Bachelor's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Nora Altamimi
Emina Engh
Katrine Brække Lyngen
Camilla Dagsgård Molland

Enhancing Communication and Collaboration between a Security Operation Center (SOC) and a Municipality

Bachelor's thesis in Digital Infrastructure and Cyber Security
Supervisor: Jia-Chun Lin
May 2023

NTNU
Norwegian University of
Science and Technology

Nora Altamimi
Emina Engh
Katrine Brække Lyngen
Camilla Dagsgård Molland

Enhancing Communication and Collaboration between a Security Operation Center (SOC) and a Municipality

Bachelor's thesis in Digital Infrastructure and Cyber Security
Supervisor: Jia-Chun Lin
May 2023

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Norwegian University of
Science and Technology

Abstract

Title:	Enhancing Communication and Collaboration between a Security Operation Center (SOC) and a Municipality
Date:	22.05.2023
Authors:	Nora Altamimi
	Emina Engh
	Katrine Brække Lyngen
	Camilla Dagsgård Molland
Supervisor:	Jia-Chun Lin
Employers:	Ronny Olsen, Head of Security, Sigurd Biørn, Senior Consultant and Per Øyvind Vold, Security counselor, Ikomm AS
Keywords:	Municipalities, External SOC service, Cybersecurity, Collaboration, Challenges
Pages:	64
Attachments:	10
Availability:	Open

Abstract:

Ikomm is owned by seven municipalities, and serves as their IT department. They are currently in the process of acquiring an external SOC provider to deliver SOC services for their municipalities. However, existing best practices for homogeneous organizations may not be suitable for complex organizations like municipalities. The aim for this thesis was to enhance collaboration with an external SOC and identify challenges that may arise. To gain insight into these challenges, we conducted surveys, interviews and reviewed reports. Based on the findings, we have developed a set of recommendations that serve as a guideline for improving collaborations with an external SOC. This includes what competences the IT department needs to have to ensure insight and understanding with a SOC, as well as division of responsibilities.

Sammendrag

Tittel:	Forbedre kommunikasjon og samarbeid mellom et sikkerhetsoperasjonssenter (SOC) og en kommune
Dato:	22.05.2023
Deltakere:	Nora Altamimi Emina Engh Katrine Brække Lyngen Camilla Dagsgård Molland
Veileder:	Jia-Chun Lin
Oppdragsgivere:	Ronny Olsen, Sikkerhetssjef, Sigurd Biørn, Seniorrådgiver og Per Øyvind Vold, Sikkerhetsrådgiver, Ikomm AS.
Stikkord:	Kommuner, Ekstern SOC tjeneste, Cybersikkerhet, Samarbeid, Utfordringer
Antall sider:	64
Antall vedlegg:	10
Publiseringsavtale inngått:	Åpen
Sammendrag:	Ikomm eies av syv kommuner hvor de fungerer som deres IT-avdeling. For tiden er de i prosessen av å skaffe seg en ekstern SOC-leverandør, for å levere SOC-tjenester til sine kommuner. Imidlertid, kan eksisterende beste praksis for homogene organisasjoner være uegnet for sammensatte organisasjoner som kommuner. Målet for denne oppgaven var å forbedre samarbeidet med en ekstern SOC og identifisere utfordringene dette medfører. For å få innsikt i disse utfordringene, gjennomførte vi undersøkelser, intervjuer og studerte rapporter. Basert på funnene har vi utviklet en rekke anbefalinger som fungerer som retningslinjer for å forbedre samarbeidet med en ekstern SOC. Dette inkluderer hvilke kompetanse IT-avdelingen trenger for å sikre innsikt og forståelse med en SOC, samt ansvarsfordeling.

Preface

Thank you to all those who have contributed to our bachelor's thesis. We are thankful for our employer Ikomm AS, who provided us with a highly engaging task of significant societal value, that aligns closely with our academic pursuits. We would also like to express our gratitude for the continuous support and guidance Ikomm and our supervisor Jia-Chun Lin has provided us with throughout this project. We truly appreciate those who have helped us along the way, especially Janne Cathrin Hetle Aspheim, Thea Lovise Leikvoll Fagerli, Ingrid Langevei Mæland who created the statistical diagrams from our survey. Furthermore, we are very grateful of everyone that participated in answering our surveys and agreed to an interview.

Contents

Figures

Tables

Glossary

CSIRT Computer Security Incident Response Team. A team consisting of IT professionals that provide services, support and incident response coordination for organizations. 14

HelseCERT Helse Computer Emergency Response Team. A specialized cybersecurity incident response team dedicated to the healthcare sector . 28, 54

ICT Information and Communications Technology . ix, 7, 11, 12, 14, 22

intermunicipal A collaboration between two or more municipalities with the purpose of managing shared problems or challenges. x, 15, 18, 19, 21, 22, 24–28, 30, 34, 50, 57, 62

IRT Incident Response Team. A group of professionals responsible for handling and responding to critical security incidents.. 7, 8, 27, 32, 53

ISAC Information Sharing and Analysis Center. An organization that works as a resource for information on cyber threats, as well as sharing experience and knowledge among organizations. 54

K-CSIRT Kommune-CSIRT. National center that provide relevant information regarding digital threats, incidents and vulnerabilities for municipalities. 4, 27, 28, 54

KiNS Foreningen Kommunal Informasjonssikkerhet. An association with the purpose of increasing information security in municipalities. 4, 19, 27, 28, 43, 54

NSM The Norwegian National Security Authority. The directorate for preventive national security. xi, xiii, 2, 7, 11, 12, 28, 36, 49–55

onboarding A process to integrate new employees or customers into an organization, to get familiar with its services or products. 8, 52

SOC Security Operations Center. An IT team comprising of professionals that continually monitors an organization's complete IT infrastructure round the clock, to promptly detect cybersecurity events in real-time and efficiently resolve them. ix, x, xiii, 1–5, 7, 8, 13, 14, 17, 18, 21, 24, 25, 27–32, 49–55, 57, 61, 62

TLP Traffic Light Protocol. TLP is a framework for designating and handling sensitive information based on its level of confidentiality to ensure appropriate audience access and prevent unauthorized disclosure[1]. xiii, 50

[1] `https://www.first.org/tlp/`, visited 23.04.23

Chapter 1

Introduction

This chapter will cover the background and provide an in-depth description and limitation of our task. Additionally, the effect, result, and learning goals will be provided, as well as the frames that define how we plan to achieve them. Furthermore, information about the team and the intended audience for the thesis will be included.

1.1 Project Background

We are living in a digital society where our infrastructure is built and reliant on advanced technology. The need for detecting and monitoring our systems has increased over the last few years, especially after the Covid-19 pandemic and the war in Ukraine. Having an in-house security operations center (SOC) or paying for external SOC services is therefore becoming increasingly common.

Ikomm is owned by, and serves as the IT department for seven municipalities, with nearly two decades of experience in this area. Currently, Ikomm provides services to over 40,000 users, and employs more than 130 individuals[1]. Ikomm is in the process of acquiring an external SOC provider to deliver SOC services to their municipalities, but establishing monitoring services for a municipality presents some new difficulties. Hence, they want help to highlight and create solutions for these challenges.

1.2 Project Area

This section provides a comprehensive overview of the problem area and problem statement for the thesis. It highlights the objectives of the research and scope of limitations considered.

[1] `https://www.ikomm.no/`, visited 23.01.23

1.2.1 Problem Area

Implementing a SOC can be both time-consuming and expensive if not done right. Many of the best practices have been established for homogeneous organizations and are not well suited for more complex organizations like a municipality. The problem statement is therefore as follows: *Is a well-functioning and qualified SOC service sufficient to secure the municipality from an information security perspective?*

The objective of the thesis is to enhance collaboration with an external SOC from a municipal perspective, and how to best handle this interaction. To effectively implement security measures based on feedback from the SOC, the municipality needs a broad understanding of information security. Therefore, mapping what competence a municipality, focusing on the IT department, at least needs to acquire to ensure insight and understanding, is necessary. The goal is to develop a set of recommendations that work as a guideline for improving interaction and collaboration with an external SOC. The recommendations will be influenced by The Norwegian National Security Authority (NSM) basic principles for ICT Security [1].

1.2.2 Limitations

The focus will be on necessary competence and how communication and responsibilities should be distributed for optimal collaboration. The parties consist of a municipality and an external SOC. Hence, the development of utilizing in-house resources to create an internal SOC will not be discussed. Issues related to economics and politics will not be investigated, as this would cover a new field of study. The specific equipment a municipality owns and operates, and any security related threats residents may expose themselves to using their devices at home, will not be considered. In addition, analyzing the necessary competence that a SOC provider must possess to provide quality services is out of scope.

1.3 Target Group

The thesis will primarily be of interest for sensors, fellow students, as well as anyone with interest in this topic. To understand all aspects, it is not necessary to have a comprehensive technical understanding, but a fundamental knowledge in information security is recommended. The results are intended to benefit Ikomm, as well as those involved in IT related activities, especially within a municipality.

1.4 Goals

The project goals are divided into three parts: effect-, result- and learning goals. The effect goals are the long-term objectives that describe the specific outcome that we aim to achieve through the completion of the final product. The result goals are the desired outcomes for the final project delivery, and the learning goals defines the specific knowledge we seek to gain throughout the project.

1.4.1 Effect Goals

1. Easier SOC implementation by providing a general set of guidelines
2. Increase collaboration between a SOC and a municipality
3. Reduce workload by optimizing the implementation of a SOC for a municipality
4. Improve general information security understanding by increasing awareness about the importance of knowledge
5. Prevent security breaches by having sufficient monitoring and response mechanisms

1.4.2 Result Goals

1. Propose a set of best practice recommendations to improve interaction between a SOC and a municipality
2. Map what competence a municipality should at least acquire to be able to effectively implement feedback from the SOC
3. Create a service catalog that comprises the minimum services a SOC should offer

1.4.3 Learning Goals

1. Improve our project management abilities
2. Improve our knowledge within scrum-based development
3. Enhance our communication proficiency
4. Learn more about the organization of a municipality and a SOC

1.5 Project Members

In this section, the team will be presented, together with knowledge we had to acquire in order to write the thesis. Furthermore, it provides a description of various individuals who have played a significant role in the research and writing process.

1.5.1 Project Team

The team consists of four students pursuing a bachelor's degree in Digital Infrastructure and Cyber Security at the Norwegian University of Technology and Science (NTNU) Gjøvik[2]. Various courses the team have attended are relevant to the thesis, including software development (PROG1004), ethical hacking (IIK3100), network (DCSG1006/DCSG2001), cloud services (INFT2504), risk management (DCSG2005), incident response (IIKG320) and reverse engineering (IMT4116). To fully comprehend the task, it was necessary to gain a better understanding of the organizational structure of a municipality, as well as the functioning of a SOC. The interviews with IT personnel were the biggest contributor to build the needed competence, and they were conducted over a period of two months.

1.5.2 External Members

Employers: Ronny Olsen, Head of Security, Sigurd Biørn, Senior Consultant, and Per Øyvind Vold, Security Counselor, for Ikomm.

Supervisor: Jia-Chun Lin, Associate Professor who works at the Department of Information Security and Communication Technology[3].

Statistics: Janne Cathrin Hetle Aspheim, Thea Lovise Leikvoll Fagerli, Ingrid Langevei Mæland, from Department of Mathematical Sciences[4], helped form the statistics from the surveys.

Additional help: Bjørn Tveiten, CEO at K-CSIRT, Erik Hjelmås, Associate Professor at the Department of Information Security and Communication Technology, and Frank Kirkeng, IT secure Operation Manager at Netsecurity AS[5], who provided helpful feedback. Harald Torbjørnsen, CEO of KiNS, presented the team with the contact information of relevant people in different municipalities.

1.6 Frames

The report was written in English using Overleaf[6], to make it accessible to a wider audience, as well as accommodate our supervisor's preference. With a shared OneDrive folder, all team members had access to the updated version of all documents. A separate document was dedicated to keep track of tasks and their completion. Most of the work was done collectively to encourage discussions and ensure more perspectives, but the workload related to the surveys and any additional

[2] `https://www.ntnu.no/studier/bdigsec`, visited on 12.02.23
[3] `https://www.ntnu.edu/iik`, visited 10.02.23
[4] `https://www.ntnu.edu/imf`, visited 10.02.23
[5] `https://www.netsecurity.no/`, visited 14.05.23
[6] `https://www.overleaf.com/`, visited 17.02.23

reading was done individually. With an average of 30 hours a week, Discord[7] and on campus has been our primary methods of working. Microsoft Teams[8] has been the preferred communication channel for meetings with Ikomm, supervisor and IT personnel.

1.7 Thesis Structure

The report is divided into eight chapters that should be read sequentially to gain a comprehensive understanding of the research conducted.

Chapter 1 – Introduction
Covers the background for writing the thesis, along with details on the intended audience, and relevant information about the team.

Chapter 2 – Background
Includes key information helpful for the rest of this thesis, the purpose, and why the topic is relevant.

Chapter 3 – Related Work
Covers what existing work we have used that is relevant for our research and how our approach is different.

Chapter 4 – Methodology
An overview of the methods used to gather information and a detailed description of how the data will be processed and analyzed.

Chapter 5 – Analysis results
Presents all findings from interviews and surveys, which forms the foundation for the recommendations.

Chapter 6 – Recommendations
Based on the analysis results, the team has formulated concrete recommendations for enhancing collaboration between a municipality and a SOC.

Chapter 7 – Discussion
Presents a reflection on decisions, thoughts on the teamwork throughout the thesis period, and any potential areas of improvement.

Chapter 8 – Conclusion
Evaluate if goals were achieved, review the problem statement, and describe possible further work.

[7] `https://discord.com/`, visited 10.2.23
[8] `https://www.microsoft.com/nb-no/microsoft-teams/`, visited 13.02.23

Chapter 2

Background

This chapter will introduce and elaborate the necessary theory in order to understand the rest of the thesis, including SOC, IRT and NSM´s basic principles for ICT Security. Moreover, the organization of municipalities, including communication and the challenges they face, such as limited funding and lack of technical expertise, will be mentioned. Furthermore, the purpose of the thesis will be explained, along with why it is relevant today.

2.1 Security Operations Center

A security operations center (SOC) is a team of IT security professionals that monitors an organization's IT infrastructure to detect and respond to cybersecurity events in real-time as quickly and effectively as possible[1]. The SOC´s responsibilities and activities can be categorized into prevention, detection and response. Prevention sets the foundation for how effective and successful the SOC can carry out its tasks. Important activities include incident response planning, routine maintenance and asset inventory. The primary responsibilities of a SOC is to detect and respond to incidents before they cause significant damage. To accomplish this, the SOC engages in activities such as monitoring, threat hunting, and log management, which are critical for identifying and mitigating potential threats in a timely and effective manner. It is essential to acknowledge that providers may offer and deliver SOC services differently.

2.1.1 SOC Services

SOC is not yet a widely established term and may be subject to varying interpretations. To establish a precise definition of the term we have included a service catalog. Table 2.1 contains the service catalog with a short description of the services we expect the SOC to offer. In conjunction to the service catalog, it is necessary to

[1] `https://www.ibm.com/topics/security-operations-center`, visited on 03.03.23

have a good onboarding, management and handling. The process of optimizing the SOC to effectively cater to the organization's requirements is time-consuming, as it needs to be tuned. Consequently, there will be a need for thorough communication in the beginning, and testing of the SOC service, to ensure the service works as expected. Granting the SOC appropriate power of attorney is essential to maximize its efficiency. Without the necessary privileges, the service may encounter limitations in its capabilities.

Table 2.1: Service catalog

Service	**Description**
24/7/365 Surveillance	At least one or two employees are available around the clock every day of the year
Threat Hunting	Proactive search for advanced threats and indicators of compromise
Vulnerability Assessment	Identification, assessment, and remediation of system vulnerabilities
Monitor	• Logs • Users • Endpoints • System • Network
Detect and Prevent	Detect abnormalities and suspicious activity in the system before it can cause damage
Analyze	Analyze alerts and be able to categorize and determine severity
Response	Take necessary actions to mitigate an incident, and support in incident response
Report	Create reports after incidents, and ensure timely communication with all customers regarding recent risks and updates

2.1.2 Incident Response Team

In cybersecurity, an incident response team (IRT) refers to a team of experienced IT professionals that are highly certified across multiple disciplines. The team will often consist of a team leader, lead investigator, communication liaison, and may include representatives from IT, management, and legal departments. IRT manages, responds and recovers significant cyber incidents that have been escalated to an emergency [2], such as successful cyber attacks, data breaches or system failures. The objective is to minimize damage and remediate vulnerabilities, to effectively get organizational operation back to normal after an incident. Recovery is an important activity as it focuses on eradicating threats and restoring affected assets to an improved pre-incident state. Equally important in the recovery process, is the review of incidents and the enhancement of the response plan for future incidents.

2.2 Municipalities in Norway

Norway has 356 municipalities ranging from about 200 residents to 700 000[2]. A municipality is a local self-governing unit, responsible for providing a range of public services to the residents in its geographical area. The idea behind local democracy is that those who live in a municipality know the local problems best and how to solve them [3].

2.2.1 Organizational Structure

Municipalities have similar organizational structures, commonly featuring a mayor who serves as the political leader, and a chief municipal executive, responsible for ensuring that the administration is conducted in accordance with laws and regulations[3]. Reporting to these positions are various departments, who are responsible for implementing decisions. Each department has several agencies that oversee activities within their field. The presence of various departments and agencies reflects a non-homogeneous nature. Unlike homogeneous organizations, characterized by consistency and standardization, a municipality encompasses diverse entities with distinct roles and responsibilities. Figure 2.1 displays a simplification of a typical municipality's hierarchy structure, including its departments and agencies.

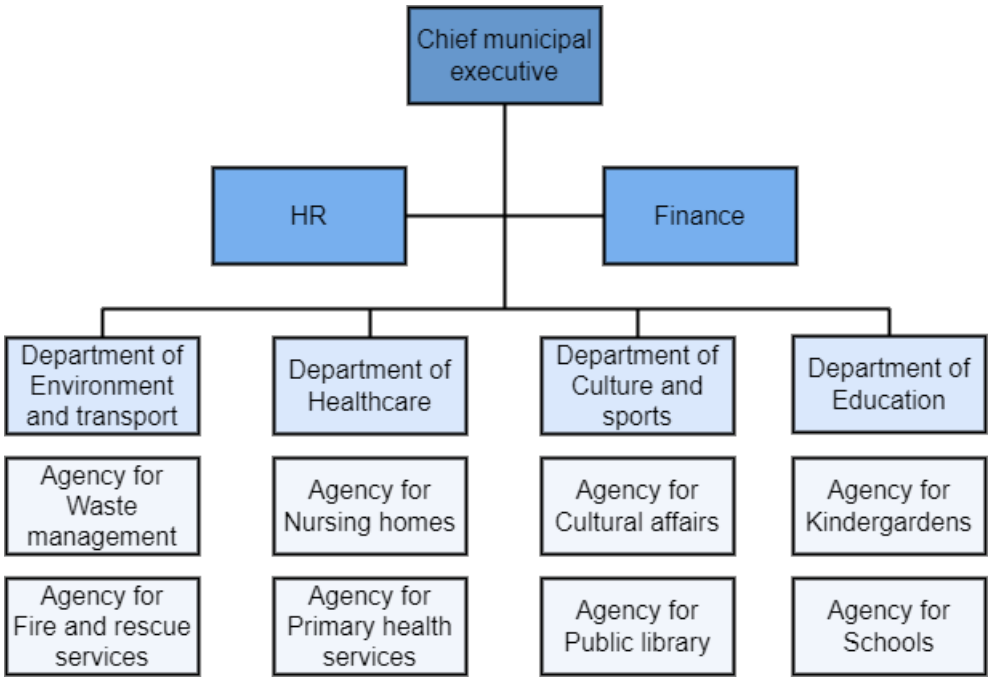


Figure 2.1: Example of an organizational chart of a municipality

[2] `https://www.ssb.no/statbank/table/11342/tableViewLayout1/`, visited 03.03.23
[3] `https://www.oslo.kommune.no/politikk/`, visited 19.03.23

2.2.2 Internal Communication

Distributing information and having communication between municipalities and its residents play a vital part in building trust. Transparency is a key factor, as highlighted by an article published by The Government of Norway in 2018 [4]. According to the article, municipalities that prioritize transparency tend to have the most satisfied residents, underscoring the importance of openness and honesty in promoting a positive relationship between elected representatives and the residents. In addition, it is important to use plain language, and ensure easily accessible information about the municipality's politics and services. If residents or employees want to make contact, or need help, it should be clear where they can do so, as the municipalities often has multiple channels for communication. This can be through paper, websites, dedicated communication platforms or meetings [5].

2.2.3 Challenges

Municipalities face several challenges when trying to establish IT security, reasons being economic constraints, lack of competence, and large-scale infrastructures. Receiving funds can be challenging, as resources are often prioritized for essential sectors such as education and healthcare. Municipalities often lack awareness that digitalization requires necessary competence and resources in the cybersecurity field. Due to limited resources, employees often cover multiple roles, and few are able to hire dedicated security specialists. Which can lead to a lack of technical expertise required to understand the importance of cybersecurity, and the need for adequate equipment. Despite having the appropriate tools, the complexity of the municipality's infrastructure can pose challenges when it comes to the configuration and implementation of systems. Municipalities are not homogeneous organizations, as their employees are spread across different departments, agencies and units. Each department operates independently, with its own set of agencies overseeing specific activities within their respective fields. This decentralization introduces complexities in terms of coordination, communication, and decision-making, as different departments may have unique objectives and approaches. As a result, achieving unity and centralized control becomes challenging within the organizational structure of a municipality.

2.3 The Norwegian National Security Authority Basic Principles for ICT Security

"NSM is Norway's directorate for preventive national safety. NSM also have a national responsibility to discover, inform and coordinate the handling of serious ICT attacks" [6]. In 2020 NSM made a framework for ICT security. The framework consists of 21 principles that "give advice on how to protect information systems, data and other services against unauthorized accessibility, damage or misuse." [7]. These principles are relevant for all organizations, and can help to secure information systems. Depending on the organization's size and available resources, it may be necessary to prioritize which ones to implement.

Figure 2.2 illustrates NSM´s basic principles split into four categories, where each represents an important stage in securing information systems. The framework includes the topics identification and mapping, protect and maintain, discovering, and handling and recovering. Each subsection mentions their specific principles for information security.

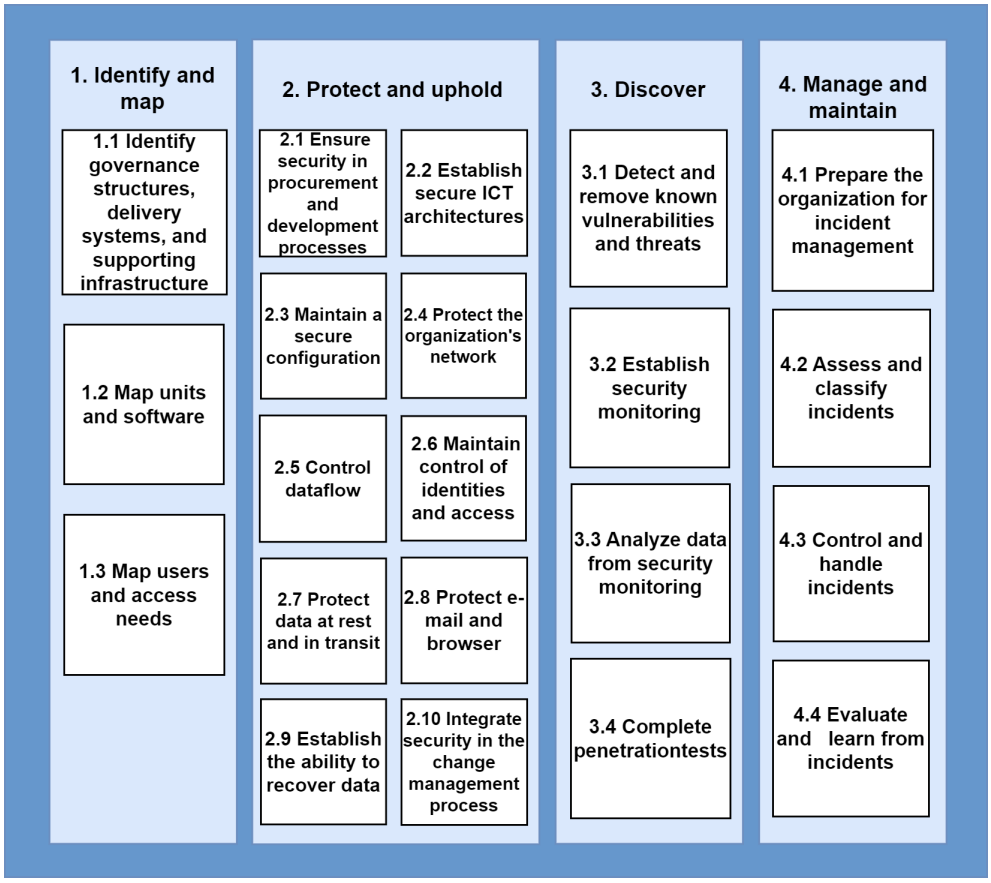


Figure 2.2: NSM´s basic principles

Table 2.2 presents all the measures, with a short description, that are included further in the thesis. The full measures are found on NSM´s web page: NSM [1].

Table 2.2: NSM measures used in the thesis

Measure	Description
2.1.2	"Buy modern and updated hardware and software so that newer security features are built-in"
2.1.3	"Prefer ICT products that are certified and evaluated by a trusted third party"
2.1.10	"Investigate the security of service providers when outsourcing services"
2.3.1	"Establish a centrally controlled regime for security updates"
2.7.5	"Define security level requirements for different types of information with varying needs for confidentiality protection"
3.1.1	"Conduct regular vulnerability assessments in the information system using automated tools. The assessment should cover clients, servers, and networks"
3.3.4	"Collect and process threat information from relevant sources so that it can be used in the assessment of potential security incidents"
4.1.1	"Establish an incident management framework that addresses the need for business continuity in emergency and crisis situations"
4.1.3	"Develop a role and responsibility description for personnel who will be involved in incident management"
4.1.5	"Determine which communication channels should be used in connection with incidents"

2.4 Project Purpose

Digital threats are becoming increasingly sophisticated and are constantly evolving. Responding to all types of threats requires an intricate competence that only a few possess. When thinking about the future, most municipalities are not capable of handling all of this by themselves. Therefore, a better solution for monitoring and incident response is necessary.

Chapter 3

Related work

This chapter covers what existing literature have been utilized to inform and support our research. This will include reports and articles with information about municipalities, and the functioning and implementation of a SOC. Furthermore, a description of the reports, the inspirations drawn, and their influence on the project, will be presented.

3.1 DigiViken

DigiViken is a partnership between municipalities in the county Viken in Norway [1]. Their primary objective is to develop robust digital solutions for municipalities and their residents. Through this collaboration, DigiViken aims to facilitate information sharing, enhance interaction, and elevate the technical and digital competence of the participating municipalities [8]. In 2022, DigiViken extended an invitation to its partnering municipalities, asking about their interest in acquiring a SOC service[2]. By September, more than 40 municipalities had expressed their interest to participate, indicating a significant level of engagement and enthusiasm [3]. They also provided a draft tender document that included an example offer that we found relevant and interesting for the thesis. The topics covered were found to be similar to the ones we already decided to write about, but they did not contain much information. The example service catalog was especially inspiring and we recognized it would be beneficial to develop our own version.

[1] https://digiviken.no/om-digiviken/, visited 15.03.23

[2] https://digiviken.no/skjonnsmidler-til-felles-soc-siem-hvem-vil-vaere-med/, visited 15.03.23

[3] https://digiviken.no/prosjektleder-for-soc-siem-prosjektet-tilsatt/, visited 15.03.23

3.2 MITRE Attackers Tactics, Techniques and Common Knowledge Framework

The MITRE report addresses challenges in cybersecurity and proposes strategies to protect organizations from cyber threats [9]. This includes knowledge about a SOC, that we found highly beneficial. The MITRE report consists of 11 strategies, but the team identified only three as particularly relevant for our objective. These were Strategy 2 (Give the SOC the authority to do its job), Strategy 4 (Hire AND grow quality staff) and Strategy 9 (Communicate clearly, collaborate often, share generously). Their report was highly focused on the implementation of an in-house SOC, specifically discussing the process of who to hire. While this information was not directly applicable to the team's focus on collaboration with an external SOC, it provided valuable insights on how to effectively work with, and utilize a SOC. Thus, the team had to consider this perspective and investigate if the same principles could be applied when working with an external SOC.

3.3 The Norwegian Center of Information Security

In 2015, the Norwegian center of information security (NorSIS) collaborated with Lillehammer and Gjøvik to conduct a study aimed at highlighting the necessity for a CSIRT to mitigate and manage ICT incidents within the municipalities. The findings and recommendations derived from this study were documented in the "Kommune CERT" report [10]. A significant portion of the report was dedicated to assessing the existing information security competence in the municipalities. Inspired by the study's approach, we conducted our own survey to determine the level of information security expertise among employees within the municipalities. While their report focused on the need for a CSIRT, ours is centered on the need for a SOC.

3.4 The Norwegian Digitalisation Agency

The report "The work with information security in county municipality and municipalities" by The Norwegian Digitalisation Agency´s (DIGDIR) intend to get a better understanding of how the county municipality and municipalities work with information security [11]. This report strengthened our knowledge on what municipalities lack regarding their internal control, preparedness, exercises, incident management, safety culture and competence. DIGDIR's findings concluded that many small and medium sized municipalities lack knowledge in all the mentioned fields. Gaining this knowledge inspired us to group municipalities by size, determined by the number of residents, when creating the survey. However, the grouping of municipalities in our survey did not align with the three groups specified in the report. Instead, we opted for four groups, to divide the municipalities into smaller sections in order to identify more pronounced differences.

3.5 The Norwegian Directorate for Civil Protection

Every year, The Norwegian Directorate for Civil Protection (DSB) publishes a report where they review the year's activities with context to risk and vulnerabilities to society. We read the 2021-year report, to see if there was any information about municipalities that could be useful [12]. Although, a significant portion of the report was not directly relevant to the thesis, certain sections contained valuable information that was useful for the team to investigate further. One section mentioned that municipalities generally have good emergency plans, and a comprehensive risk and vulnerability evaluation, but they may not be updated regularly. Consequently, we determined to explore whether this was also the case for the IT departments within municipalities. This involved examining the existing information security measures in place, and how they are maintained. Furthermore, the report highlighted the advantages of intermunicipal collaborations across various fields, which inspired the team to investigate how IT organizations collaborate with municipalities, other potential information security collaborations, and why this could be a beneficial approach.

Chapter 4

Methodology

Within this chapter, methods that were utilized to gather relevant information, and why these proved to be effective, will be discussed. The research process has incorporated both qualitative and quantitative methods, with a focus on collecting and analyzing data [13].

4.1 Interview Process

Interviews were selected as one of the preferred methods for gathering information, as they facilitate obtaining insights and in-depth knowledge. Engaging in dialogue during interviews enhances communication, and reduces the likelihood of misinterpretation. Furthermore, interviews offer the advantage of asking follow-up questions directly, enabling further clarification or addressing any uncertainties that may arise.

A total of 13 structured interviews were conducted as part of this project, each following a predefined set of questions with additional and customized ones depending on the respondent. The questions aimed to gather extensive information and insights regarding IT operation, including challenges faced by municipalities when implementing a SOC. All the participants were individuals possessing significant expertise in IT security, from both a municipal and SOC perspective. Out of the 13 interviews, six were respondent interviews that specifically focused on individuals who had firsthand experience with a SOC from a municipality perspective. These interviews provided valuable insights into the practical aspects of implementing and operating a SOC for a municipality. The remaining interviews were informational interviews[1], where the participants had extensive knowledge and expertise either with a SOC or a municipality. These interviews provided a broader perspective and in-depth understanding of the challenges and best practices related to SOC services and municipalities. The questions for the municipalities and

[1] https://www.shiksha.com/online-courses/articles/different-types-of-interview/?fbclid=IwAR3qhV7nO2d1SFUvn0TW5S2A1Borh3UVouJnZ3DgBAAsExVO47JSQhgZoRs,visited 12.04.23

intermunicipal collaborations were identical, facilitating easier comparison of responses at a later stage. The process of conducting the interviews can be seen in Figure 4.1.

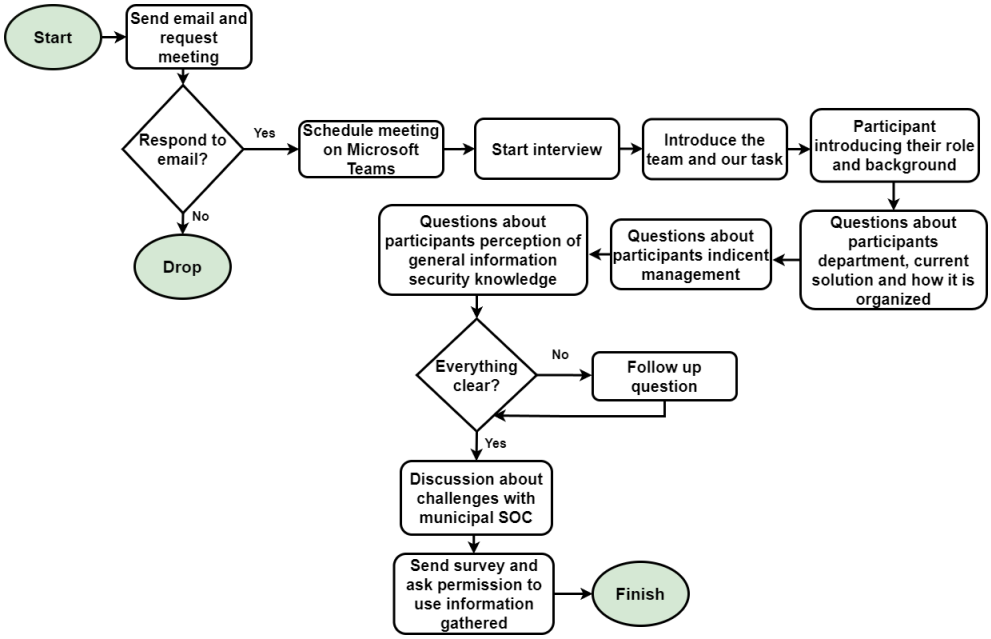


Figure 4.1: Flowchart of interview process for municipalities

4.2 Conducting Surveys

Survey were the second method for information gathering because of its numerous benefits. They allow for systematic collection of data from a larger number of respondents, enabling easy comparison and statistical analysis of responses. Additionally, the flexibility of surveys allow the respondent to answer at their convenience. These advantages make surveys a versatile tool for gathering information and obtaining valuable insights. To achieve the objective of identifying the necessary competence for a municipality to effectively utilize feedback from a SOC, we conducted two surveys. One survey was sent to the email address of the municipality, while the second was targeted towards IT departments. These surveys were essential in enabling us to gather information on the current competence within municipalities.

The survey for all departments included questions regarding their familiarity with both their own, and their municipality´s use of information technology. In an effort to maximize participation, emails were distributed with the survey and a brief description of its purpose to the service centers of all the municipalities in Nor-

way. With the help from Ikomm, the survey was also made available on the KiNS website. As a result, the survey received an overwhelming response, surpassing 300 participants in total. The response rate exceeded expectations, considering municipalities often fail to see emails due to a high volume of messages, or take an extended period of time to respond.

The second survey was distributed using the same method, but directed to the IT manager rather than the municipality's email. In addition, the survey was sent to all individuals we interviewed from municipalities who worked in the IT department. The purpose of the survey was to assess the existing information security measures implemented by municipalities, and gather their perspectives on inter-municipal collaborations.

4.2.1 Survey Structure

The structure of the surveys were designed to be very simple, and easily understandable for all participants. To ensure clarity, the surveys were written in Norwegian, and explanations for any terms that might have been unfamiliar were provided. The options were structured in a clear and concise manner, primarily consisting of yes/no options of varying degree, which can be seen in Figure 4.2. By following this approach, we ensured that all participants would be able to confidently and accurately respond to all the questions.

To ensure ease of statistical grouping and analysis, the surveys did not include text boxes for participants to provide open-ended answers. Additionally, a limited number of questions were included, to avoid overwhelming participants and minimize survey completion time. The intention was to make the survey brief and efficient, with most respondents being able to complete it within 3-4 minutes. All questions were carefully structured in a logical and chronological order, to provide a seamless and intuitive user experience.

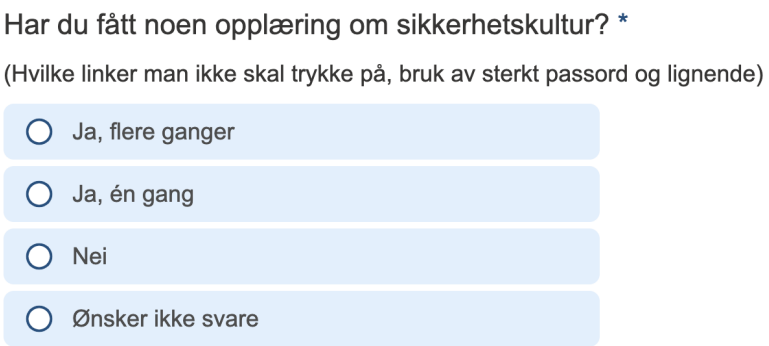


Figure 4.2: Example question from survey

4.3 Analysis Method

The analysis was divided into two distinct sections. The first section covered the interviews, where the responses were presented and organized in tables. The primary objective for this section was to identify similarities among the interviewees, allowing us to develop a baseline for understanding. Differences were especially interesting since it made room for discussions and further research. The next section was dedicated to the statistical analysis of the surveys, that were visualized using Python in Jupyter Notebook[2]. This was done to enable efficient graph creation, while tailoring the presentation format to best convey the intended purpose of each question. The results were utilized to inform, and support the proposed recommendations. To analyze the variation in responses based on the size of municipalities, the data was grouped according to the number of residents: $< 10\,000$, $10\,000 – 20\,000$, $20\,000 – 50\,000$ and $> 50\,000$. Figure 4.3 illustrates how the statistics were planned to be visualized.

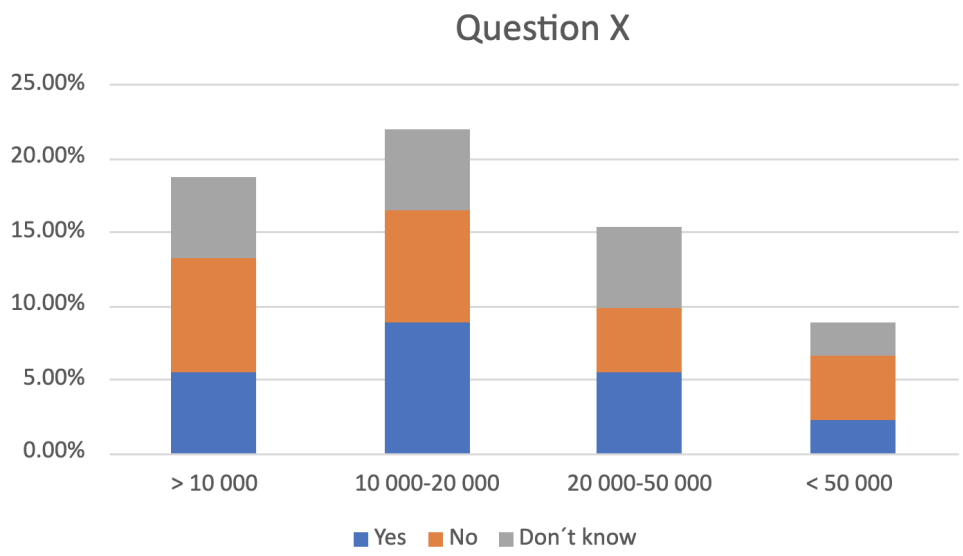


Figure 4.3: Example of statistics

[2] `https://jupyter.org/`, visited 15.04.23

Chapter 5

Analysis Result

This chapter presents the results obtained from the interviews and the surveys. The interviews were grouped based on individuals working in a municipality or intermunicipal collaboration, and SOC providers. The interviews with municipalities were categorized into six tables, while the SOC providers were divided into three. Each table provides a summary of the answers, which are then followed by an analysis of the results. The survey results are visualized using figures, accompanied by a detailed analysis of the responses. The results serve as the foundation for the recommendations that will be presented in the subsequent chapter.

5.1 Interview Results

In this section, an overview of the information and topics discussed during the interviews with municipalities, intermunicipal collaborations, and SOC providers, will be presented. The interviews were divided into two sections, namely municipalities and SOC providers, for better organization and understanding. The results were organized by topics and presented in structured tables that include corresponding themes and answers. Each bullet point represents an answer, but in certain interviews, not all questions were asked due to time constraints, or the discussion may have deviated from the intended topics, so the number of points may vary.

5.1.1 Municipalities and Intermunicipal Collaboration Results

After introducing the project area, the respondent's background and current role were discussed to gain a better understanding of their professional profile. It was also a natural starting point for building a more personal connection. Insight into the IT department's structure and services was sought to form a comprehensive overview of the current situation. This was to determine the extent of services that could be managed by an IT department of that size. Table 5.1 presents the answers about these topics.

Table 5.1: The interviewees role, their IT department, and which services they provide

Theme	Municipality answers	Inter-Municipality answers
Role and background	• 23 years of experience in the IT industry, 13 years in the municipality • Head of Security • Chief Information Security Officer • Digital Transformation Advisor • Service Manager and Information Security Manager • Technical Leader	• Daily leader, with ICT education • Chief Executive Officer • Chief Information Security Officer
Organization	• Operation department, a lot of technicians • Flat structure, will later be changed • Each department has its own digitalization resource	• Delivers all IT related services for their municipalities • A hierarchical structure • The intermunicipal collaboration is their IT department • No separate IT department in their owner municipalities
System and service	• Operation department, a lot of technicians • Flat structure now, but this will be changed • Each department has its own digitalization resource	• The municipalities are data controllers, system owners and system adminis, while the intermunicipal does security monitoring, detection, analysis and incident response • Operates their own platform, data storage, communication and infrastructure • Works with security mechanisms, protocols, vulnerabilities, security reviews and threat intelligence • Operational, one-to-one advisory and recommendations for incident management, as well as digital security expertise covering the entire range of tasks required by a municipality • IT support, IT operations and project management

The interviewees were highly educated in the field of interest for the thesis, with firsthand experience working with IT in municipalities. Their knowledge and experience greatly contributed to the interviews and the gathering of information, ensuring the credibility and relevance of the obtained data. It was evident from the interviews that regardless of size, all municipalities are required to deliver the same general set of IT services, but the difference lies in how they are organized. A shared IT department between multiple municipalities offer several advantages, including the ability to share resources and expertise, which can be particularly beneficial for smaller municipalities with limited budgets. Pooling resources allows for improved and more efficient IT services, while also reducing costs and enhancing overall efficiency.

During our discussions with the interviewees, we discovered that the average age of employees in the municipalities was considerably high. Multiple interviewees expressed their concern about this trend, as it presents challenges in terms of recruiting and attracting younger talents. Working for a municipality can carry certain stereotypes, and recent graduates may be attracted to bigger businesses for various reasons. Some may be unaware that working for a municipality is even an option, while others may prefer to work with colleagues in their age group or seek better salary options elsewhere. Acquiring new competence is always desirable, but hiring younger talents may be challenging and require a dedicated effort.

Current and wanted competence
To gain a comprehensive understanding of current and required competence, we inquired about the information security knowledge of both the IT department and general employees. A key objective for the thesis was to map the necessary competence in a municipality. As a result, obtaining insights from IT professionals on their perceptions of general information security knowledge proved to be particularly insightful. Table 5.2 shows the answers for current and wanted competence in municipalities.

Table 5.2: Current and wanted competence in municipalities

Theme	Municipality answers	Inter-Municipality answers
IT department	• Overweight with operation competence • Dedicated data protection officer and information security officer • 50% come from upper secondary school and have obtained a certificate of apprenticeship in IT operations. The rest have bachelor or higher degrees	• Operation and service, good competence in security and project management • High school diploma is a minimum • No IT competence in the municipality, the intermunicipal collaboration is their IT department • Mostly employees with operation competence
Wanted competence in the IT department	• Would need 1-2 specialists with experience regarding a SOC • Further develop the internal competence • Need for more security competence • Eventually all systems will be moved to cloud solutions and a different type of expertise will be needed in the future	• Competence that enables the municipality to order and control product and service deliveries themselves • Want more in digitalization, and should also be competence in operation, server, data storage, network, communication
General information security in the municipality	• All departments are more mindful of information security, but it is a continuous job to raise awareness • Room for improvement, but people are more aware of phishing links • Some leaders are highly aware of security	• The competence is low, so it is hard to establish a good security culture • It varies, but generally weak • Big difference between small and large municipalities
Wanted competence for municipality	• A fundamental knowledge about phishing, strong password and routines for changing passwords • Regularly mandatory information security training • New employees should be educated and integrated into their security culture as soon as possible • Generally, be more security aware	• Need a basic competence in privacy protection and information security. • The administration and leaders need a more advanced competence • Everyone in a municipality need more competence in information security • Should be able to differentiate fake phishing and spam emails from legitimate ones
Challenges	• Challenging getting experienced personnel • Difficult to attract experts from bigger organizations	• Vulnerable when standing alone, regarding security and competence

The findings indicated a strong level of project management and security competence in terms of operation and service. However, it was evident that there was an imbalance with an overrepresentation of operation competence. The municipality expressed the need to enhance the internal expertise within their IT departments and improve the overall information security knowledge of their employees. This is crucial for establishing a robust security culture. The wanted competence was that all employees have a fundamental knowledge of phishing, password creation, and changing routines, with regular mandatory security training. It was also identified a need for more IT personnel with security competence, as well as one or two specialists experienced in SOC. The desired competence includes digitalization, operation, server, data storage, network, and communication. However, it seemed to be challenging to acquire experienced personnel due to better salary and job opportunities available elsewhere.

Smaller municipalities usually lack security competence and are therefore more vulnerable when standing alone. An intermunicipal collaboration with multiple small municipalities is therefore considered a good solution for acquiring competence and resources.

Communication channels
The interviews included questions regarding communication channels, aiming to understand how communication was conducted, and to determine whether security was a primary consideration when selecting platforms. Identifying the tools used for reporting security incidents was also done, with the purpose of gaining an overview of the reporting process and assessing the ease of use. Any challenges regarding communication were also discussed to help identify problems. Table 5.3 presents the answers about communication channels.

Table 5.3: Communication channels used by municipalities

Theme	Municipality answers	Inter-Municipality answers
Standard communication channel	• Microsoft Teams with different channels • Email • Microsoft Teams	• Has a standard channel where employees can communicate • Office 365, Teams, because a lot of people have knowledge of using this beforehand • Encrypted emails or Mattermost • Microsoft Teams and dedicated forum • Microsoft Teams
Channel or tool used to report security incidents	• Have a self-service portal	• Quality management system • Service desk or messages directly to IT • Report to their supervisor that will forward it, or make direct contact • Report by either calling or submit on their website • A self-service portal accessible to everyone. Some events are autogenerated by systems. Have standard ABC-incidents
Challenges	• Too many channels	• Too many Teams channels can become unmanageable. A risk that someone might accidentally post information in the wrong group, leading to potential data breach • High threshold for reporting

The interviews revealed that Microsoft Teams was commonly used for communication with various channels serving different purposes, implying some consideration for security. However, only one mentioned encryption or Mattermost[1]. Most municipalities lacked a specific tool or channel for reporting security incidents, which may explain the high reporting threshold. Having too many channels was recognized as a problem since it led to confusion and disorganization. This is a common challenge, and may lead to information getting accidentally misplaced. Overall, the findings suggest that while some intermunicipal collaborations have established effective communication channels, there is still room for improvement. Particularly in terms of reporting security incidents and managing Teams channels to mitigate security risks.

[1] `https://mattermost.com/`, visited 20.04.23

Incident management

To understand how incident management is handled by municipalities, questions regarding incident response and responsible entities were asked. The aim was to ascertain whether municipalities possess the capability to manage incidents independently, or if they rely on external resources for assistance. The answers can be found in Table 5.4.

Table 5.4: How municipalities handle incident management

Theme	Municipality answers	Inter-Municipality answers
Incident response	• Capable of handling a lot themselves • Uses K-CSIRT and Ikomm, along with an additional third-party • Incident response plan are continuously being developed, with improvements made every time an incident occurs • In most cases, incidents are handled by the IT department, but IRT can take over • Their external SOC service requires a shift scheduled that ensures that at least one employee is always available	• The municipality handles most themselves, but contacts KiNS and K-CSIRT if they need help • Resolve incidents themselves and reach out to the response teams if they need extra assistance, but concerned about long queues • Handle most incidents themselves but have an agreement with a security company

A recurring theme evident in these answers is that municipalities predominantly handle incidents internally, but are willing to seek external assistance when necessary. This may indicate that the municipality underestimates the need for professional assistance, probably due to the cost and a belief in their own capacity to manage it themselves. A concern were expressed regarding potential delays in receiving immediate aid if multiple customers require assistance simultaneously with more critical situations. It is therefore important for municipalities to establish clear agreements with external resources, and explore alternative solutions.

Collaboration and partnerships

We aimed to examine whether the municipalities engaged in collaborations or maintained contact with other municipalities for information or assistance. Since an intermunicipal collaboration already suggests that the municipalities have arrangements with others, it was interesting to learn more about any further collaborations they had with organizations. The question was asked to identify collaborations, understand the ways in which the organizations proved beneficial, and assess their satisfaction with them. We sought to identify common ones and

explore reasons for not being part of any. Table 5.5 shows the collaborations mentioned in the interviews.

Table 5.5: Partnership municipalities have

Theme	Municipality answers	Inter-Municipality answers
Collaborations	• K-CSIRT, Ikomm and third-party vendor • HelseCERT, NSM, kraftCERT, additional third-party • Have dialog with other municipalities • KiNS, K-CSIRT, HelseCERT and Atea • Collaborate with other municipalities nearby and notify each other	• Members of KiNS, but not K-CSIRT (money, was not prioritized) • HelseCERT, K-CSIRT and KiNS • Members of K-CSIRT • Orange, K-CSIRT and HelseCERT • KiNS, not K-CSIRT (financial reasons)

The municipalities and intermunicipal collaborations all had partnerships in place, allowing access to more information and assistance than they would have on their own. In today's digital society, a sharing culture is vital as new threats and better solutions are constantly emerging. The interviews revealed that intermunicipal collaborations often involve external organizations, with a few recurring partners mentioned multiple times. However, there appeared to be a lack of formal agreements or partnerships among the intermunicipal collaborations, unlike neighboring municipalities that often maintained close contact. The extent of membership in K-CSIRT varies significantly due to financial considerations. These findings suggest that collaboration and partnerships are common, and financial considerations play a significant role in prioritizing collaborations or memberships. Overall, these findings highlight the importance of communication and sharing among municipalities in order to stay informed and prepared for potential threats and challenges.

Municipality´s viewpoint on SOC

The focus of these questions was to identify the expertise required by a municipality for effective SOC utilization, and to ascertain whether they already have, or are planning to implement a SOC. Potential challenges that may arise during SOC implementation were also discussed, along with the municipality's future plans and expectations for SOC. The answers about SOC are presented in Table 5.6.

Table 5.6: Thoughts on a SOC service from a municipal viewpoint

Theme	**Municipality answers**	**Inter-Municipality answers**
Competence wanted in the IT department with SOC	• Need to at least have worked in the municipality for 6 months before being able to enroll in their SOC program • Need to be familiar with the workspace, systems and accounts • Penetration testers, preferably in their own department • Security, incident response, specialists	• Individuals with high expertise in how IT security should be implemented and maintained in a municipality • Need to be able to handle large infrastructures with many users and handle this accordingly
Considered own/external SOC	• Had their own SOC for years • Yes, but only internal • Yes, they have a SOC • No, do not have the competence needed	• Yes, are in the process of buying their own SOC • No, does not have necessary resources • Yes, have an external SOC • No, we do not need it
Challenges	• Do not have the necessary resources, as it acquires an expertise and staff that would be too expensive • It is difficult to get money for it • Compete with other SOC customers for assistance, may be put in queue • SOC does not catch everything, need to tune it for a long time	• Needs to speak the same "language" • Financially difficult • Manage the process of building, organizing and operating the service • Not enough resources and competence • Figuring out what type of system failures the municipality wants the SOC to react upon and classifying these • The wish to have municipal self-governance and the fear that the SOC will make decisions for the municipality • SOC will never be able to do everything, so it is important for a municipality to have relevant competence
Future	• Thinking about getting a SOC service, but have no official plans	• Having a SOC for each department/sector, or for each SaaS would maybe be better • Implementing a SOC would be very useful if everything were in a cloud that the municipalities could control

The majority of municipalities and intermunicipal collaborations have expressed their interest in implementing or have already implemented a SOC. One of the primary challenges they face, was the lack of expertise and competence in monitoring, detection and incident response. The IT departments were aware of the competence needed to operate a SOC, but were unable to acquire it due to lack of resources. Another challenge was establishing effective communication between the SOC and IT department. Misunderstandings may arise if they do not share the same technical vocabulary, resulting in delays and inefficiencies. The IT department may not fully understand the specific requirements of a SOC, or may have competing priorities that make it difficult to allocate resources to support the service. Financial constraints also pose a significant challenge for municipalities. Implementing and operating a SOC can be costly, requiring investments in infrastructure, technology, and skilled personnel. Many municipalities face budget limitations that hinder their ability to invest in such services, making it challenging to establish and maintain a SOC.

5.1.2 SOC Provider Results

We interviewed a SOC leader and a department manager who possessed both knowledge and experience with SOC services. Although they had helped municipalities after incidents, they had no official collaborations. Their experience in serving a diverse range of customers provided valuable insights into the varying expectations for SOC services. This contributed to an improved understanding of the varying levels of support and monitoring required by different customers. Overall, their experience working with municipalities, and perspective on SOC services enriched our understanding in this field.

Required competence in a municipality
One of the objectives for the thesis was to identify the key competences required for optimizing collaboration between a SOC and a municipality. To achieve this, it was important to obtain knowledge about any associated challenges in fully utilizing a SOC service. By exploring these challenges, we aimed to uncover the specific areas where municipalities may encounter difficulties or barriers when integrating SOC capabilities. This understanding would then enable us to propose recommendations for enhancing collaboration and integration with a SOC. Table 5.7 presents the answers from SOC providers.

Table 5.7: SOC view on establishing a SOC service for a municipality

Theme	SOC providers answers
Competence needed	• Should be aware of their own risk and know what they are exposed to. The strategic aspect is important • No technical demand of competence, but would be unfortunate if they cannot utilize their service right due to lack of competence. Customers have the responsibility that it gets handled
Challenges of getting a SOC for a municipality	• Acquiring competence as they need people to handle all types of alerts. Such a team cost a lot of money which would be problematic • Need a lot of resources to be able to deliver 24/7 services

All interviews revealed that resources and competence were the main challenges when it comes to getting a SOC for a municipality. Regarding competence, the interviewees stressed the importance of municipalities being aware of their own risks and having a strategic outlook. These findings confirmed the previously identified barriers and requirements for implementing a SOC in a municipality.

Communication with customers

The following questions aimed to gain an understanding of the customer-SOC relationship and the extent to which customers rely on the service. Additionally, we sought to understand the specific customer information that providers require to effectively deliver their services. These aspects were crucial in formulating some of the recommendations, as they identified key factors for establishing effective partnerships between customers and SOC providers. The answers can be found in Table 5.8.

Table 5.8: Communication channels a SOC use

Theme	SOC providers answers
Standard communication channel	• Portal and equipment. They have training with customers in their tools so they know how to use them
Challenges	• If answers are short and not elaborate, or if they do not know their own systems well enough
Information about customers	• Good insight on customers, but depends on how much equipment and services they buy. The more insight they have the better recommendations and services they can give them

Having clear and concise communication between the SOC provider and the cus-

tomer is essential. SOC providers should prioritize training their customers on the tools they use, as the customers might not be familiar with them. It can be challenging for the SOC to provide appropriate solutions if customers provide brief and insufficient answers. The level of insight required by a SOC provider into a customer's systems varies, depends on the services purchased. However, it is important for the SOC provider to have necessary access and visibility into the customer's systems to effectively monitor and respond to any potential threats.

Incident management

To gain insight into how incident response is handled and prioritized, we asked about the process and areas of responsibilities. Questions regarding how to stay updated on current and emerging threats were also discussed. Additionally, we investigated wether IRT were part of the services offered by the SOC providers. This was asked to assess the extent tho which the providers recognized the IRTs significance in effective incident management. The answers are presented in Table 5.9.

Table 5.9: How SOC handles incident management

Theme	**SOC providers answers**
Prioritizing incident response	• Default policies with severity, but analysts can put it higher or lower
Staying updated	• Over 300 employees that work with security and have a lot of experience in the field • Daily news to all customers that explains what has happened the last day
IRT	• They have IRT if this is needed, but this is quite expensive • IRT can be as an add on, when purchasing SOC service
Areas of responsibility	• Responsible to notify and recommend solution. It depends on what service the customer buys from them. 24/7 with always 2 people on watch, more during the day

Incident management and staying updated seems to be a high priority for the SOC, which is positive as the threat landscape changes constantly. The SOC´s responsibility is determined by the specific services the municipality chooses to purchase. The accessibility of the SOC´s IRT service might be limited for certain municipalities due to its high costs. Without access to IRT, a municipality's response to a large-scale security incident may suffer, causing prolonged downtime, data loss, and a weakened reputation. Therefore, it is crucial for municipalities to carefully evaluate their security needs and invest in the appropriate services to ensure optimal incident response. Ultimately, proactive planning and investment in incident management can help minimize the impact of security incidents and protect the municipality from significant damage.

5.2 Survey Results

The survey answers and analysis are divided into two parts, the general municipality employee and the IT department. From the survey given to the municipalities, the goal was to form a picture of the employees' understanding of information security. The IT survey was more technical and aimed to gather information on how municipalities conduct their security practices. The following section will include pie charts to show the distribution, otherwise histograms will be used with the x-axis representing the municipality groups and the y-axis displaying the percentage of answers. Since the responses were categorized based on the municipality's size, those who did not answer this question were excluded from the statistics.

5.2.1 Distribution of Respondents

To increase the number of respondents the survey was anonymous, and participants were only identifiable by the municipality's size. Hence, it was impossible to to determine the exact number of participants from each municipality, which may have skewed the results. A pie chart was created to illustrate how the distribution of responses would ideally look if there had been a realistic distribution of responses. Two additional charts were generated based on the actual distribution of responses obtained from the surveys. Figure 5.1 illustrates the distribution of municipalities if approximately all municipality employees participated.

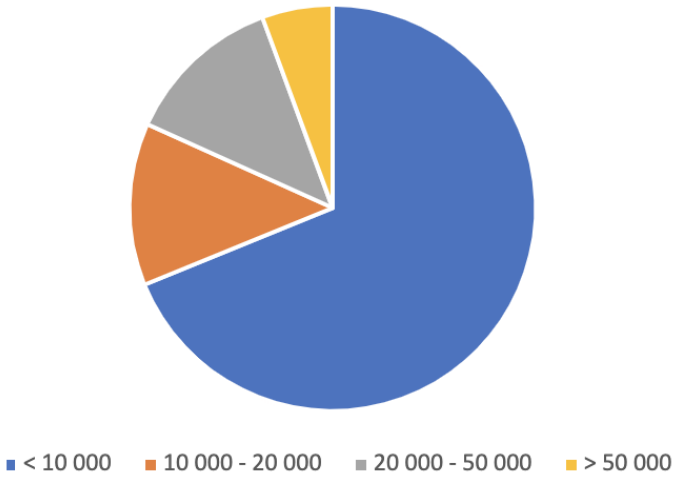


Figure 5.1: Distribution of municipalities based on number of residents

Figure 5.2 demonstrates how the municipalities are distributed based on the responses received from the survey.

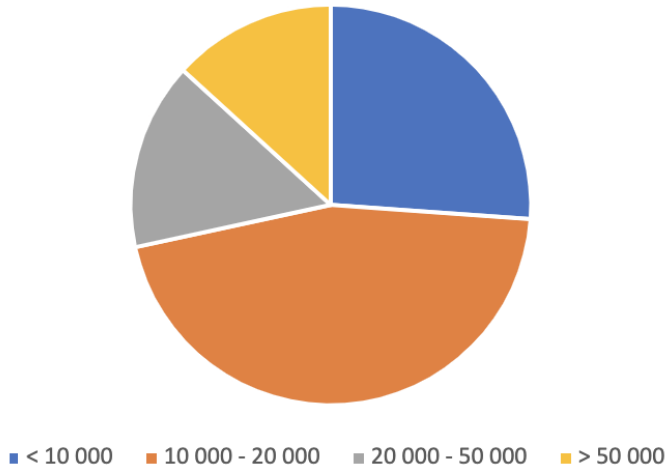


Figure 5.2: Distribution of municipalities based on municipality survey

Our goal was to obtain responses from one representative from each IT department, aiming for a distribution similar to the distribution of municipalities. However, the distribution of responses deviated from this ideal due to the existence of intermunicipal collaborations in several municipalities and lack of responses, which resulted in the following distribution. Figure 5.3 illustrates the distribution of IT departments based on the number of residents in their respective municipalities.

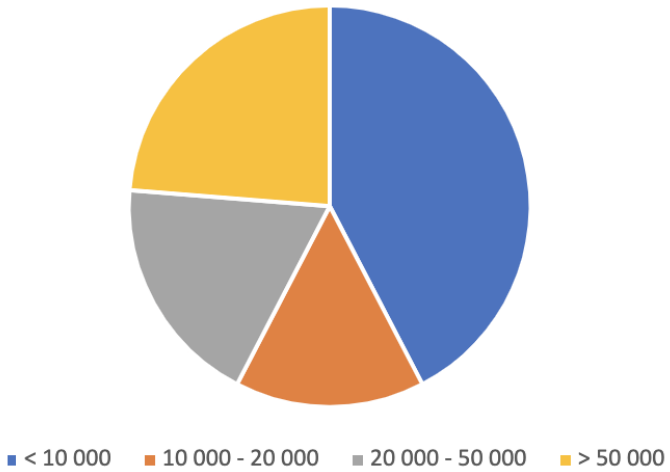


Figure 5.3: Distribution of municipalities based on IT survey

5.2.2 Municipalities Results

In this subsection, we present the results from the survey that was distributed among municipalities, with 314 responses collected from varying-sized municipalities. The result from the survey given to IT will be analyzed in Subsection 5.2.3.

General security knowledge
To quickly assess an individual's level of information security competence, a question containing different terms were included. Participants were asked to click on the terms they were familiar with. However, it is important to note that the level of familiarity may vary among participants, as there were no clear instructions provided to define what was meant by familiar. Figure 5.4 displays the familiarity level of employees from different sized municipalities with information security terms.

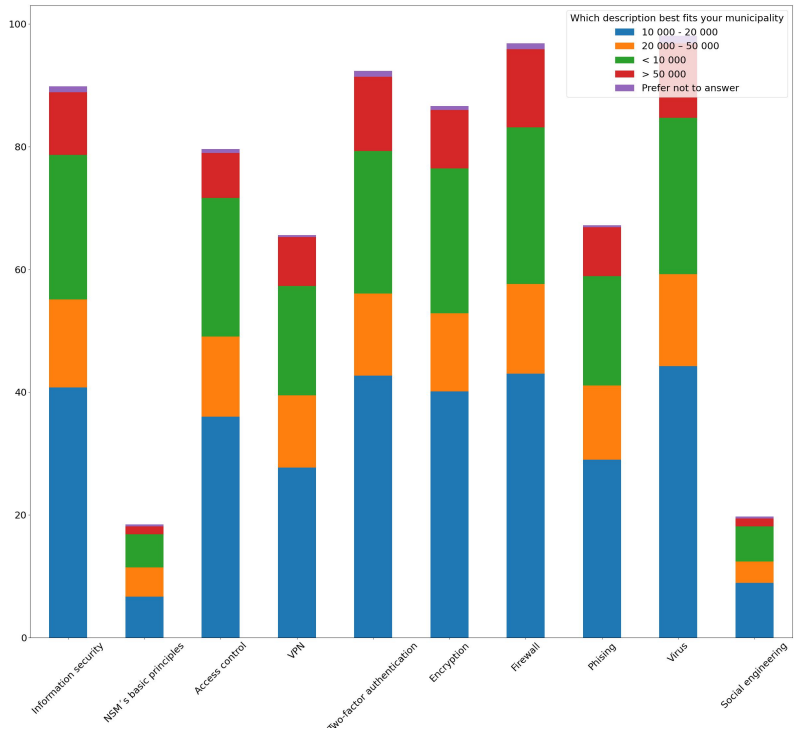


Figure 5.4: Statistic result of "How many of these terms are you familiar with?"

The most known terms were "Virus" (98.4%), "Firewall" (97.1%), "Two-factor authentication" (92.7%) and "Information security" (90.2%) that all received over 90% that were familiar with these terms. This was expected considering these terms are common in the field of cybersecurity, which has gained a lot of attention and media coverage in recent years. This outcome suggests that having a

basic level of information security is sufficient to be familiar with these terms. The least known terms were "NSM´s basic principles" and "Social engineering", which is not surprising since they are more specialized and technical compared to the other terms included in the survey. Overall, it appears to be a good understanding of various information security terms among respondents.

It has previously been mentioned in Table 5.2 that the desired level of competence for an employee should be to identify a phishing email. We therefore included a question in the survey asking participants if they have received a phishing email. Figure 5.5 displays the distribution of employees receiving a phishing email.

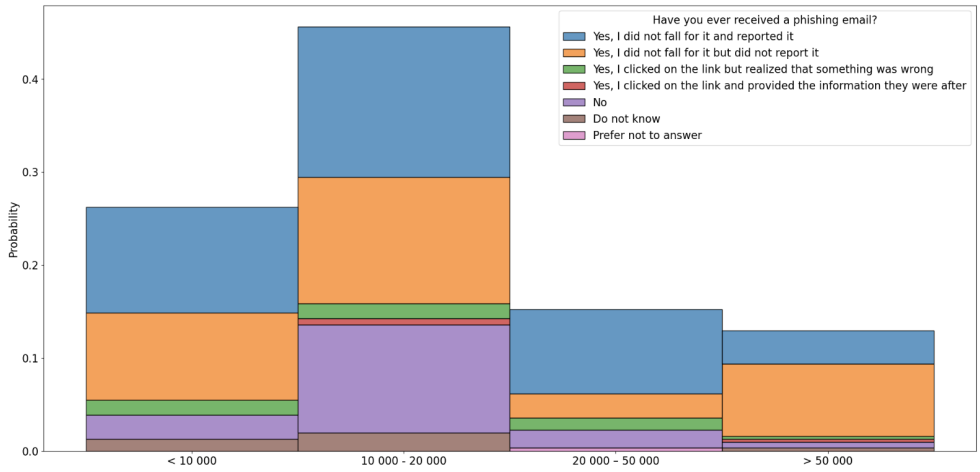


Figure 5.5: Statistic result of “Have you ever received a phishing email?”

The result was somewhat surprising, given that 67.6% of the respondents clicked on the term “phishing,” indicating that they were familiar with it, when 20.3% of the same respondents either have never received a phishing email or are unsure if they have received one. This may suggest that some respondents are not fully aware of what defines a phishing email or how to identify one. This difference could be due to a lack of education or training in information security best practices or simply a lack of attention to phishing attempts.

Ever asked for IT assistance

Asking if employees seek IT assistance indicates contact frequency and how high the threshold for asking for help is. Figure 5.6 shows how often employees in a municipality have asked for help when facing technical problems over the span of a year.

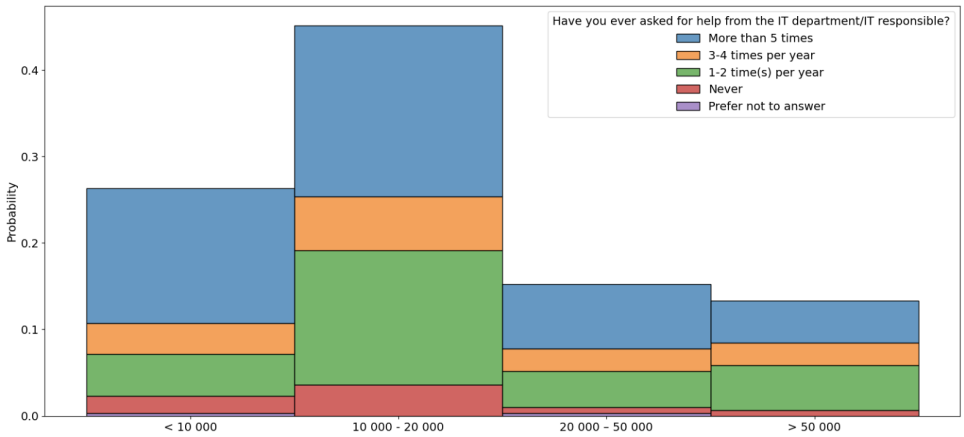


Figure 5.6: Statistic result of "Have you ever asked for help from the IT department/IT responsible?"

As revealed from Figure 5.6, the distribution of how often employees need help when facing technical problems is independent of the size of the municipality. More than 90% of employees have sought help from the IT department within the course of a year. This suggests the municipalities have informed employees of the option to seek assistance from the IT department. While it is not realistic to expect all employees to have the ability to solve all IT related problems independently, having some level of knowledge can reduce the need for assistance in certain situations. This emphasizes the importance of providing employees with IT training to encourage them to resolve issues themselves, while also promoting a culture of self-sufficiency and continuous learning.

Protocols

We asked if employees were familiar with the security protocols in place to gain insight into how the municipality train and prepares its employees to respond to potential security incidents. Figure 5.7 displays if employees are familiar with any protocols in case of a security incident.

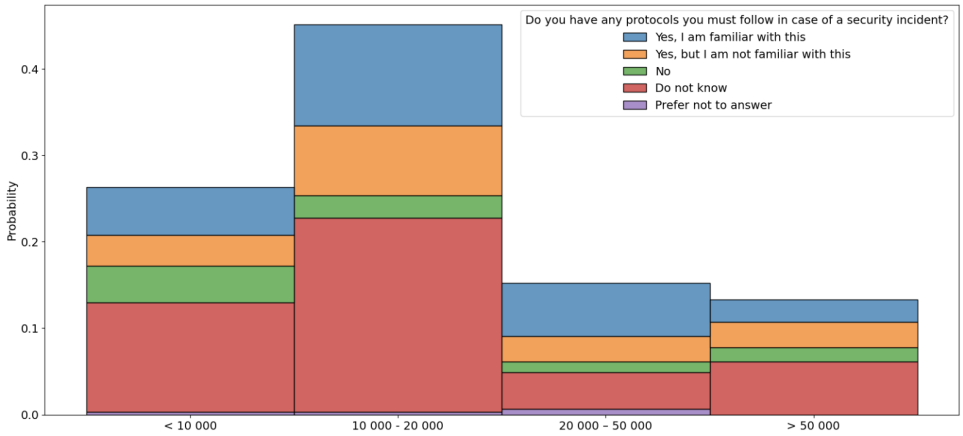


Figure 5.7: Statistic result of "Do you have any protocols you must follow in case of a security incident?"

A mere 26% of the respondents confirmed that they were familiar with the protocols in the event of a security incident, and the largest proportion of "yes" responses was observed in the group 20 000 – 50 000. The remaining 74% of respondents either reported not being familiar with the security protocols, were unsure whether any were established, or believed there were none. Given the unlikelihood of no security protocols being in place, the more probable reason is failure to communicate and inform their employees of them. Lack of adequate knowledge regarding the protocols can result in employees being uncertain about the appropriate actions to take, potentially causing confusion and unnecessary chaos.

Communication channels

Having designated communication channels for employees to report security incidents is important as it provides the IT department with valuable information. Being able to see incidents in context to each other, provides the IT department with a broader perspective and better understanding of the overall situation. If such a channel exists, it indicates that the municipality takes security incidents seriously and has a structured approach of how to handle them. This also encourages the employees to be aware of any incidents or potential threats. In the absence of a channel this might suggest that the municipality is not fully prepared to handle security incidents or may not prioritize them adequately. Figure 5.8 presents how many have a communication channel where they can report a security breach.

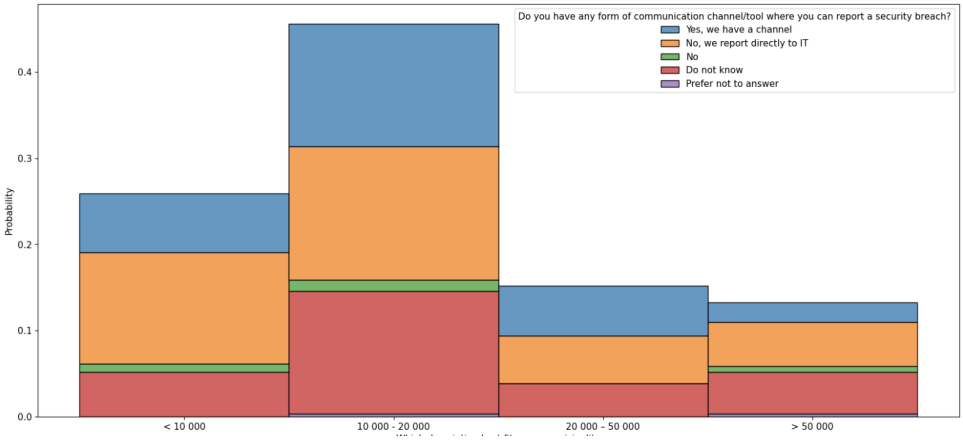


Figure 5.8: Statistic result of "Do you have any form of communication channel/tool where you can report a security breach?"

Only 26.7% of respondents reported having a channel to report potential security threats, suggesting that either some municipalities do not have this option, or have not effectively communicated it to their employees. It is worth noting that some municipalities may not have a designated channel, and employees have been instructed to report directly to IT instead. While it is easier to discuss security matters in person, this approach can also be time-consuming and do not contribute to lower the reporting threshold, which is already high. Seeing that 27% of employees are unaware of such a channel is worrying and highlights the need for a more structured approach of communication to ensure every employee is well-informed . It is surprising that group $>$ 50 000 had the lowest portion of "yes" despite typically being better prepared for security incidents. Without a designated communication channel, reporting security breaches may be inefficient, leading to delays in addressing issues while also making it harder to encourage employees to report potential threats. This reinforces the importance of having a clear and easily accessible reporting mechanism to improve incident response times and promote a culture of security awareness.

Security culture

Security culture is essential in ensuring that all employees are well-informed regarding risks associated with information security and ways to mitigate them. By promoting a strong security culture, employees are more likely to adhere to security policies and procedures, be alert to potential threats, and take necessary actions to prevent security breaches. Security courses play a vital role in educating employees on best practices and guidelines for information security, thereby contributing to a stronger security culture. Figure 5.9 shows if and how often employees have attended a security course.

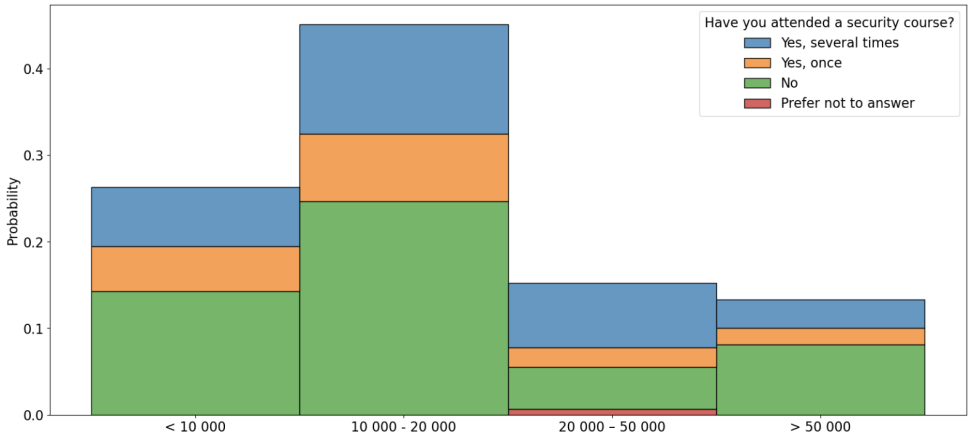


Figure 5.9: Statistic result of "Have you attended a security course?"

There was a majority who have never attended a security course, which can be caused by either not having the opportunity to take one, or they have decided not to participate. This is concerning, since these courses offer knowledge and skills that can help employees understand the significance of information security. By attending security courses, employees can gain insights into best practices, risk mitigation strategies, and emerging threats, equipping them with the necessary tools to contribute actively to a secure work environment. Thus, promoting and providing opportunities for employees to attend security courses should be a priority.

To encourage self-awareness and self-reflection we included a question where the recipient needed to evaluate how critical they are when downloading. This question also provides valuable insights into how employees perceive and approach information security. This can help the municipality identify areas of improvement in their information security practices, which can be addressed proactively to prevent security incidents. Overall, asking reflective questions can contribute to a more comprehensive understanding of a municipalities security culture and how to improve it. Figure 5.10 present the individual's critical level when downloading.

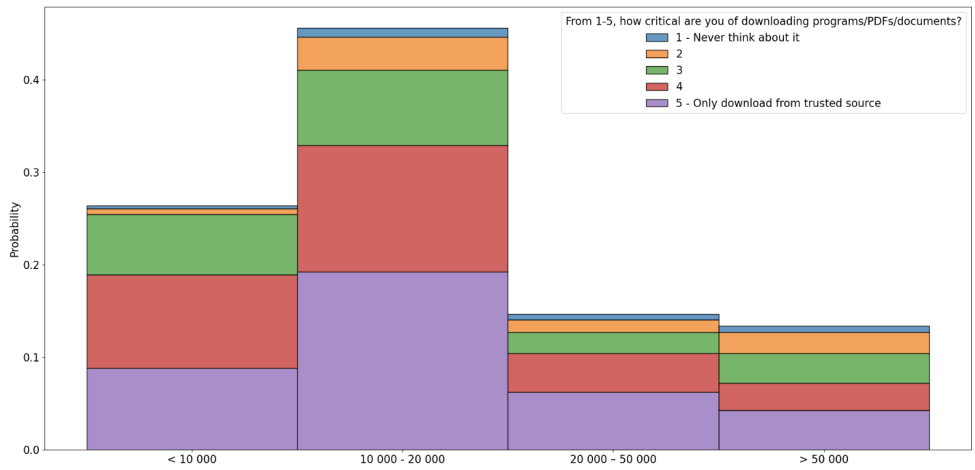


Figure 5.10: Statistic result of “From 1-5, how critical are you of downloading programs/PDFs/documents?”

The average score for this question was 3.9. This is a satisfactory result, as it suggests that the respondents are cautious when downloading, and perceive it as a potential security risk. The last survey question did not directly assess the participants’ competence in information security, but it served to demonstrate the value of having to reflect on your own security awareness. Figure 5.11 shows if the survey made the participants more aware of information security.

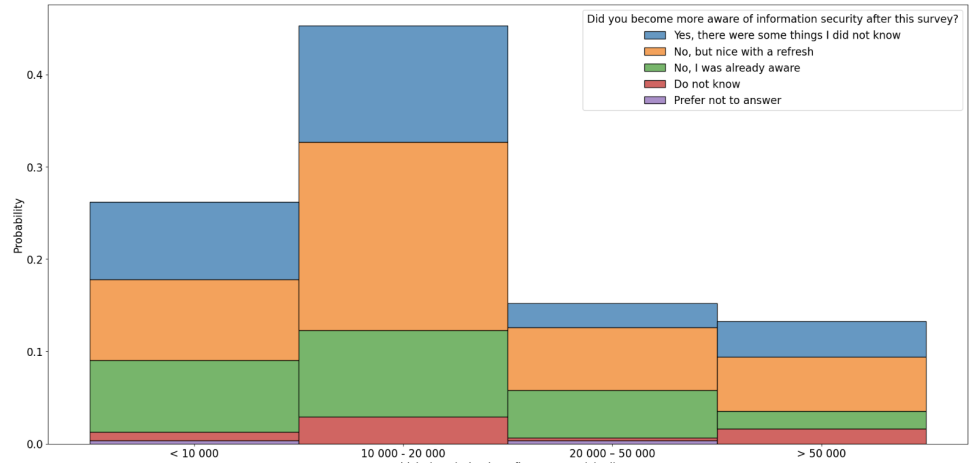


Figure 5.11: Statistic result of "Did you become more aware of information security after this survey?"

The average completion time for the survey was $\sim$ 6 minutes. Some were already familiar with the topics, but the majority appreciated the refresher. This suggests that enhancing security awareness does not require significant investments of time, resources, or money.

5.2.3 IT Personnel Results

In this section we present the result and analysis from the survey handed exclusively to the IT department in each municipality, which generated 59 responses. The aim of this survey was to get some insight into the IT department´s responsibilities, and how involved they are with improving the general information security knowledge.

Collaboration and partnerships
To gain an overview of the collaborations the IT departments had, we included a question where they could choose which ones apply to them. Having some sort of collaboration is important in all fields, as this provides more resources. Collaborations can also encourage the exchange of ideas and experiences, which can offer valuable insights and opportunities for learning. Figure 5.12 shows different partnerships. It was possible to choose multiple options, as some may have multiple collaborations.

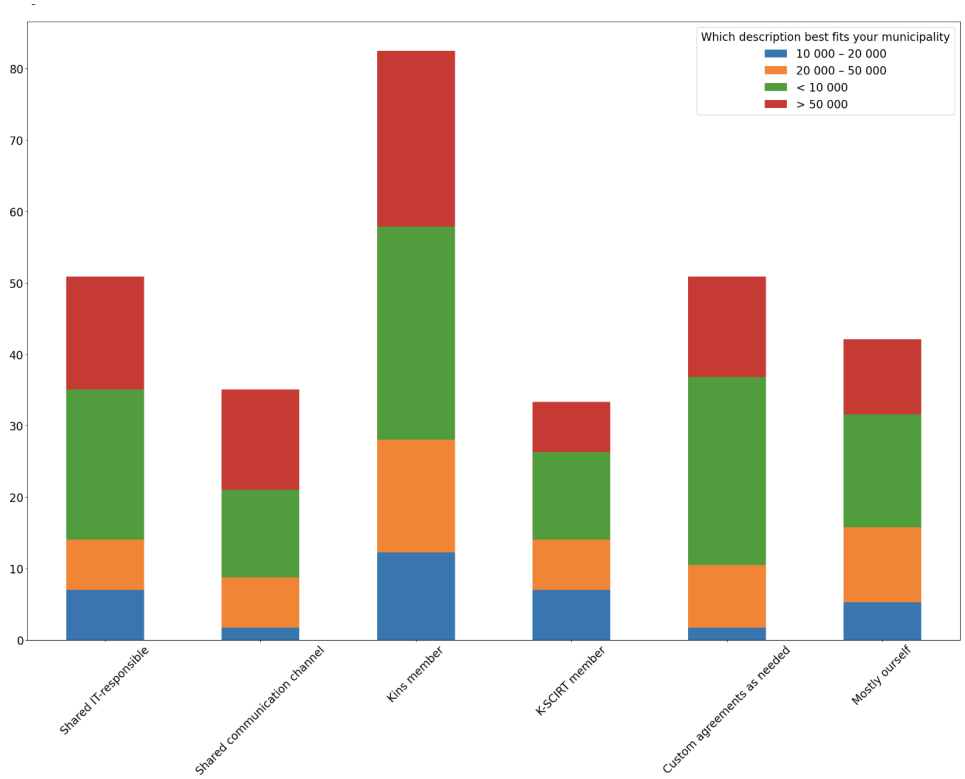


Figure 5.12: Statistic result of “Which of these apply to your municipalities IT collaboration with other municipalities?"

As revealed in interviews, there are many collaborations, both between municipalities and external organizations. Approximately 83% of the survey respondents are registered members of KiNS. Giving them access to a shared forum where they can communicate and be updated on the latest news and information from other municipalities. Multiple municipalities have "Shared IT responsible" (50.8%) and "Shared communication channels" (35.6%). This can enable direct and efficient contact with others, if they have faced similar issues or have prior experience with a particular problem. This contributes to a sharing culture which is important in security work, since threats are constantly evolving, and no single organization can keep up with new threats on their own. By sharing information organizations can learn from one another and improve their own defenses.

Risk assessment

We wanted to gain knowledge about the IT department´s risk assessment to ascertain whether they have conducted and continue to maintain these assessments. By obtaining this information, we aimed to explore if there was any difference or correlation between their security work and the municipalities' size. Figure 5.13 displays how often a vulnerability assessment is conducted.

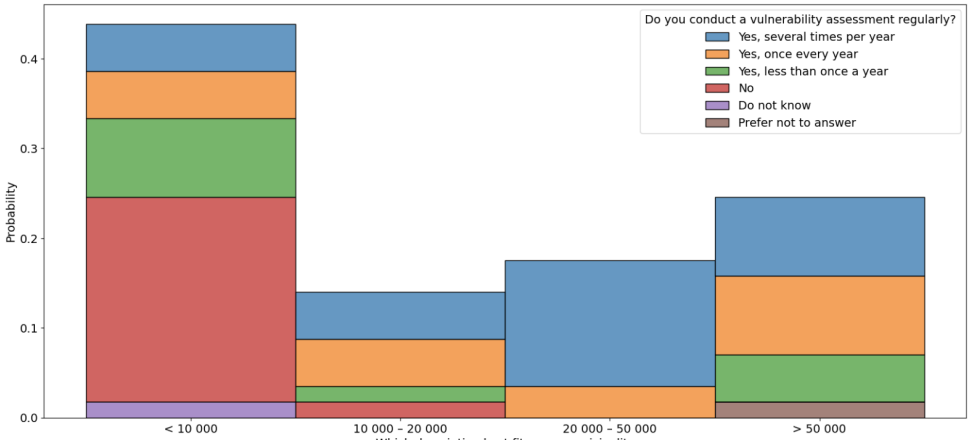


Figure 5.13: Statistic result of "Do you conduct a vulnerability assessment regularly?"

Figure 5.14 displays how often a risk analysis is conducted.

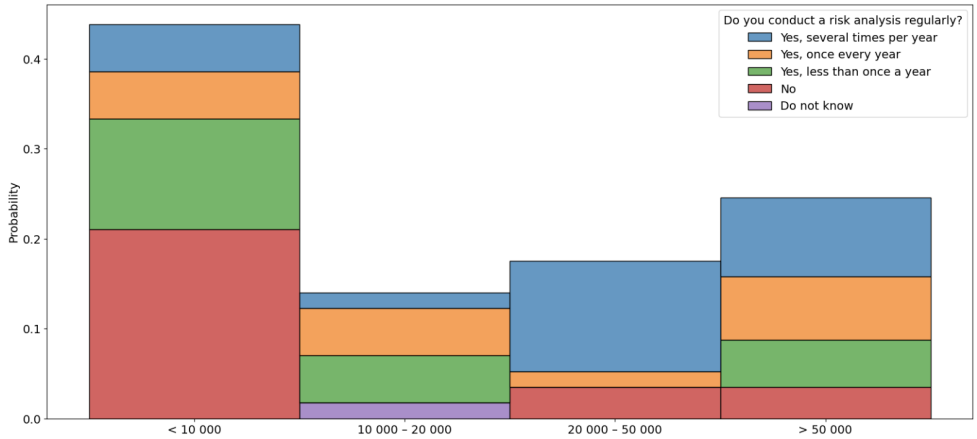


Figure 5.14: Statistic result of "Do you conduct a risk analysis regularly?"

Figure 5.15 displays how often a penetration test is conducted.

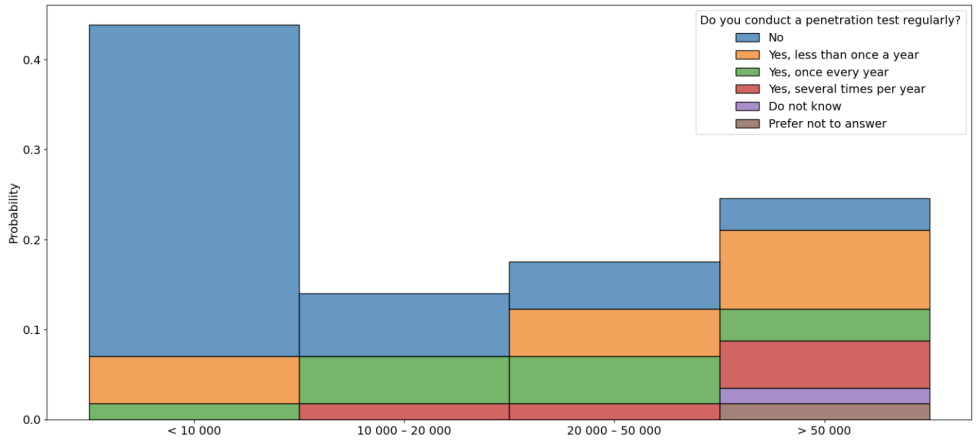


Figure 5.15: Statistic result of "Do you conduct a penetration test regularly?"

The largest portion of the answers were “no”, and the reasoning behind this may be that they have not conducted an assessment in the first place. It is evident that the small (< 10 000) municipalities do not have the same resources as they have predominantly answered “no” to all these questions. Vulnerability- and risk assessment are a fundamental part in security work, helping the municipalities prioritize and be proactive. For the big municipalities (20 000 – 50 000 and > 50 000), all answered “yes” that they do a vulnerability assessment regularly, which is most likely due to having more resources. In addition to their affirmative response, it is pertinent to highlight that the vulnerability assessment is conducted on an annual

basis. This makes them better equipped to detect vulnerabilities early on, providing them with the opportunity to protect themselves before any incidents occur. As the questions become more technical, there is a noticeable increase in the number of respondents answering "no." This trend suggests that there may be a prioritization of vulnerability assessments, since it requires the least amount of resources and is a necessary step for a risk assessment. Penetration testing demands specialized expertise that may be missing in municipalities, making it necessary to purchase this service. As a result, conducting a penetration test may not be prioritized due to limited financial resources.

Communication channels

The IT departments were asked a question regarding communication channels to support the analysis of Figure 5.8. We wanted to determine if employees were unaware of security related channels, or if they were missing entirely. Figure 5.16 illustrates if a communication channel is established in the municipality where employees can report security incidents.

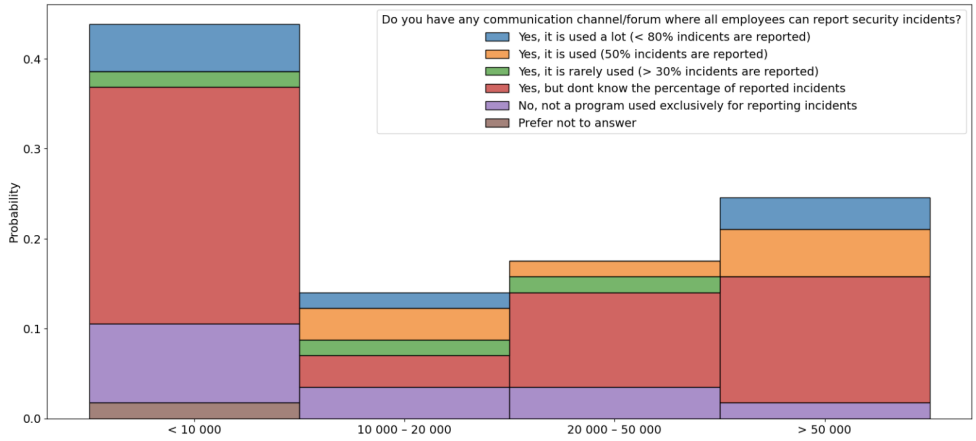


Figure 5.16: Statistic result of "Do you have any communication channel/forum where all employees can report security incidents?"

The results reveal that a majority (81.4%) of IT departments have established a method for employees to report incidents. This indicates that some municipalities are deficient in informing their employees about where incidents can be reported, as 27% (see Figure 5.8) report that they do not know if they have a channel. The IT department should ensure accessibility and visibility for the employees, as this can improve the percentage of reported incidents. We also wanted to see if the municipalities knew the percentage of reported incidents compared to the actual rate. While it is rare to know this percentage, the answers suggest that the rate of reported incidents is relatively low. This could be due to employees not knowing where to report, or because of the high threshold for reporting. Overall, the findings suggest that while most municipalities have established effective communication channels, the reported incidents from employees could be much higher.

Security course
An important part of the security work in a municipality is to improve the general information security knowledge and prompt a strong security culture. A method for achieving this is conducting security courses for all employees. This demonstrates that the IT department recognize the importance of educating in information security, and their proactive steps to improve overall security. Figure 5.17 shows how many municipalities have annual security courses.

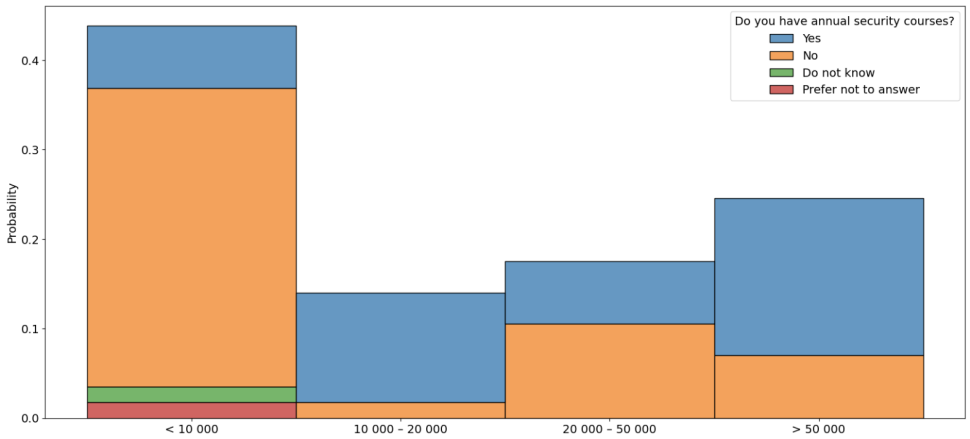


Figure 5.17: Statistic result of “Do you have annual security courses?”

Roughly 50% of the answers reveal that most municipalities have little to no annual security courses for their employees. This is especially lacking for small municipalities (< 10 000). A possible explanation for this, as previously discussed, could be due to limited resources. However, it is interesting to see that medium municipalities (10 000 - 20 000) have almost all participants saying "yes," compared to the other groups. This group have overall performed better than expected and seem to be equally prepared as the 20 000 – 50 000 group.

Governing documents

Governing documents offer explicit guidelines and policies which are crucial for establishing consistent framework for information security practices. It also helps to ensure that the IT department has an understanding of their responsibilities and the expectations for information security within the municipality. We therefore wanted to address if these documents were present for IT security. Figure 5.18 displays if governing documents are present and whether they are followed.

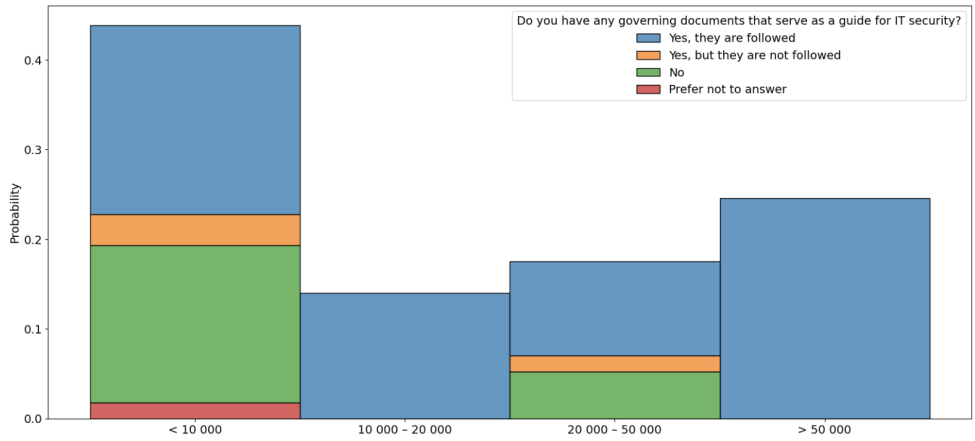


Figure 5.18: Statistic result of "Do you have any governing documents that serve as a guide for IT security?"

The results gave us the impression that most IT departments have governing documents for IT security. Two groups (10 000 – 20 000 and > 50 000) exclusively answered that they follow their governing documents. We expected the larger municipalities (20 000 – 50 000 and > 50 000) to have better IT security practices in place. Therefore, it was surprising that 40% of the responses for group 20 000 – 50 000 answered "No" and "Yes, but they are not followed". However, since there are fewer responses from the group of 10 000 – 20 000, we can not be completely certain that this result is representative for all municipalities of this size. There is also a significant number of responses from group < 10 000 that answered "No" and "Yes, but they are not followed", which is not surprising given the previous results. This is still concerning as it shows a lack of prioritizing IT security within this group.

An incident response plan should be in place to provide a clear and organized approach for mitigating security incidents, minimizing impact, and enabling a prompt recovery. However, it is important to note that incident response plan may have different interpretations. Some plans may only cover one specific scenario, while others include several situations. Figure 5.19 presents those who have established an incident response plan.

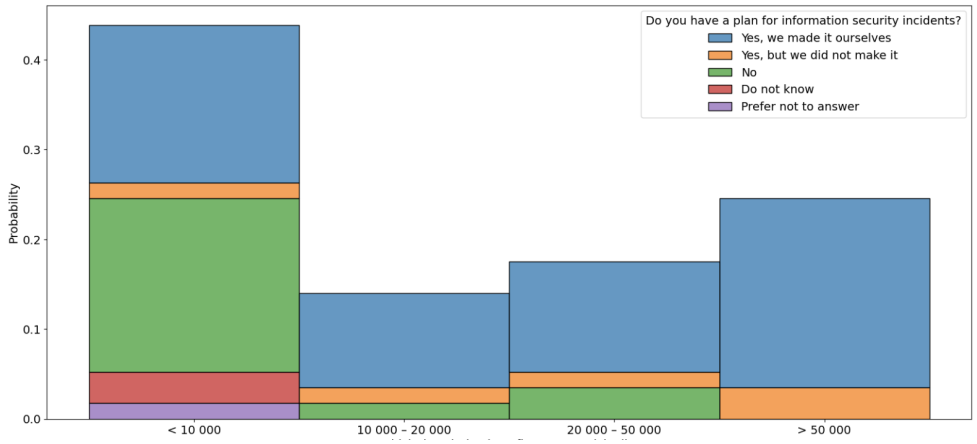


Figure 5.19: Statistic result of "Do you have a plan for information security incidents?"

According to the statistics, group $< 10\ 000$ stood out as they were the only ones that did not almost exclusively answer "Yes". Additionally, this group also answered, "Do not know", which was not the case for any other group. Based on our previous analysis and knowledge, it seems that resources are the biggest challenge for this group, which explains their lower score in this regard.

Chapter 6

Recommendations

This chapter presents the concrete recommendations derived from the analysis results, and information that has been gathered. The format used consists of subtitles followed by a short description that provides additional information. The recommendations are formulated and influenced by NSM's basic principles, in addition to insights gathered through interviews and the statistics from the surveys. The recommendations offer a structured guideline, like MITRE and NSM's basic principles, but are specifically tailored to meet the unique needs of larger and more complex organizations.

Due to the high volume of perspectives and opinions, the recommendations are formed based on an overall assessment. The recommendations are made as general as possible, and a customization is expected in order to meet the individuals needs. It is important to note that the recommendations should be viewed in context of the municipality, as each recommendation may not be applicable to all. Ultimately, the municipality is responsible for any loss, misplacement, or damage of data.

6.1 Improving Interaction Between a Municipality and a SOC

In this section, we have categorized our recommendations into three subsections: organization, communication, and division of responsibility. We believe these categories are key to improving the interaction between a municipality and a SOC. By implementing the following recommendations, we aim to improve collaboration and facilitate a more productive partnership.

6.1.1 Organization Choice and Mapping

Intermunicipal collaboration
Intermunicipal collaboration with a shared SOC between multiple municipalities can provide a cost-effective solution for smaller municipalities that lack the resources to purchase a SOC. This approach can allow more people to benefit from a SOC service while optimizing the available resources. It is easier and faster to implement a SOC if the included municipalities have similar equipment, regulations and topology. However, this is not a requirement as long as the SOC has complete coverage of all relevant assets.

Experienced SOC provider
Choose an experienced SOC provider with a proven record in incident response, deep understanding of threats and trends, mature security framework, and a highly skilled team. This aligns with NSM's measure 2.1.3 [1].

Map network topology and systems
Mapping network topology and systems is crucial for optimizing SOC implementation. It ensures correct configuration and provides insight into network structure, security solutions, and systems used. Both parties should have access to this information to enable protection of existing assets. This aligns with NSM's basic principle 1.2 [1].

6.1.2 Communication Between SOC and the Municipality

Traffic light protocol (TLP)
Use traffic light protocol when communicating to ensure that sensitive information is handled appropriately. This aligns with NSM´s measures 2.7.5 and 4.1.5 [1]. The different TLP designations are presented in Table 6.1.

Table 6.1: TLP definitions and usage

Designation	Description
TLP: CLEAR	Information is not sensitive and can take place on a desired channel
TLP: GREEN	Information can be shared with limited audience and take place on a desired channel
TLP: AMBER	Information is shared on a need-to-know basis and should be conveyed over an encrypted channel like Mattermost
TLP: RED	Information is sensitive and should be addressed over telephone to the agreed key contact

Two-way communication
Effective collaboration between a SOC and a municipality requires continuous communication, feedback, and coordination. Two-way communication is essential to ensure that both parties are on the same page and working towards the same goals. It helps in building trust, promoting transparency, and enables quick decision-making.

Identify key contacts and roles
In the event of an incident, it is important for the SOC and municipality to have a clear understanding of which individuals hold specific roles and whom to contact for assistance. It is necessary to identify alternative contacts in case the first responder is unavailable. To prevent confusion, it is recommended to create a flowchart that illustrates the roles and responsibilities of each individual. This aligns with NSM´s measure 4.1.3 [1].

Clear division of communication channels
To avoid the risk of information getting lost or misplaced due to having too many communication channels, limit and define the purpose of each channel.

Choice of language
The municipalities in Norway is subject to the Language Act[1], with the exception of paragraph 12-18, with an aim to strengthen the Norwegian language. Therefore, Bokmål or Nynorsk should be used when communicating with the SOC. For Non-Norwegian speakers, English is recommended as the secondary language. Regardless of chosen language, it is essential to agree on using the same language consequently. When communicating, it is important to consider the varying levels of knowledge among the involved parties and adjust the vocabulary used accordingly.

6.1.3 Division of Responsibility

SOC delivers the service
The SOC possesses the necessary experience and expertise, making them the most suitable to handle activities related to detection, monitoring and incident response. However, it is important to involve the municipality in the SOC´s operations as they have unique insight into their tasks and employees, which the SOC may lack. The involvement ensures that their services and values are taken care of. By entrusting the SOC with the majority of the responsibility, the municipality can be confident that prompt and effective measures are taken, to minimize the impact of any security incidents. Additionally, this allows the municipality's IT department to focus on other critical IT operations, which can improve the overall efficiency of the organization. This aligns with NSM´s basic principles 3.2 and 4.3 [1].

[1] `https://lovdata.no/dokument/NL/lov/2021-05-21-42`, visited 25.04.23

Onboarding
Onboarding is necessary when the municipality hires a SOC provider. Representatives from the SOC, chief municipal executive, head of IT and other relevant employees should be present. The municipality needs to understand the different risk levels, as well as policies and regulations that can have an impact on securing the systems. Onboarding includes training and assessments in different situations. This aligns with NSM´s basic principles 1.1, 2.10 and 4.4 [1].

Power of attorney
During the interviews, some expressed hesitance towards providing the SOC with access to their systems and data. It is worth noting that since the SOC will have access to personal data, this requires contractually agreed handling through a data processor agreement [2]. It is vital for the SOC to have this visibility in order to gain a comprehensive understanding of incidents, and without it, the quality of service may be compromised. The municipality needs an employee that has extensive security competence, that understands the balance between the quality of service and the risk if they do not grant enough access. Due to the high probability of cyber attacks occurring outside of office hours, time is of the essence. The SOC should therefore have the ability and power of attorney to handle alerts and possible incidents.

Security packages for software
Municipalities should choose to buy security packages for software they already own, instead of acquiring new tools. This should include logging, endpoint- and identity protection that can be integrated with a SOC service. It is preferred to use a recognized provider like Microsoft, as they offer security solutions that are easy to purchase and configure [3]. This aligns with NSM´s measures 2.1.2 and 2.1.3 [1].

Priorities on alerts
SOC are better equipped to determine the priority of each alert, as they have the necessary expertise. Municipalities do not acquire the same level of understanding regarding the severity of each alert, and are not completely objective. This aligns with NSM´s basic principle 4.2 [1].

[2] `https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/databehandleravtale/`, visited 27.04.23

[3] `https://www.microsoft.com/en-us/security/business/solutions/siem-xdr-threat-protection`, visited 05.05.23

Managing alerts
There needs to be a common terminology and classification of incidents across the municipality´s IT department, SOC and IRT. Incident classification is important when determining the severity of an event. All parties involved must understand the meaning of a classification and the processes these statuses trigger. A classification may change over time and be both escalated and downgraded. Table 6.2 presents an example on classifications and involved parties.

Table 6.2: Classification of incidents and involved parties

Status	**Example**	**Involved**
User error	Accidentally sent email to wrong recipient	Municipality´s IT department
Technical error	Configuration issue	Municipality´s IT department
Potential security incident	Employee received phishing email	Municipality´s IT department and SOC
Minor security incident	Loss of encrypted company device	Municipality´s IT department and SOC
Major security incident	Compromised user account	Municipality´s IT department and SOC
Critical security incident	Ransomware attack	Municipality´s IT department, SOC and IRT

6.2 What Competence a Municipality Needs to Acquire

To effectively handle cyber threats and safeguard sensitive data, municipalities must prioritize information security competence. This section provides recommendations on what competence a municipality should acquire, focusing on raising the general level of knowledge for both the general municipal employee and the IT department. By implementing these recommendations, municipalities can enhance their information security culture and improve their incident response capabilities.

Governing documents for information security
Governing documents such as incident response plans and vulnerability assessments are essential for municipalities to identify potential risks, address vulnerabilities, and ensure ongoing improvement and evaluation. Regularly reviewing and updating these documents can help municipalities stay current with emerging threats and technologies, ensuring that they are prepared to respond to incidents that may occur. This aligns with NSM´s measures 3.1.1 and 4.1.1 [1].

Establish periodic updates to make sure that systems are up to date and are not exposed to vulnerabilities. This aligns with NSM´s measure 2.3.1 [1].

Member of an Information Sharing and Analysis Center (ISAC)
Municipalities can become more proactive and enhance their incident response capabilities and mitigate potential security risks by joining ISACs, such as K-CSIRT, KiNS, or HelseCERT. Through membership in these organizations, municipalities can stay informed about the latest threats and vulnerabilities, learn from others with similar challenges, and share their own experiences. When compared to consulting organizations with limited experience with municipalities, an ISAC offers a cost-effective solution and facilitates for information exchange. This aligns with NSM´s measure 3.3.4 [1].

Data protection
Competence about data protection is needed to ensure that all data is being handled and stored safely. Routines for frequent backup and recovery must be in place, including both offsite and immutable solutions. This aligns with NSM´s basic principle 2.9 [1].

The municipality must choose for themselves based on their needs, whether to use cloud or local storage. This requires an overall assessment that needs to consider aspects such as type and amount of data, the reliability and security of the cloud provider, and any legal and regulatory requirements. This aligns with NSM´s measure 2.1.10 [1].

Involving all divisions in the security culture
Developing a security culture is necessary as the threats for the municipality are complex, from theft and loss of devices to hacking [10]. An article from the government of Norway states that 80% of incidents NSM assists, could have been avoided with fundamental security measures [14]. Increasing awareness and establishing a good security culture in the municipality can therefore help decrease the risk. It is important that all divisions of the municipality take responsibility and show interest in security work, as mentioned in ISO 27001:2017:5.2[4]. An open and inclusive security culture can lower the threshold for employees reporting and engaging in security issues.

Acquiring security competence
Interviews revealed an overrepresentation of competence in operation and support, indicating a need to balance out competences and prioritize security. To address this, municipalities should prioritize hiring more employees with security expertise, especially relevant experience regarding a SOC.

[4] `https://standard.no/no/Nettbutikk/produktkatalogen/Produktpresentasjon/?ProductID=913029`, visited 04.05.23

Project management competence
IT personnel should have a knowledge of project management, because they are often involved in various technology projects. Management skills allow for effective planning, communication, and execution while ensuring that the project is completed on time and within budget.

Relevant experience or education
The IT department's ability to effectively work with a SOC depends on having relevant education and experience. Skilled and knowledgeable employees will improve the municipality's overall security. When such competence is lacking, the municipality needs to prioritize facilitating further development of relevant skills. While prioritizing higher education can be an effective means of ensuring competence, it is also important to consider motivation and interest.

Recruitment and visibility
To ensure the latest security competence, municipalities should focus on hiring newly educated individuals who have updated security knowledge. This can help increase the competence level of the municipality, and ensure that it is up to date with the latest security practices and technologies. To achieve this, municipalities need to increase their visibility and give students insight into the possibilities they can provide. This can be done through partnerships with universities, offering internships, job fairs and other recruitment events.

Obligatory and periodic courses
The municipality needs to strive to increase awareness and knowledge about information security, not only for the IT department, but for all employees. The desired level of competence for all employees should be to differentiate between a legitimate email and a phishing email. This is shown to be difficult, as almost 20% of the municipality survey (see Figure 5.5) answered either that they have never received one or they do not know.

Designated channel or forum for security related topics
To enhance general awareness of information security, a dedicated channel or forum for the municipality to discuss security related topics should be created. Although, the channel's content may vary, it should serve as a platform to share information about new threats and encourage dialogue, reflections, and users to use the channel. All users should get training in how to use the channel. This aligns with NSM´s measure 4.1.5 [1].

Results from the survey indicate that the threshold for reporting issues is too high. A designated channel can help alleviate this issue and make reporting less intimidating.

Chapter 7

Discussion

In this chapter we will reflect on the decision-making process and teamwork throughout the thesis writing. It will also involve evaluating areas of improvement and discussing how various approaches can enhance the outcome. By reflecting on these aspects, we can gain insights into the strengths and weaknesses of the project process and the teamwork.

7.1 Project decisions

In the process of writing the thesis, we encountered various decisions that needed to be made in order to present our work in the best possible way. This included decisions related to conducting surveys, interviews, statistics, analysis, and language.

Interview process
We primarily reached out to interview participants through email, which proved to be effective for most municipalities and intermunicipal collaborations. However, it was challenging to get in touch with SOC providers, resulting in a limited number of SOC representatives. This caused us to not to obtain the broad specter of viewpoints as envisioned.

As mentioned in 4.1 interviews with municipal and intermunicipal collaborations all had the same prepared set of questions, which had some complications. During interviews we found that some questions were not relevant to everyone, and some were misunderstood. This lead to difficulties when interpreting and categorizing answers in Section 5.1. Looking back, we could have avoided general questions, worded them clearer and explained the intention. By doing greater research beforehand, we would have discovered that general questions often were not suitable for everyone, and needed customization. All interviews followed the same structure and order of questions, but sometimes the conversation drifted. In the

end these interviews were the ones that was the most insightful, but again hard to categorize. The participants level of competence also led to certain individuals providing unclear and atypical responses. Some had strong opinions and a lot to share, while others were satisfied with their solution and did not provide us with much information.

Conducting surveys
There were several difficulties we faced when conducting the surveys. To lower the threshold for participating and avoid regulations with storing personal data, we removed and rephrased questions that could be interpreted as requesting personal information. But still, with anonymity, the number of respondents remained low, and we quickly learned that the email did not give the right impression. The feedback we received was that it looked like an advertisement, unsure who it was targeted towards, and the recipients didn't feel like they gained anything from answering. It was difficult to articulate what we wanted in a short email, so the email body was changed a multiple times based on the feedback.

Initially, we considered using Google Forms[1] for the surveys and sent out a few in this format, but we experienced not establishing enough trust. To gain more credibility, we switched to Nettskjema due to its priority of security measures for handling data[2]. Since the survey was sent to the municipalities email, there was often only one person responding on behalf of the entire municipality, which could also explain the low response rate. We did ask for the survey to be distributed on an internal channel, but only received one confirmation that this was done by group 10 000 – 20 000. This resulted in an imbalance of distribution of answers, and to compensate we had to send out the survey to more targeted groups, especially group $>$ 50 000. All survey answers were to be visualized and categorized by the municipalities size, and when several skipped this question we had to ignore their entire response. To eliminate this issue we made it mandatory to answer all questions.

The survey for IT departments faced many of the same problems with getting responses. It took a significant amount of time to find who to contact and their email address. Many of the municipalities had IT collaborations which made it difficult to get the representation envisioned. To help categorize the collaborations, the respondent was asked to provide the average population for all the municipalities involved. Another challenge was to prevent several people from the same IT department from answering, since they would be nearly identical. By only sending to individuals instead of the department and specifying only one answer per municipality, we had some control over the distribution. However, there is an uncertainty if this was upheld since it was anonymous.

[1] `https://www.google.com/forms/about/`, visited 15.03.23

[2] `https://www.uio.no/tjenester/it/adm-app/nettskjema/mer-om/informasjonssikkerhet/`, visited 10.03.23

Creating statistics for the surveys
As mentioned in Section 4.3, the survey results were visualized using histograms. Due to the imbalance of responses, we decided to have the y-axis display percentage instead of the actual number. This made it possible to compare answers regardless of the numbers of responses. To form the statistics from the raw Excel data, we contacted the statistic help advertised on Blackboard. They provided us with a shell code that we could modify to our needs. The process of translating the survey to English was both time consuming and prone to errors.

We faced several difficulties when visualizing the results and the outcome is still not optimal. There were no structure in how the dataset was created, so the order of the answers decided the formation of the figures. Since we wanted the x-axis to represent the groups by size, it was logical to arrange them in ascending order. Similarly, we wanted the different options to be displayed in the same order as the survey, with varying degrees of yes/no. Meaning we needed to restructure the answers for each figure. The first row had to contain an answer from a participant from group $< 10\ 000$ that answered "Yes", and the fourth row from group $> 50\ 000$ that answered "No". The figures could also have been more cohesive by having the same colours for similar options. These issues could have been addressed and implemented in the shell code, had we been more aware when writing the description for the statistics.

Presenting the analysis results
Our task did not require any development or implementation, so the analysis results was therefore one of the most important parts and needed to be portrayed in a structured manner. This proved to be difficult, as we had a lot of material to include. For the survey results, we decided early on that making statistics was the best solution, but for the interviews we were unsure. We ultimately decided on presenting the answers using tables. We considered having all survey questions in the analysis, but decided to only include the ones that were relevant regarding our recommendations.

Based on feedback from the first draft, it was too difficult to understand what was presented in the tables. To make the tables more explanatory, we shortened the answers, made the titles clearer and gave an introductory description of the layout. To further improve the presentation of the interview results, we would have made statistics. However, since the answers were personalized, it would be nearly impossible to categorize them in a simple structure. This would require a different approach when formulating the questions, making them less open.

Language barrier
Finding the right English words for Norwegian terms was challenging at times, since some words did not have a translation. We decided to use the Norwegian Data Protection Authority´s vocabulary to translate technical terms to English[3]. Another solution for this was to view the municipalities web pages in English, to see if there were more suitable translations.

7.2 Teamwork Evaluation

Throughout our three years of study we have collaborated on several projects, and are therefore used to working with each other. This was beneficial as we already have established a well-working group dynamic, leading to a great project period. In the beginning we decided to meet physically on campus Mondays and Thursdays, but ended up not having any set workdays, due to different schedules and the nature of the individual tasks. The number of hours per week varied, with some very intensive work sessions periodically. In retrospect, it would have been beneficial with a more balanced and structured approach to our work schedule. This way we could have avoided the intense periods and maintained a more consistent level of productivity throughout. Additionally, we noticed that we were more efficient when working together on campus, which we should have utilized more, rather than using digital solutions.

During our information gathering phase, we collected sufficient data through interviews and surveys to perform a comprehensive analysis based on the responses. We utilized a calendar to ensure adherence to the Gantt chart in our project plan. This calendar outlined our objectives, helped us maintain focus, and meet deadlines throughout the project period. While we were consistent in using it at the beginning and end of our work period, there were occasions throughout when we did not, making it difficult to keep track of our progress. Overall, the calendar proved to be an effective tool in ensuring that we got all the work done. In addition, we distributed responsibilities fairly and equally among team members to ensure a balanced workload. This demonstrates our commitment to teamwork and collaboration, which are critical to achieving success in any project.

[3] `https://www.datatilsynet.no/en/regulations-and-tools/vocabulary/`, visited 20.02.23

Chapter 8

Conclusion

In this chapter we will reflect on the learning outcomes of our study and evaluate the extent to which our research has met the desired goals. The problem statement will also be reviewed, and suggestions for further work will be provided.

8.1 Achieved Goals

Measuring the extent to which we have achieved the effect goals is challenging, as they pertain to the long-term outcomes of our thesis and are targeted towards municipalities. However, based on the data presented in Figure 5.11, it is evident that the survey was highly appreciated and contributed to enhancing information security knowledge. As for the result goals, all of these were met. The first two were achieved through Chapter 6 , where we presented a set of recommendations, and in Section 6.2 the competence the municipality should possess is presented. Furthermore, the service catalog, which was our last result goal, can be found in Section 2.1.

Improvement in project management and communication skills was achieved through project planning, thesis writing, interviews, and using a Scrum-based development process. This approach allowed for a clear structure and efficient workflow. We acquired the ability to ask insightful questions while actively listening and taking notes of important details. Furthermore, we have gained knowledge regarding the organizational structure and work dynamic of municipalities and the services provided by a SOC.

8.2 Reviewed Problem Statement

Our problem statement reads as follows: "Is a well-functioning and qualified SOC service sufficient to secure the municipality from an information security perspective?". Although, a SOC helps prevent, detect and recover from security incidents, the effectiveness is dependent on the integration with the municipality. This includes clearly defined roles and responsibilities, communication channels, and incident response procedures that aligns with the municipality's specific needs and requirements. Insufficient communication and collaboration will impact the functionality of the SOC, and hinder its ability to fully assist the municipality. Our recommendations aims to identify necessary competence and how to improve communication and interaction. By implementing these security measures, there is a higher likelihood of detecting and preventing potential attacks, before they can cause significant damage, but a certain level of risk is inevitable.

8.3 Further Work

We did not have time or capacity to cover everything involving a SOC, or other possible SOC solutions for municipalities in this period. We only focused on collaboration with an external SOC service, but for some municipalities establishing an internal SOC would be more relevant. Investigating what additional requirements is necessary to establish an internal SOC, would be a natural extension of our thesis. This process would require looking into what specific competence is needed to work with a SOC, as well as workload and financial resources. Establishing one SOC to many municipalities is also a possibility, especially for intermunicipal collaborations.

One of the things we wished we had used more time on was planning the survey and interviews, as well as how to present the findings. As we realized that the amount of information presented in the tables can be overwhelming. Creating questions that are easier to categorize would have allowed us to utilize graphics more, making it easier to read and understand.

Bibliography

[1] NSM, 'Grunnprinsipper for ikt-sikkerhet 2.0,' 2020, Accessed: 10 February 2023. [Online]. Available: https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/.

[2] M. H. Isabel Skierka Robert Morgus and T. Maurer, 'Csirt basics for policy makers: The history, types culture of computer security incident response teams,' 2015, Accessed: 1 April 2023. [Online]. Available: https://www.gppi.net/media/CSIRT_Basics_for_Policy-Makers_May_2015_WEB.pdf.

[3] Kommunesektorens-Organisasjon, 'Lokaldemokratiet i norge,' 2021, Accessed: 18 February 2023. [Online]. Available: https://www.ks.no/fagomrader/barn-og-unge/ks-ung/faglig-fordypning/samfunnsfag/lokaldemokrati-tekst-moppgaver/.

[4] Regjeringen, 'Informasjon og kommunikasjon mellom kommune og innbyggerne,' 2018, Accessed: 3 February 2023. [Online]. Available: https://www.regjeringen.no/no/tema/kommuner-og-regioner/kommunestruktur/Verktoy/lokaldemokrativeilederen/kommunen-og-innbyggerne/informasjon-og-kommunikasjon-mellom-kommune-og-innbyggerne/id2425537/.

[5] M. Winsvold, 'Veier til god lokaldemokratisk styring,' 2013, Accessed: 10 February 2023. [Online]. Available: https://oda.oslomet.no/oda-xmlui/handle/20.500.12199/5478.

[6] NSM, *Dette er nsm*, Accessed: 3 February 2023. [Online]. Available: https://nsm.no/om-oss/dette-er-nsm/.

[7] NSM, 'Grunnprinsipper for ikt-sikkerhet,' 2023, Accessed: 3 February 2023. [Online]. Available: https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt.

[8] Digiviken, 'Hva er digiviken?,' Accessed: 10 February 2023. [Online]. Available: https://digiviken.no/om-digiviken/.

[9] K. Knerler, I. Parker and C. Zimmerman, '11 strategies of a world-class cybersecurity operations center,' 2022, Accessed: 11 February 2023. [Online]. Available: https://www.mitre.org/news-insights/publication/11-strategies-world-class-cybersecurity-operations-center.

[10] NorSIS, 'Kommune cert,' 2015, Accessed: 4 February 2023. [Online]. Available: https://norsis.no/content/uploads/2022/06/KommuneCSIRT-print.pdf.

[11] D. Direktoratet, 'Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner,' 2022, Accessed: 5 February 2023. [Online]. Available: https://www.digdir.no/informasjonssikkerhet/arbeidet-med-informasjonssikkerhet-i-fylkeskommuner-og-kommuner/2102.

[12] DSB, 'Dsbs årsrapport 2021,' 2022, Accessed: 6 February 2023. [Online]. Available: https://www.dsb.no/globalassets/dokumenter/rapporter/andre-rapporter/dsb-arsrapport-2021.pdf.

[13] K. S. Brinkmann S, 'Det kvalitative forskningsintervju,' vol. 3, 2015, Accessed: 12 April 2023.

[14] Regjeringen, 'Digitale angrep mot norske kommuner kan få store konsekvenser,' 2022, Accessed: 3 April 2023. [Online]. Available: https://www.regjeringen.no/no/aktuelt/-digitale-angrep-mot-norske-kommuner-kan-fa-store-konsekvenser/id2900215/.

Appendix A

Project Plan

DCSG2900

Project plan

Authors: Camilla Molland, Emina Engh, Katrine Brække Lyngen & Nora Altamimi

Table of contents

1. Background and goals

1.1 Background

IKOMM is a fully Norwegian owned company where value is both created and remains in Norway. Recognizing the challenges faced by small and medium-sized municipalities in keeping up with technological advancements, the company aims to achieve greater success by merging and gathering expertise. What started as a vision to improve the IT-services for 3 municipalities with 8 employees in 2003, has resulted in a company with over 120 employees spread across five offices.

In today's digital age, all data that is created, processed, and stored in a municipality is done electronically. The need for adequate security measures is therefore extremely important since we are relying on our systems to be compliant with confidentiality, integrity, and availability. A security operation center (SOC) is a "*team of IT professionals that monitors an organization's entire IT infrastructure, 24/7, to detect cybersecurity events in real time and address them as quickly and effectively as possible*" (IBM, n.d.).

Implementing a SOC can be both time-consuming and expensive if not done right. And many of the best practices have been established for homogeneous and "simple" organizations and are not well suited for more complex structured organizations like a municipality.

1.2 Project goals

We have divided the project goals into 3 parts: effect-, result- and learning goals. The effect goals are the long-term goals and describes which effect we want to achieve though our finished product. The result goals are what we want our final project delivery to be, and the learning goals are what we are hoping to learn throughout this project.

1.2.1 Effect goals

- Improve information security by increasing awareness and cooperation.

- Increase collaboration between the SOC and the municipality.
- Reduce workload by optimizing the implementation of a SOC for a municipality.

1.2.2 Result goals

- Create a general set of recommendations to improve interaction between a SOC and a municipality.
- Map what competence a municipality should at least have to be able to effectively implement feedback from the SOC.
- Make both technical and non-technical recommendations for the municipality, in areas such as infrastructure, communication and environment.

1.2.3 Learning goals

- Improve our knowledge about project management.
- Improve our knowledge within scrum-based development.
- Enhance our communication skills.
- Learn more about the structure of a municipality and a SOC.

1.3 Timeframes

- The project plan and project agreement need to be signed and delivered by January 31st.
- The bachelor thesis is due 22nd of May 2023.

1.3.1 Other

The report will be written in English using Overleaf, a web-based collaboration LaTeX tool.

2. Scope

2.1 Problem area

Norway has 365 municipalities ranging from 192 residents to 700 000 (Regjeringen, 2021). A municipality is a local self-governing unit responsible for providing a range of public services to the residents in its geographical area. The idea behind this local democracy is that those who live in a municipality know the local problems best and know how to solve them. These services include education, health, technical infrastructure and social services, as well as maintaining the local environment and the municipality's economy. A municipality depends on having updated technology in order to carry out its tasks effectively. To effectively carry out these tasks, municipalities depend on having updated technology. However, as the cyberattack on Østre Toten in January 2021 reminded us, our reliance on technology also makes us vulnerable to catastrophic consequences if our systems are compromised.

Cybersecurity has gotten an increased focus the last few years especially after the Covid-19 pandemic and the war in Ukraine. Having an in-house SOC or paying for external SOC services is becoming increasingly common, not only in the technical sector, but establishing monitoring services for a municipality presents some new challenges.

2.2 Problem statement

For this project, IKOMM wants us to come up with a best practice proposal for interaction between a municipality and a SOC. To be able to implement security measures based on feedback from the SOC the municipality needs a broad understanding of information security. The proposal will therefore contain a mapping of what competence a municipality, including all sectors with an extra focus on the IT department, at least needs to require to ensure insight and understanding by both parties.

Our problem statement is therefore as follows: Having a well-functioning and qualified SOC service is sufficient to secure the municipality from an information security perspective.

2.3 Limitations

Due to the task being so open we will limit ourselves to focus on these three points:

- Communication and responsibility distribution between a SOC and a municipality.

- What needs to be mapped to ensure insight and understanding between the SOC and the municipality.
- Identify what competence a municipality needs to have to be able to make use of external SOC services.

3. Project organization

This team consists of four students from digital infrastructure and cybersecurity. We have decided to split and have fixed roles during this project. This way it's more organized and we always know our tasks.

3.1 Roles

Leader – Katrine

Secretary – Nora

Quality controller – Camilla

Communication manager – Emina

Reference manager – All

3.1 Responsibilities

Team Leader: The team leaders' main task is to make sure all members have something to do. It's also important that the team leader oversees that all members understand their task. This way, the work will be done in an efficient manner. If someone is not able to be at a meeting, they will notify the team leader.

Secretary: The secretary’s task is to take notes when we have a meeting, whether it's just the team, or with our employer or supervisor. These notes will be uploaded to a document we have on our OneDrive.

Quality controller: All members will read through everything we write, but the quality manager needs to take an extra look at what we have produced, and make sure there are no errors or misspellings.

Communication manager: Makes sure all communication between the employer and supervisor are seen by all team members. The communication manager also sends out messages and schedules meetings with the team, and/or with employer and supervisor if this is needed.

Reference manager: Makes sure all references are added along the way, so that none are forgotten. All sources should be listed in the reference management tool EndNote for effective source referencing.

3.2 Routines

- The number of hours for each week must be written down in a separate document and must be up to date by the end of each week.
- We will work up to 30 hours a week but are prepared to work more if needed.
- Meet physically on campus Mondays and Thursdays and work together.
- Meetings with employer will be scheduled as needed and meetings with supervisor are scheduled for Tuesdays at 14:30.
- To keep track of our sources we will be using EndNote.
- Communication channels are Discord and Microsoft Teams.
- We will use a shared OneDrive folder to store all shared documents.

3.2 Rules

Meetings

The communication manager is responsible for sending out meeting summons to all team members at least 2 days in advance. This will be done using our internal communication channel

on Discord. There should be at least 1 meeting per week in addition to the weekly meetings with our supervisor.

Documentation

After all meetings and workdays, we will document everything that has been done. All team members are responsible for writing down how long they worked and what they did. For all meetings with our employer and our supervisor our secretary will make a minute of meeting.

Distribution of tasks

All team members are expected to work equally as much and share the work tasks as evenly among us as possible. The team is open to members wanting to contribute to specific tasks based on interest and abilities.

Attendance and preparation

All meetings are mandatory to attend for team members. Everyone should be prepared for the meetings, and not be late.

Absence

If anyone is not able to attend the meetings or any other scheduled work, they need to notify the team leader beforehand.

Violations

If someone ends up violating any of the rules it will first be taken up internally with the team, and if no changes are made our supervisor will be contacted.

4. Planning, follow-up and reporting

4.1 Process framework

We will use Scrum as our process framework to organize the periods and tasks during this project. In this board we will have different sprints and in these we will divide the tasks into to-do, doing, verify and done. There will also be a backboard, where all our tasks/projects are mentioned as we get knowledge about them before we divide them up and start on them. This

way we will always know where in the sprint we are with each task. Table 1 shows how we will divide the sprints, and each will have a duration of 1 week.

Table 1 – Sprints

Activity	Nr. of sprints
Planning	2
Interviews, meetings	4
Report writing	9
Evaluation	1
Report writing	5
Proof reading	3

4.2 Methodology

We will use different methods in the process of collecting data and information. Before we start the process of getting the actual data, we must establish who we need information from. We have for this come up with a list consisting of different municipalities, SOC providers and others who works in the field of interest.

To collect the data, we will use different methods, including a survey to determine the level of knowledge regarding information security and technology among employees in municipalities. Additionally, we will conduct interviews and meetings with more specialized people in the IT field who have extensive knowledge and experience regarding how the municipalities are set up. Furthermore, we will talk to SOC providers to gain a technical understanding of how they are used and what knowledge is necessary for their users. Lastly, we will look at a lot of documents and reports, so already existing data. These will be about SOC requirements, implementation, how it works and generally about municipalities.

The collected and processed information will be the data that we base our thesis on. From the surveys we will statistically analyze and map the average competence and knowledge in the municipalities. All documents and information obtained from the interviews will be stored in our OneDrive for future reference. We will then further analyze all documents and statistics and compare them to formulate a set of best practice recommendations.

4.3 Plan for status meeting and decision points in the working period

We will have a longer status meeting at least once a week, and this will happen on Thursdays when we meet physically on campus. Here we will go through what we have done up until that point, the people we have talked to, meetings we have had and go through what we have planned for the upcoming period. We will also have small status meetings after each meeting with our employer and supervisor and at the end of our workday. We will then go through what we have done or the information we have got to get a better overview.

We will mainly use time to make any decisions when we are done with a period in our Gantt chart, and when we are finished with a sprint in Scrum. This way we can see if we managed to do what we wanted and if we are prepared for a new period to start as planned. Or if we might need to adjust and change our plan.

4.3.1 Meetings with supervisor

Before our meetings with our supervisors on Tuesdays, we are going to make a small report about last week´s work. This way everyone will know the status of our progression and how far we have come in the project and what we are missing. We will also talk about our plan for the upcoming week.

5. Organizing of quality assurance

5.1 Documentation, standards, utilities

To ensure that our workflow is as efficient as possible, we have a list of different tools that will help us organize the documentation and keep track of responsibilities. This will ensure that everyone knows where to find what we are working on, what responsibilities each of us have and which tasks to do next.

Table 2 – Tools we use

Name	Type	Usage
Discord	Communication platform	Communication and meetings
Microsoft Teams	Communication platform	Meeting with employers and other externals
OneDrive	Online file sharing/collaboration platform	Collaborate on documents, as well as organize our files
Overleaf	LaTeX editor	Writing our report
EndNote	Reference manager	Creating, storing and manages our references/citations

5.2 Plan for evaluations

- The quality controller will need to make sure everyone proofreads all documents. All team members will read everything we have done before handing it over to our supervisor.
- We will deliver the first draft of our thesis to our supervisor, where we have everything roughly finished.
- Our supervisor will look over all our documents before the final deadline.

5.3 Risk analysis on project level

In the risk matrix below are the different risk factors organized with probability, consequence and risk. The colors represent the overall risk, with red being very high, yellow is high, and green is ok. The risks are all explained with descriptions and measures.

Table 3 – Risk matrix

	Very high consequence	High consequence	Medium consequence	Some consequence	No consequence
Very high probability					
High probability		1	4		
Probable			3		

Some probability	2		5		
No probability	6	7			

Risk 1

Risk scenario	Too complex for the team
Description	Some tasks are too difficult for the team members to understand, so we will not be able to meet the requirements needed
Probability	High
Consequence	High
Overall risk	Very high

Measures: We need to ask for help from people who know the topic. We can also minimize the amount of material so it's only relevant to our own task, this way we won´t get overwhelmed with a lot of information we might not even need and get confused.

Risk 2

Risk scenario	Loss of documentation
Description	Losing our report or other documentation due to technical error etc.
Probability	Some
Consequence	Very high
Overall risk	High

Measures: We have backups of all our documentation, so we would have to see if these are still usable.

Risk 3

Risk scenario	Sickness
Description	If one or more team members get sick over a longer period
Probability	Probable
Consequence	Medium
Overall risk	High

Measures: Every team member knows what tasks they need to do, and everyone can see what other members' tasks are. So, if someone gets sick and cannot work, the other members need to split the work from the sick member amongst themselves.

Risk 4

Risk scenario	We limit the project too little
Description	The team gets too deep in the wrong parts of the project to answer the task appropriately
Probability	High
Consequence	Medium
Overall risk	High

Measures: The team need to follow our scope, and not dig deep into information we will not need. Have evaluation periods to make sure we are sticking to the task description and answer our problem statement.

Risk 5

Risk scenario	Conflicts within the team
Description	If the team has a disagreement that cannot be solved
Probability	Some
Consequence	Medium
Overall risk	High

Measures: First, the team needs to have a meeting to try to resolve the problem. If this does not help, we need to take the disagreement to our supervisor, and let her help us solve the problem. Whatever the supervisor decides, all team members must listen to this.

Risk 6

Risk scenario	Thesis will not be ready in time for deadline
Description	The team will not be able to deliver thesis by the deadline, due to too much work.
Probability	No
Consequence	Very high
Overall risk	Low

Measures: Need to have a meeting with our employer to ask them if we can reduce the amount of work.

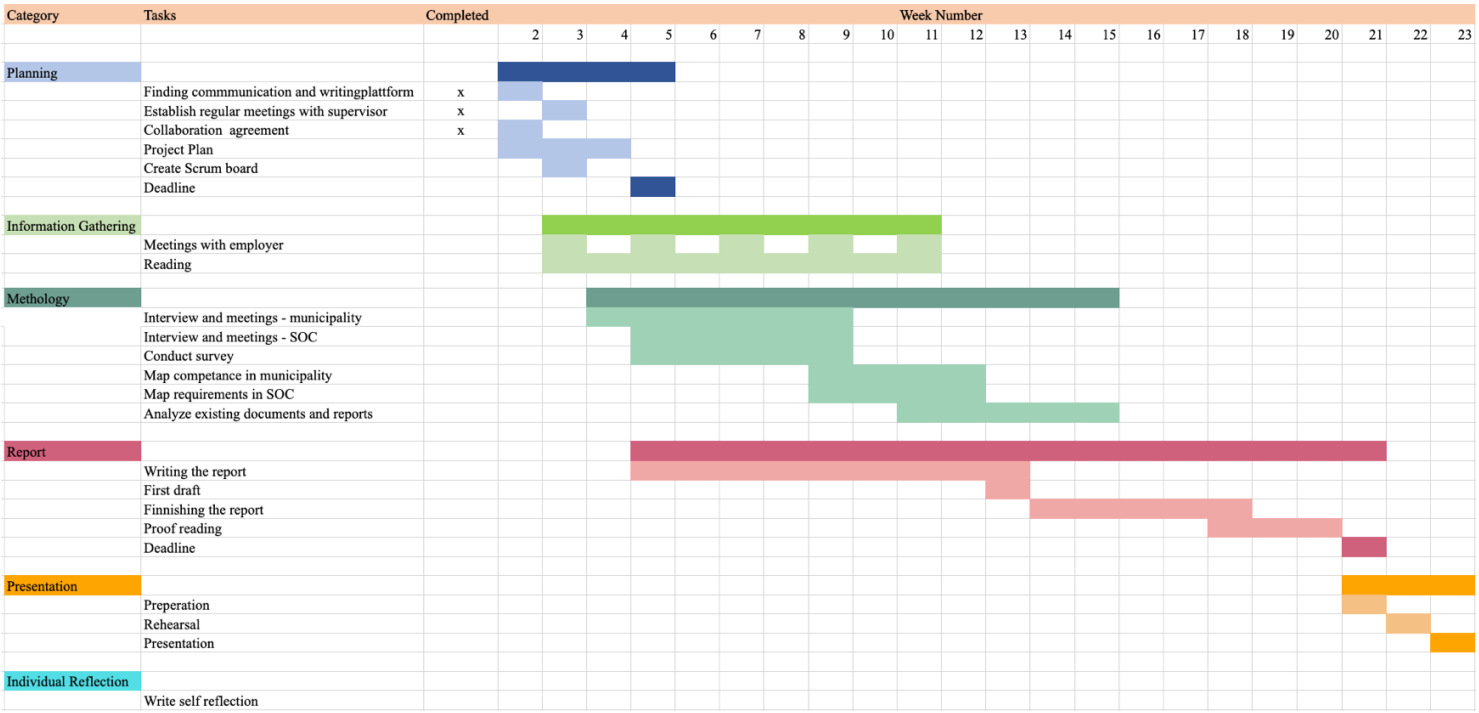
Risk 7

Risk scenario	One or more members does not participate
Description	Members of our team do little to no work.
Probability	No
Consequence	High
Overall risk	Low

Measures: Try to resolve the matter within the team. If this does not work, our supervisor will be contacted.

6. Plan for execution

6.1 Gantt



6.2 Project specific activities

First milestone:

- Sign and deliver the confidentiality agreement.
- Sign and deliver the standard agreement.
- Finish the project plan.

Second milestone:

- Get in contact with key persons.
- Interview and meet with people working in the municipalities.
- Interview and meet with people working with SOC services.

- Conduct survey for the employees working in the municipalities
- Map competence in technology and information security in the municipalities.
- Map put the requirements necessary for a SOC to function properly.

Third milestone:

- Deliver first draft.

Fourth milestone:

- Finish the report.
- Presentation.

7. Bibliography

Regjeringen (2021). *Historisk utvikling.* Available from: https://www.regjeringen.no/no/tema/kommuner-og-regioner/kommunestruktur/utviklingen-av-den-norske-kommunestruktu/id751352/ (Accessed on 19.01.2023)

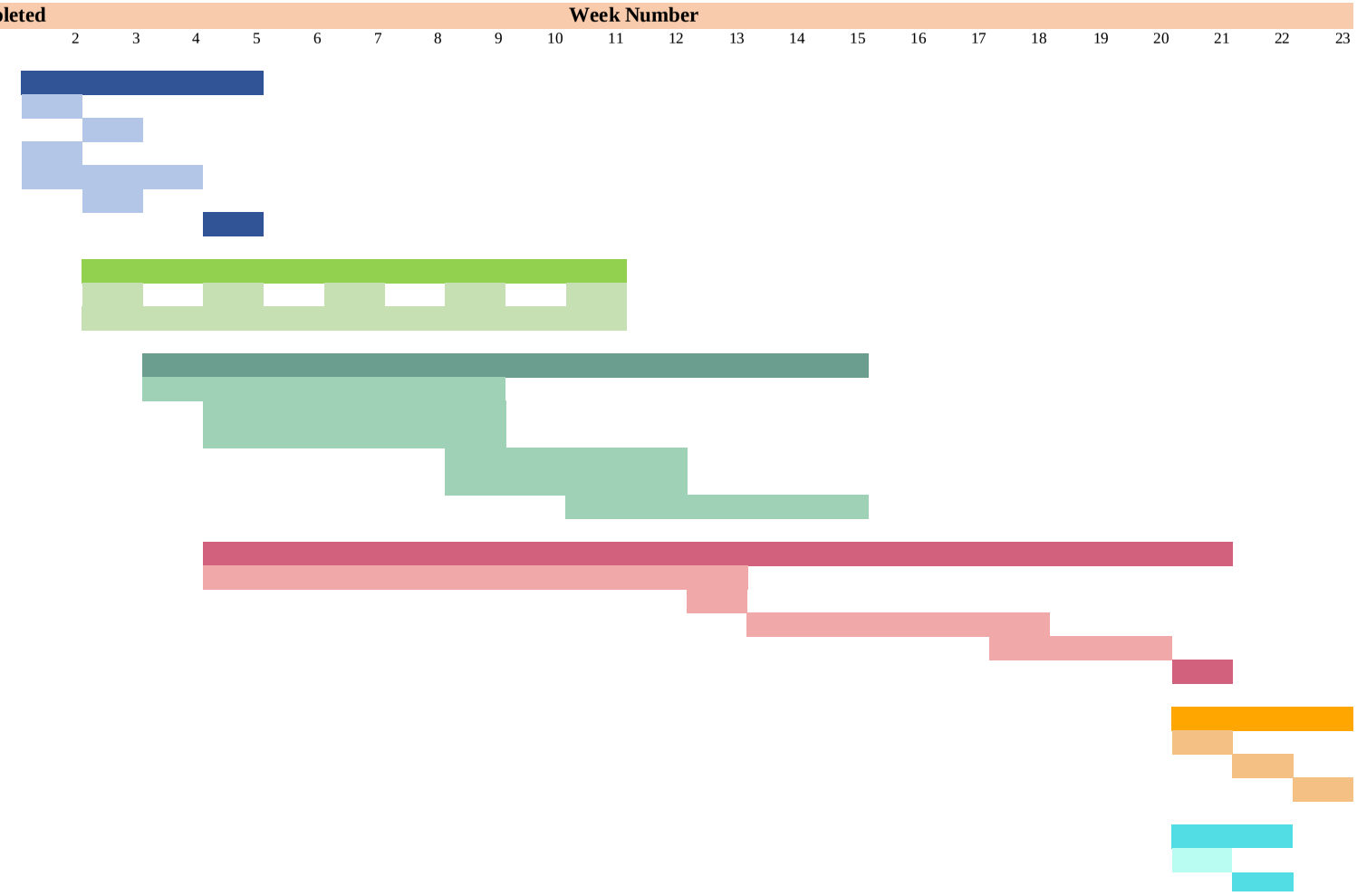
IBM (n.d.) *Security Operations Centre (SOC)*. Available from: https://www.ibm.com/topics/security-operations-center (Accessed on 24.01.2023)

Indeed Editorial Team. (26.08.2022). *Methodology in a research paper: definitions and example.* Available from: https://www.indeed.com/career-advice/career-development/example-of-methodology-in-research-paper (Accessed on 24.01.2023)

Appendix B

Gantt Chart

Category	Tasks	Completed
Planning		
	Finding commmunication and writingplattform	x
	Establish regular meetings with supervisor	x
	Collaboration agreement	x
	Project Plan	x
	Create Scrum board	x
	Deadline	x
Information Gathering		
	Meetings with employer	x
	Reading	x
Methology		
	Interview and meetings - municipality	x
	Interview and meetings - SOC	x
	Conduct survey	x
	Map competance in municipality	x
	Map requirements in SOC	x
	Analyze existing documents and reports	x
Report		
	Writing the report	x
	First draft	x
	Finnishing the report	x
	Proof reading	x
	Deadline	x
Presentation		
	Preperation	
	Rehearsal	
	Presentation	
Individual Reflection		
	Write self reflection	
	Deadline	



Appendix C

Task Description

Om Ikomm AS

Ikomm er et heleid norsk selskap hvor all verdiskapningen skjer og forblir i Norge. Vi har et eget datasenter, trygt plassert i kjelleren på Fakkelgården der vi har vårt hovedkontor på Lillehammer. I disse dager kan det være betryggende med muligheten til å lagre data og drifte applikasjoner helt lokalt, det ser vi bare på som et konkurransefortrinn. Samtidig beveger jo også vi oss stadig mer opp i skya.

Vi er representert over hele Østlandet og våre eierkommuner er i dag Lillehammer, Gausdal, Øyer, Indre Østfold, Nesodden, Østre Toten, og Våler i Viken. Vårt hovedkontor er på Lillehammer og vi har et stort avdelingskontor Askim. I tillegg har vi filialer på Nesodden, i Hamar, og på Lena.

Vi ser at å etablere overvåkingstjenester for kommunale tjenester gir noen utfordringer som vi ønsker belyst i samarbeid med bachelorstudiet ved NTNU Gjøvik. Det er flere kommunale samarbeid og kommuner som ønsker å tjenesteutsette SOC-funksjonalitet og som vil komme til å måtte forholde seg til en SOC-tjeneste som en ekstern part.

Mye av «beste praksis» er etablert for homogene og «enkle» organisasjoner og ikke godt egnet for for eksempel en kommune (NIST)

<u>Oppgave:</u>

Vi ønsker å få belyst samarbeid med SOC fra et kommunalt perspektiv og hvordan denne samhandlingen best mulig håndteres. Et bredt perspektiv på forståelsen av informasjonssikkerhet vil kreves for at en kommune skal kunne samhandle og iverksette tiltak basert på tilbakemelding fra SOC. Hvilke tiltak vil kunne berøre kommunal praksis og hvilke oppgaver bør håndteres av kommunens IT-avdeling eller samarbeidspart.

Mål for oppgaven:
Komme opp med et forslag til «beste praksis» for samhandling med SOC for en kommune.

- Kommunikasjon mellom og ansvar for de ulike parter
- Kartlegging – hva må kartlegges for å sikre innsikt og forståelse hos begge parter
- Identifisere kompetanse hos kommunen for å kunne nyttiggjøre seg eksterne SOC-tjenester

<u>Oppgavekrav:</u>
Forslag bør inneholde anbefalinger av både teknisk og ikke-teknisk art for å sikre hele verdikjeden i et informasjonssikkerhetsperspektiv. Oppgaven bør belyse muligheter å utfordringer knyttet til tiltak som kommer som en følge av å etablere SOC-tjenester i en kommune.

Tiltak og oppgaver bør kunne settes i sammenheng med NSM grunnprinsipper for IKT-sikkerhet.

Appendix D

Standard Agreement

NTNU

Norges teknisk-naturvitenskapelige universitet

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDAVTALE

om utføring av studentoppgave i samarbeid med ekstern virksomhet

Avtalen er ufravikelig for studentoppgaver (heretter oppgave) ved NTNU som utføres i samarbeid med ekstern virksomhet.

Forklaring av begrep

Opphavsrett
Er den rett som den som skaper et åndsverk har til å fremstille eksemplar av åndsverket og gjøre det tilgjengelig for allmennheten. Et åndsverk kan være et litterært, vitenskapelig eller kunstnerisk verk. En studentoppgave vil være et åndsverk.

Eiendomsrett til resultater
Betyr at den som eier resultatene bestemmer over disse. Utgangspunktet er at studenten eier resultatene fra sitt studentarbeid. Studenten kan også overføre eiendomsretten til den eksterne virksomheten.

Bruksrett til resultater
Den som eier resultatene kan gi andre en rett til å bruke resultatene, f.eks. at studenten gir NTNU og den eksterne virksomheten rett til å bruke resultatene fra studentoppgaven i deres virksomhet.

Prosjektbakgrunn
Det partene i avtalen har med seg inn i prosjektet, dvs. som vedkommende eier eller har rettigheter til fra før og som brukes i det videre arbeidet med studentoppgaven. Dette kan også være materiale som tredjepersoner (som ikke er part i avtalen) har rettigheter til.

Utsatt offentliggjøring
Betyr at oppgaven ikke blir tilgjengelig for allmennheten før etter en viss tid, f.eks. før etter tre år. Da vil det kun være veileder ved NTNU, sensorene og den eksterne virksomheten som har tilgang til studentarbeidet de tre første årene etter at studentarbeidet er innlevert.

1. Avtaleparter

Norges teknisk-naturvitenskapelige universitet (NTNU) Institutt:
Veileder ved NTNU: jia-chun.lin@ntnu.no e-post og tlf.
Ekstern virksomhet: Ekstern virksomhet sin kontaktperson, e-post og tlf.:
Student: Emina Engh Fødselsdato: 16/07/2000
Student: Katrine Brekke Lyngen Fødselsdato: 18/12/2000
Student: Camilla Molland Fødselsdato: 27/03/2000
Student: Nora Altamimi Fødselsdato: 15/10/2001

Partene har ansvar for å klarere eventuelle immaterielle rettigheter som studenten, NTNU, den eksterne eller tredjeperson (som ikke er part i avtalen) har til prosjektbakgrunn før bruk i forbindelse med utførelse av oppgaven. Eierskap til prosjektbakgrunn skal fremgå av eget vedlegg til avtalen der dette kan ha betydning for utførelse av oppgaven.

2. Utførelse av oppgave

Studenten skal utføre: (sett kryss)

Masteroppgave	
Bacheloroppgave	X
Prosjektoppgave	
Annen oppgave	

Startdato: 11/01
Sluttdato: 22/05

Oppgavens arbeidstittel er: Bacheloroppgave IKOMM as

Ansvarlig veileder ved NTNU har det overordnede faglige ansvaret for utforming og godkjenning av prosjektbeskrivelse og studentens læring.

3. Ekstern virksomhet sine plikter

Ekstern virksomhet skal stille med en kontaktperson som har nødvendig faglig kompetanse til å gi studenten tilstrekkelig veiledning i samarbeid med veileder ved NTNU. Ekstern kontaktperson fremgår i punkt 1.

Formålet med oppgaven er studentarbeid. Oppgaven utføres som ledd i studiet. Studenten skal ikke motta lønn eller lignende godtgjørelse fra den eksterne for studentarbeidet. Utgifter knyttet til gjennomføring av oppgaven skal dekkes av den eksterne. Aktuelle utgifter kan for eksempel være reiser, materialer for bygging av prototyp, innkjøp av prøver, tester på lab, kjemikalier. Studenten skal klarere dekning av utgifter med ekstern virksomhet på forhånd.

Ekstern virksomhet skal dekke følgende utgifter til utførelse av oppgaven:

Dekning av utgifter til annet enn det som er oppført her avgjøres av den eksterne underveis i arbeidet.

4. Studentens rettigheter

Studenten har opphavsrett til oppgaven[1]. Alle resultater av oppgaven, skapt av studenten alene gjennom arbeidet med oppgaven, eies av studenten med de begrensninger som følger av punkt 5, 6 og 7 nedenfor. Eiendomsretten til resultatene overføres til ekstern virksomhet hvis punkt 5 b er avkrysset eller for tilfelle som i punkt 6 (overføring ved patenterbare oppfinnelser).

I henhold til lov om opphavsrett til åndsverk beholder alltid studenten de ideelle rettigheter til eget åndsverk, dvs. retten til navngivelse og vern mot krenkende bruk.

Studenten har rett til å inngå egen avtale med NTNU om publisering av sin oppgave i NTNUs institusjonelle arkiv på Internett (NTNU Open). Studenten har også rett til å publisere oppgaven eller deler av den i andre sammenhenger dersom det ikke i denne avtalen er avtalt begrensninger i adgangen til å publisere, jf. punkt 8.

5. Den eksterne virksomheten sine rettigheter

Der oppgaven bygger på, eller videreutvikler materiale og/eller metoder (prosjektbakgrunn) som eies av den eksterne, eies prosjektbakgrunnen fortsatt av den eksterne. Hvis studenten

[1] Jf. Lov om opphavsrett til åndsverk mv. av 15.06.2018 § 1

skal utnytte resultater som inkluderer den eksterne sin prosjektbakgrunn, forutsetter dette at det er inngått egen avtale om dette mellom studenten og den eksterne virksomheten.

Alternativ a) (sett kryss) Hovedregel

X	Ekstern virksomhet skal ha bruksrett til resultatene av oppgaven

Dette innebærer at ekstern virksomhet skal ha rett til å benytte resultatene av oppgaven i egen virksomhet. Retten er ikke-eksklusiv.

Alternativ b) (sett kryss) Unntak

	Ekstern virksomhet skal ha eiendomsretten til resultatene av oppgaven og studentens bidrag i ekstern virksomhet sitt prosjekt

Begrunnelse for at ekstern virksomhet har behov for å få overført eiendomsrett til resultatene:

6. Godtgjøring ved patenterbare oppfinnelser

Dersom studenten i forbindelse med utførelsen av oppgaven har nådd frem til en patenterbar oppfinnelse, enten alene eller sammen med andre, kan den eksterne kreve retten til oppfinnelsen overført til seg. Dette forutsetter at utnyttelsen av oppfinnelsen faller inn under den eksterne sitt virksomhetsområde. I så fall har studenten krav på rimelig godtgjøring. Godtgjøringen skal fastsettes i samsvar med arbeidstakeroppfinnelsesloven § 7. Fristbestemmelsene i § 7 gis tilsvarende anvendelse.

7. NTNU sine rettigheter

De innleverte filer av oppgaven med vedlegg, som er nødvendig for sensur og arkivering ved NTNU, tilhører NTNU. NTNU får en vederlagsfri bruksrett til resultatene av oppgaven, inkludert vedlegg til denne, og kan benytte dette til undervisnings- og forskningsformål med de eventuelle begrensninger som fremgår i punkt 8.

8. Utsatt offentliggjøring

Hovedregelen er at studentoppgaver skal være offentlige.

Sett kryss

	Oppgaven skal være offentlig

I særlige tilfeller kan partene bli enige om at hele eller deler av oppgaven skal være undergitt utsatt offentliggjøring i maksimalt tre år. Hvis oppgaven unntas fra offentliggjøring, vil den kun være tilgjengelig for student, ekstern virksomhet og veileder i denne perioden. Sensurkomiteen vil ha tilgang til oppgaven i forbindelse med sensur. Student, veileder og sensorer har taushetsplikt om innhold som er unntatt offentliggjøring.

Oppgaven skal være underlagt utsatt offentliggjøring i (sett kryss hvis dette er aktuelt):

Sett kryss		Sett dato
	ett år	
	to år	
	tre år	

Behovet for utsatt offentliggjøring er begrunnet ut fra følgende:

Dersom partene, etter at oppgaven er ferdig, blir enig om at det ikke er behov for utsatt offentliggjøring, kan dette endres. I så fall skal dette avtales skriftlig.

Vedlegg til oppgaven kan unntas ut over tre år etter forespørsel fra ekstern virksomhet. NTNU (ved instituttet) og student skal godta dette hvis den eksterne har saklig grunn for å be om at et eller flere vedlegg unntas. Ekstern virksomhet må sende forespørsel før oppgaven leveres.

De delene av oppgaven som ikke er undergitt utsatt offentliggjøring, kan publiseres i NTNUs institusjonelle arkiv, jf. punkt 4, siste avsnitt. Selv om oppgaven er undergitt utsatt offentliggjøring, skal ekstern virksomhet legge til rette for at studenten kan benytte hele eller deler av oppgaven i forbindelse med jobbsøknader samt videreføring i et master- eller doktorgradsarbeid.

9. Generelt

Denne avtalen skal ha gyldighet foran andre avtaler som er eller blir opprettet mellom to av partene som er nevnt ovenfor. Dersom student og ekstern virksomhet skal inngå avtale om konfidensialitet om det som studenten får kjennskap til i eller gjennom den eksterne virksomheten, kan NTNUs standardmal for konfidensialitetsavtale benyttes.

Den eksterne sin egen konfidensialitetsavtale, eventuell konfidensialitetsavtale den eksterne har inngått i samarbeidprosjekter, kan også brukes forutsatt at den ikke inneholder punkter i motstrid med denne avtalen (om rettigheter, offentliggjøring mm). Dersom det likevel viser seg at det er motstrid, skal NTNUs standardavtale om utføring av studentoppgave gå foran. Eventuell avtale om konfidensialitet skal vedlegges denne avtalen.

Eventuell uenighet som følge av denne avtalen skal søkes løst ved forhandlinger. Hvis dette ikke fører frem, er partene enige om at tvisten avgjøres ved voldgift i henhold til norsk lov. Tvisten avgjøres av sorenskriveren ved Sør-Trøndelag tingrett eller den han/hun oppnevner.

Denne avtale er signert i fire eksemplarer hvor partene skal ha hvert sitt eksemplar. Avtalen er gyldig når den er underskrevet av NTNU v/instituttleder.

Signaturer:

Instituttleder: Dato:
Veileder ved NTNU: Dato:
Ekstern virksomhet: Dato:
Student: Nora Altamimi Dato: 11.01.23
Student: Katrine Brodtkorb Dyrgen Dato: 11/01/23
Student: Emina Eryk Dato: 11/01/23
Student: Camilla Moklund Dato: 11.01.23

Appendix E

Timesheet

Camilla

Week	Day	No. Hours	Activity
2	Monday	1	Planned meeting with supervisor
	Tuesday	1	Planned meeting with IKOMM
	Wednesday	7	Project plan
	Thursday	5	Project plan
	Friday	4	Project plan
	Saturday		
Total: 18	Sunday		
3	Monday	4	Meeting with IKOMM
	Tuesday	6	Meeting with supervisor + project plan
	Wednesday	1	Communication with external resources
	Thursday	8	Planning several meetings + project plan
	Friday	3	Questions for meeting
	Saturday		
Total: 22	Sunday		
4	Monday	4	Plan presentation + improve project plan
	Tuesday	3	Meeting with supervisor + improve project plan
	Wednesday	2	Improve project plan
	Thursday	7	Meeting with kommune-csirt + further planning
	Friday	3	Planned meeting with Mnemonic
	Saturday		
Total: 22	Sunday	2	Research
5	Monday	3	Research
	Tuesday	8	Research
	Wednesday	4	Make outline for report
	Thursday	3	Research
	Friday	3	Survey questions
	Saturday	4	Survey questions
Total: 25	Sunday		
6	Monday	3	Planned meeting with IKOMM
	Tuesday	6	Research
	Wednesday	4	Research
	Thursday	7	Meeting with IKOMM + surveys + research
	Friday	3	Survey + emails
	Saturday		
Total: 23	Sunday		
7	Monday	4	Surveys + emails
	Tuesday	7	Meeting with supervisor + surveys
	Wednesday	2	Emails
	Thursday	4	Research
	Friday	8	Report + plan meetings
	Saturday		
Total: 25	Sunday		
8	Monday	3	Further planning
	Tuesday	8	Meeting with supervisor + questions for meeting
	Wednesday	4	Surveys + emails
	Thursday	8	Meeting with IKT-fjellregionen + survey
	Friday	7	Meeting with Haugesund + questions for meeting
	Saturday		
Total: 30	Sunday		
9	Monday	3	Planned the week + survey
	Tuesday	4	Thesis writing course + outline
	Wednesday	3	Emails + survey
	Thursday	8	Planned meetings + survey + research
	Friday	5	Meeting with Janne for statistics
	Saturday		
Total: 25	Sunday	2	Planned meeting with IKOMM
10	Monday	7	Meeting with IKOMM + thesis writing course
	Tuesday	6	Meeting with Indigo IKT + supervisor + thesis writing
	Wednesday		
	Thursday	8	Meeting with Oslo + Netsecurity + Bergen
	Friday	5	Meeting with statistics + thesis writing
	Saturday		
Total: 30	Sunday	4	Thesis writing
11	Monday	4	Thesis writing
	Tuesday	4	Emails
	Wednesday		
	Thursday	8	Thesis writing
	Friday	5	Surveys
	Saturday		
Total: 27	Sunday	6	Statistics in JupyterNotebook
12	Monday	5	Thesis writing
	Tuesday	4	Thesis writing + meeting with supervisor
	Wednesday	5	Thesis writing
	Thursday	8	Thesis writing
	Friday	5	Thesis writing
	Saturday	5	Thesis writing
Total: 35	Sunday	3	Thesis writing
13	Monday	6	Thesis writing
	Tuesday	5	Thesis writing + meeting with supervisor
	Wednesday		
	Thursday	7	
	Friday	6	Statistics in JupyterNotebook
	Saturday	3	Thesis writing
Total: 32	Sunday	5	Thesis writing
14	Monday		Easter break
	Tuesday		
	Wednesday		
	Thursday		
	Friday		
	Saturday		
Total: 0	Sunday		
15	Monday	8	Thesis writing
	Tuesday	5	Thesis writing
	Wednesday	2	Thesis writing
	Thursday	8	Thesis writing
	Friday	4	Thesis writing
	Saturday	4	Thesis writing
Total: 31	Sunday		
16	Monday	7	Thesis writing
	Tuesday	5	Thesis writing + meeting with supervisor
	Wednesday		
	Thursday	8	Thesis writing
	Friday	6	Thesis writing
	Saturday	6	Thesis writing
Total: 32	Sunday		
17	Monday		
	Tuesday	8	Thesis writing + meeting with supervisor
	Wednesday	4	Thesis writing
	Thursday	8	Thesis writing
	Friday		
	Saturday	7	Thesis writing
Total: 30	Sunday	3	Thesis writing
18	Monday	9	Thesis writing
	Tuesday	4	Thesis writing + meeting with supervisor
	Wednesday	4	Thesis writing
	Thursday	8	Thesis writing
	Friday	3	Thesis writing
	Saturday	5	Thesis writing
Total: 33	Sunday	3	Thesis writing
19	Monday	7	Thesis writing
	Tuesday	2	Thesis writing + meeting with supervisor
	Wednesday	5	Thesis writing
	Thursday	8	Thesis writing
	Friday	3	Thesis writing
	Saturday	8	Thesis writing
Total: 26	Sunday		
20	Monday	7	Thesis writing
	Tuesday	6	Thesis writing
	Wednesday		
	Thursday	5	Thesis writing
	Friday	8	Thesis writing
	Saturday		
Total:	Sunday		

Emina

Week	Day	No. Hours	Activity
2	Monday	1	Planned meeting with supervisor
	Tuesday	1	Planned meeting with IKOMM
	Wednesday	7	Project plan
	Thursday	5	Project plan
	Friday	4	Project plan
	Saturday		
Total: 18	Sunday		
3	Monday	4	Meeting with IKOMM
	Tuesday	3	Meeting with supervisor
	Wednesday	3	Project plan
	Thursday	8	Project plan and organized meetings
	Friday	3	Made questions for meeting/research
	Saturday		
Total: 21	Sunday		
4	Monday	4	Planned presentation and improve project plan
	Tuesday	2	Meeting with supervisor
	Wednesday	3	Research
	Thursday	7	Meeting with CSIRT and info gathering
	Friday	3	Planned meeting with Mnemonic
	Saturday	3	Research
Total: 23	Sunday		
5	Monday	3	Research
	Tuesday	9	Meeting with Mnemonic, meeting with supervisor and researcl
	Wednesday	4	Make outline for report
	Thursday	2	Research
	Friday	3	Working with survey questions
	Saturday	4	Working with survey questions
Total: 25	Sunday		
6	Monday	2	Planning meeting with IKOMM
	Tuesday		
	Wednesday	3	Research
	Thursday	8	Meeting with IKOMM and Survey planning
	Friday	4	Research
	Saturday	4	Emails and research
Total: 21	Sunday		
7	Monday		
	Tuesday	7	Meeting with supervisor and research
	Wednesday	2	Emails and survey
	Thursday	4	Research
	Friday	8	Planned meetings and research
	Saturday		
Total: 21	Sunday		
8	Monday	3	Planned the week
	Tuesday	8	Meeting with supervisor and made questions for meetings
	Wednesday	4	Survey and emails
	Thursday	8	Meeting with IKT Fjellregionen and survey work
	Friday	7	Meeting with Haugesund and plan other meetings
	Saturday		
Total: 30	Sunday		
9	Monday	3	Planned the week and survey statistics
	Tuesday	4	Thesis writing course
	Wednesday	3	Emails and survey + phone meeting with a municipality
	Thursday	8	Survey work and research
	Friday	5	Meeting with statistics guidence
	Saturday		
Total: 25	Sunday	2	Planned meeting with IKOMM
10	Monday	7	Thesis writing course, meeting with IKOMM + thesis writing
	Tuesday	8	Meeting wtk Indigo IKT, supervisor and thesis work
	Wednesday		
	Thursday	8	Meeting with Oslo, NetSecurity and Bergen
	Friday	5	Meeting with statistics help and thesis work
	Saturday	3	Thesis work
Total: 31	Sunday		
11	Monday	4	Thesis work
	Tuesday	4	Sent out mails and meeting with supervisor
	Wednesday		
	Thursday	8	Thesis work
	Friday	3	Sent out mails
	Saturday		
Total:32	Sunday	3	Thesis work
12	Monday	5	Thesis work
	Tuesday	4	Thesis work and meeting with supervisor
	Wednesday	5	Thesis work
	Thursday	7	Thesis work
	Friday	5	Thesis work
	Saturday	5	Thesis work
Total: 35	Sunday	5	Thesis work
13	Monday	5	Thesis work
	Tuesday	6	Thesis work and supervisor meeting
	Wednesday		
	Thursday	7	Thesis work
	Friday	6	Thesis work
	Saturday		
Total:29	Sunday	5	Thesis work
14	Monday		Easter break
	Tuesday		
	Wednesday		
	Thursday		
	Friday		
	Saturday		
Total:	Sunday		
15	Monday	8	Thesis work
	Tuesday	5	Thesis work
	Wednesday	2	Thesis work
	Thursday	8	Thesis work
	Friday	4	Thesis work
	Saturday	4	Thesis work
Total:31	Sunday		
16	Monday	7	Thesis work
	Tuesday	5	Thesis work and supervisor meeting
	Wednesday		
	Thursday	8	Thesis work
	Friday	6	Thesis work
	Saturday	6	Thesis work
Total:32	Sunday		
17	Monday		
	Tuesday	8	Thesis work and meeting with supervisor
	Wednesday	4	Thesis work
	Thursday	8	Thesis work
	Friday		
	Saturday	7	Thesis work
Total:30	Sunday	3	Thesis work
18	Monday	9	Thesis work
	Tuesday	4	Thesis work and meeting with supervisor
	Wednesday	4	Thesis work
	Thursday	8	Thesis work
	Friday	2	Thesis work
	Saturday	5	Thesis work
Total:35	Sunday	3	Thesis work
19	Monday	7	Thesis work
	Tuesday	2	Meeting with supervisor
	Wednesday	5	Thesis work
	Thursday	8	Thesis work
	Friday	3	Thesis work
	Saturday	8	Thesis work
Total:33	Sunday		
20	Monday	7	Thesis work
	Tuesday	6	Thesis work
	Wednesday		
	Thursday	5	Thesis work
	Friday	8	Thesis work
	Saturday		
Total:	Sunday		

Katrine

Week	Day	No. Hours	Activity
2	Monday	1	Planned meeting with supervisor
	Tuesday	1	Planned meeting with IKOMM
	Wednesday	7	Project plan
	Thursday	5	Project plan
	Friday	4	Project plan
	Saturday		
Total: 18	Sunday		
3	Monday	4	Meeting with IKOMM
	Tuesday	3	Meeting with supervisor + project plan
	Wednesday	4	Project plan
	Thursday	8	Project plan + contact sources
	Friday	3	Research + plan questions for meeting
	Saturday		
Total: 22	Sunday		
4	Monday	4	Impove project plan + presentation for supervisor
	Tuesday	4	Meeting with supervisor + project plan
	Wednesday		
	Thursday	7	Meeting with K-CSIRT + research
	Friday	3	Planned meeting with Mnemonic
	Saturday	4	Reading
Total: 22	Sunday		
5	Monday	3	Reseach
	Tuesday	8	Meeting Mnemonic & supervisor + research
	Wednesday	4	Make outline for thesis
	Thursday	3	Reading
	Friday	3	Make survey + go through intervju answers
	Saturday	4	Make survey
Total: 25	Sunday		
6	Monday	3	Research + plan meeting with IKOMM
	Tuesday		
	Wednesday	4	Research
	Thursday	7	Meeting with IKOMM + emails + research
	Friday	3	Emails + research
	Saturday	4	Research
Total: 23	Sunday	2	Emails + research
7	Monday		
	Tuesday	7	Meeting with supervisor + emails + survey
	Wednesday	2	Emails + survey
	Thursday	4	Reading reports
	Friday	8	Report + reaseach + plan meetings
	Saturday		
Total: 25	Sunday	4	Weekly report + questions for interview
8	Monday	3	Planning
	Tuesday	7	Plan meetings + emails + meet supervisor
	Wednesday	4	Survey + emails
	Thursday	7	Meeting with IKT Fjellregionen + survey + plan
	Friday	7	Meeting with Haugesund + plan question for next
	Saturday		
Total: 32	Sunday		
9	Monday	3	Plan the week + start with statistics
	Tuesday	4	Thisis writing course + update outline
	Wednesday	2	Emails to municipalities/IT
	Thursday	8	Survey + plan questions for meeting + reseach
	Friday	5	Meeting with statistics people + futher discussion
	Saturday		
Total: 25	Sunday	3	Reading + plan meeting with IKOMM
10	Monday	7	Meeting with supervisor (thisis) & IKOMM
	Tuesday	6	Meeting with Indigo IKT + supervisor + thisis
	Wednesday		
	Thursday	8	Meeting with Oslo + NetSecurity + Bergen
	Friday	5	Meeting with statistics people + thisis writing
	Saturday	3	Thisis writing
Total: 32	Sunday		
11	Monday	4	Thisis writing
	Tuesday	3	Emails + survey
	Wednesday		
	Thursday	8	Thisis work
	Friday	4	Emails
	Saturday		
Total: 22	Sunday	3	Thesis work
12	Monday	5	Thisis writing
	Tuesday	4	Thisis writing + meeting with supervisor
	Wednesday	5	Thisis writing
	Thursday	8	Thisis writing
	Friday	5	Thisis writing
	Saturday	5	Thisis writing
Total: 35	Sunday	3	Thisis writing
13	Monday	6	Thisis writing
	Tuesday	5	Thisis writing + meeting with supervisor
	Wednesday		
	Thursday	7	Thisis writing
	Friday	4	Thisis writing
	Saturday	2	Thisis writing
Total: 29	Sunday	5	Thisis writing
14	Monday		EASTER BREAK
	Tuesday		EASTER BREAK
	Wednesday		EASTER BREAK
	Thursday		EASTER BREAK
	Friday		EASTER BREAK
	Saturday		EASTER BREAK
Total:	Sunday		EASTER BREAK
15	Monday	8	Thisis writing
	Tuesday	5	Thisis writing
	Wednesday	2	Thisis writing
	Thursday	8	Thisis writing
	Friday	4	Thisis writing
	Saturday	4	Thisis writing
Total: 31	Sunday		
16	Monday	7	Thisis writing
	Tuesday	5	Thisis writing + meeting with supervisor
	Wednesday		
	Thursday	8	Thisis writing
	Friday	6	Thisis writing
	Saturday		
Total: 32	Sunday	6	Thisis writing
17	Monday		
	Tuesday	8	Thisis writing + meeting with supervisor
	Wednesday	4	Thisis writing
	Thursday	8	Thisis writing
	Friday		
	Saturday	7	Thisis writing
Total: 30	Sunday	3	Thisis writing
18	Monday	6	Thisis writing
	Tuesday	5	Thisis writing + meeting with supervisor
	Wednesday	4	Thisis writing
	Thursday	8	Thisis writing
	Friday	2	Thisis writing
	Saturday	5	Thisis writing
Total: 35	Sunday	3	Thisis writing
19	Monday	7	Thisis writing
	Tuesday	2	Thisis writing + meeting with supervisor
	Wednesday	5	Thisis writing
	Thursday	8	Thisis writing
	Friday	3	Thisis writing
	Saturday	8	Thisis writing
Total: 33	Sunday		
20	Monday	7	Thisis writing
	Tuesday	6	Thisis writing
	Wednesday		
	Thursday	5	Thisis writing
	Friday	8	Thisis writing
	Saturday		
Total:	Sunday		

Nora

Week	Day	No. Hours	Activity
2	Monday	1	Planned meeting with supervisor
	Tuesday	1	Planned meeting with IKOMM
	Wednesday	7	Project plan
	Thursday	5	Project plan
	Friday	4	Project plan
	Saturday		
Total: 18	Sunday		
3	Monday	4	Project plan + meeting with IKOMM
	Tuesday	3	Meeting with supervisor + project plan
	Wednesday	4	Project plan + meeting with IKOMM
	Thursday	8	Finnish project plan + answering emails
	Friday	3	Quetions for meeting + research
	Saturday		
Total: 22	Sunday		
4	Monday	4	Prepared presentation + improve project plan
	Tuesday	4	Meeting with supervisor + improve project plan
	Wednesday	4	Summary from meeting with IKOMM + minutes of meeting
	Thursday	7	Meeting with kommune CSIRT + further planning
	Friday	3	Planned meeting with Mnemonic
	Saturday		
Total: 26	Sunday	4	Individual reading
5	Monday		
	Tuesday	8	Meeting with Mnemonic and supervisor + other research
	Wednesday	4	Make thesis outline
	Thursday		
	Friday	3	Create survey + go through answers from intervju
	Saturday	4	Finnish first draft of survey
Total: 21	Sunday	2	Research
6	Monday	5	Individual reading + planned meeting with IKOMM
	Tuesday		
	Wednesday	3	Research
	Thursday	8	Meeting with IKOMM + sent out survey
	Friday	4	Fixed things regarding survey
	Saturday		
Total: 24	Sunday	4	Email + research
7	Monday	4	Individual reading
	Tuesday	7	Meeting with supervisor + emails + survey
	Wednesday	2	Emails + survey
	Thursday	3	Research
	Friday	8	Report + planned meetings + research
	Saturday		
Total: 24	Sunday		
8	Monday	3	Planning week
	Tuesday	8	Meeting with supervisor + questions + emails
	Wednesday	4	Survey + emails
	Thursday	7	Meeting with IKt-fjellregion + survey
	Friday	7	Meeting with Haugesund + plan questions
	Saturday		
Total: 30	Sunday		
9	Monday	3	Plan the week + start creating statistics
	Tuesday	4	Theesis writing course + update outline
	Wednesday	3	Emails + reading
	Thursday	8	Survey + emails + plan meetings + research
	Friday	5	Statistics meeting
	Saturday		
Total: 25	Sunday	2	Planned meeting with IKOMM
10	Monday	7	Meeting with IKOMM
	Tuesday	6	Meeting with Indigo IKT + supervisor + thesis
	Wednesday		
	Thursday	8	Meeting with Oslo, NetSecurity and Bergen
	Friday	5	Meeting regarding statistics + thesis writing
	Saturday	2	Thesis writing
Total:	Sunday		
11	Monday	4	Thesis work
	Tuesday		
	Wednesday	4	Sent out emails
	Thursday	8	Thesis work
	Friday	3	Thesis work
	Saturday	3	Sent out emails
Total: 22	Sunday		
12	Monday	5	Thesis work
	Tuesday	4	Thesis work
	Wednesday	4	Thesis work
	Thursday	8	Thesis work
	Friday	5	Thesis work
	Saturday	5	Thesis work
Total: 34	Sunday	3	Thesis work
13	Monday	4	Thesis work
	Tuesday	5	Thesis work
	Wednesday		
	Thursday	7	Thesis work + meeting with supervisor
	Friday	5	Thesis work
	Saturday	4	Thesis work
Total: 29	Sunday	4	Thesis work
14	Monday		Easter break
	Tuesday		
	Wednesday		
	Thursday		
	Friday		
	Saturday		
Total: 0	Sunday		
15	Monday	8	Thesis work
	Tuesday	5	Thesis work
	Wednesday	2	Thesis work
	Thursday	8	Thesis work
	Friday	4	Thesis work
	Saturday	4	Thesis work
Total: 31	Sunday		
16	Monday	7	Thesis work
	Tuesday	5	Thesis work + meeting with supervisor
	Wednesday		
	Thursday	8	Thesis work
	Friday	6	Thesis work
	Saturday		
Total: 32	Sunday	6	Thesis work
17	Monday		
	Tuesday	8	Thesis work
	Wednesday	4	Thesis work
	Thursday	8	Thesis work
	Friday		
	Saturday	7	Thesis work
Total: 30	Sunday	3	Thesis work
18	Monday	9	Thesis work
	Tuesday	4	Thesis work + meeting with supervisor
	Wednesday	4	Thesis work
	Thursday	8	Thesis work
	Friday	2	Thesis work
	Saturday	5	Thesis work
Total: 35	Sunday	3	Thesis work
19	Monday	7	Thesis work
	Tuesday	2	Thesis work + meeting with supervisor
	Wednesday	5	Thesis work
	Thursday	8	Thesis work
	Friday	3	Thesis work
	Saturday	8	Thesis work
Total: 33	Sunday		
20	Monday	7	Thesis work
	Tuesday	6	Thesis work
	Wednesday		
	Thursday	5	Thesis work
	Friday	8	Thesis work
	Saturday		
Total: 26	Sunday		

Appendix F

Week Status Report

Week 3 status report

Week of writing the report:

We have not started on the report yet, only the project plan. But we have made it ready in Overleaf, as we are going to be using LaTeX for it.

What you have done in the previous week:

- We have finished the first draft of our project plan.
- Have made contact with two external sources and have planned a meeting with them on 26th and 31st of January. Also made questions ready for the meeting on the 26th. We have also contacted others and are waiting for a response.
- We had a meeting with our employer where we got more information about the task and what they are expecting out of it.
- Fixed times for meetings with the group on campus.

Do you encounter any problems, how did you solve them:

Find time to work together, as we didn't have any fixed times in the beginning, we found it hard to meet as we just asked randomly to meet. But during last week we decided that we are all going to meet on campus on Mondays and Thursdays to work together, and continue having a meeting online after the meeting with our supervisor on Tuesdays.

What do you want to discuss in this meeting:

- Project plan

What are you going you do in this week:

- We are going to have interviews with one from CIRST.
- If the project plan needs any changes, we will do these and finish it.

Is your group still on track according to your Gantt chart:

We are on track, ahead in the project plan if we get this approved.

Week 4 status report

Week of writing the report:

We have not started on the report yet, but we have started to think about what type of recommendations we would make and grouped them into different categories.

What you have done in the previous week:

- We have fixed and implemented the changes to our project plan that our supervisor had pointed out to us.
- Had a meeting with Kommune-CSIRT and sent him questions on email.
- Made the questions for the meeting 31st with Mnemonic.
- Read a lot of reports and documents that were handed to us by IKOMM.
- Talked with NTNU´s SOC.

Do you encounter any problems, how did you solve them:

Some of the documents were a bit difficult to read as you would need a good understanding of how CERT, CSIRT, SOC, IRT, ISAC, laws, organization and administration of the municipality works to make use of the information. To solve this, we talked with the SOC at NTNU who is a member of Uninett-CERT and the meeting with Kommune-CSIRT helped a lot as well.

What do you want to discuss in this meeting:

- The plan moving forward.

What are you going you do in this week:

- We are going to have a meeting with Mnemonic.
- Make questions for the different surveys we are planning to conduct.
- Get in contact with multiple municipalities.

Is your group still on track according to your Gantt chart:

We are on track according to our Gantt chart.

Week 5 status report

Week of writing the report:

We have started on making the outline of the report.

What you have done in the previous week:

- Had a meeting with Mnemonic
- Made questions for the survey
- Planned a meeting with IKOMM

Do you encounter any problems, how did you solve them:

The laws and regulations regarding data collection were unclear. We asked our supervisor.

What do you want to discuss in this meeting:

- Look at the current outline of the report
- Plan for interviews and status
- Talk about the survey and any regulations/laws for data collection

What are you going you do in this week:

- We are going to have a meeting with IKOMM.
- Send out the survey to many municipalities.
- Look over interview notes

Is your group still on track according to your Gantt chart:

We are on track according to our Gantt chart.

Week 6 status report

Week of writing the report:

We have started on making the outline of the report.

What you have done in the previous week:

- Had a meeting with IKOMM to show them the surveys and ask some clarifying questions.
- Sent surveys to municipalities

Do you encounter any problems, how did you solve them:

We were a bit unsure about the regulations and laws regarding surveys, with collecting and storing personal data, and interviews. To solve this, we talked with our supervisor and looked at NTNUs own documentation about the matter. In addition, we removed any questions that could be characterized as personal data. We also asked all the people we interviewed if it was okey for us to refer to our conversation in the thesis.

Due to lack of response from our surveys, we decided to change the wording of the email and change the survey platform from Google forms to nettskjema.

What do you want to discuss in this meeting:

- Look at the current outline of the report
- Plan for interviews and status

What are you going you do in this week:

- Send out the survey to more municipalities
- Get in contact with the IT people we were recommended to speak with from KINS.

Is your group still on track according to your Gantt chart:

We are on track according to our Gantt chart.

Week 7 status report

Week of writing the report:

We have started on making the outline of the report and got some feedback from our supervisor to improve this. Have started coming up with key points for what we are going to write about in each section.

What you have done in the previous week:

- Planned meetings with two people/municipalities for next week and one for March 7th
- Read some reports that are relevant for our thesis (MITRE, Digdir, Norsis etc)

Do you encounter any problems, how did you solve them:

It was difficult to keep track of all the municipalities that we had sent the survey to, as we just had them in tables in a word document at first. But we found out we needed a better solution, so we made an excel document that had all of them in with their information and their status if they have replied or denied.

What do you want to discuss in this meeting:

- Look at the current outline of the report (what we didn't have time for last meeting)
- When we are going to have the meeting about how to write a report

What are you going you do in this week:

- Continue with our report and try to see if we can come up with more recommendations, and what we need to ask about.
- Futher plan our questions and topics to cover in our interviews on Thursday and Friday.
- Go roughly through the answers we have got from the surveys so far, to get more knowledge about the competence in municipalities.

Is your group still on track according to your Gantt chart:

We are on track according to our Gantt chart.

Week 8 status report

Week of writing the report:

We have not done anything further regarding the writing of the report, but we have made a few more requirements that will be a part of the report.

What you have done in the previous week:

- Sent out the survey to all the municipalities in Norway including the IT-departments/responsible/collaborations.
- Had a meeting with IKT-Fjellregionen
- Had a meeting with the Haugesund's IT-responsible

Do you encounter any problems, how did you solve them:

For some of the municipalities it was very difficult to find the contact information for the IT department. If someone were not able to find the information, we helped each other by trying to find the email address for each other's municipalities. If we were unsuccessful some of the people were contacted through LinkedIn. It was also a bit challenging to keep track, when multiple municipalities had a shared IT collaboration. To make it easier for us we decided to color code which municipalities were a port of the same IT collaboration.

What are you going you do in this week:

- Plan questions for the meeting we are having 07.03 with Hedmark IKT
- Writing the thesis background
- Start to go through the survey answers we have received so far

Is your group still on track according to your Gantt chart:

We are on track according to our Gantt chart.

Week 9 status report

Week of writing the report:

We have not done anything further regarding the writing of the report.

What you have done in the previous week:

- Decided on how we wanted to present the results from the survey
- Meeting with Janne, Thea and Ingrid to get some help with how to visualize the results from the surveys in bar charts
- Planned a meeting with NetSecurity and IKOMM

Do you encounter any problems, how did you solve them:

We were not sure how to make the statistics for the surveys, so we asked for help.

What do you want to discuss in this meeting:

We want to discuss whether our timesheets are well organized or not.

What are you going you do in this week:

- Plan for the meetings we are having 06.03 with IKOMM, 07.03 with Hedmark IKT, and 09.03 with NetSecurity
- Writing the thesis background
- Start to go through the survey answers we have received so far

Is your group still on track according to your Gantt chart:

We are on track according to our Gantt chart.

Week 10 status report

Week of writing the report:

We have started writing on the preface, introduction and background

What you have done in the previous week:

- Meeting with IKOMM where we asked them the questions we have asked all other IT-personnel. They also helped us gather more answers for our surveys.
- Meeting with Indigo IKT where we discussed challenges with implementing a SOC for a municipality
- Meeting with Oslo municipality about our survey and we also asked him some questions about their SOC
- Meeting with Netsecurity about their SOC service
- Meeting with Bergen municipality
- Meeting with Janne, Thea and Ingrid where they showed us the Python code for visualizing the results from our municipality survey.

Do you encounter any problems, how did you solve them:

In some of the meetings we felt a bit overwhelmed, since some of them introduced new topics we had not thought of, and therefore we got a bit discouraged after those meetings. To regain motivation, we reflected and discussed within the group and remembered what our scope is. We have also talked with a lot of people that are very engaging and positive about our project, which helped as well.

What are you going you do in this week:

- Try to come in contact with and plan a meeting with Defendable
- Continue writing the thesis preface, introduction and background
- Make the statistics for the IT survey

Is your group still on track according to your Gantt chart:

We are on track according to our Gantt chart.

Week 11 status report

Week of writing the report:

We have continued writing the preface, introduction and background.

What you have done in the previous week:

- Sent out the survey to some more potential participants
- Written some more on the report
- Worked on creating the statistics (Jupyter python code) for both of our surveys.
- Sent email to Defendable regarding meeting

Do you encounter any problems, how did you solve them:

We felt that we didn't have enough answers from big municipalities (over 50 000 residents) on our survey for general employees in municipalities. To solve this, we tried to send out the survey to more potential participants, in hope that some more people will take the time to answer. We also struggled a bit with the code for creating the statistics for our surveys. To solve this, we tried searching for solutions on the internet and asked for help from the girls that helped us create the statistics code.

What do you want to discuss in this meeting:

We want to know if we have to include the code for the statistics in our report.

What are you going you do in this week:

- Continue writing the report
- Finish the python code for both our surveys
- Maybe contact more SOC companies for meeting.

Is your group still on track according to your Gantt chart:

We are on track according to our Gantt chart.

Week 12 status report

Week of writing the report:

We have finished writing the introduction and background. Related work and methodology are also close to done.

What you have done in the previous week:

- Sent out the survey to some more potential participants
- Written and proofread introduction, background, related work and methodology
- Sent email to NetSecurity with some questions about the services they provide
- Sent the IT survey to the IKT Hedmark municipalities

Do you encounter any problems, how did you solve them:

We started feeling a bit stressed and overwhelmed because of the workload and everything that needed to be done by the end of March. To deal with this we made a shared calendar containing that day's agenda, so we had a specific plan. We also encountered some questions regarding the thesis structure and content, that was solved by sending a message to the Teams chat.

What do you want to discuss in this meeting:

- We want to know if we have to include the code for the statistics in our report.
- Should the description of Ikomm be under preface?
- Do we need to mention all tools we have used (JupyterNotebook, Drawio)? And where?

What are you going you do in this week:

- Finish methodology and related work
- Start analyzing our findings and start writing on the *Analysis Results*

Is your group still on track according to your Gantt chart:

We are on track according to our Gantt chart.

Week 17 status report

Week of writing the report:

We have worked mostly on the analysis and recommendations this week.

What you have done in the previous week:

- Recommendations about finished, sent these to Ikomm for feedback
- Analysis about finished, ready for feedback

Do you encounter any problems, how did you solve them:

There were a lot of statistics from the surveys to go through, so we needed to find the most effective way to do so. We decided to do this together, and then we divided the pictures we chose to keep between us and wrote about these.

What do you want to discuss in this meeting:

- Your thoughts on our thesis so far
- How to reference surey quesiton/interviews X
- How to reference NSM basic prinicples

What are you going to do in this week:

- Send the report to Bergen municipality, netsecurity and Ikomm for feedback.
- Start on discussion
- Transfer the thesis to latex

Is your group still on track according to your Gantt chart:

We are on track according to our Gantt chart.

Week 18 status report

Week of writing the report:

We have worked on feedback and discussion.

What you have done in the previous week:

- Feedback
- Discussion

Do you encounter any problems, how did you solve them:

We did not understand all the feedback, so we had to ask some follow up questions.

What do you want to discuss in this meeting:

- Small NSM measures
- Terminology in feedback
- Find a better word than purpose

What are you going to do in this week:

- Finish discussion and feedback comments
- Start on conclusion and summary
- Transfer the thesis to latex

Is your group still on track according to your Gantt chart:

We are on track according to our Gantt chart.

Week 19 status report

Week of writing the report:

We have worked on feedback, discussion and conclusion

What you have done in the previous week:

- Feedback
- Discussion
- Conclusion

Do you encounter any problems, how did you solve them:

We encountered some problems with layout in tables in latex. We managed to fix this after trying out different solutions.

What do you want to discuss in this meeting:

- Latex

What are you going to do in this week:

- Finish discussion and feedback comments
- Finish conclusion and summary
- Proofread the entire thesis

Is your group still on track according to your Gantt chart:

We are on track according to our Gantt chart.

Appendix G

Minutes of Meeting

Minutes of meeting with IKOMM

Date: 16.01.23

Time: 13:00 – 14:00

Location: Microsoft Teams

Participants: Ronny Olsen, Sigurd Biørn and all team members

Agenda

Case	What was discussed/done
Contracts	• Sign and deliver confidentiality agreement and standard agreement
About IKOMM	• Their history and what services they provide
Project background and goals	• Got more information and clarity about the task • What they want to achieve with the project
Scope	• Thoughts about how we limited the task description
Documents	• Received documentation about IKOMM and our task
Other questions and topics	• Got recommended people to contact

What is planned for later

- Contact the resources that IKOMM recommended and set up potential meeting
- Read through documents we received

Minutes of meeting with supervisor

Date: 17.01.23

Time: 14:30 – 15:10

Location: Microsoft Teams

Participants: Jia-Chun Lin and all team members

Agenda

Case	What was discussed/done
Intro	• Introduction and information about the start of the bachelor thesis
Project plan	• Information about the project plan
Other information	• To-do and to-know list

What is planned for later

- Finish the project plan
- Create presentation
- Write and send status report
- Come up with a grade we want to aim for

Minutes of meeting with supervisor

Date: 24.01.23

Time: 14:30 – 15:15

Location: Microsoft Teams

Participants: Jia-Chun Lin and all team members

Agenda

Case	What was discussed/done
Project plan	• Went through the first draft of the project plan together and discussed improvements

What is planned for later

- Implement the discussed improvements
- Send the improved project plan and get it approved
- Write and send status report

Minutes of meeting with Kommune-CSIRT

Date: 26.01.23

Time: 17:00 – 18:00

Location: Microsoft Teams

Participants: Bjørn Tveiten and all team members

Agenda

Case	What was discussed/done
About Kommune-CSIRT	• What they do and the background for why they were established
Communication	• How and what they communicate with their members
Service	• What services they provide and why aren't there more municipalities that are members of the CSIRT
Challenges	• What his perception of the information security competence in the municipalities are • Challenges of having multiple CSIRT´s
Other topics	• Got information on relevant people to talk to

What is planned for later

- Send the questions on mail
[redacted]
[redacted]

Minutes of meeting with Mnemonic

Date: 31.01.23

Time: 09:00 – 10:00

Location: Mnemonic communication service

Participants: Bjørnar Prestaasen and all team members

Agenda

Case	What was discussed/done
About Mnemonic	• General information about the company
Information about their service/SOC	• Questions regarding Mnemonic's SOC service • What type of clients they have • Incident response • Common incidents
Communication	• Information about the communication between Mnemonic and their clients • What platforms they use
Division of responsibility	• Questions about the responsibilities that Mnemonic have, and their client
Challenges	• Municipality SOC • The clients information security competence • How to deal with communication problems if they occur

What is planned for later

- Possible to ask more questions if we need later

Minutes of meeting with supervisor

Date: 31.01.23

Time: 14:30 – 15:00

Location: Microsoft Teams

Participants: Jia-Chun Lin and all team members

Agenda

Case	What was discussed/done
How to conduct an interview properly	• Laws and regulations when interviewing third parties
About our surveys	• Find relevant questions to ask in the survey

What is planned for later

- Show our survey questions to IKOMM.
- Plan on who we are going to interview, what we are going to ask and how to conduct them.

Minutes of meeting with IKOMM

Date: 09.02.23

Time: 10:00 – 11:00

Location: Microsoft Teams

Participants: Sigurd Biørn and all team members

Agenda

Case	What was discussed/done
Survey questions for municipalities	• We wanted input on the questions we had made for the municipalities, and ask if they had any questions we could add
Other questions regarding the thesis task	• We had some general questions about our task, and we got the answers we wanted
Progress report	• Updated them on how we were doing

What is planned for later

- Send out the survey to municipalities
- Wait for response

Minutes of meeting with supervisor

Date: 14.02.23

Time: 14:30 – 15:10

Location: Microsoft Teams

Participants: Jia-Chun Lin and all team members

Agenda

Case	What was discussed/done
Weekly report	• Went through our weekly report and commented on some parts
Key contacts	• Went through who we have contacted so far and which municipalities we have sent the surveys to.
Thesis outline	• Went over our first draft of the thesis outline • Made some changes and improvements

What is planned for later

- Find time for meeting with all groups and supervisor

Minutes of meeting with supervisor

Date: 21.02.23

Time: 14:30 – 14:55

Location: Microsoft Teams

Participants: Jia-Chun Lin and all team members

Agenda

Case	What was discussed/done
Survey	• Talked about the surveys and our plan for collecting and analyzing the result
Thesis outline	• Finished going over our first draft of the thesis outline • Made some changes and improvements
Thesis title	• Showed our ideas for the thesis title and agreed on which one to choose

What is planned for later

- Come up with questions for scheduled meetings
- [redacted]

Minutes of meeting with IKT Fjellregionen

Date: 23.02.23

Time: 14:00 – 15:00

Location: Microsoft Teams

Participants: Sverre Jenssen and all team members

Agenda

Case	What was discussed/done
Introduction	• Talked about our thesis and our background • He told us about his background and his role at IKT-Fjellregionen
Interview	We had prepared some questions regarding IKT Fjellregionen: • General about their organization • Their collaborations • Communication • Competence for IT department and generally in the municipalities • Their view on a SOC service
Follow up questions	• Questions we had that we did not prepare in advance
Survey and consent	• Asked if he could answer our IT survey and if we could use the information we had gotten in the interview in our thesis.

What is planned for later

- Send the IT- survey to him
- Contact him if we want to go more in depth regarding what was discussed (non disclosure agreement)

Minutes of meeting with Haugesund municipality

Date: 24.02.23

Time: 09**:**00 – 10:00

Location: Microsoft Teams

Participants: Eirik Østensjø and all team members

Agenda

Case	What was discussed/done
Introduction	• Talked about our thesis and our background • He told us about his background and his role at Haugesund municipality
Interview	We had prepared some questions regarding Haugesund: • General about their municipality • Their collaborations • How their SOC service works • Competence for IT department and generally in the municipalities • About their cyberattack that happened in fall 2022
Follow up questions	• Questions we had that we did not prepare in advance
Survey and consent	• Asked if he could answer our IT survey and if we could use the information we had gotten in the interview in our thesis.

What is planned for later

- Send the IT- survey to him
- Get their revision report and documents regarding their security

Minutes of meeting with NTNU (department of Mathematical Sciences)

Date: 03.03.23

Time: 09:00 – 09:30

Location: Microsoft Teams

Participants: Janne Cathrin Hetle Aspheim, Thea Lovise Leikvoll Fagerli, Ingrid Langevei Mæland and all team members

Agenda

Case	What was discussed/done
Introduction	• Described our task and why we have decided on using the surveys
Survey	• Showed them our survey so far, and what thoughts we had on making the charts
Further plans	• We sent them our raw data, so that they can make the code for us to use in jupyter

What is planned for later

- Send them the data in our Excel spreadsheet and a more in-depth description of what we wanted the bar chart to look like

Minutes of meeting with IKOMM

Date: 06.03.23

Time: 13:00 – 13:45

Location: Microsoft Teams

Participants: Ronny Olsen, Sigurd Biørn, Per Øyvind Vold and all team members

Agenda

Case	What was discussed/done
Survey	• Showed them the survey results and discussed how we could get more answers
Questions	• Asked them the questions we have asked IT-personnel in previous meetings
Further plans	• Agreed that we post our survey on a Facebook IT group, and for IKOMM to post on Kins.no and other sites.

What is planned for later

- Send Ronny the links to our surveys so he can forward them to relevant people

Minutes of meeting with Indigo IKT

Date: 06.03.23

Time: 12:00 – 13:00

Location: Microsoft Teams

Participants: Håvard Helland and all team members

Agenda

Case	What was discussed/done
Introduction	Introduction about ourselves and the task, then he introduced himself and his role.
Questions	We had prepared some questions regarding Indigo IKT: • General about their municipality collaboration • Competence for IT department and generally in the municipalities • A possible municipality-SOC • Challenges • Discussed moving everything to the cloud
Survey and consent	Told him about our survey's, and if we could use the information he gave us in our thesis

What is planned for later

- Send survey for IT-personnel to all of Indigo IKT' clients

Minutes of meeting with [redacted]

Date: 09.03.23

Time: 11:00 – 11:45

Location: Microsoft Teams

Participants: [redacted] and all team members

Agenda

Case	What was discussed/done
Introduction	• Introduction about ourselves and our task, then he introduced himself and his role [redacted]
Survey	• He had some questions regarding the relevance of our survey, so we talked about how and what we wanted to do with the result
Questions about their SOC	• What competence does the SOC need and have in order to do their job • Difficulties with implementing a SOC for a municipality and is this preferable • How they are organized and communicate with their users

What is planned for later

- Send the IT-survey

Minutes of meeting with NetSecurity

Date: 09.03.23

Time: 13:00 – 14:00

Location: Microsoft Teams

Participants: Frank Kirkeng and all team members

Agenda

Case	What was discussed/done
Introduction	• Introduction about ourselves and our task, then about himself
About NetSecurity	• General information about the company
Information about their service/SOC	• Questions regarding NetSecurity's SOC service • Needed competence from clients • Incident response
Communication	• Information about the communication between NetSecurity and their clients • What platforms they use
Division of responsibility	• Questions about the responsibilities that NetSecurity have, and their client
Challenges	• Municipality SOC • The users information security competence • How to deal with communication problems if they occur

What is planned for later

- Send him the report when we are done
- Send follow-up questions if we have some

Minutes of meeting with Bergen municipality

Date: 09.03.23

Time: 14:30 – 15:00

Location: Microsoft Teams

Participants: Andrè Granli and all team members

Agenda

Case	What was discussed/done
Introduction	• Introduction about ourselves and our task, then he introduced himself and about Bergen
Questions	• [redacted] • Internal vs external SOC • Competence
Further	• Agreed to send him our survey and keep in touch if we need any more answers.

What is planned for later

- Send him our survey
- Send him our thesis before we hand it in, so he can read it.

Minutes of meeting with NTNU (department of Mathematical Sciences)

Date: 10.03.23

Time: 14:30 – 15:00

Location: Microsoft Teams

Participants: Janne Cathrin Hetle Aspheim, Thea Lovise Leikvoll Fagerli, Ingrid Langevei Mæland and all team members

Agenda

Case	What was discussed/done
Statistics	• Went through the code and showed us how they had made the statistics
Further	• We will look over the code and try to make our own for the second survey

What is planned for later

- Send email if we need any help with making the second one

Minutes of meeting with supervisor

Date: 21.03.23

Time: 14:30 – 15.05

Location: Microsoft Teams

Participants: Jia-Chun Lin and all team members

Agenda

Case	What was discussed/done
Questions	• About appendix, footnotes and some words to use in the thesis
Statistics	• Went through the code and showed how we have the statistics
Thesis	• What we have done so far with the thesis and what we plan to have finished before delivering the first draft (10th April)

What is planned for later

- Write in the thesis until the first draft (10th April)

Minutes of meeting with supervisor

Date: 28.03.23

Time: 14:30 – 14.40

Location: Microsoft Teams

Participants: Jia-Chun Lin and all team members

Agenda

Case	What was discussed/done
Questions	• About thesis structure
Tools	• Showed the tools we had used and asked if we needed to include them in the thesis

What is planned for later

- Write in the thesis until the first draft (10th April)
- Finish methodology and related work
- Start analyzing our findings and start writing on the *Analysis Results*

Minutes of meeting with supervisor

Date: 18.04.23

Time: 14:30 – 14.40

Location: Microsoft Teams

Participants: Jia-Chun Lin and all team members

Agenda

Case	What was discussed/done
First draft feedback	• Went through all comments supervisor had
Other questions	• How to reference organizations/services

What is planned for later

- Continue writing on analysis and recommendations chapters

Minutes of meeting with supervisor

Date: 25.04.23

Time: 14:30 – 14.45

Location: Microsoft Teams

Participants: Jia-Chun Lin and all team members

Agenda

Case	What was discussed/done
Questions	• Titles, introductions to chapters, feedback

What is planned for later

- Continue writing

Minutes of meeting with supervisor

Date: 02.05.23

Time: 14:30 – 15.30

Location: Microsoft Teams

Participants: Jia-Chun Lin and all team members

Agenda

Case	What was discussed/done
Go over feedback	• Went through some more comments supervisor had, that we didn't understand
Tables	• How to best show the results from interviews in tables
Other questions	• Hierarchy with titles

What is planned for later

- Continue writing

Minutes of meeting with supervisor

Date: 09.05.23

Time: 14:30 – 14.50

Location: Microsoft Teams

Participants: Jia-Chun Lin and all team members

Agenda

Case	What was discussed/done
Other questions	• How to reference the small NSM principles • Feedback we got from others

What is planned for later

- Finish and deliver final report

Appendix H

Municipality Survey

Nettskjema

Spørreundersøkelse for kommuneansatte

Hvilken beskrivelse passer best for din kommune?

- Under 10 000 innbyggere
- Mellom 10 000 - 20 000 innbyggere
- Mellom 20 000 – 50 000 innbyggere
- Mer enn 50 000 innbyggere
- Ønsker ikke svare

Hvor mange av disse begrepene er du kjent med?

- Informasjonssikkerhet
- NSMs grunnprinsipper
- Adgangskontroll
- VPN
- To-faktor autorisering
- Kryptering
- Brannmur
- Phishing
- Virus
- Social engineering

Har du noen gang hatt problem med en datamaskin eller annet IT-system? Hvordan ble problemet løst?

- Ja, gikk til IT-avdeling/-ansvarlig)
- Ja, løste det selv
- Ja, spurte en kollega
- Ja, annet
- Nei
- Ønsker ikke svare

Har du noen gang bedt om hjelp fra IT- avdeling/-ansvarlig?

- Mer enn 5 ganger
- 3-4 ganger per år
- 1-2 gang(er) per år
- Aldri
- Ønsker ikke svare

Har du fått noen opplæring om sikkerhetskultur?

(Hvilke linker man ikke skal trykke på, bruk av sterkt passord og lignende)

- Ja, flere ganger
- Ja, én gang
- Nei
- Ønsker ikke svare

Nettskjema

Har du deltatt på sikkerhetskurs?
(Hvor dere går gjennom grunnleggende forståelse for hvordan beskytte data og IT systemer mot trusler og sikkerhetsbrudd)

- Ja, flere ganger
- Ja, én gang
- Nei
- Ønsker ikke svare

Har dere noen protokoll dere må følge om det skjer en sikkerhetshendelse?
(Datainnbrudd, hacking, virus, malware, uautorisert tilgang, data-tap og lignende)

- Ja, jeg er kjent med denne
- Ja, men jeg er ikke kjent med den
- Nei
- Vet ikke
- Ønsker ikke svare

Har dere noe kommunikasjonskanal/forum hvor dere kan diskutere sikkerhetsrelaterte hendelser?

- Ja, vi har en aktiv kanal
- Ja, men bruker den aldri
- Nei, men skulle ønske det
- Nei
- Vet ikke
- Ønsker ikke svare

Har dere noen form for kommunikasjonskanal/verktøy hvor dere kan melde inn et sikkerhetsbrudd?

- Ja, vi har en fast kanal
- Nei, vi melder direkte til IT ansvarlig
- Nei
- Vet ikke
- Ønsker ikke svare

Har du noen gang vært gjennom/opplevd et cyberangrep?
(Datainnbrudd, hacking, virus, malware, uautorisert tilgang, data-tap og lignende)

- Ja, flere ganger
- Ja, én gang
- Nei, aldri
- Vet ikke
- Ønsker ikke svare

Har du noen gang fått en phishing mail?
(En mail som ser ut som den kommer fra en pålitelig kilde som banken, posten, Telenor eller politiet som ber om personlige opplysninger som brukernavn/passord eller bank informasjon)

- Ja, jeg klikket på linken og ga informasjonen de var ute etter

Ja, jeg klikket på linken, men skjønte da at noe var galt
Ja, jeg lot meg ikke lure og meldte det inn
Ja, jeg lot meg ikke lure men meldte det ikke inn
Nei
Vet ikke
Ønsker ikke svare

Har du noe rutine på å oppdatere mobil, nettleser (Chrome, Safari, Firefox) og programmer/applikasjoner?

Ja, har på automatisk oppdatering
Ja, hver gang jeg får varsel
Nei, men gjør det når jeg får beskjed
Nei, gjør det ikke før jeg må
Vet ikke
Ønsker ikke svare

Fra 1-5 hvor kritisk er du til å laste ned programmer/pdf-er/dokumenter?

1 - Tenker aldri over det
2
3
4
5 - Laster kun ned om det kommer fra en anerkjent kilde

Når tok du sist backup av din pc/mobil?

Har på automatisk
Gjør det hver gang en oppdatering kommer
1 år siden
Mer enn 1 år
Vet ikke
Ønsker ikke svare

Ble du noe mer bevisst på informasjonssikkerhet etter denne undersøkelsen?

Ja, her var det litt jeg ikke kunne fra før
Nei, men fint med en oppfriskning
Nei, dette var jeg klar over fra før
Vet ikke
Ønsker ikke svare

Appendix I

IT Personnel Survey

Nettskjema

Spørreundersøkelse til IT-personell i kommuner

Hvilken beskrivelse passer best for din kommune?

- Under 10 000 innbyggere
- Mellom 10 000 – 20 000 innbyggere
- Mellom 20 000 – 50 000 innbyggere
- Mer enn 50 000 innbyggere
- Ønsker ikke svare

Hvordan er deres IT avdeling satt opp?

- Har en person som er IT-ansvarlig, men ingen egen IT-avdeling
- Har en felles IT-avdeling for alle sektorer
- Har en IT-avdeling for hver sektor
- Ønsker ikke svare

Har dere en formelt utnevnt person som er fagansvarlig for informasjonssikkerhet?

- Ja
- Nei
- Vet ikke
- Ønsker ikke svare

Er dere med i K-CSIRT?

- Ja, er veldig fornøyd med de
- Ja, men bruker dem ikke så mye
- Nei, vet ikke hva det er
- Nei, valgt å ikke være med
- Ønsker ikke svare

Har dere gjennomført en sårbarhetskartlegging?

(Nessus-scan, shodan)

- Ja
- Nei
- Vet ikke
- Ønsker ikke svare

Gjennomfører dere en sårbarhetskartlegging periodisk?

- Ja, flere ganger i året
- Ja, én gang i året
- Ja, sjeldnere enn én gang i året
- Nei
- Vet ikke
- Ønsker ikke svare

Har dere gjennomført en risiko-sårbarhetsanalyse?

- Ja
- Nei
- Vet ikke
- Ønsker ikke svare

Gjennomfører dere en risiko-sårbarhetsanalyse periodisk?

- Ja, flere ganger i året
- Ja, én gang i året
- Ja, sjeldnere enn én gang i året
- Nei
- Vet ikke
- Ønsker ikke svare

Har dere gjennomført en penetrasjonstest?

- Ja
- Nei
- Vet ikke
- Ønsker ikke svare

Gjennomfører dere en penetrasjonstest periodisk?

- Ja, flere ganger i året
- Ja, én gang i året
- Ja, sjeldnere enn én gang i året
- Nei
- Vet ikke
- Ønsker ikke svare

Har dere en plan for håndtering av informasjonssikkerhetshendelser (IRT)?

- Ja, bruker denne aktivt
- Ja, men denne blir lite brukt i praksis
- Nei, jeg håndterer det som det kommer
- Vet ikke
- Ønsker ikke svare

Har dere en beredskapsplan for informasjonssikkerhetshendelser?

- Ja, vi lagde den selv
- Ja, vi har en, men lagde den ikke selv
- Nei
- Vet ikke
- Ønsker ikke svare

Holdes beredskapsplanen vedlike?

- Ja, gjennomgår denne regelmessig
- Ja, men vi har ingen rutine på gjennomgang

Nei
Vet ikke
Ønsker ikke svare

Har dere styrende dokumenter som fungerer som en veileder for IT-sikkerhet?

Ja, de blir fulgt
Ja, men de blir ikke brukt
Nei
Vet ikke
Ønsker ikke svare

Har dere brukt ovelse.no? (DSB)

(Øvelsene utvikles som diskusjonsøvelser, og det gis en enkel veileder for evaluering av egne øvelser)

Ja, flere ganger i året
Ja, én gang i året
Ja, sjeldnere enn en gang i året
Nei
Ønsker ikke svare

Har dere årlige sikkerhetskurs?

Ja
Nei
Vet ikke
Ønsker ikke svare

Har dere vært i kontakt med NSM og var de lett å komme i kontakt med?

Ja, de var lett å få tak i
Ja, men de var vanskelige å få tak i
Nei, tok kontakt med noen andre
Nei, har ikke hatt behov
Vet ikke
Ønsker ikke svare

Har dere noe kommunikasjonskanal/forum hvor alle kommune-ansatte kan diskutere sikkerhetsrelaterte emner?

Ja, denne blir aktivt brukt
Ja, men den blir ikke brukt
Nei
Vet ikke
Ønsker ikke svare

Har dere noen form for kommunikasjonskanal/verktøy kommune-ansatte kan melde inn sikkerhetshendelser?

Ja, det blir mye brukt (< 80% av hendelsene blir rapportert)

Ja, det blir brukt (50% av hendelsene blir rapportert)
Ja, det blir lite brukt (> 30% av hendelsene blir rapportert)
Ja, men vet ikke prosentandelen på hvor mange av hendelsene som faktisk blir rapportert
Nei, ikke et eget program som kun brukes for innmelding av sikkerhetshendelse
Nei
Vet ikke
Ønsker ikke svare

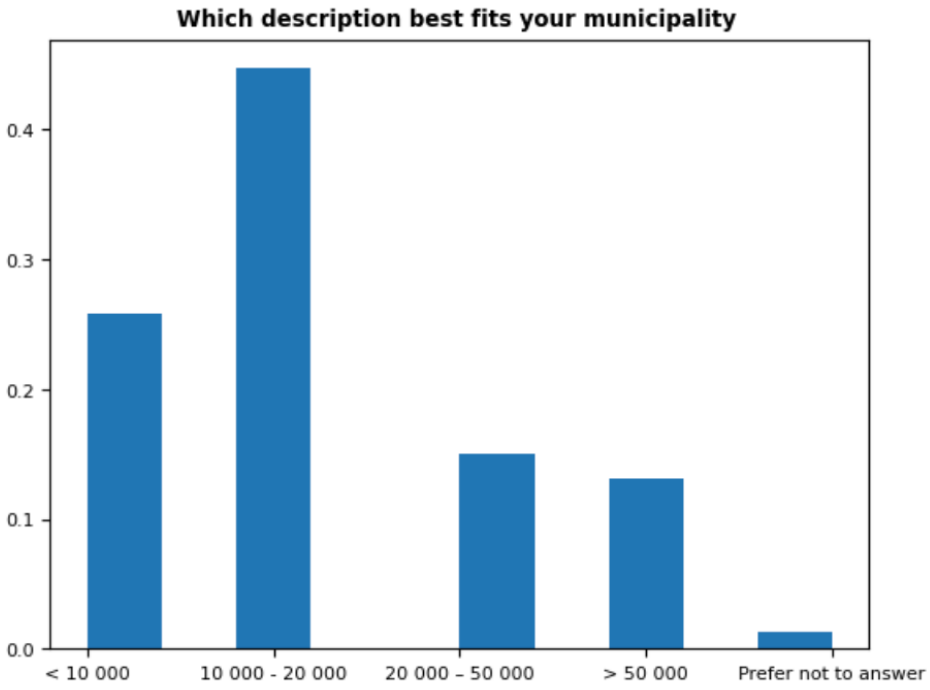
Kryss av for hvilke av disse som gjelder for din kommunes IT-samarbeid med andre kommuner

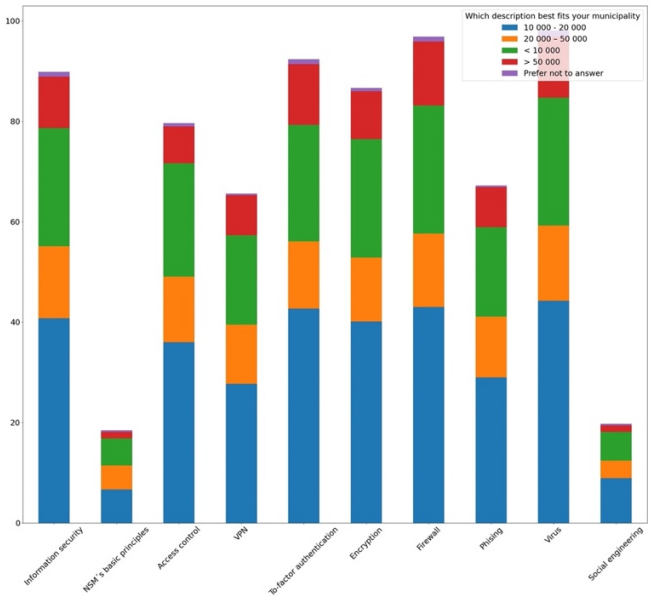
Vi har felles IT ansvarlige
Vi har en felles kommunikasjonskanal
Vi er medlem av Kins
Vi er medlem av K-CSIRT
Vi har avtaler dersom det skulle være behov
Vi gjøre mesteparten selv
Ingen
Vet ikke
Ønsker ikke svare

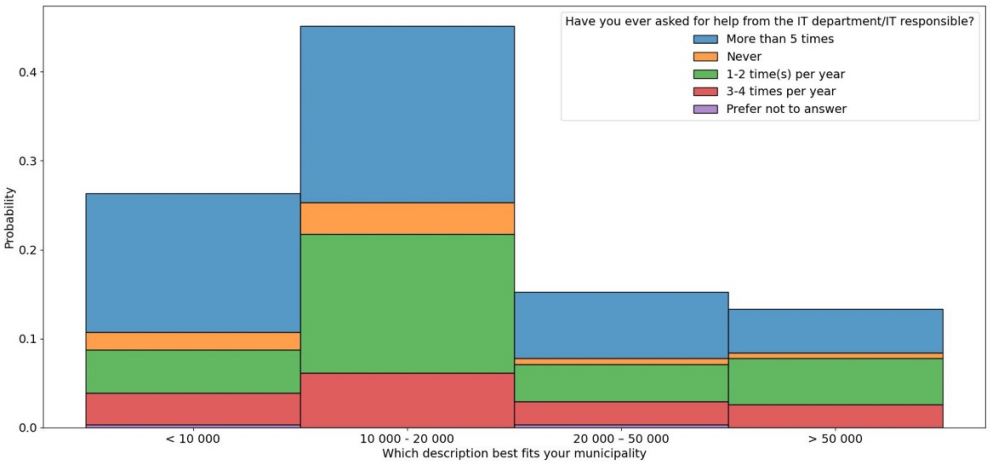
Appendix J

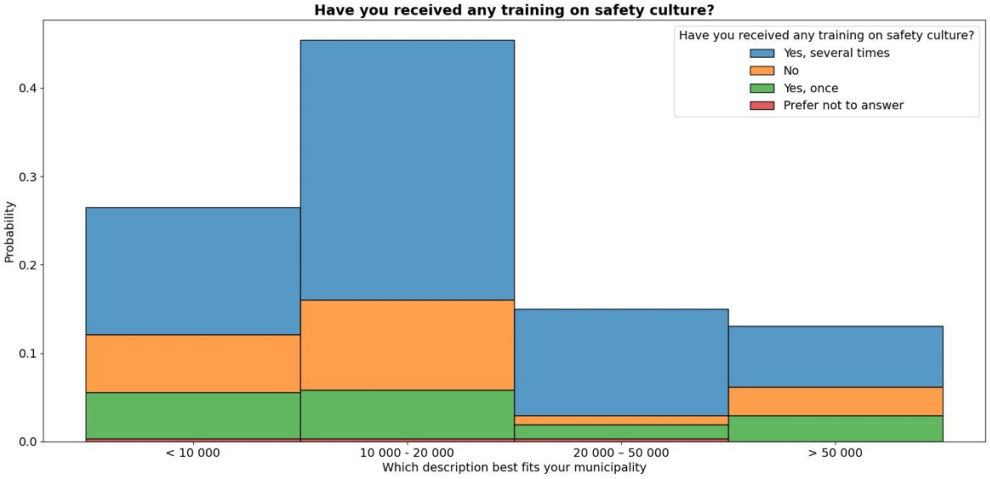
All Survey Statistics

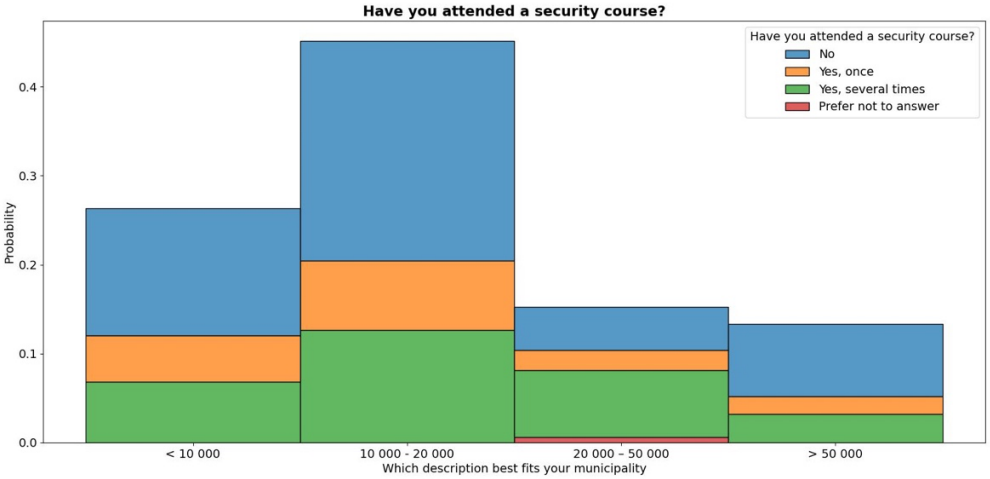
Municipality Survey

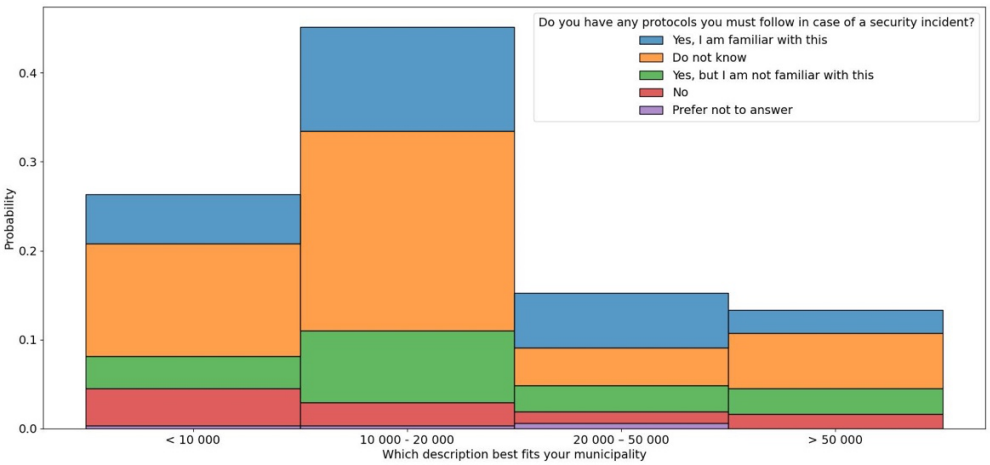


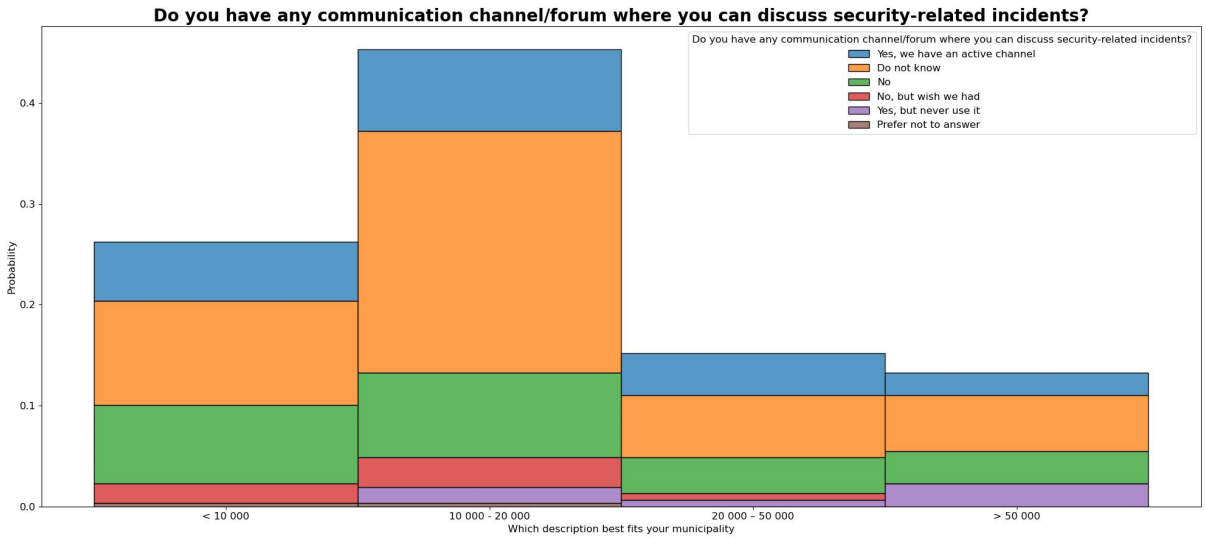

Which description best fits your municipality
10 000 - 20 000
20 000 – 50 000
< 10 000
> 50 000
Prefer not to answer
100
80
60
40
20
0
Information security
NSM's basic principles
Access control
VPN
To-factor authentication
Encryption
Firewall
Phising
Virus
Social engineering

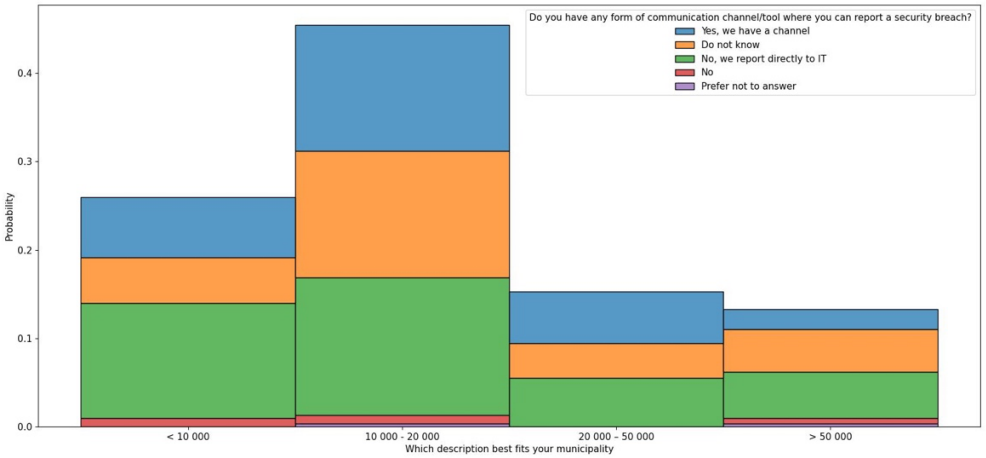

Have you ever asked for help from the IT department/IT responsible?
More than 5 times
Never
1-2 time(s) per year
3-4 times per year
Prefer not to answer
Probability
0.4
0.3
0.2
0.1
0.0
< 10 000
10 000 - 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

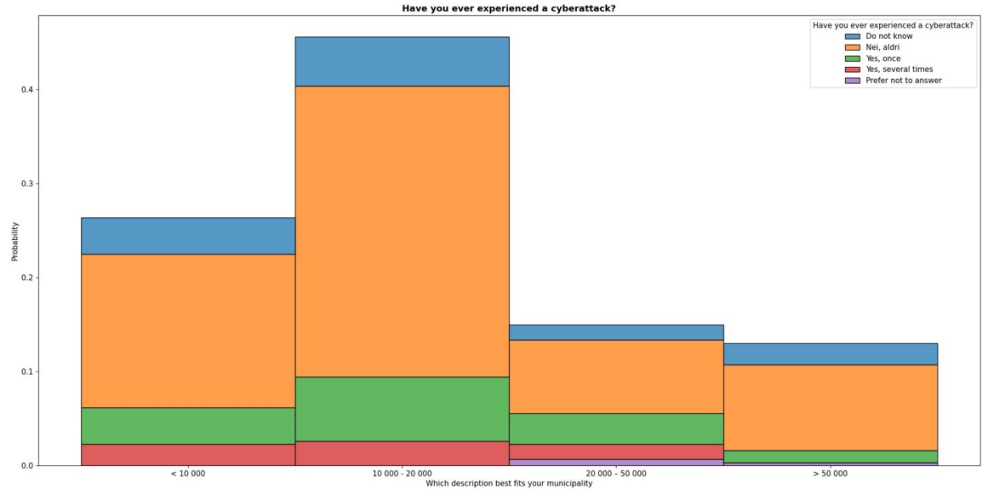

Have you received any training on safety culture?
Have you received any training on safety culture?
Yes, several times
No
Yes, once
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 - 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

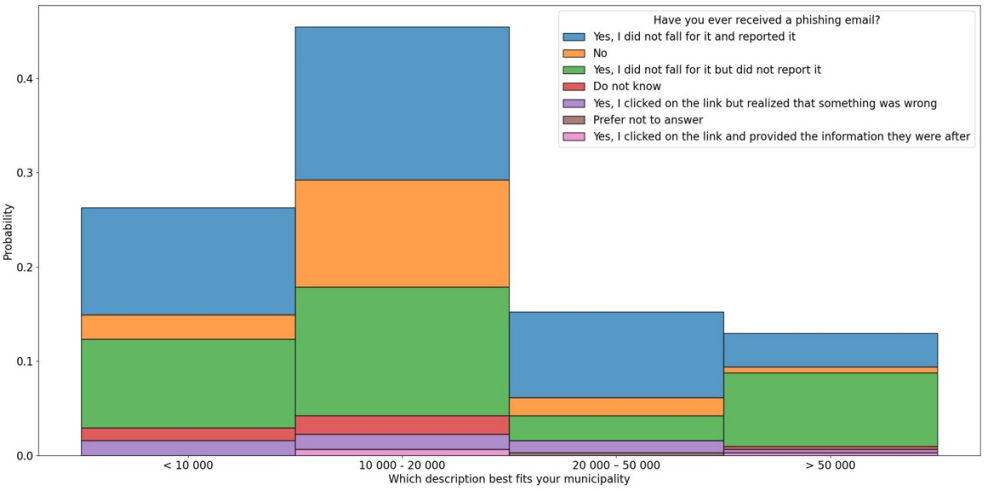

Have you attended a security course?
Have you attended a security course?
No
Yes, once
Yes, several times
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 - 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

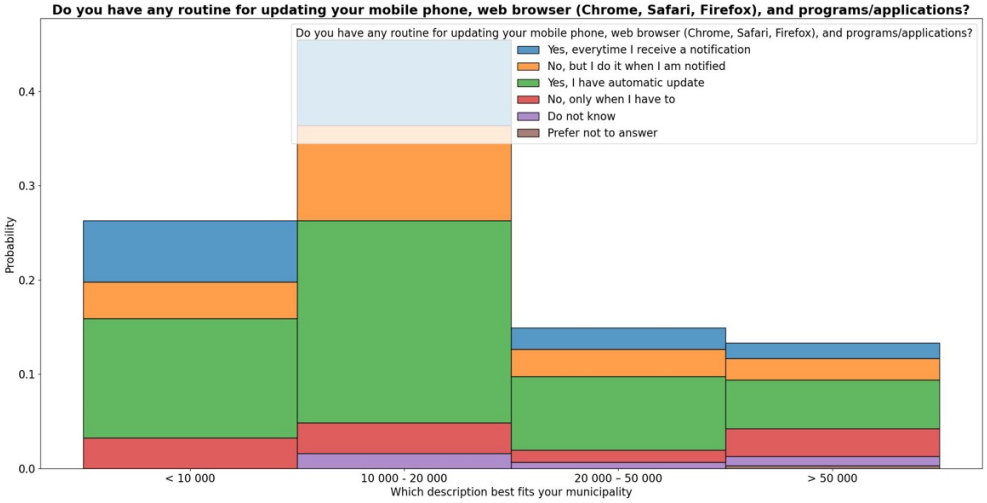

Do you have any protocols you must follow in case of a security incident?
Yes, I am familiar with this
Do not know
Yes, but I am not familiar with this
No
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 - 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

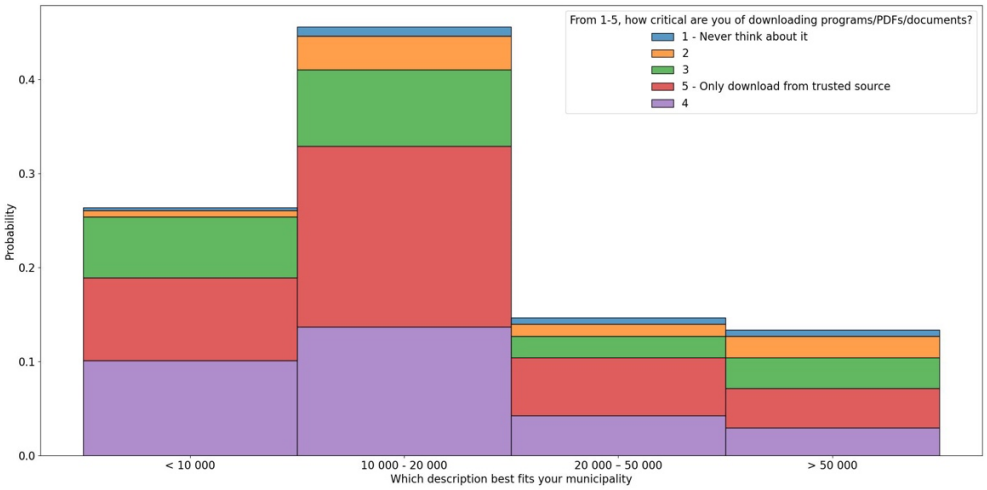

Do you have any communication channel/forum where you can discuss security-related incidents?
Do you have any communication channel/forum where you can discuss security-related incidents?
Yes, we have an active channel
Do not know
No
No, but wish we had
Yes, but never use it
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 - 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

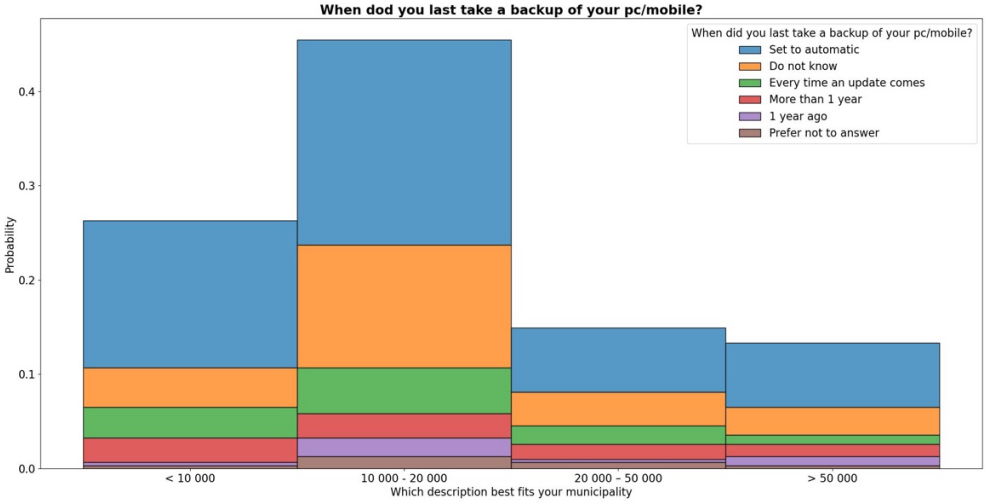

Do you have any form of communication channel/tool where you can report a security breach?
Yes, we have a channel
Do not know
No, we report directly to IT
No
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 - 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

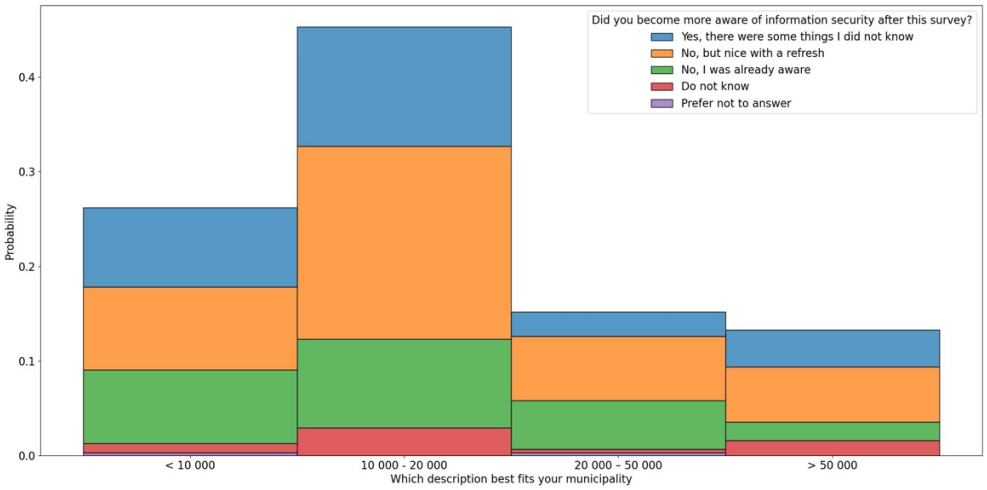

Have you ever experienced a cyberattack?
Have you ever experienced a cyberattack?
Do not know
Nei, aldri
Yes, once
Yes, several times
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 - 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality


Have you ever received a phishing email?
Yes, I did not fall for it and reported it
No
Yes, I did not fall for it but did not report it
Do not know
Yes, I clicked on the link but realized that something was wrong
Prefer not to answer
Yes, I clicked on the link and provided the information they were after
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 - 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

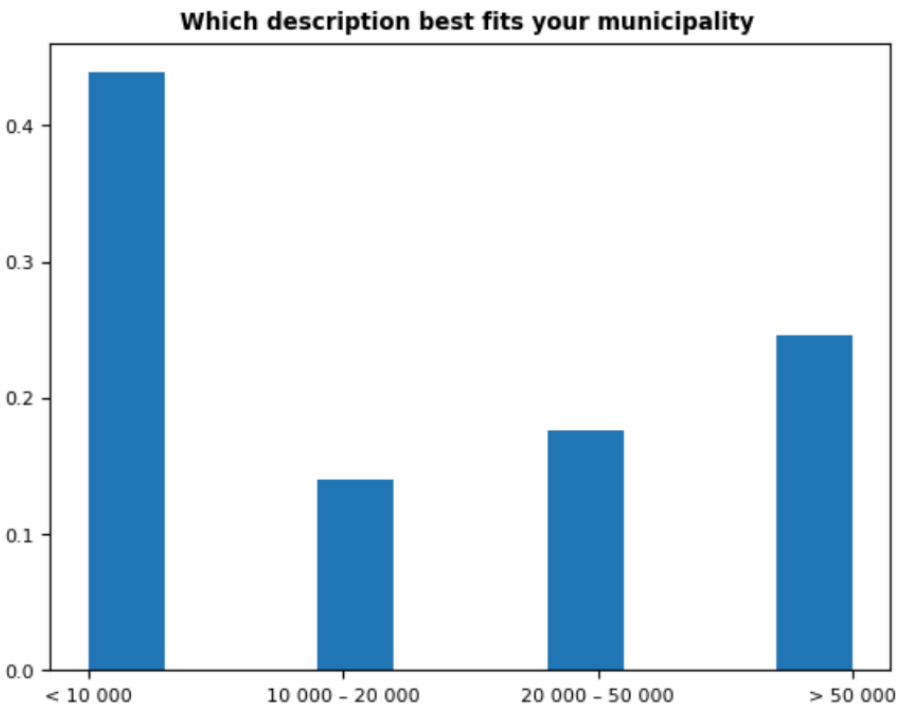

Do you have any routine for updating your mobile phone, web browser (Chrome, Safari, Firefox), and programs/applications?
Yes, everytime I receive a notification
No, but I do it when I am notified
Yes, I have automatic update
No, only when I have to
Do not know
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 - 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

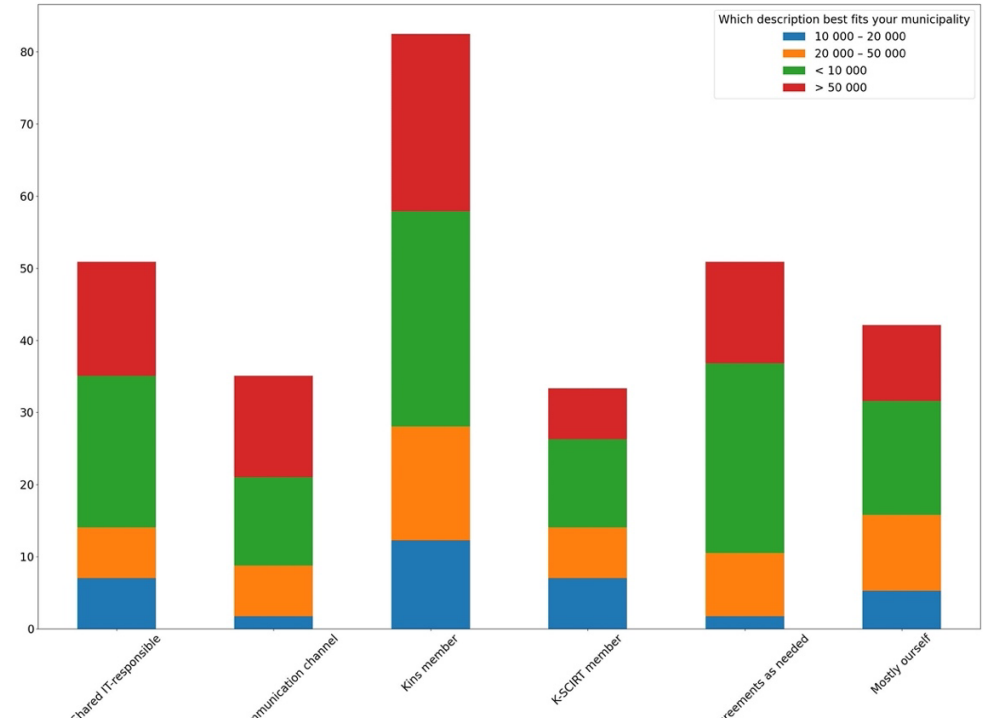

From 1-5, how critical are you of downloading programs/PDFs/documents?
1 - Never think about it
2
3
5 - Only download from trusted source
4
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 - 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

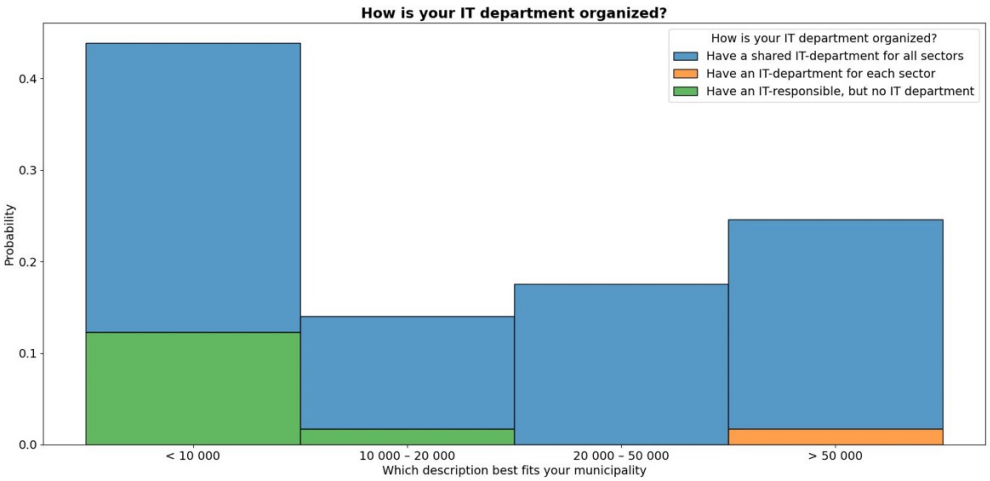

When dod you last take a backup of your pc/mobile?
When did you last take a backup of your pc/mobile?
Set to automatic
Do not know
Every time an update comes
More than 1 year
1 year ago
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 - 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

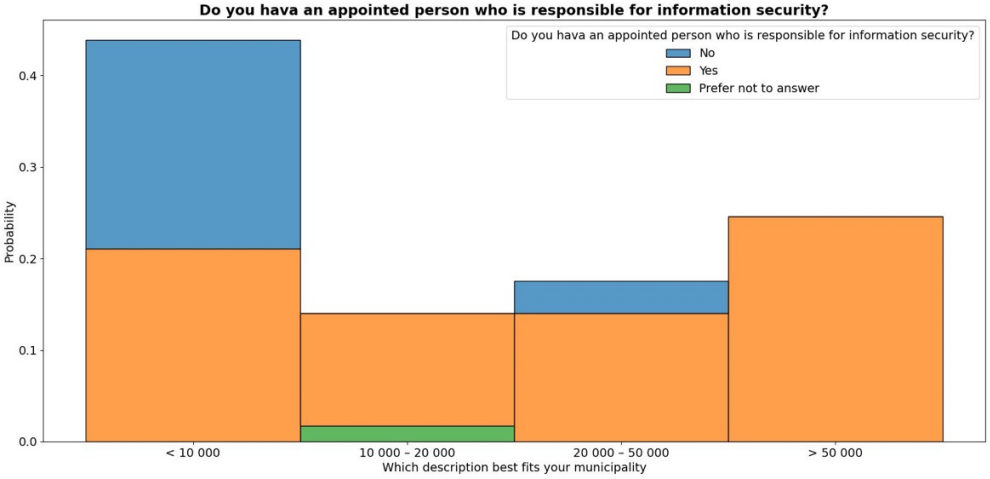

Did you become more aware of information security after this survey?
Yes, there were some things I did not know
No, but nice with a refresh
No, I was already aware
Do not know
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 - 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

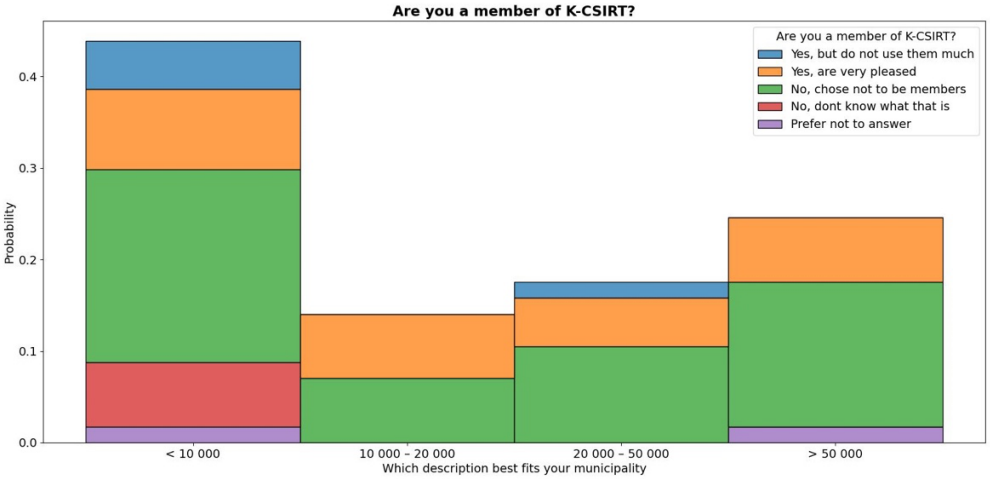
IT Personnel Survey

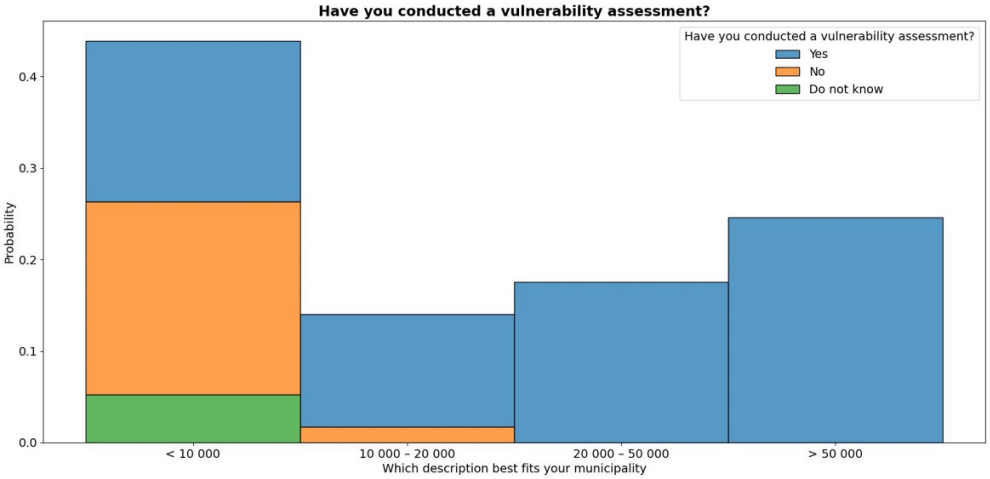


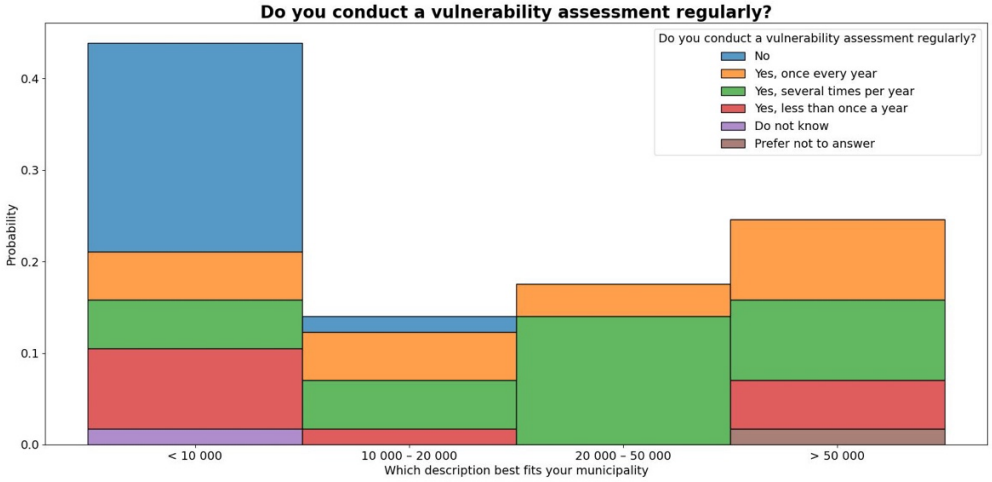

Which description best fits your municipality
10 000 – 20 000
20 000 – 50 000
< 10 000
> 50 000
0
10
20
30
40
50
60
70
80
Kins member
K-SCIRT member
Mostly ourself

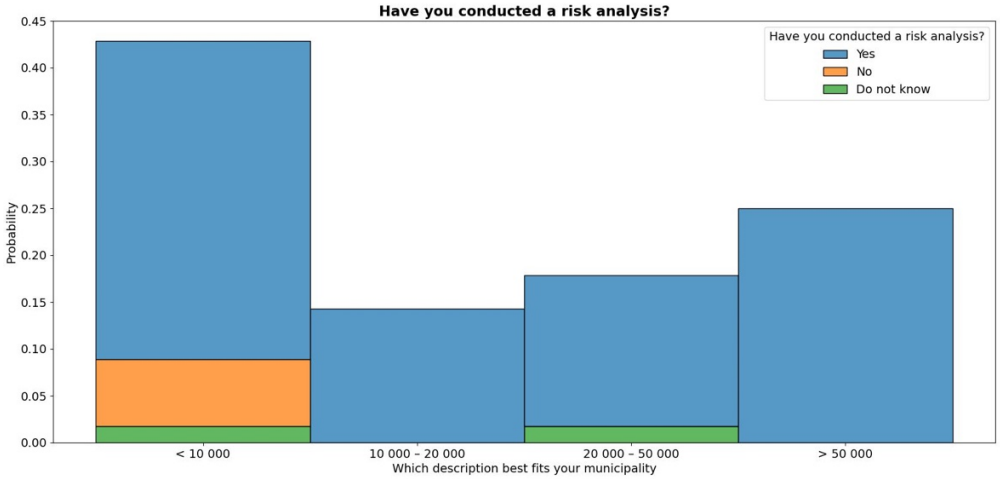

How is your IT department organized?
How is your IT department organized?
Have a shared IT-department for all sectors
Have an IT-department for each sector
Have an IT-responsible, but no IT department
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

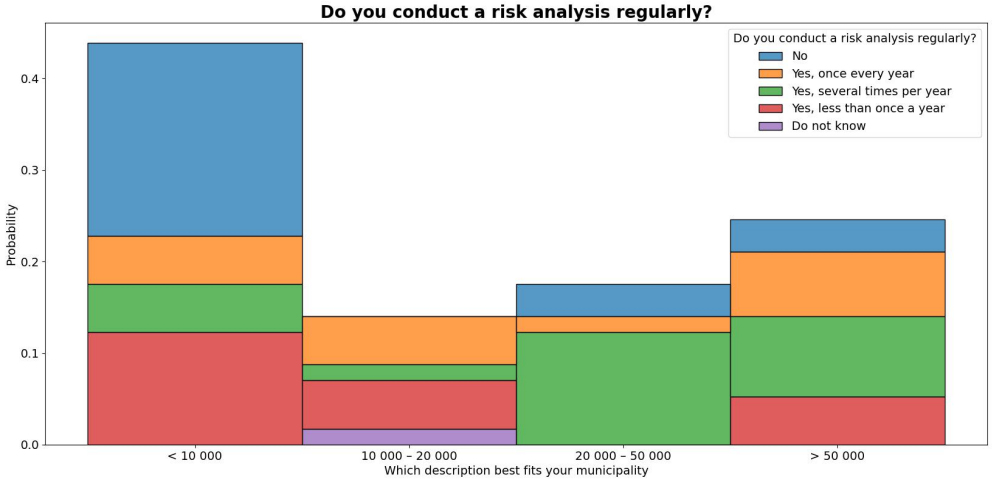

Do you hava an appointed person who is responsible for information security?
Do you hava an appointed person who is responsible for information security?
No
Yes
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

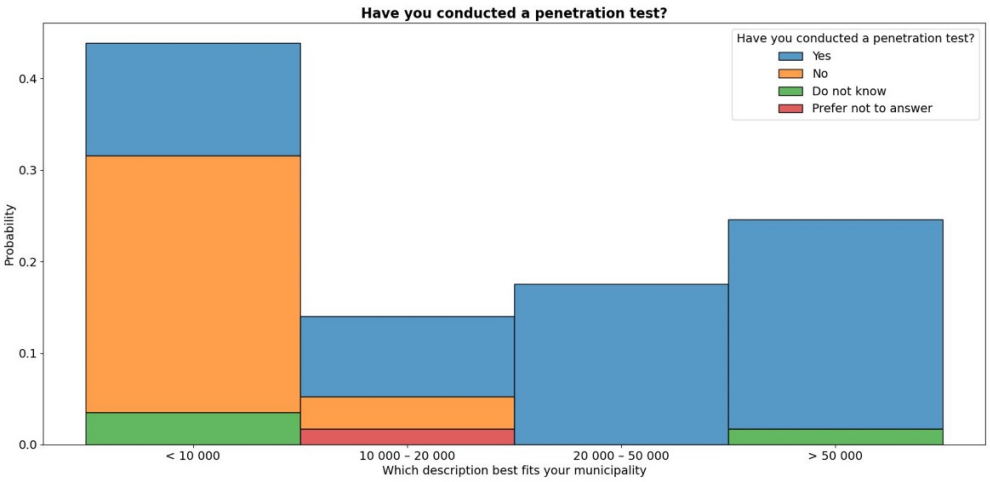

Are you a member of K-CSIRT?
Are you a member of K-CSIRT?
Yes, but do not use them much
Yes, are very pleased
No, chose not to be members
No, dont know what that is
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

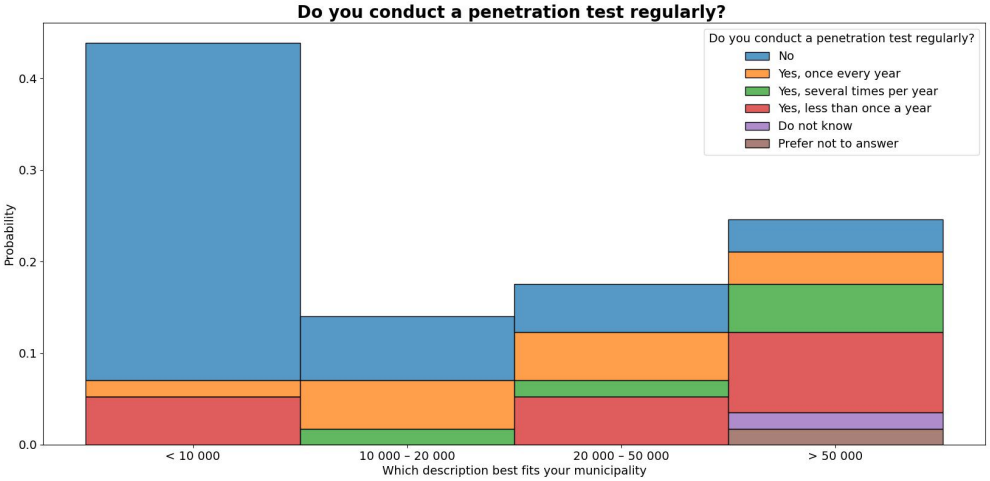

Have you conducted a vulnerability assessment?
Have you conducted a vulnerability assessment?
Yes
No
Do not know
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

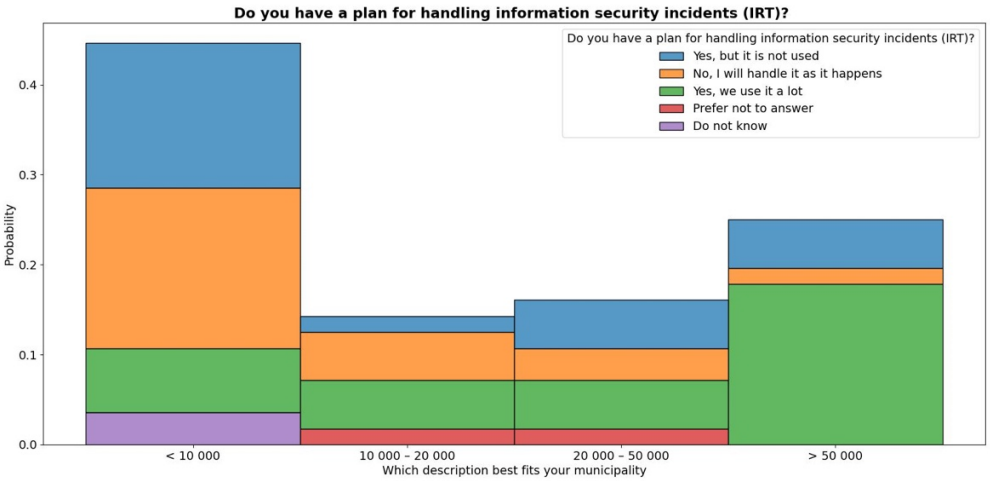

Do you conduct a vulnerability assessment regularly?
Do you conduct a vulnerability assessment regularly?
No
Yes, once every year
Yes, several times per year
Yes, less than once a year
Do not know
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

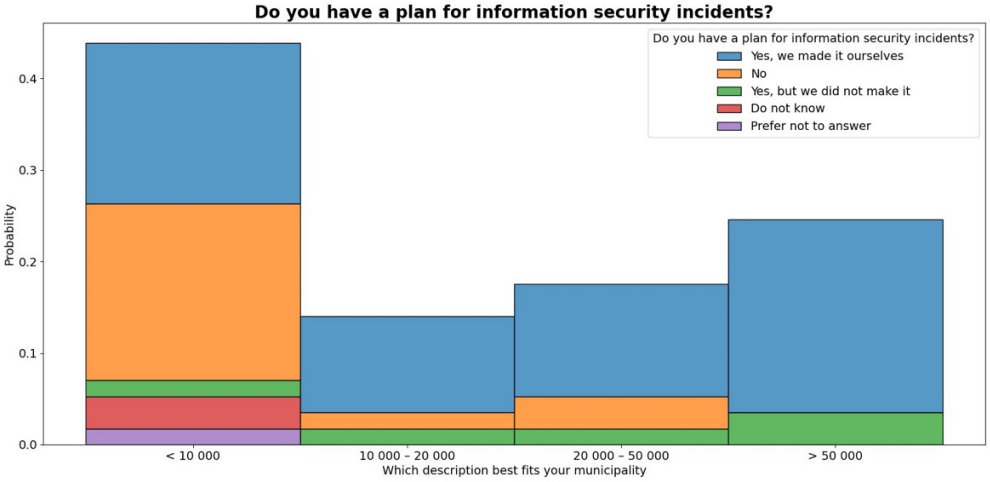

Have you conducted a risk analysis?
Have you conducted a risk analysis?
Yes
No
Do not know
Probability
0.00
0.05
0.10
0.15
0.20
0.25
0.30
0.35
0.40
0.45
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

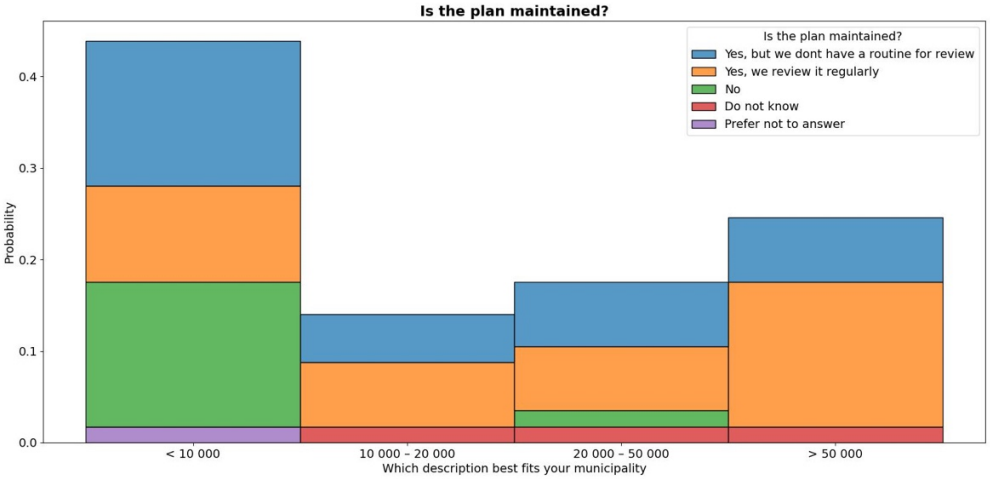

Do you conduct a risk analysis regularly?
Do you conduct a risk analysis regularly?
No
Yes, once every year
Yes, several times per year
Yes, less than once a year
Do not know
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

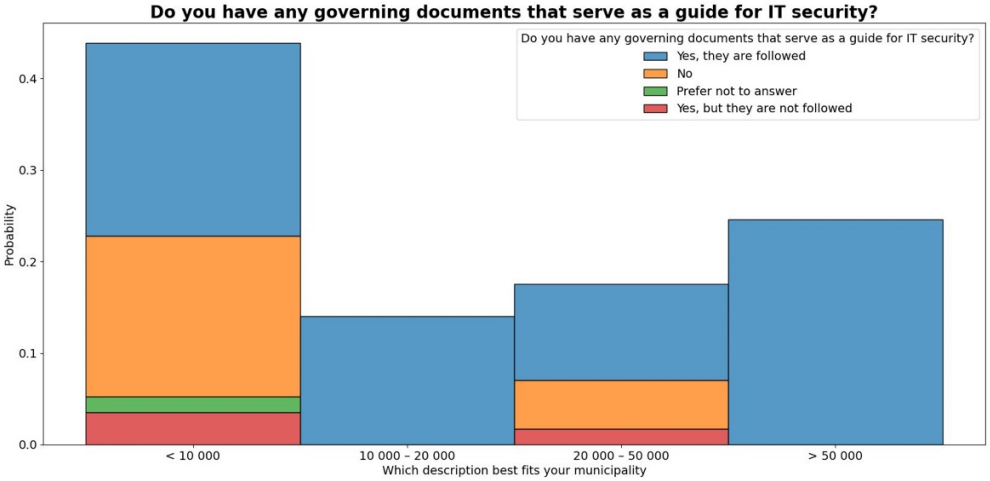

Have you conducted a penetration test?
Have you conducted a penetration test?
Yes
No
Do not know
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

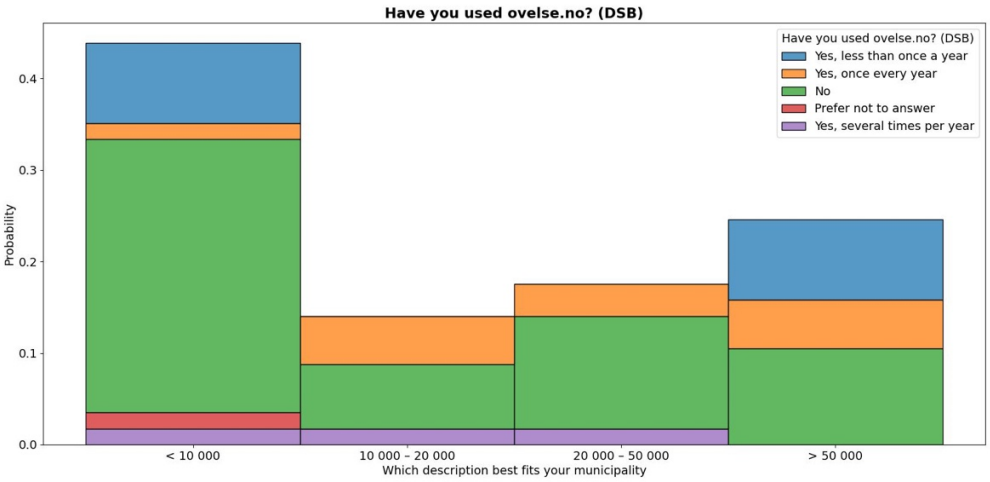

Do you conduct a penetration test regularly?
Do you conduct a penetration test regularly?
No
Yes, once every year
Yes, several times per year
Yes, less than once a year
Do not know
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

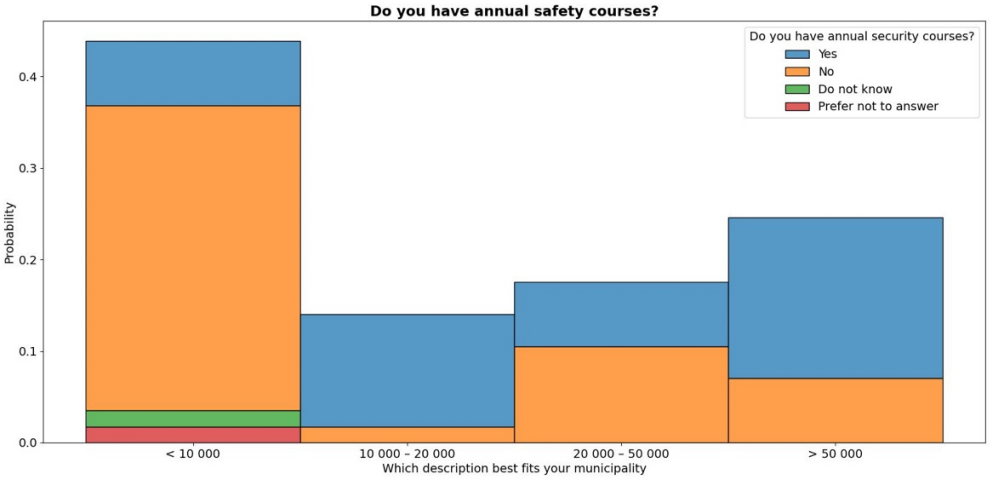

Do you have a plan for handling information security incidents (IRT)?
Do you have a plan for handling information security incidents (IRT)?
Yes, but it is not used
No, I will handle it as it happens
Yes, we use it a lot
Prefer not to answer
Do not know
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

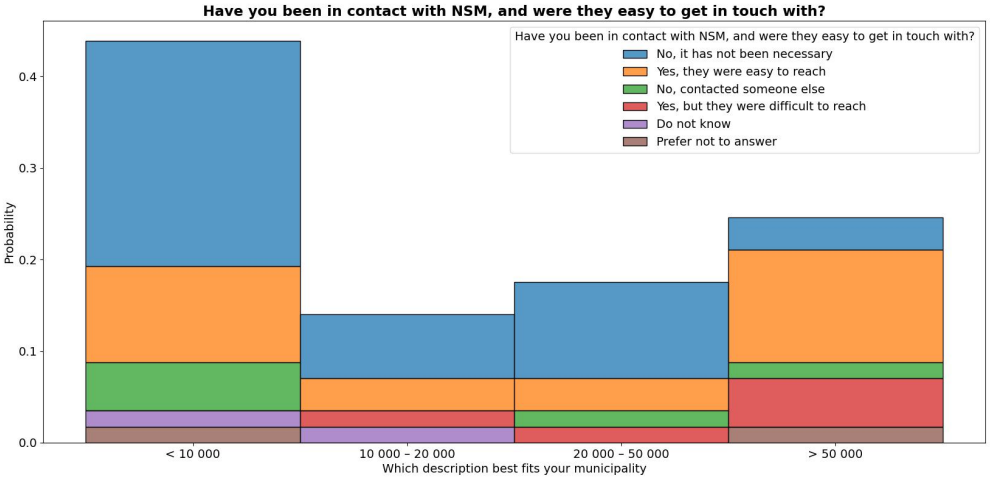

Do you have a plan for information security incidents?
Do you have a plan for information security incidents?
Yes, we made it ourselves
No
Yes, but we did not make it
Do not know
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

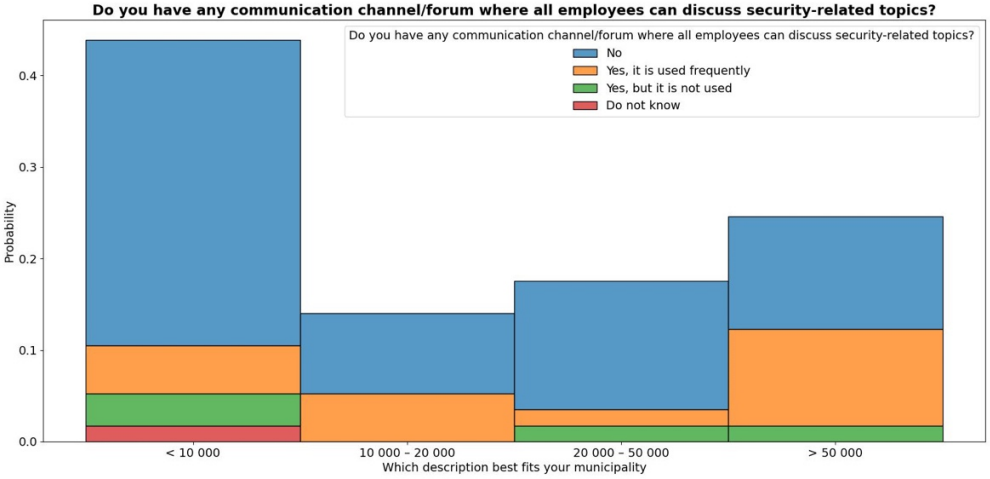

Is the plan maintained?
Is the plan maintained?
Yes, but we dont have a routine for review
Yes, we review it regularly
No
Do not know
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

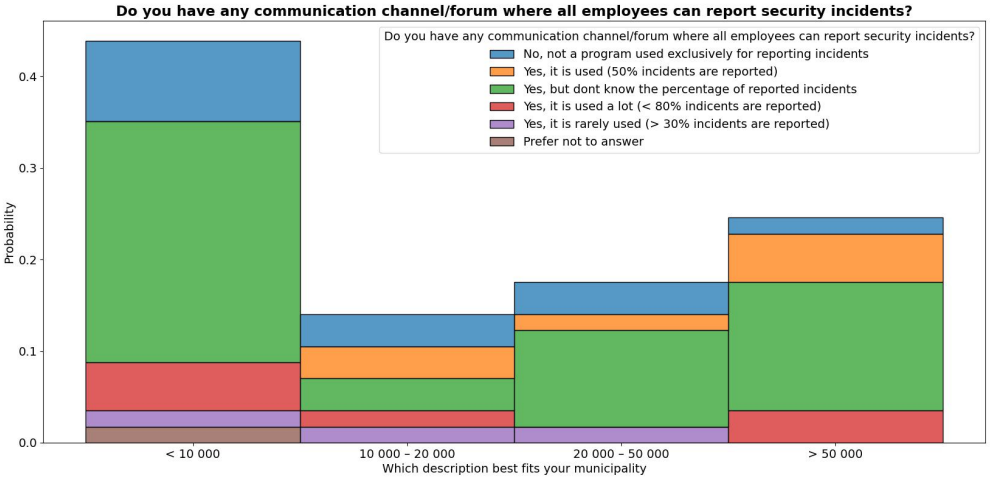

Do you have any governing documents that serve as a guide for IT security?
Do you have any governing documents that serve as a guide for IT security?
Yes, they are followed
No
Prefer not to answer
Yes, but they are not followed
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality

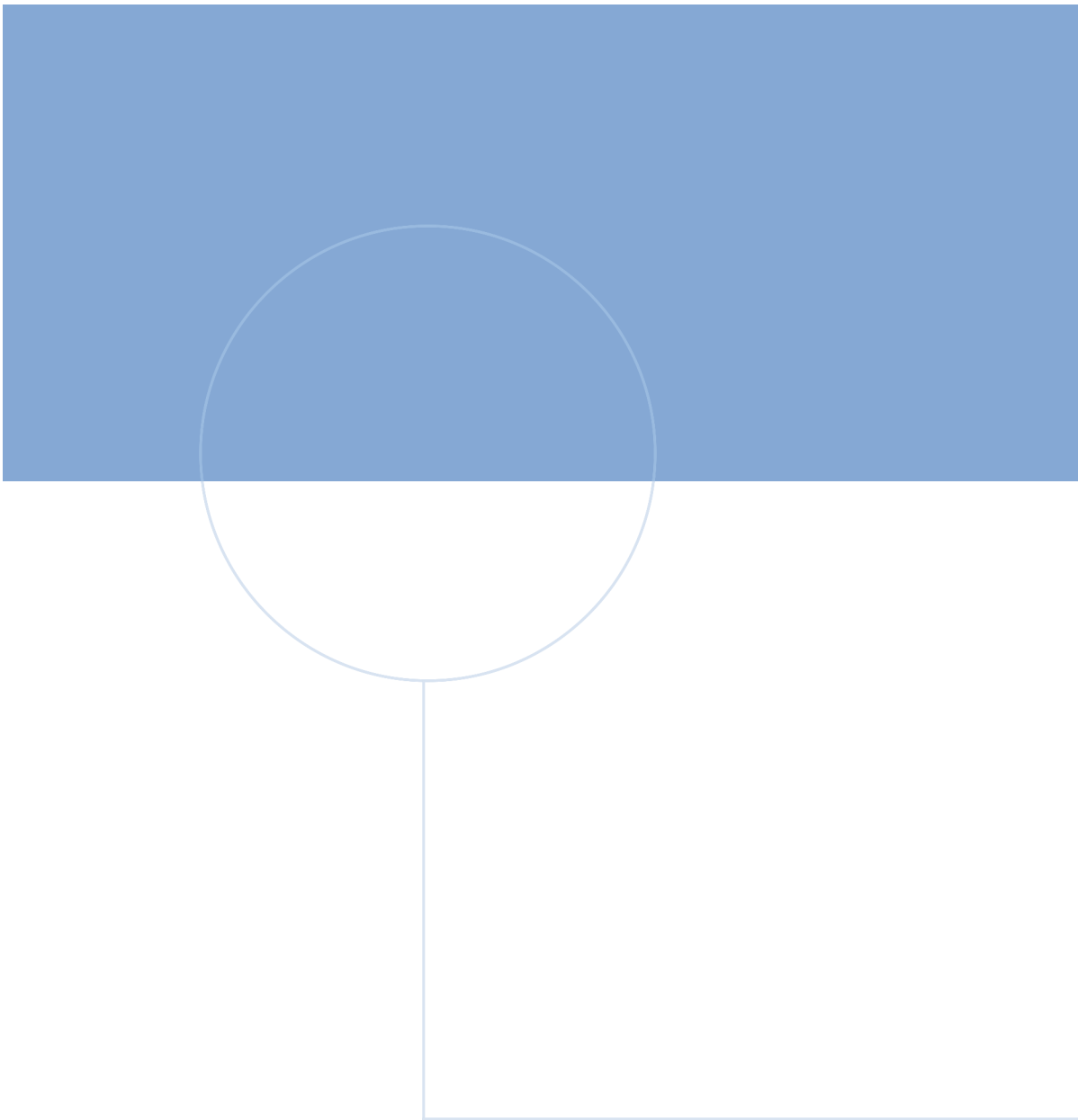

Have you used ovelse.no? (DSB)
Have you used ovelse.no? (DSB)
Yes, less than once a year
Yes, once every year
No
Prefer not to answer
Yes, several times per year
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality


Do you have annual safety courses?
Do you have annual security courses?
Yes
No
Do not know
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality


Have you been in contact with NSM, and were they easy to get in touch with?
Have you been in contact with NSM, and were they easy to get in touch with?
No, it has not been necessary
Yes, they were easy to reach
No, contacted someone else
Yes, but they were difficult to reach
Do not know
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality


Do you have any communication channel/forum where all employees can discuss security-related topics?
Do you have any communication channel/forum where all employees can discuss security-related topics?
No
Yes, it is used frequently
Yes, but it is not used
Do not know
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality


Do you have any communication channel/forum where all employees can report security incidents?
Do you have any communication channel/forum where all employees can report security incidents?
No, not a program used exclusively for reporting incidents
Yes, it is used (50% incidents are reported)
Yes, but dont know the percentage of reported incidents
Yes, it is used a lot (< 80% indicents are reported)
Yes, it is rarely used (> 30% incidents are reported)
Prefer not to answer
Probability
0.0
0.1
0.2
0.3
0.4
< 10 000
10 000 – 20 000
20 000 – 50 000
> 50 000
Which description best fits your municipality



NTNU

Norwegian University of
Science and Technology