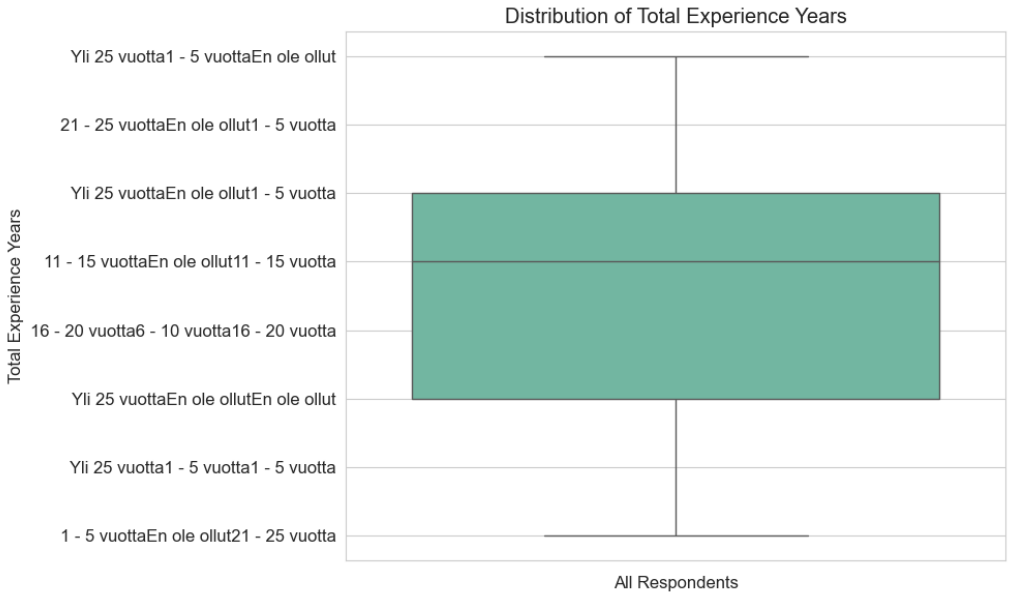

Figure 2 - Distribution of Total Experience Years

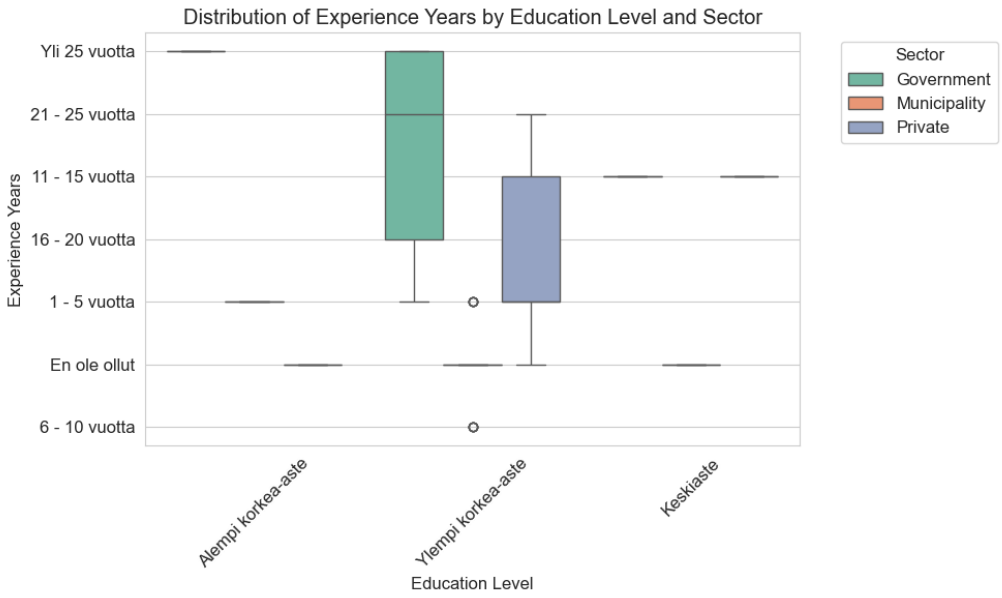

Figure 3 - Distribution of Experience Years by Education Level and Sector

The dataset was analysed from several different perspectives. However, due to the limited number of responses, drawing scientific conclusions is not feasible. The survey included Likert-type questions and statements regarding cybersecurity, cloud adoption, risk management, and data protection from an overall security perspective, and statements about legislation, regulation, and contracts. The objective was to investigate the effects of various work histories (duration and quality) and educational backgrounds in relations with each other.

As stated before, the dataset is highly skewed, which was also evident in the correlation analysis. Multiple correlation effects were explored using the help of different AI[11] tools, see which would yield new relevant information. One explored method was the Kruskal-Wallis test to determine if educational background influences answers given of cybersecurity measures or cloud usage. These results are presented in Tables 6.3.2 – 6.3.5, but with the small sample size these values do not present scientific result. Specifically, we aimed to assess whether additional education or the lack thereof has any significance.

[11] The inputs or prompts were: “What type of analysis can you make based on the following dataset?” and “Can you find correlation between education and the Likert answers” The answers itself were not used, but provided the direction, where the Kruskall-Walls test arouse.

Survey questions and their statements that had likert -type scale with the Kruskall-Wallis p-value:

Have the following events had a weakening or improving effect on the organization's cybersecurity?		
Likert Scale Statements	**Sub-questions**	**Kruskall-Wallis p-value**
1 = "Significantly weakens"	Covid-19	6.1419
2 = "Weakens somewhat"	Threat of war (Ukraine war)	0.0017
3 = "Neither weakens nor improves"	Finlands joining NATO	0.0500
4 = "Improves somewhat"	Increase in remote and hybrid work	0.0017
5 = "Significantly improves"		

Table 6.3.2

What is your opinion on the following statements?		
Likert Scale Statements	**Sub-questions**	**Kruskall-Wallis p-value**
1 = "Strongly disagree"	Cloud services are inherently less secure than traditional (on-premise) solutions.	0.0017
2 = "Disagree"	Traditional (on-premise) solutions provide better control over security measures compared to cloud services.	0.1326
3 = "Neutral"	Cloud services are less compatible with industry regulations and standards compared to local solutions.	0.0022
4 = "Agree"	Data stored in the cloud is more vulnerable to cyber-attacks and breaches than data stored on-premise.	0.1072
5 = "Strongly agree"	Traditional (on-premise) solutions are more cost-effective in the long term than cloud services.	0.0008

Table 6.3.3

Does the adoption of cloud services weaken or improve the organization's, in your opinion?		
Likert Scale Statements	**Sub-questions**	**Kruskall-Wallis p-value**
1 = "Significantly weakens"	Cybersecurity	0.0023
2 = "Weakens somewhat"	Business continuity management and preparedness	0.0010
3 = "Neither weakens nor improves"	Risk management	0.0016

4 = "Improves somewhat"	Data protection	0.0029
5 = "Significantly improves"		

Table 6.3.4

What is your opinion on the following statements?		
Likert Scale Statements	**Sub-questions**	**Kruskall-Wallis p-value**
1 = "Strongly disagree"	Finnish legislation can influence foreign actors (e.g., Amazon, Apple, Google, Microsoft).	5.1314
2 = "Disagree"	The legislation of another state can influence Finnish actors (e.g., TietoEVRY)?	3.4697
3 = "Neutral"	EU legislation can influence foreign actors (e.g., Amazon, Apple, Google, Microsoft).	0.0019
4 = "Agree"	Large global actors (e.g., Amazon, Apple, Google, Microsoft) set cybersecurity standards.	0.0432
5 = "Strongly agree"	Agreements between actors (e.g., Amazon, Apple, Google, Microsoft, TietoEVRY) and the state (e.g., service and confidentiality agreements) are sufficient, and no separate national legislation is needed.	0.0151
	Agreements between actors (e.g., Amazon, Apple, Google, Microsoft, TietoEVRY) and the state (e.g., service and confidentiality agreements) along with national legislation are sufficient, and no EU-level regulation is needed.	0.2557
	In addition to legislation, it is essential that activities are guided and specified through special agreements between the actor (e.g., Amazon, Apple, Google, Microsoft, TietoEVRY) and the state (e.g., DPIA).	0.0256

Table 6.3.5

The Kruskal-Wallis test revealed significant differences in Likert response distributions across education levels for 13 of 20 survey questions ($p < 0.05$). This indicates that there might be correlation between education and answers given. Table 6.3.2 “Threat of war (Ukraine war)” ($p=0.0017$) and “Increase in remote and hybrid work” ($p=0.0017$) showed strong differences indicating varied perceptions, possibly due to differing exposure to cybersecurity measures and understanding. Similar indication can be seen in all of the results tables 6.3.3 to 6.3.5, with table 6.3.4 having all p-values below established limit ($p<0.05$).

7 Discussion

In an era where trust is at the centre for both national and citizen, the management of classified information is emerging as a new challenge, where we become increasingly depended on cyberspace. We live largely on devices and everyday life is fast-paced, and sometimes we are forced to react, and rapid responses are necessary to emerging threats and opportunities. This dynamic poses a new challenge on how we process and handle classified information that historically was confined to physical mediums such as paper. Simultaneously, while evolving and enhancing accessibility and responsiveness, we must uphold the integrity of the CIA triad – confidentiality, integrity, and availability. Once more, the question arises: Who we can trust? During the study, it became clear that local national servers, which were previously state-of-the-art and managed and protected by us, have fallen behind. They have become obsolete, legacy systems marked by vulnerabilities to cyberattacks, limited scalability, and prohibitive maintenance costs. In contrast, cloud services are the future, offering unparalleled system efficiency, cost-effectiveness, scalability, and modern robust cybersecurity measures. Furthermore, drawing from personal experience, the physical and virtual security and fortifications of Microsoft's data centres are in a class of its own, without a comparison and outstripping many national efforts. The literature review and throughout the interviews revealed that trust is at the epicenter of the cloud computing discourse, particularly concerning classified information.

Classified information typically contains information that could cause financial losses, reputational damage, physical harm, or even life-threatening situation and national stability. Entrusting this information to international and global cloud providers inevitably creates a geopolitical problem. Even when these largest cloud providers are located in allied nations, their operations remain subject foreign legal jurisdictions and intelligence oversight. This theoretical possibility that allied authorities cloud access classified information undermines the autonomy states seeks to preserve. However, trust is not just about geopolitics and these private providers introduces additional complexity; a private company is also accountable to its shareholders. It is possible that security standards may be compromised for profit maximization or cost reduction reasons. This creates a paradox in my opinion on which the study core idea

lies. Neither private companies nor foreign, even an allied, state are inherently trustworthy, but both are essential and necessary for cybersecurity.

In the literature review, we noticed that only a fraction of the state and their agencies has transitioned to cloud-based services. These systems were once robust and state-of-the-art, but some are certainly currently suffering from outdated technology, vulnerabilities and limited scaling capabilities. Attacks that have targeted state systems, either healthcare or directly core state operations, are made public almost annually. However, the problem is certainly to be found in the massiveness of the systems. Estonia, which only began to develop its own infrastructure in the 1990s, has been able to utilize and harness digitalization to the greatest extent. Other states have lagged behind and interviews show that the problem is also partly in bureaucracy. The law may be partly outdated, or they overlap, which creates challenges and problematic situations. The ship of state is slow to change, although change is nevertheless inevitable. However, the transition is not a binary choice, but a gradual development that requires resourcing and risk assessments to determine which data can be transferred safely and which data must be kept under national control.

To borrow Lessing's idea, I would say that cybersecurity is global, but regulation is local. This imbalance creates particular challenges when it comes to processing classified information in the cloud. EU-level directives pose the first challenge for global actors to enter the EU economic area, which is strongly followed by national-level laws and regulations. In addition to all this, agency-specific rules may be encountered, creating a regulatory jungle in which global cloud service providers, authorities and people have to navigate. Interviews revealed that compliance with requirements burdens authorities when they have to interpret multi-level regulations and at the same time keep up with the pace of change. The challenge is also for international companies, which have to rely on teams of legal experts who are familiar with a narrow field.

Interviews conducted for the study revealed challenges in cooperation or the lack thereof between authorities. The biggest problem was that sharing classified information is usually incredibly restrictive even when sharing information between authorities. The phenomenon, where people only see their point of view, weakens collective defense against cyber threats,

especially in a small country like Finland, where resources are at best tight. Traditional systems are strongly tied to a specific authority and sharing identities and codes is not easy. Technically, of course, it can be created, but this does not necessarily fit or align with the agency's protocols or management models. Therefore, bureaucracy and the issue of trust come to the fore. With a unified environment (cloud environment), there could be opportunities to create new modern ways to manage classified information, not only from the perspective of one agency, but from the perspective of the whole of Finland. The same thinking could be practiced at other levels as well, of course this requires a different attitude and unification of practices between different nations.

The deep analysis of the structured survey results revealed or showed that there could be a correlation between the level of education and the answers provided. The problem with this conclusion is the minuscule number of survey results (n=51), but the matter itself is logical and reasonable. It could be clear that a person with a higher education has a broader understanding and knowledge of the whole, while those with a low level of education may remain on the practical level. However, this is more of a speculation at this point, but an interesting finding that should be investigated in the future.

8 Conclusions

8.1 Key Results and Findings

Through the research, literature review, the methodology, and data collection process, it can be said that the findings in this thesis have answered the main questions, and the initial hypothesis were indeed correct – at least partially.

One of the main challenges has been the limited scope collection of data, which was focused on one EU country – Finland. In addition, there may have been misunderstandings in the survey questions or in the thematic interviews. One of the possibilities of interpretation in the thesis words such as "proper". These factors likely influenced the final key results and findings. Based on these results and findings, it is difficult to claim anything, and they are not definitive. Nevertheless, it provides directional information for future research. The technology rapid advancements can lead to inefficiency and challenges in the government bodies. Also, the delay in legal adaptation can leave current cyber-security measures in classified information measures outdated. It is important to remembered that the attacker, or criminal, are not hindered by legalities and they are able to use the full spectrum of modern technologies to exploit these gaps and launch surprise attacks.

Throughout the research did any factors emerge that would have specifically prohibited processing of classified information in cloud services. However, the matter is complex, and some information can still be considered so top-secret that it cannot be entrusted to global vendor – or to another state. From a technological perspective, it is entirely possible to store information that is critical to the state in the cloud services. Global giant providers such as Microsoft, Google and Amazon have developed and designed products specifically for this and they have cases to show for. Nevertheless, several risks and limitations were identified. One of the significant concerns, which emerged from the literature review, surveys, and conducted interviews was the validation of the supplier and a thorough review of the contracts. It is crucial to ensure that service providers meet security standards and are also prepared to comply with national laws and local authorities. For example, the restrictions set by the EU GDPR on where data can be processed and how data can be processed and stored are important. Similar

restrictions exist at the national level for classified information and cyber-security, and there is currently no EU-level regulation on this. However, it is clear that several EU countries have moved or are moving to cloud services, which therefore forces them to consider this issue.

My conclusion from this study is that the trust is the major issue. Can global companies or another country be trusted? Government classified information are generally highly sensitive and falling into the wrong hands can cause physical damage, loss of reputation, major financial loss, and even death of citizens. Currently, mostly all classified information in EU member states is stored on traditional servers, with management and security under national control. Some countries have made transition to cloud services, but this is still single states. While these systems may have been state-of-the-art at one time, but over time they have become old or obsolete and are highly vulnerable to modern cyber threats. Today the democratic activities and functions are primarily influenced through the cyber world. This makes cyber-security crucial, and the challenges lies in balancing the need for advanced, secure systems with the inherent risk of trusting global companies that has its main operations in a different country. The issue is complex and debatable, but it's clear that the current approach needs to evolve, or it will perish with face of modern threats.

Navigation through regulation and legislation is a complex task. While cybersecurity and the cyber space are global, regulation and guidance are usually local. These legislation or regulations are often multi-level, such as at the EU, national, and even agency level, which further increases the challenges and complexity. For global companies this jungle of regulation and legislation poses a major problem and significant challenges as they must comply with the legislation of various countries. This compliance requires significant human resources with specific expertise in a narrow sector, e.g. laws on data protection or AI. Furthermore, companies need a meticulous planning to address future challenges and changes in the legislation field. Similarly, at the national level, civil servants need to understand multi-level entities and keep up with technological developments more closely. The situation becomes even more challenging when new government is elected and they may change the direction of the national level – either for cloud or against.

Resisting change or waking up too late to it is also a clear problem. Over the past five years, significant changes have occurred globally, which have direct and indirect impacts on cybersecurity and how states have done things in the past. Furthermore, over the past decade, technology has advanced significantly, and as the study indicates, governments are facing severe challenges and pressure. While there is interest in adopting new technologies, legislation is lagging behind and is not fully adoptable to today's requirements and needs. Future technologies are on the horizon, and I don't believe that we are ready for them as a nation or in the government's perspective. At the same time, the operating environment has become increasingly uncertain and challenging. The pandemic, the war in Ukraine and NATO have brought new challenges to the EU and Finland, which is forcing us to rethink our strategies. In my opinion and based on the thesis, technology is central to these considerations. The study underscores the critical and crucial importance of leveraging new technologies to ensure adequate cybersecurity measures in the cyberspace.

Regarding cooperation, the study showed that there is far too little of it. Although, a more detailed review this area would have been beneficial, the primary focus this time was on proving or disproving the hypothesis. However, the interviews revealed that cooperation is fragile, and information does not flow from one authority to another. This is partly because the information must be kept confidential, including other branches of the government, and partly because there are no established mechanisms or management models for information sharing.

8.2 Future Research

There are several significant gaps in the research to my opinion and knowledge. One of the notable gaps is the insufficient number of interviews, which were too few to provide a clear picture of the current situation. While some indications and conclusions could be made, but to my understanding, it is not possible to speak of a scientific result.

There is need for understanding the relations between classified material handling in the cloud services and from my findings further research could be beneficial to governments and global

companies. Further test the theory and hypothesis set I have developed the following future research ideas:

1. **Broaden the scope:** The research has focused, at least in terms of the semi-structured interviews and structured surveys, on the issues of one country, Finland. For further research and studies should consider a wider group. For comparison purposes, it would be good to include at least another EU country that has similar challenges or that has solved the challenges.

2. **Multi-level analysis:** Further work on the research at different levels. As the research highlights in the results, it has been possible to see entities at different levels, such as the EU, national and agency levels. Investigating these different levels and uncovering their challenges and problems could bring more insight and deeper insights.

3. **Cooperation:** The study lacks sufficient lateral research on the subject. Unraveling the challenges of cooperation between different agencies, ministries or countries could provide insight and new areas to discover.

Overall, the research only scratches the surface. Governments and companies alike would benefit from further exploration and analysis on the subject. Given future technological developments such as artificial intelligence and quantum mechanics, I believe future exploration is essential. Following advancements in the technology will revolutionize the current cyberspace. This will demand new capabilities from both the private and public sectors.

References

Alenizi, B. A., Humayun, M., & Jhanjhi, N. (2021). Security and Privacy Issues in Cloud Computing. *Journal of Physics: Conference Series*, *1979*(1), 012038. https://doi.org/10.1088/1742-6596/1979/1/012038

Al-Faham, H., Davis, A. M., & Ernst, R. (2019). Intersectionality: From Theory to Practice. *Annual Review of Law and Social Science*, *15*, 247–265. https://doi.org/10.1146/annurev-lawsocsci-101518-042846

Amazon. (n.d.). *Securing government data in the cloud in a time of crisis*. https://d1.awsstatic.com/institute/AWS-Institute-Accelerate-public-service-transformation-4-Security-Ukraine.pdf

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, *12*(6), 1333. https://doi.org/10.3390/electronics12061333

Avaliku teabe seadus 2000, E. (2000). *Public Information Act (Avaliku teabe seadus)*. https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/506072018002/consolide

AWS secures £894m in cloud spend across three contracts with UK government on same day | Computer Weekly. (2024, January 12). *ComputerWeekly.Com*. https://www.computerweekly.com/news/366566172/AWS-secures-894m-in-cloud-spend-across-three-contracts-with-UK-government-on-same-day

Bezzi, M., De Capitani Di Vimercati, S., Foresti, S., Livraga, G., Samarati, P., & Sassi, R. (2012). Modeling and preventing inferences from sensitive value distributions in data release1. *Journal of Computer Security*, *20*(4), 393–436. https://doi.org/10.3233/JCS-2012-0457

Bispham, M., Creese, S., Dutton, W. H., Esteve-González, P., & Goldsmith, M. (2022). An Exploratory Study of Cybersecurity in Working from Home: Problem or Enabler?

Journal of Information Policy, *12*, 353–386. https://doi.org/10.5325/jinfopoli.12.2022.0010

Butler, G. (2024, August 14). *UK's HMRC 70 percent through cloud migration*. https://www.datacenterdynamics.com/en/news/uks-hmrc-70-percent-through-cloud-migration/

Cambridge Dictionary. (n.d.). Retrieved 4 February 2024, from https://dictionary.cambridge.org/dictionary/english/cyber

Chen, L., Takabi, H., & Le-Khac, N.-A. (Eds.). (2019). *Security, privacy and digital forensics in the cloud*. John Wiley & Sons.

Council Decision 2013/488/EU on the security rules for protecting EU classified information. (2013). https://eur-lex.europa.eu/EN/legal-content/summary/council-security-rules-for-protecting-classified-information-euci.html

Cyber security—Ministry of the Interior. (n.d.). Sisäministeriö. Retrieved 4 February 2024, from https://intermin.fi/en/national-security/cyber-security

Cybersecurity: How the EU tackles cyber threats. (2023, July 25). https://www.consilium.europa.eu/en/policies/cybersecurity/

Dataskyddslagen 2018:218, S. (2018). *Data Protection Act (Dataskyddslagen)*. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/dataskyddslag-2018218_sfs-2018-218

Dwivedi, Y. K., Hughes, D. L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J. S., Gupta, B., Lal, B., Misra, S., Prashant, P., Raman, R., Rana, N. P., Sharma, S. K., & Upadhyay, N. (2020). Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International Journal of Information Management*, *55*, 102211. https://doi.org/10.1016/j.ijinfomgt.2020.102211

Enterprises purchasing cloud computing services over the internet—Statistics Estonia. (n.d.). Retrieved 30 November 2024, from https://andmed.stat.ee/en/stat/majandus__infotehnoloogia__infotehnoloogia-ettevettes/IT030/table/tableViewLayout2

Erl, T., Puttini, R., & Mahmood, Z. (2013). *Cloud computing: Concepts, technology, & architecture*. Prentice Hall.

EU Commission. (2022a, January 1). *State aid: Commission adopts revised State aid rules* [Text]. European Commission - European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6245

EU Commission. (2022b, February 14). *Data Act—Factsheet | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/library/data-act-factsheet

EU Commission. (2024a, March 1). *Cloud computing | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

EU Commission. (2024b, July 1). *Free flow of non-personal data | Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en/policies/non-personal-data

European Commission. Directorate General for Communications Networks, Content and Technology., Capgemini., Sogeti., IDC., & Politecnico di Milano. (2021). *eGovernment benchmark 2021: Entering a new digital government era : insight report.* Publications Office. https://data.europa.eu/doi/10.2759/55088

European Data Protection Board. (2023, January 17). *2022 Coordinated Enforcement Action Use of cloud-based services by the public sector*. European Data Protection Board. https://www.edpb.europa.eu/system/files/2023-01/edpb_20230118_cef_cloud-basedservices_publicsector_en.pdf

General Data Protection Regulation (GDPR) – Official Legal Text. (n.d.). General Data Protection Regulation (GDPR). Retrieved 30 October 2022, from https://gdpr-info.eu/

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, tyv011. https://doi.org/10.1093/cybsec/tyv011

Government Cloud First policy. (2023, June 19). GOV.UK. https://www.gov.uk/guidance/government-cloud-first-policy

Hirsjärvi, S., & Hurme, H. (2008). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö*. Gaudeamus Helsinki University Press.

ICT indicators for enterprises: Germany, years—Statistics Germany. (n.d.). Retrieved 30 November 2024, from https://www-genesis.destatis.de/datenbank/online/statistic/52911/table/52911-0001

info@bb.agency, B. A., & Slingerland, C. (2024, July 18). *13 Top Cloud Service Providers Globally (UPDATED 2024)*. CloudZero. https://www.cloudzero.com/blog/cloud-service-providers/

Isikuandmete kaitse seadus 2018, E. (2018). *Personal Data Protection Act (Isikuandmete kaitse seadus)*. https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/506072018002/consolide

Jansen, W., & Grance, T. (2011). *Guidelines on security and privacy in public cloud computing* (No. NIST SP 800-144; 0 ed., p. NIST SP 800-144). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-144

Julkisuuslaki 621/1999, S. (1999). *Julkisuuslaki (Act on the Openness of Government Activities)*. https://finlex.fi/fi/laki/ajantasa/1999/19990621

Kyberturvallisuuden sanasto (TSK 52). (2018). Sanastokeskus TSK ry. https://sanastokeskus.fi/tsk/fi/kyberturvallisuuden_sanasto_tsk_52-1125.html

Lessig, L. (2000). *Code and other laws of cyberspace* (Nachdr.). Basic Books.

Mäenpää, O. (2020). *Julkisuusperiaate* (4., uudistettu painos). Alma Talent.

Mahmood, Z., & Hill, R. (2011). *Cloud computing for enterprise architectures*. Springer-Verlag.

Microsoft. (2022). *Defending Ukraine: Early Lessons from the Cyber War* (p. 29). https://static.poder360.com.br/2022/06/Relatorio-Microsoft-ataques-cibernetico-Russia.pdf

Naming the coronavirus disease (COVID-19) and the virus that causes it. (2022a). https://www.who.int/emergencies/diseases/novel-coronavirus-2019/technical-guidance/naming-the-coronavirus-disease-(covid-2019)-and-the-virus-that-causes-it

Offentlighets- och sekretesslag 2009:400, S. (2009). *Public Access to Information and Secrecy Act (Offentlighets- och sekretesslag)*. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/offentlighets--och-sekretesslag-2009400_sfs-2009-400

Regulation—2019/881—EN - EUR-Lex. (n.d.). Retrieved 4 February 2024, from https://eur-lex.europa.eu/eli/reg/2019/881/oj?locale=en

Sehgal, N. K., & Bhatt, P. C. P. (2018). *Cloud Computing: Concepts and Practices*. Springer.

Tiedonhallintalaki 906/2019, S. (2019). *Tiedonhallintalaki (Act on Information Management in Public Administration)*. https://finlex.fi/fi/laki/ajantasa/2019/20190906

Tietosuojalaki 1050/2018, S. (2018). *Tietosuojalaki (Data Protection Act)*. https://finlex.fi/fi/laki/ajantasa/2018/20181050

Tilastokeskus. (2022, December 20). *Use of information technology in enterprises [online publication]. - Helsinki: Statistics Finland*. https://pxdata.stat.fi/PxWeb/pxweb/en/StatFin/StatFin__icte/statfin_icte_pxt_13vg.px/

Tryckfrihetsförordning 1949:105, S. (1949). *Freedom of the Press Act*. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/tryckfrihetsforordning-19491205_sfs-1949-105

UK Home Office: Saving millions of pounds every year…. (n.d.). PA Consulting. Retrieved 5 January 2025, from https://www.paconsulting.com/client-story/home-office-saving-millions-every-year-through-smart-management-of-cloud-resources

Wang, Y., & Wang, X. (2020). A review of cloud computing adoption by small and medium-sized enterprises. *Journal of Cloud Computing*, *9*(1), 1–14. https://doi.org/10.1186/s13677-020-00162-0

What is Cyber Security? (2023, August 17). www.kaspersky.com. https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

What is Cybersecurity? | CISA. (2021, February 1). https://www.cisa.gov/news-events/news/what-cybersecurity

What Is Cybersecurity? | Microsoft Security. (n.d.). Retrieved 4 February 2024, from https://www.microsoft.com/en-us/security/business/security-101/what-is-cybersecurity

White, R. (2022, June 22). *How the cloud saved Ukraine's data from Russian attacks*. C4ISRNet. https://www.c4isrnet.com/2022/06/22/how-the-cloud-saved-ukraines-data-from-russian-attacks/

WHO Director-General's opening remarks at the media briefing on COVID-19—11 March 2020. (2022b, March 11). https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020

Appendices

Appendix 1 - Abbreviations

AI	Artificial Intelligence
APT	Advanced Persistent Threat
AWS	Amazon Web Services
CFAA	Computer Fraud and Abuse Act
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	Coronavirus disease 2019
CRRT	Cyber Rapid-Response TEam
CSP	Cloud Service Provider
DWP	Department for Work and Pensions
EDPB	European Data Procetion Board
ENISA	European Union Agency for Cybersecurity
EU	European Union
EUCI	European Union Classified Infromation
FaaS	Function as a Service
GCP	Google Cloud Platform
GDPR	General Data Protection Regualtion
HMRC	Her Majesty's Revenue and Customs
IaaS	Infrastructure as a Service
IPCEI	Important Project of Common European Interest
MFA	Multi-factor Authentication
MSTIC	Microsoft Threat Intelligence Center
NCSC	National Cyber Security Center
PaaS	Platform as a Service
SaaS	Software as a Service
SIMPL	Smart and secure middleware platform
UK	United Kingdom

Appendix 2 - Emails (ads) to possible participants

Semi-structured Survey:

Hei,

tl;dr

Diplomityö teemahaastattelu turvaluokitellun tiedon käsittelystä pilvessä. Kaipaan asiantuntijoita ja johtajia/päälliköitä. Laita viestiä (krhapa@utu.fi), niin pääset mukaan hemmetin hyvään tutkimukseen.

Teen diplomityötä osana *Cyber Security* maisterivaiheen opintoja Turun yliopistolla. Diplomityön aihe on - Processing of classified information in a cloud service - risks and benefits. Olen suorittamassa aiheeseen liittyviä teemahaastatteluita, joihin haluaisin teidän organisaation edustajien osallistuvan. Uskon, että organisaation edustajan/asiantuntijan näkemykset ja näkökulmat olisivat korvaamattomia tutkimukselleni sekä mahdollisesti myös teidän organisaatiollenne. Olisin kiitollinen, jos välittäisitte viestin henkilölle, jolla on tietämystä tai näkemystä pilviteknologiasta ja niiden käytöstä – niin asiantuntijat kuin johtajat/päälliköt. Mikäli organisaatio edellyttää tutkimuslupaa, niin voisitteko ystävällisesti osoittaa minulle suunnan, jossa voin ko. lupaa hakea. Kiitos.

Varaisin haastattelulle aikaa 1,5h, mutta voimme sopia lyhyemmän ajan tarvittaessa. Haastattelu käydään Teams/Zoom välityksellä ja se on tarkoitus nauhoittaa sekä litteroida. Sovitaan aika niin, että se sopii parhaiten sinun aikatauluusi. Käyn haastattelun alkuun tarkemmin itse tutkimusta sekä tietosuojaan ja -turvaan liittyviä kysymyksiä. Haastattelu anonymisoidaan lähtökohtaisesti. Mikäli organisaatiosi vaatii, niin teen erillisen tutkimuslupahakemuksen ennen haastattelua.

"Miksi mä tähän osallistuisin?" Erinomainen kysymys, kiitos siitä. Pitkään valtiohallinnossa on käyty keskustelua siitä, miten pilveä voidaan ja tulisi käyttää (pun intended 😉). Jotkut odottavat lainsäätäjää, toiset VM:n ja osa Kyberturvallisuuskeskuksen linjauksia, ohjeita ja

reagointia. Se kuuluisa "joku" tekee jotain jossain kohtaa… Oma lähtökohta, intressi ja motivaatio on, että saan tämän tutkimuksen kautta asiaa ponnistettua eteenpäin ja kohti jotain järkevää lopputulosta. Ehkä jopa julkaisu, jonka myötä saadaan keskustelua aikaan julkisesti? Jos en saa tähän sinulta apuja, niin tämäkin jää yhdeksi monien muiden töiden joukkoon: "jotain väsäsin, että pääsin läpi". Tätä en haluaisi…

Meillä on iso suo edessä, otatko kuokan ja tulet mukaan talkoisiin? Kiitos etukäteen ja jään odottamaan yhteydenottoasi.

Structured Survey:

Hei,

tl;dr

Diplomityö teemahaastattelu turvaluokitellun tiedon käsittelystä pilvessä. Kaipaan asiantuntijoita ja johtajia/päälliköitä. Laita viestiä (krhapa@utu.fi), niin pääset mukaan hemmetin hyvään tutkimukseen.

Teen diplomityötä osana *Cyber Security* maisterivaiheen opintoja Turun yliopistolla. Diplomityön aihe on - **Processing of classified information in a cloud service - risks and benefits.** Olen suorittamassa aiheeseen liittyviä teemahaastatteluita, joihin haluaisin teidän organisaation edustajien osallistuvan. Uskon, että organisaation edustajan/asiantuntijan näkemykset ja näkökulmat olisivat korvaamattomia tutkimukselleni sekä mahdollisesti myös teidän organisaatiollenne. Olisin kiitollinen, jos välittäisitte viestin henkilölle, jolla on tietämystä tai näkemystä pilviteknologiasta ja niiden käytöstä – niin asiantuntijat kuin johtajat/päälliköt. Mikäli organisaatio

edellyttää tutkimuslupaa, niin voisitteko ystävällisesti osoittaa minulle suunnan, jossa voin ko. lupaa hakea. Kiitos.

Varaisin haastattelulle aikaa 1,5h, mutta voimme sopia lyhyemmän ajan tarvittaessa. Haastattelu käydään Teams/Zoom välityksellä ja se on tarkoitus nauhoittaa sekä litteroida. Sovitaan aika niin, että se sopii parhaiten sinun aikatauluusi. Käyn haastattelun alkuun tarkemmin itse tutkimusta sekä tietosuojaan ja -turvaan liittyviä kysymyksiä. **Haastattelu anonymisoidaan lähtökohtaisesti.** Mikäli organisaatiosi vaatii, niin teen erillisen tutkimuslupahakemuksen ennen haastattelua.

"Miksi mä tähän osallistuisin?" Erinomainen kysymys, kiitos siitä. Pitkään valtiohallinnossa on käyty keskustelua siitä, miten pilveä voidaan ja tulisi käyttää (pun intended 😉). Jotkut odottavat lainsäätäjää, toiset VM:n ja osa Kyberturvallisuuskeskuksen linjauksia, ohjeita ja reagointia. Se kuuluisa "joku" tekee jotain jossain kohtaa… Oma lähtökohta, intressi ja motivaatio on, että saan tämän tutkimuksen kautta asiaa ponnistettua eteenpäin ja kohti jotain järkevää lopputulosta. Ehkä jopa julkaisu, jonka myötä saadaan keskustelua aikaan julkisesti? Jos en saa tähän sinulta apuja, niin tämäkin jää yhdeksi monien muiden töiden joukkoon: "jotain väsäsin, että pääsin läpi". Tätä en haluaisi…

Meillä on iso suo edessä, otatko kuokan ja tulet mukaan talkoisiin? Kiitos etukäteen ja jään odottamaan yhteydenottoasi.

Appendix 3 - Structured Survey Questions

Section 1

Perustiedot

1. Organisaatiosi *

Enter your answer

2. Koulutustasosi (ylin) *

- Perusaste
- Keskiaste
- Alempi korkea-aste
- Ylempi korkea-aste

3. Kuinka monta vuotta olet ollut työelämssä? *

	En ole ollut	1 - 5 vuotta	6 - 10 vuotta	11 - 15 vuotta	16 - 20 vuotta	21 - 25 vuotta	Yli 25 vuotta
Julkinen sektori (valtio)	◯	◯	◯	◯	◯	◯	◯
Julkinen sektori (kunta)	◯	◯	◯	◯	◯	◯	◯
Yksityinen sektori	◯	◯	◯	◯	◯	◯	◯

4. Kuinka monta päivää viikossa keskimäärin teet etätöitä tällä hetkellä? *

- 0 - 1 päivää
- 2 - 3 päivää
- 4 - 5 päivää

5. Kuinka monta päivää viikossa keskimäärin teit etätöitä ennen koronaa (Covid-19)? *

- 0 - 1 päivää
- 2 - 3 päivää
- 4 - 5 päivää

Section 2

6. Onko seuraavilla tapahtumilla ollut heikentävä tai parantava vaikutus organisaation kyberturvallisuuteen? *

	En osaa sanoa	Heikentää merkittävästi	Heikentää jonkin verran	Ei heikennä, eikä paranna	Parantaa jonkin verran	Parantaa merkittävästi
Covid-19	◯	◯	◯	◯	◯	◯
Sodan uhka (Ukrainan sota)	◯	◯	◯	◯	◯	◯
Natoon liittyminen	◯	◯	◯	◯	◯	◯
Etätyön ja hybrityön lisääntyminen	◯	◯	◯	◯	◯	◯

7. Mitä olet mieltä seuraavista väittämistä?

	Vahvasti eri mieltä	Osittain eri mieltä	En eri mieltä, enkä samaa mieltä	Osittain samaa mieltä	Täysin samaa mieltä
Pilviratkaisut (cloud-services) ovat lähtökohtaisesti vähemmän turvallisia kuin perinteiset (on-premise) ratkaisut.	◯	◯	◯	◯	◯
Perinteiset (On-premise) ratkaisut tarjoavat paremman hallinnan tietoturvaan liittyviin kontrolleihin pilviratkaisuihin verrattuna.	◯	◯	◯	◯	◯
Pilviratkaisut (cloud-services) ovat vähemmän yhteensopivia alan säännösten ja standardien kanssa verrattuna paikallisiin ratkaisuihin.	◯	◯	◯	◯	◯
Pilveen tallennetut tiedot ovat haavoittuvampia kyberhyökkäyksille ja tietomurroille kuin paikan päällä (on-premise) tallennetut tiedot.	◯	◯	◯	◯	◯
Perinteiset (On-premise) ratkaisut ovat pitkällä aikavälillä kustannustehokkaampia kuin pilviratkaisut.	◯	◯	◯	◯	◯

8. Heikentääkö vai parantaako pilvipalveluiden käyttöönotto mielestäsi organisaation? *

	En osaa sanoa	Heikentää merkittävästi	Heikentää jonkin verran	Ei heikennä, eikä paranna	Parantaa jonkin verran	Parantaa merkittävästi
Tietoturvallisuutta	◯	◯	◯	◯	◯	◯
Toiminnan jatkuvuuden hallintaa ja varautumista	◯	◯	◯	◯	◯	◯
Riskienhallintaa	◯	◯	◯	◯	◯	◯
Tietosuojaa	◯	◯	◯	◯	◯	◯

9. Voit halutessasi kertoa muutamalla lauseella aiheeseen liittyviä ajatuksia?

Enter your answer

10. Mitä mieltä olet seuraavista väittämistä: *

	Vahvasti eri mieltä	Osittain eri mieltä	En eri mieltä, enkä samaa mieltä	Osittain samaa mieltä	Täysin samaa mieltä
Suomen lainsäädännöllä voidaan vaikuttaa ulkomaalaisiin toimijoihin (esim. Amazon, Apple, Google, Microsoft).	◯	◯	◯	◯	◯
Toisen valtion lainsäädännöllä voidaan vaikuttaa Suomen toimijoihin (esim. TietoEVRY)?	◯	◯	◯	◯	◯
EU:n lainsäädännöllä voidaan vaikuttaa ulkomaalaisiin toimijoihin (esim. Amazon, Apple, Google, Microsoft).	◯	◯	◯	◯	◯
Suuret globaalit toimijat (esim. Amazon, Apple, Google, Microsoft) määrittävät kyberturvallisuuden standradit.	◯	◯	◯	◯	◯
Toimijoiden (esim. Amazon, Apple, Google, Microsoft, TietoEVRY) ja valtion väliset sopimukset (esim. palvelu- ja salassapitosopimukset) ovat riittävät, eikä erillistä kansallista lainsäädäntö tarvita.	◯	◯	◯	◯	◯
Toimijoiden (esim. Amazon, Apple, Google, Microsoft, TietoEVRY) ja valtion väliset sopimukset (esim. palvelu- ja salassapitosopimukset) sekä kansallinen lainsäädäntö ovat riittävät, eikä EU tason sääntelyä tarvita.	◯	◯	◯	◯	◯
Lainsäädännön lisäksi on ehdotonta, että toimintaa ohjataan ja tarkkennetaan toimijan (esim. Amazon, Apple, Google, Microsoft, TietoEVRY) ja valtion erityissopimuksilla (esim. DPIA)	◯	◯	◯	◯	◯

11. Voit halutessasi kertoa muutamalla lauseella aiheeseen liittyviä ajatuksia?

Enter your answer

12. Onko Suomen lainsäädäntöä tarpeen päivittää vastaamaan tämän päivän kyberturvallisuuden haasteisiin? *

◯ Kyllä

◯ Ei

13. Perustelu muutamalla sanalla miksi lainsäädäntö tulisi päivittää tai miksi sitä ei ole tarpeen päivittää?

Enter your answer

14. Seuraavassa väittämässä "*turvaluokiteltu tieto*" tarkoittaa tietoa, johon pääsevät käsiksi lain tai säännösten vuoksi vain henkilöt, joilla on erikseen perusteltu välttämätön tarve päästä käsiksi siihen.

Mitä olet mieltä seuraavasta väittämästä:

"Turvaluokiteltua tietoa voidaan käsitellä pilvipalveluissa, jos sen riittävästä suojauksesta on huolehdittu." *

- ◯ Vahvasti samaa mieltä
- ◯ Osittain samaa mieltä
- ◯ Osittain eri mieltä
- ◯ Vahvasti eri mieltä

15. Kerro muutamalla lauseella, miksi olet samaa mieltä? *

Enter your answer

16. Mikä seuraavista kuvaa parhaiten näkemystäsi? *

- ☐ Pilvipalveluiden tietoturva on parempi.
- ☐ Pilvipalveluiden toiminnan jatkuvuuden hallinta ja varautuminen on parempi.
- ☐ Pilvipalveluiden riskien hallinta on helpompaa.
- ☐ Pilvipalveluiden tietosuoja on parempi.
- ☐ Other

17. Kerro muutamalla lauseella, miksi olet eri mieltä? *

Enter your answer

18. Mikä seuraavista kuvaa parhaitan näkemystäsi? *

- [ ] Pilvipalveluiden tietoturva on heikompi.
- [ ] Pilvipalveluiden toiminnan jatkuvuuden hallinta ja varautuminen on heikompi.
- [ ] Pilvipalveluiden riskien hallinta on vaikeaa.
- [ ] Pilvipalveluiden tietosuoja on huono.
- [ ] Other

19. Tuleeko sinulla mieleen jotain aiheeseen liittyvää, joka olisi syytä huomioida?

Enter your answer

20. Olisitko halukas osallistumaan teemahaastatteluun aiheesta? Jätä yhteystietosi, niin sovitaan haastattelu aika. Tietojasi ei jaeta eikä käytetä mihinkään muuhun, kuin tähän. Tiedot poistetaan tutkielman valmistuttua.

Enter your answer

Appendix 4 - Semi-structured Interview Material and Questions

Processing of Classified Information in a Cloud Service – Risks and Benefits

Turun yliopisto, Tietotekniikan laitos
Diplomityö

Kris Papaleonidas
krhapa@utu.fi

TURUN YLIOPISTO

1

Tietosuojasta ja -turvasta

- Haastattelu nauhoitetaan ja litteroidaan
- Haastattelu anonymisoidaan
- Ennen anonymisointia
  - Tallennus tapahtuu käyttäen Teams/ Zoom alustaa
  - Tallenne on olemassa henkilökohtaisesti hallituilla tietokoneilla ja pilvipalveluissa
  - Kaikki laitteet ja palvelut on suojattu sekä siirrot tapahtuvat salattuna
- Aineiston säilytys
  - Alkuperäinen (sis. henkilötiedot) tallenne säilytetään siihen asti, kunnes diplomityö on hyväksytty tai viimeistään 31.12.2023, riippumatta hyväksynnästä
  - Diplomityössä käytetyn datan säilyttämisestä sovelletaan Turun yliopiston käytäntöjä

TURUN YLIOPISTO

2

Hyväksy / Hylkää

TURUN YLIOPISTO

Kuka olet?

- Nimi
- Titteli
- Organisaatio
- Ylin koulutusaste
- Työhistoria yhteensä
- Työhistoria IT
- Työhistoria IT-pilvi
- Anonymisointi

Tutkimuksen tarkoitus ja lähtökohta

1. Saada selkeä vastaus esitettyyn kysymykseen.
2. Vahvistaa tai kumota hypoteesi.
3. Yksiselitteiset päätelmät, joita voidaan jatkotyöstää tarvittaessa.

TURUN YLIOPISTO

5

TUTKIMUSKYSYMYS	HYPOTEESI
Miten ja millä rajoituksilla turvaluokiteltua tietoa voidaan käsitellä (luku, kirjoitus, tallennus) pilviympäristössä?	***Turvaluokiteltua tietoa voidaan käsitellä pilvessä, jos sen riittävästä kokonaisturvallisuudesta on huolehdittu.***

TURUN YLIOPISTO

6

Teemat

- Teknologia
  - Pilvi vs. on-premise
  - Tulevaisuus
- Lait, asetukset, määräykset ja sopimukset
  - Kansallinen vs. EU vs. US
  - Sopimukset vs. lait
- Kyberturvallisuus
  - Tietoturva
  - Tietosuoja
  - Riskienhallinta
  - Ihminen
- Muutos
  - Onko em. teemoissa tapahtunut muutosta?
  - 2018 - 2023

TURUN YLIOPISTO

7

Teema - Teknologia

- Mitä hyötyjä tai heikkouksia on
  - On-premise ratkaisussa
  - Pilviteknologiassa
- Onko jokin tilanne tai käyttötarkoitus, jossa toinen teknologia on merkittävästi paremassa tai huonomassa asemassa?
- Mikä on mielestäsi teknologian kehityksen sunnta? Mikä on tulevaisuus?

Tutkimuskysymys

Miten ja millä rajoituksilla turvaluokiteltua tietoa voidaan käsitellä (luku, kirjoitus, tallennus) pilviympäristössä?

Hypoteesi

Turvaluokiteltua tietoa voidaan käsitellä pilvessä, jos sen riittävästä kokonaisturvallisuudesta on huolehdittu.

TURUN YLIOPISTO

8

Teema – Lait, asetukset, määräykset ja sopimikset

- Onko lait ajantasaisia?
  - Mahdollistavatko vai estäväkö ne toimintaa?
- Miten mielestäsi kansallisella lailla voidaan vaikuttaa ulkomaan toimijoihin?
  - Voiko esim. Suomen lailla pakottaa Microsoftin tekemään jotain?
- Miten näet EU tason asetukset (The Big Five)?
  - Mahdolistavatko vai rajoittavatko ne toimintaa?
- Miten näet kahdenväliset sopimukset?
  - Yritys X (Suomi) ja Microsoft. Onko riittävä?

Tutkimuskysymys

Miten ja millä rajoituksilla turvaluokiteltua tietoa voidaan käsitellä (luku, kirjoitus, tallennus) pilviympäristössä?

Hypoteesi

Turvaluokiteltua tietoa voidaan käsitellä pilvessä, jos sen riittävästä kokonaisturvallisuudesta on huolehdittu.

Teema – Kyberturvallisuus

- Mitä kyberturvallisuus tarkoittaa?
- Mikä on eri osa-alueiden merkitys?
  - Tietoturvallisuus
  - Lait (tietosuoja ym.)
  - Riskienhallinta
  - Ihminen
- Kuka valvoo tai vahtii luotettavasti palveluntoimittajaa?

Tutkimuskysymys

Miten ja millä rajoituksilla turvaluokiteltua tietoa voidaan käsitellä (luku, kirjoitus, tallennus) pilviympäristössä?

Hypoteesi

Turvaluokiteltua tietoa voidaan käsitellä pilvessä, jos sen riittävästä kokonaisturvallisuudesta on huolehdittu.

Teema – Muutos

- Ajatellaan em. teemoja vuosien 2018 – 2023 väliä
- Onko tuona aikana tapahtunut muutosta?
- Onko jollakin tapahtumalla ollut merkittävää muutosta?

Tutkimuskysymys

Miten ja millä rajoituksilla turvaluokiteltua tietoa voidaan käsitellä (luku, kirjoitus, tallennus) pilviympäristössä?

Hypoteesi

Turvaluokiteltua tietoa voidaan käsitellä pilvessä, jos sen riittävästä kokonaisturvallisuudesta on huolehdittu.

TURUN YLIOPISTO

Kris Papaleonidas

krhapa@utu.fi

Appendix 5 - Jupyter Notebook Python Code and Dataset

```
# Part 1: Import Libraries and Configure Settings
# Use relevant virtualization or install the used libraries to the operating machine.
# Description: Imports pandas, seaborn, matplotlib, and scipy for analysis and visualization.
# Sets seaborn style and matplotlib parameters for consistent plots.

import pandas as pd
import seaborn as sns
import matplotlib.pyplot as plt
from scipy.stats import kruskal
import numpy as np

# Configure plot style
sns.set_style("whitegrid")
plt.rcParams['figure.figsize'] = (10, 6)
plt.rcParams['font.size'] = 12

print("Setup complete: Libraries imported and plot settings configured.")
```

```
# Part 2: Load Data and Inspect Columns
# Description: Loads the Excel file and prints column names to verify external factor
columns.

try:
    data = pd.read_excel('Deep_Analysis_of_Processing-of-classified-information-in-cloud-
services.xlsx')
    print("Dataset loaded successfully.")
except FileNotFoundError:
    print("Error: Excel file not found. Ensure 'Deep_Analysis_of_Processing-of-classified-
information-in-cloud-services.xlsx' is in the directory.")
    raise

# Print column names for inspection
print("\nDataset Column Names:")
for col in data.columns:
    print(col)
```

```
# Part 3: Clean and Transform Data
# Description: Selects education (Koulutustasosi (ylin)) and
# experience columns (Julkinen sektori (valtio), Julkinen sektori (kunta), Yksityinen sektori)),
# calculates total experience, and prepares data for plotting.
# Creates two datasets: one for individual plots (education counts, total experience) and one
melted for sector-specific plotting.

# Define column names
education_col = 'Koulutustasosi (ylin)'
```

```
experience_cols = [
    'Julkinen sektori (valtio)',
    'Julkinen sektori (kunta)',
    'Yksityinen sektori'
]

# Check if all columns exist to prevent errors
missing_cols = [col for col in [education_col] + experience_cols if col not in data.columns]
if missing_cols:
    print(f"Error: Columns {missing_cols} not found. Check Part 2 output.")
    raise KeyError("Column not found.")

# Select relevant columns
data_clean = data[[education_col] + experience_cols].copy()

# Rename columns from FI to EN for clarity
data_clean = data_clean.rename(columns={
    education_col: 'Education_Level',
    'Julkinen sektori (valtio)': 'Government_Years',
    'Julkinen sektori (kunta)': 'Municipality_Years',
    'Yksityinen sektori': 'Private_Years'
})

# Remove rows with missing values
data_clean = data_clean.dropna()

# Calculate total experience years (sum of all sectors)
data_clean['Total_Experience'] = data_clean[['Government_Years', 'Municipality_Years',
'Private_Years']].sum(axis=1)

# Melt data for sector-specific plotting (combined plot)
data_melted = pd.melt(
    data_clean,
    id_vars=['Education_Level'],
    value_vars=['Government_Years', 'Municipality_Years', 'Private_Years'],
    var_name='Sector',
    value_name='Experience_Years'
)

# Map sector names for readable plot labels
data_melted['Sector'] = data_melted['Sector'].replace({
    'Government_Years': 'Government',
    'Municipality_Years': 'Municipality',
    'Private_Years': 'Private'
})

# Verify cleaned and transformed data
print("Education Levels:", data_clean['Education_Level'].unique())
print("Data cleaned: Missing values removed, total experience calculated.")
print(f"Clean dataset shape: {data_clean.shape}")
```

```
print("Sample clean data:")
print(data_clean.head())
print(f"Melted dataset shape: {data_melted.shape}")
print("Sample melted data:")
print(data_melted.head())
```

```
# Part 4: Bar Plot for Education Level
# Description: Generates a bar plot to show the count of respondents by education level.
# Visualizes the distribution of Ylempi korkea-aste, Alempi korkea-aste, and Keskiaste.
# Saves the output as PNG for the thesis

plt.figure()
sns.countplot(x='Education_Level', data=data_clean, palette='Set2')
plt.title('Distribution of Respondents by Education Level')
plt.xlabel('Education Level')
plt.ylabel('Count')
plt.xticks(rotation=45)
plt.tight_layout()
plt.savefig('bar_plot_education.png')
plt.show()
print("Bar plot saved to 'bar_plot_education.png'")
```

```
# Part 5: Box Plot for Total Experience
# Description: Generates a box plot to show the distribution of total experience years (sum of
Government, Municipality, Private sectors) across all respondents.
# Displays median, IQR, whiskers, and outliers for overall experience.
# Saves the output as PNG for the thesis

plt.figure()
sns.boxplot(y='Total_Experience', data=data_clean, palette='Set2')
plt.title('Distribution of Total Experience Years')
plt.ylabel('Total Experience Years')
plt.xlabel('All Respondents')
plt.tight_layout()
plt.savefig('box_plot_experience.png')
plt.show()
print("Box plot saved to 'box_plot_experience.png'")
```

```
# Part 6: Box Plot for Experience by Sector and Education
# Description: Generates a box plot to show the distribution of experience years for each
sector (Government, Municipality, Private) by education level.
# Displays median, IQR, whiskers, and outliers, with sectors as hues for comparison.
# Saves the output as PNG for the thesis

plt.figure()
sns.boxplot(x='Education_Level', y='Experience_Years', hue='Sector', data=data_melted,
palette='Set2')
```

```
plt.title('Distribution of Experience Years by Education Level and Sector')
plt.xlabel('Education Level')
plt.ylabel('Experience Years')
plt.xticks(rotation=45)
plt.legend(title='Sector', bbox_to_anchor=(1.05, 1), loc='upper left')
plt.tight_layout()
plt.savefig('box_plot_education_sector_experience.png')
plt.show()
print("Box plot saved to 'box_plot_education_sector_experience.png'")
```

```
# Part 7: Correlation Between Education Level and Likert Questions
# Description: Computes correlations between education level (categorical) and Likert-scale survey responses (ordinal)
# using the Kruskal-Wallis test to compare response distributions across education levels (Ylempi, Alempi, Keskiaste).
# Saves p-values to CSV for thesis inclusion.

# Define survey question columns
cybersecurity_cols = [
    'Covid-19',
    'Sodan uhka (Ukrainan sota)',
    'Natoon liittyminen',
    'Etätyön ja hybrityön lisääntyminen'
]
statement_security_cols = [
    'Pilviratkaisut (cloud-services) ovat lähtökohtaisesti vähemmän turvallisia kuin perinteiset (on-premise) ratkaisut.',
    'Perinteiset (On-premise) ratkaisut tarjoavat paremman hallinnan tietoturvaan liittyviin kontrolleihin pilviratkaisuihin verrattuna.',
    'Pilviratkaisut (cloud-services) ovat vähemmän yhteensopivia alan säännösten ja standardien kanssa verrattuna paikallisiin ratkaisuihin.',
    'Pilveen tallennetut tiedot ovat haavoittuvampia kyberhyökkäyksille ja tietomurroille kuin paikan päällä (on-premise) tallennetut tiedot.',
    'Perinteiset (On-premise) ratkaisut ovat pitkällä aikavälillä kustannustehokkaampia kuin pilviratkaisut.'
]
cloud_adoption_cols = [
    'Tietoturvallisuutta',
    'Toiminnan jatkuvuuden hallintaa ja varautumista',
    'Riskienhallintaa',
    'Tietosuojaa'
]
statement_regulation_cols = [
    'Suomen lainsäädännöllä voidaan vaikuttaa ulkomaalaisiin toimijoihin',
    'Toisen valtion lainsäädännöllä voidaan vaikuttaa Suomen toimijoihin (esim. TietoEVRY)?',
    'EU:n lainsäädännöllä voidaan vaikuttaa ulkomaalaisiin toimijoihin',
    'Suuret globaalit toimijat määrittävät kyberturvallisuuden standradit.',
```

```
    'Toimijoiden ja valtion väliset sopimukset ovat riittävät, eikä erillistä kansallista
lainsäädäntö tarvita.',
    'Toimijoiden ja valtion väliset sopimukset sekä kansallinen lainsäädäntö ovat riittävät, eikä
EU tason',
    'Lainsäädännön lisäksi on ehdotonta, että toimintaa ohjataan ja tarkkennetaan toimijan ja
valtion erityissopimuksilla'
    ]

# Define education column
education_col = 'Koulutustasosi (ylin)'

# Check if columns exists
# Major problems with the statemen_regulatio_cols, there might be problem with encoding
(en-fi) or something..
all_cols = [education_col] + cybersecurity_cols + statement_security_cols +
cloud_adoption_cols + statement_regulation_cols
missing_cols = [col for col in all_cols if col not in data.columns]
print("\n=== Debug: Missing Columns Check ===")
if missing_cols:
    print(f"Missing columns: {missing_cols}")
    print("\n=== Checking for Similar Column Names ===")
    for missing_col in missing_cols:
        similar_cols = [col for col in data.columns if missing_col.lower() in col.lower() or
col.lower() in missing_col.lower()]
        print(f"Missing: {missing_col}\nSimilar in dataset: {similar_cols}")
    raise ValueError("Column name mismatch detected. Check debug output above and update
statement_regulation_cols.")


# Select relevant data and clean
data_corr_edu = data[[education_col] + cybersecurity_cols + statement_security_cols +
cloud_adoption_cols + statement_regulation_cols].copy()
data_corr_edu = data_corr_edu.dropna()

# Initialize results dictionary
kruskal_results = {}

# Function to perform Kruskal-Wallis test
def run_kruskal(data, col, education_col):
    try:
        groups = [data[data[education_col] == edu][col].values for edu in
data[education_col].unique()]
        if all(len(g) > 0 for g in groups):  # Ensure non-empty groups
            stat, p = kruskal(*groups)
            return p
        else:
            return np.nan  # Return NaN if any group is empty
    except ValueError:
        return np.nan  # Handle errors (e.g., insufficient data)
```

```
# Compute p-values for each survey question group
for col in cybersecurity_cols:
    kruskal_results[col] = run_kruskal(data_corr_edu, col, education_col)
for col in statement_security_cols:
    kruskal_results[col] = run_kruskal(data_corr_edu, col, education_col)
for col in cloud_adoption_cols:
    kruskal_results[col] = run_kruskal(data_corr_edu, col, education_col)
for col in statement_regulation_cols:
    kruskal_results[col] = run_kruskal(data_corr_edu, col, education_col)

# Convert results to DataFrame
kruskal_df = pd.DataFrame({
    'Question': list(kruskal_results.keys()),
    'Kruskal_Wallis_p_value': list(kruskal_results.values())
})

# Save results to CSV
kruskal_df.to_csv('kruskal_education_likert.csv', index=False)
print("\nKruskal-Wallis results saved to 'kruskal_education_likert.csv'.")

# Display results
print("\nKruskal-Wallis Test Results (Education vs. Likert Questions):")
print(kruskal_df)
print("\nNote: p < 0.05 indicates significant differences in response distributions across
education levels.")
```