INFORMATION SECURITY AWARENESS TRAINING FOR END-USER
A Survey on the Perspective of Nordic Municipalities

Bachelor’s Degree Project in Information Technology with a Specialization in Network and System Administration
IT610G

Bachelor’s Level – 22.5 ECTS
Spring Term 2021

Aous Al Salek

Supervisor: Joakim Kävrestad
Examiner: Marcus Nohlberg

School of Informatics
University of Skövde
Preface

Before you lies a thesis about Information Security Awareness Training, the basis of which is a survey on Information Security Awareness Training for end-users in Nordic municipalities. This is a bachelor’s degree project in the Network and System Administration program at the University of Skövde. This work would have never been realized without the continuous guidance and help of my esteemed supervisor Joakim Kävrestad throughout the research process. Additional special thanks go to my esteemed examiner Marcus Nohlberg for contributing his precise and patient advice for the success of this work. Moreover, many thanks go to my peers for reviewing my work and providing constructive input. Lastly, I want to express my immense gratitude towards my educators for their invaluable support throughout this great endeavour.
Abstract

The reliance on information systems in daily operations in organizations made these systems and the security thereof a vital asset that must be protected. Traditionally, technical solutions were thought to be the critical factor in achieving security requirements. However, this has changed with research advancements into information security, suggesting that users are the root cause of the majority of information security incidents. It is widely accepted that an integral part of the methodology of securing information systems is end-user Information Security Awareness Training (ISAT). The goal of ISAT is described to be a change in user behavior. As a result, research into the area has been steadily improving the ways ISAT is carried out. Yet, information security incidents are still on the rise with no indication of slowing down. Previous research has mainly examined users’ experience in relation to ISAT with very little focus on the organizational perspective. In this study, the organizational perspective on the preferences and expectations of ISAT is examined by inviting all Nordic municipalities to participate in an online survey. The survey consisted of two parts; the first part focused on the current state of ISAT in Nordic municipalities. The second part examined the ideal design of ISAT according to participants. The results obtained from the survey revealed that the participating Nordic municipalities are well aware of recent developments in ISAT. Furthermore, their preferences and expectations of ISAT and what they consider an ideal design of ISAT conform to what is suggested in the literature—with some exceptions. However, there seems to be a gap between knowing about recent developments and having a desired ideal design that conforms to the literature on one side, and actually applying these in production on the other side.

**Keywords:** information security, information security awareness training, information systems, ISAT, user security training
Table of Contents

1 Introduction .................................................................................................................. 1

2 Background .................................................................................................................. 2
  2.1 Definition .................................................................................................................. 2
  2.2 Importance of Security Training .............................................................................. 2
  2.3 Early Stages ............................................................................................................. 2
  2.3.1 The Five Dimensions of Information Security Awareness ............................. 3
  2.3.2 The Ten Commandments of Information Security Awareness Training ...... 4
  2.4 Challenges ............................................................................................................. 5
  2.4.1 User Compliance ............................................................................................... 5
  2.4.2 Knowledge Retention ....................................................................................... 5
  2.5 Recent Developments ......................................................................................... 5
  2.5.1 User Adherence ............................................................................................... 5
  2.5.2 Training Delivery ............................................................................................. 6
  2.5.3 Context-Aware Training ............................................................................... 6
  2.6 ISAT in the Nordic Countries .............................................................................. 7
  2.6.1 Denmark .......................................................................................................... 7
  2.6.2 Finland ............................................................................................................. 8
  2.6.3 Iceland ............................................................................................................. 8
  2.6.4 Norway ............................................................................................................ 8
  2.6.5 Sweden ........................................................................................................... 8

3 Problem Statement ...................................................................................................... 9
  3.1 Problem Area ........................................................................................................ 9
  3.2 Research Question ............................................................................................... 9
  3.3 Motivation ............................................................................................................. 9
  3.4 Delimitation .......................................................................................................... 10
  3.5 Expected Results ................................................................................................. 10

4 Methodology .............................................................................................................. 11
  4.1 Sampling ............................................................................................................... 11
  4.2 Questionnaire Design ......................................................................................... 12
  4.3 Standardization .................................................................................................... 13
  4.4 Instrumentation .................................................................................................... 13
  4.5 Questionnaire Validity and Reliability ............................................................... 14
  4.6 Ethics .................................................................................................................... 15
  4.7 Pretesting ............................................................................................................ 16
  4.8 Analysis ............................................................................................................... 16
  4.8.1 Statistical Analysis ......................................................................................... 16
  4.8.2 Thematic Analysis .......................................................................................... 19
  4.9 Analysis Validity and Reliability ........................................................................ 20
  4.9.1 Statistical Analysis ......................................................................................... 20
  4.9.2 Thematic Analysis .......................................................................................... 22

5 Results and Analysis .................................................................................................. 23
1 Introduction

In today’s digital era, the human element imposes a great vulnerability to the security of an organization’s information systems, which can be exploited by bad actors for malicious gains (Parsons et al. 2014). Organizations tend to rely on technology-based solutions in mitigating information security risks (Bulgurcu, Cavusoglu & Benbasat 2010). However, research has shown that information systems security methods, which focus on technology-based security solutions, are not enough, as they tend to ignore the importance of the socio-organizational nature of information systems (Siponen 2005). Therefore, information security success factors include both technology-based and socio-organizational solutions (Al-Daeef, Basir & Saudi 2017; Bulgurcu, Cavusoglu & Benbasat 2010).

Furthermore, the risks of information security are growing in both quantity and severity of consequences, as research indicates that the number of information security incidents is continuously growing (Bulgurcu, Cavusoglu & Benbasat 2010; Ghafir et al. 2018; Siponen, Mahmood & Pahnila 2014). Additionally, the most common approach in dealing with attacks exploiting end-user behavior is security awareness training (Kävrestad & Nohlberg 2020c; Puhakainen & Siponen 2010). This creates a need for improved training methods that are developed to be more sophisticated and less cumbersome at the same time in order to be effective (Kävrestad & Nohlberg 2020c). This makes Information Security Awareness Training (ISAT) “the most important factor” in mitigating attacks that take advantage of vulnerabilities introduced by the human element (Safa & Von Solms 2016, p. 442). In order to reduce the risks of attacks based on exploiting user behavior, it is important to make users aware of the potential consequences of their behavior (Desman 2003).

As attacks on organizations have increased significantly in recent years, organizations’ efforts to combat said attacks are being slowed down by the lack of users following security policies and training (Siponen, Mahmood & Pahnila 2014). This problem is further accelerated by the lack of clear empirical evidence indicating the validity of best-practice guidelines of many training methods used today. Thus, organizations are facing enormous challenges in deploying effective end-user ISAT (Al-Daeef, Basir & Saudi 2017; Alshaikh, Maynard, Ahmad & Chang 2018; Kävrestad & Nohlberg 2020c; Siponen & Willison 2009). Moreover, the success of ISAT for end-users depends heavily on the training delivery method. Traditionally, training has been delivered through a classroom setting. However, research has shown that traditional methods of training delivery are ineffective when covering multiple security areas for large audiences (Al-Daeef, Basir & Saudi 2017).

To that end, many key questions need to be addressed by organizations in the planning phase of end-user ISAT, such as (i) What training model to deploy? (ii) How should said model be deployed and integrated into existing systems? (iii) When should training be provided to end-users? (iv) Where should said training occur? (e.g., in classrooms or at the users’ own desks).

These questions in combination with others are used in this thesis to survey Nordic municipalities on their perspective in regards to end-user ISAT. This survey provides a better understanding of the thought process of these organizations in decision choices and helps the research community in tailoring their work to organizations in general. Additionally, this study touches on the disconnection between the researcher and practitioner communities.
2 Background

This section aims to provide the reader with sufficient information to understand the problem area addressed in this thesis and touch on some of the aspects of end-user ISAT.

2.1 Definition

Information security awareness is defined by Al-Daeef, Basir, and Saudi (2017) as “the security knowledge that has been gradually acquired through a continuous and updated catchy training manner to influence trainees’ behavior.” (Al-Daeef, Basir & Saudi 2017, p. 447). Another definition by Wolf, Haworth, and Pietron (2011) is “the effort to impart knowledge of or about factors in information security to the degree that it influences users’ behaviour to conform to policy.” (Wolf, Haworth & Pietron 2011, p. 10).

2.2 Importance of Security Training

The spread of technology use in organizational operations at all levels has enlarged the attack surface and the number of vulnerabilities in organizations (Ghafir et al. 2018; Siponen 2001). This is apparent through the observation of significantly increasing information security incidents affecting organizations all around the globe (Ghafir et al. 2018; Siponen, Mahmood & Pahnila 2014). Furthermore, a general consensus on several widely adopted ideas seems to exist in the literature relating to information security. These ideas are (Al-Daeef, Basir & Saudi 2017; Al-shaikh et al. 2018; Bada, Sasse & Nurse 2015; Ghafir et al. 2018; Kävrestad & Nohlberg 2020b; Kävrestad & Nohlberg 2020c; Siponen, Mahmood & Pahnila 2014):

- Human behavior is often exploited by attackers and constitutes an information security risk.
- Technical solutions—when used solely—are not sufficient for the mitigation of information security risks.
- End-user ISAT is an essential factor in strengthening the information security posture of an organization.
- There is an emerging need for training end-users to behave more securely.

According to McCumber “education, training, and awareness may be our most prominent security measures.” (McCumber 2004, p. 106). This is supported by the fact that both governments and enterprises rely heavily on Information and Communication Technology (ICT), which makes information security in the aforementioned domains a critical factor in the survival of society (Bada, Sasse & Nurse 2015). Furthermore, individuals who operate the critical infrastructure nowadays tend to not be experts on information security, which in some fields, (e.g., healthcare), may mean life or death. The level of dependence on information security in critical infrastructures, such as emergency services, makes IT and the security thereof a “necessity of life” (Ghafir et al. 2018, p. 4987).

2.3 Early Stages

The importance of end-user ISAT is not a new subject, and although research into the area is continuously evolving it is not new per se. After the dot-com bubble, researchers realized that the increasing popularity of digitalization among organizations introduced new vulnerabilities that could affect economies. As a result, research into the area of security training has been growing
exponentially in recent years. However, the growth of research into said area is nothing new, as searching for articles regarding security training between the years 2000 and 2020 on Scopus\(^1\) shows a fairly steady growth that began around the turn of the century, and in the last five years, this growth became exponential, as shown in Figure 1.

![Research papers in the field of security training](image)

**Figure 1** - Number of publications in the field of "security training" in Scopus between 1995 and 2020. Accessed on the 12\(^{th}\) of February 2021 (the author’s own figure).

Although, Siponen points out that researchers agree on the relevance of information security awareness since, at least, the early 90’s of the last century. Furthermore, Siponen states that the issue was still unformalized at the beginning of the 21\(^{st}\) century (Siponen 2001). This view is further cemented by Desman, who tries to present the general consensus at the time in terms of guidelines in order to “take an orderly approach” to resolve the issue (Desman 2003, p. 40).

### 2.3.1 The Five Dimensions of Information Security Awareness

Intending to formalize an inherently informal issue, at the time, Siponen identified “five dimensions of information security awareness”, which are described below (Siponen 2001, p. 24):

- **"The organizational dimension"** refers to the different information needs of different organizational target groups (e.g., management, information security staff, and end-users) (Siponen 2001, p. 26).
- **"The general public dimension"** refers to the knowledge differences between IT professionals and other end-users. Siponen argues that every end-user should be aware of core information security issues the same way as other “normal” issues, which do not relate to IT (Siponen 2001, p. 26).
- **"The socio-political dimension"** refers to the need for decision-makers to have, at least, high-level awareness of information security issues and its ethical principles, otherwise, they “may fail to recognize the moral conceptions underlying their decisions” (Siponen 2001, p. 27).

\(^{1}\) https://www.scopus.com/
• “The computer ethical dimension” refers to the need to provide ethics researchers with relevant information to then learn from their conclusions on the ethics of information security (Siponen 2001, p. 27).

• “The institutional dimension” refers to a societal process by which the members of a society are better educated on information security awareness (Siponen 2001, p. 28).

2.3.2 The Ten Commandments of Information Security Awareness Training

One of the most important early contributions, that tried to formalize and standardize end-user ISAT, was an article by Desman (2003). In the article, Desman laid out 10 “commandments” (tips) to succeed in ISAT. This article was the first of its kind and gathered the learnings of all—what at the time was—current research into the area (Desman 2003, p. 40), which probably makes it the first systematic method of ISAT. These ten commandments are cited and described below.

“Information security is a people, rather than technical issue.” This refers to the importance of educating users on the potential information security threats and their responsibility to the integrity of their organization’s information security (Desman 2003, p. 40).

“If you want them to understand, speak their language.” This refers to the importance of users’ understanding of the training, which can be achieved through easy-to-follow language, otherwise, knowledge of the subject area would be a prerequisite to understanding ISAT (Desman 2003, p. 40).

“If they cannot see it, they will not learn it.” This refers to the importance of reaching out to all members of a target group and adjusting or adding communication media to encompass 100% of users (Desman 2003, p. 41).

“Make your point so that you can identify it and so can they.” This refers to having an easily identifiable goal to each point in the training, otherwise one runs the risk of users not understanding the purpose of the training or what actions are necessitated to preserve the information security of their organization (Desman 2003, p. 41).

“Never lose your sense of humor.” Desman argues that acquiring knowledge should not be “painful” and an element of humor will make it easier for trainees to follow along with and accept the training (Desman 2003, p. 41).

“Make your point, support it, and conclude it.” This point refers to being concise and to the point when educating users on information security (Desman 2003, p. 41).

“Always let the recipients know how the behavior that you request will affect them.” Desman states that it is essential for trainees to understand why and how their actions will affect their organization (Desman 2003, p. 42).

“Ride the tame horses.” This commandment refers to the importance of making use of pre-existing resources in an organization to convey training, such as communication media, public relations experts, and graphics designers (Desman 2003, p. 42).

“Formalize your training methodology.” Refers to establishing training as a habitual procedure from the start by including it in new staff orientation and regularly present existing staff with training material (Desman 2003, p. 43).
“Always be timely, even if it means slipping schedules to include urgent information.” Calls attention to keeping trainees informed about new information security revelations and making use of reports from the press (Desman 2003, p. 43).

2.4 Challenges

ISAT entails numerous challenges that are essential to address and take into account when planning, designing, and carrying out training (Bada, Sasse & Nurse 2015). The following are two of the critical challenges in ISAT.

2.4.1 User Compliance

It is established that ISAT is the most important single information security measure that an organization can take (Desman 2003; McCumber 2004). However, training without compliance by the users renders said training useless. “The first behaviorally-based research” on trainees’ compliance with a security policy in an organization found that only 60% of trainees adhered to said policy (Wolf, Haworth & Pietron 2011, p. 18).

2.4.2 Knowledge Retention

According to Al-Daeef, Basir, and Saudi (2017), the main goal of ISAT should be making users retain acquired knowledge for long periods of time in order to be effective (Al-Daeef, Basir & Saudi 2017). Kumaraguru et al. (2007) did a study to, among other things, test trainees’ knowledge retention performance. In one instance, it was found that only half of the percentage of trainees who succeeded in the test done immediately after the training, were able to succeed in a second test similar to the first one only seven days later (Kumaraguru et al. 2007).

2.5 Recent Developments

This section outlines some of the most important recent developments in research into the field of ISAT to mitigate challenges in planning and deploying.

2.5.1 User Adherence

ISAT is usually referred to as a method of changing users’ behavior to be more secure (Kävrestad & Nohlberg 2020b). However, only providing end-users with information about security risks is not sufficient, and succeeding in an information security test does not motivate users to change their behavior and adhere to security policies (Bada, Sasse & Nurse 2015). Furthermore, the perceived vulnerability from and severity of information security threats of an end-user, and their belief in their ability to and attitude towards complying with security policies, have a positive impact on their intention to adhere to said policies. These factors result in an actual positive change in behavior and compliance with information security policies in organizations (Siponen, Mahmood & Pahnila 2014). Therefore, training should use “simple consistent rules of behaviour”, as they provide users with a perception of control and heightens their acceptance of the idea of behavior change (Bada, Sasse & Nurse 2015, p. 128).
2.5.2 Training Delivery

The delivery method of ISAT is an inherently important factor in the success of the training (Abawajy & Kim 2010). There is a plethora of ISAT delivery methods, but modern methods mainly fall into five categories (Abawajy & Kim 2010; Al-Daeef, Basir & Saudi 2017). These categories are informative, promotional, online, game-based, and simulation delivery methods.

Informative training methods are one-way media of just conveying information with no interactive elements, such as emails, newsletters, and publications in general. Examples of promotional delivery methods are custom desktop backgrounds, banners, and bulletin boards. These are similar to informative methods but have the advantage of not requiring action to be seen (Abawajy & Kim 2010).

Online delivery methods tend to be user-friendly and come mainly in the form of either standalone tests followed with information or the other way around. Online training methods do usually have videos and score counters to add an element of interactivity. However, deploying such methods may introduce a risk of users just going through materials as a chore and not with the goal of actually learning. Additionally, they lack two-way communication for further dialogue (Abawajy & Kim 2010; Al-Daeef, Basir & Saudi 2017).

Game-based training methods are meant to engage the trainees and make the training experience as interactive as possible (Abawajy & Kim 2010). These methods are becoming more popular as they have been proven to provide positive outcomes (Al-Daeef, Basir & Saudi 2017). An example of a game-based training is CyberCIEGE, which is a “highly interactive video game” used as an ISAT tool (Cone, Thompson, Irvine & Nguyen 2006, p. 431).

Simulation training methods also referred to as embedded training methods, aim to integrate training into existing systems used by the target group, which allows for real-world simulated situations that are constructed to convey specific messages about information security awareness. Embedded training is usually followed by providing trainees with materials to further deepen their knowledge, and it has the advantage of two-way communication. This training method is gaining traction because it has shown positive results (Abawajy & Kim 2010; Al-Daeef, Basir & Saudi 2017; Kumaraguru, Sheng, Acquisti, Cranon & Hong 2008).

2.5.3 Context-Aware Training

A major challenge with security awareness programs is the lack of a fully developed methodology to deliver them (Abawajy & Kim 2010). However, in recent years two end-user ISAT frameworks were introduced with a new concept, called context-aware training (Ghafir et al. 2018; Kävrestad & Nohlberg 2020c). This concept is built around the idea of having an ISAT program that is aware of the user environment and capable of presenting training based on user activity. The idea is that, for example, when a user receives a suspicious email in their normal day-to-day workflow, a warning will be presented informing the user about the risk. Constructed training scenarios were an improvement over traditional generally informative training methods. This improvement is achieved through providing hands-on experience that research has shown to provide better results in almost all measurements (Kumaraguru et al. 2007; Kumaraguru et al. 2008). This is the concept behind embedded training; however, the general consensus is that the relevance of training is a key factor in the success of an ISAT program (Kävrestad & Nohlberg 2020c; Siponen 2001). Thus, although constructed training situations are necessary, training in day-to-day life is very
important as it provides users with awareness about a subject when it is the most relevant (e.g., while they are working), which makes it much more effective (Kävrestad & Nohlberg 2020c). With that said, both of the aforementioned context-aware training methods provide the ability to construct training scenarios, because it is still seen as an effective complementary method (Ghafir et al. 2018; Kävrestad & Nohlberg 2020c).

The aforementioned methods differ in some aspects. The first one by Ghafir et al. (2018) provides a specific implementation with a reward system without the ability to provide ‘learn more’ links. Additionally, it displays training to the user even when user actions do not “present a suitable context to trigger training content” (Ghafir et al. 2018, p. 4993). This can be seen as counterintuitive to the concept of context-awareness and training relevance (Desman 2003). Users tend to usually discard and ignore this kind of irrelevant and too frequent information (Al-Daeef, Basir & Saudi 2017).

The other framework is called ContextBased MicroTraining (CBMT) (Kävrestad & Nohlberg 2020c). CBMT is a comprehensive ISAT framework, that touches on new areas and integrates knowledge from multiple different sciences. CBMT provides 5 goals and 7 guidelines insisting on, inter alia, relevance, ease, and conciseness (Kävrestad & Nohlberg 2020c). The CBMT framework provides newly introduced advantages, the most important of which is generalizability, as it was developed with no restricted implementation. However, Kävrestad and Nohlberg have provided multiple example implementations with very promising results (Kävrestad & Nohlberg 2020a; Kävrestad & Nohlberg 2020b; Kävrestad & Nohlberg 2020c).

2.6 ISAT in the Nordic Countries

The Nordic countries are at the cutting edge of the digitalization trend of all sectors. They rely heavily on their digital infrastructure while expanding how this infrastructure is used and integrated into daily life. These factors make securing the digital infrastructure in the Nordic countries a matter of national security (Nøhr et al. 2020). Furthermore, being member states of the European Economic Area the Nordic countries have to comply with several regulations regarding information security and information security awareness. Subsequently all Nordic countries have national information security strategies stressing the importance of raising awareness about information security risks. The methods of raising awareness about information security mentioned in these strategies are training and education as the majority of challenges in information security are related to humans (Nøhr et al. 2020; Danish Ministry of Finance 2018; Finnish Ministry of Defence 2013; Icelandic Minister of the Interior 2015; Norwegian Ministeries 2019; Swedish Ministry of Justice 2016).

2.6.1 Denmark

The Danish information security strategy—created by the Danish Ministry of Finance—includes multiple initiatives that focus on raising awareness about information security risks. These initiatives are set to establish an informed and skilled society throughout the public and private sectors. Moreover, one of the initiatives aims to integrate ISAT into the education system to establish information security awareness as a critical subject (Danish Ministry of Finance 2018). The Local Government Denmark association postulates that all municipal employees have to receive ISAT and master digital skills (Local Government Denmark 2018). Additionally, the Local Government Denmark association provides a list of multiple ISAT programs for—among other target groups—municipal employees (Awareness og uddannelse n.d.).
2.6.2 Finland

One of the principals set by the Finnish Ministry of Defence in the Finnish information security strategy is to improve awareness about information security risks in the Finnish society as a whole. One of the aims of guideline is to increase available resources to the Finnish education system in order to accelerate this process (Finnish Ministry of Defence 2013). The Association of Finnish Local and Regional Authorities urges all its members to follow the guidelines set by the Finnish Ministry of Finance (Informationens livscykel 2021). The guidelines of Finnish Ministry of Finance state that one of the most important information security measures is to develop the skills and raise the awareness of public employees with regards to information security (Finnish Ministry of Finance 2020).

2.6.3 Iceland

The Icelandic national information security strategy was created by the Icelandic Ministry of Interior and it affirms that “knowledge is the prerequisite for being able to build up the capacity in cyber security” (Icelandic Minister of the Interior 2015, p. 9). Further, this strategy sets forth assertions about the societal value of raising awareness of information security and integrating it into the Icelandic education system to include children (Icelandic Minister of the Interior 2015). This is reflected by the Icelandic Association of Local Authorities in the form of courses provided publicly on various digital subjects, one of which is information security awareness (Auktustafræna færni þína n.d.).

2.6.4 Norway

One of the prioritized areas by the Norwegian Ministries in the Norwegian national information security strategy is raising awareness of information security risks. The strategy presents multiple methods to achieve this, such as integrating components of information security into all levels of the Norwegian education system. Moreover, the strategy specifies that ISAT should be integrated into professional training and provided to the general public (Norwegian Ministeries 2019). This is further cemented by regulations set by the Norwegian Ministry of Local Government and Modernization stating that the Norwegian Directorate for Civil Protection shall develop, facilitate, and carry out courses in the public sector addressing information security (Norwegian Ministry of Local Government and Modernisation 2019). This is further encouraged by the Norwegian Association of Local and Regional Authorities by providing Norwegian municipalities with an information security training program (Kompetansepakke for kommuner og fylkeskommuner 2019).

2.6.5 Sweden

The Swedish Ministry of Justice states in the Swedish national information security strategy that information security must be a normal part of the workflow at all levels. Furthermore, it is mentioned in the strategy that raising awareness is a critical part of the comprehensive information security framework as the human factor is—in many cases—exploited during attacks. Additionally, one of the strategic priorities in the Swedish strategy is to raise awareness and foster expertise. This is to be achieved through increasing individuals’ knowledge about information security risks in the society as a whole and providing ISAT to personnel that is relevant to their field and position (Swedish Ministry of Justice 2016). The Swedish Association of Local Authorities and Regions advises Swedish municipalities to increase the knowledge of employees about information security risks through training and awareness increasing initiatives (Swedish Association of Local Authorities and Regions 2019).
3 Problem Statement

This section focuses on detailing the problem area this study addresses, the expected results, the research question, and subgoals of the study, alongside motivating the importance of studying this problem.

3.1 Problem Area

As previously established, the importance of end-user ISAT for an organization’s assets cannot be overstated (Al-Daeeef, Basir & Saudi 2017; Ghafir et al. 2018; McCumber 2004), and despite the amount of research in this area, the number of reported information security incidents is on the rise, and a significant part of said incidents is caused by employees’ behavior (Alshaikh et al. 2018). Moreover, organizations are facing great challenges in multiple aspects of deploying ISAT programs, and many of the programs used today are not based on empirical data, which greatens said challenges (Al-Daeeef, Basir & Saudi 2017; Alshaikh, Maynard, Ahmad & Chang 2018; Kävrestad & Nohlberg 2020c; Siponen & Willison 2009). This indicates the existence of a gap between the research community and practitioners, which has been known for a long time. The gap between research and practice hinders innovation and causes it to often fail, which creates a need for bidirectional translational development in order to bridge this “immense gap” (Norman 2010, p. 9).

3.2 Research Question

The research question addressed in this study is: what are the preferences and expectations of Nordic municipalities in regards to end-user ISAT?

As most surveys on security and awareness training focus on the end-user, one could argue that it is just as important to survey the organizations that are supposed to choose and deploy such training. Therefore, this study may shed a light on the organizational perspective, which is usually overlooked. This research project will examine multiple aspects of end-user ISAT in organizational settings. These aspects are listed below:

- The deployment time period of ISAT.
- The frequency of ISAT.
- The scope of ISAT.
- The delivery methods of ISAT.
- The enforcement of behavior based on ISAT.

3.3 Motivation

Research in the subject area is growing exponentially, yet the number of information security incidents using social engineering is growing exponentially as well (Abraham & Chengalur-Smith 2010; Bulgurcu, Cavusoglu & Benbasat 2010; Ghafir et al. 2018; Siponen, Mahmood & Pahnila 2014), thus more research into the problem area is required. However, research in the area of information technology tends to be on an abstract level that is not entirely applicable to production environments without translational development (Norman 2010). Therefore, this study is tackling the issue of end-user ISAT from a usually overlooked angle and investigating the perspective of organizations and practitioners in the field.
Additionally, it is established that ISAT should be provided to the end-user when it is the most relevant, meaning that it should be integrated into information systems as suggested by Kävrestad and Nohlberg (2020a). Therefore, security and awareness training for end-users is related to the area of Network and System Administration in two ways. The first is the comprehensive and integrated nature introduced by the context-aware training concept, making ISAT an integral part of information systems. The second way it relates to the area of Network and System Administration is security, as it addresses the issues of information security and the awareness of it for end-users, who are thought to be the weak link in the security chain (Kävrestad & Nohlberg, 2020c).

3.4 Delimitation

In this study, all municipalities in the Nordic countries—Denmark, Finland, Iceland, Norway, and Sweden—will be surveyed to obtain insight into the organizational perspective in regards to ISAT for end-users. The survey is focuses on municipalities in multiple countries to include as much data as possible, but those particular five countries were chosen for the—relatively—very small cultural differences among them as classified by World Values Survey Association (n.d.). Additionally, the Nordic countries have very similar national information security strategies and are member states in the European Economic Area, thus, sharing goals and visions Nøhr et al. 2020; Danish Ministry of Finance 2018; Finnish Ministry of Defence 2013; Icelandic Minister of the Interior 2015; Norwegian Ministry of Justice 2016). This was done to not influence the results by having an extra variable—cross-cultural differences—as cultural differences are a behavioral factor in regards to information security (Ndibwile, Luhanga, Fall & Kadobayashi 2019). Furthermore, neither central governmental nor private organizations are included in the survey, as these can have different—stricter—laws and policies about what information can be shared, and—in the case of the latter—can even be multinational corporations. This means they may have different enterprise cultures and laws from other countries to comply with. Combining all these factors with the immense differences between municipalities, government agencies, and enterprises makes these three into their own very distinct populations.

3.5 Expected Results

The contribution of this study is a better understanding of decision-making factors for Nordic municipalities in deploying end-user ISAT and the current state of affairs of ISAT in these municipalities. Furthermore, this study will paint a clearer picture of what is seen as ideal ISAT design from the perspective of Nordic municipalities. This information could prove useful for organizations in general to both precisely deepen and broaden their decision-making factors in the process of deploying such training. Furthermore, this study provides an insight into the thought process of planning, designing, and deploying an end-user ISAT program in an organizational setting. These contributions can be a source of enlightenment and help to both the researcher and practitioner communities in the field of end-user ISAT and may contribute to closing the gap between said communities.
4 Methodology

The purpose of this study is to investigate the organizational perspective of municipalities in five countries on ISAT. Moreover, the topic of information security is considered sensitive for an organization, and self-administered surveying—especially computer-assisted—is demonstrated to provide better data than interviews about sensitive issues (Fowler 2014). Therefore, an online survey is considered to be a suitable data collection method for this task. The online survey is intended to cover all municipalities in the Nordic countries, which results in 1123 total potential respondents—98 in Denmark, 310 in Finland, 69 in Iceland, 356 in Norway, and 290 in Sweden.

The rest of this section details the methodology used in this study including sampling, survey development, and methods of data analysis. Figure 2 illustrates the methodology design and provides an overview of the various steps involved.

![Figure 2 - Methodology design (the author’s own figure).](image)

4.1 Sampling

An online survey allows this study to include a large population, which is deemed necessary to gather an amount of data that is relevant. This study utilizes a probability-based total population sampling method, by including all the municipalities of five countries that are very culturally similar (World Values Survey Association n.d.). This sampling technique is based on two sampling methods—purposive and convenience sampling. Purposive sampling is considered to be “ideal for exploratory research design” and it is distinguished by choosing a sample with specific common characteristics (Taherdoost 2016, p. 23)—Nordic and municipalities in this case. Convenience sampling is based on the idea of reaching out to the whole population and allowing volunteers to choose to partake in the survey and it is also characterized by being a good sampling technique for exploratory research (Burdess 2010; Daniel & Cross 2018). It is important to note that the target population this study examines is the same as the sampled population—Nordic municipalities. As mentioned above, the sampling method deployed in this study combines two sampling methods, but the resulting sample is different from what these two methods can achieve if deployed separately. This difference is mainly characterized by sampling the whole target population, yet obtaining a chance-based sample. This sampling approach will result in a dataset that
is indicative of the organizational perspective of Nordic municipalities—and should not be generalized to other populations (Daniel & Cross 2018; Fowler 2014; Taherdoost 2016). This, however, is considered suitable as this study is considered a first-best effort to survey organizations on their perspective regarding ISAT, bridge the gap between research and practice, and fulfill the need for translational development between the two disciplines (Norman 2010). Information about names, number, and contacts to Nordic municipalities is acquired through different means—either free of charge or as a paid product in the case of Norwegian municipalities—as described below:

- The Association of Local Government Denmark\(^2\) for Danish municipalities.
- The Association of Finnish Municipalities\(^3\) for Finnish municipalities.
- The Icelandic Association of Local Authorities\(^4\) for Icelandic Municipalities.
- Kommuneforlaget AS\(^5\) for Norwegian municipalities.
- The Swedish Association of Local Authorities and Regions\(^6\) for Swedish municipalities.

### 4.2 Questionnaire Design

The survey consists primarily of two sets of questions with two distinct goals. The first set of questions focuses on the current state of affairs in the surveyed organizations in regards to ISAT, while the second set of questions focuses on the preferences of said organizations in regards to the general design of ISAT programs. The questions are designed based on conducting research into the area as presented in the Background section.

This study utilizes closed multiple-choice questions for the first set of questions, which is deemed as an appropriate question design for multiple reasons. Mainly, questionees may answer the same question differently if open questions are used—answering differently in this context means that questionees may understand the questions differently. Another reason is that asking respondents to answer with their own words without means of further clarification and two-way communication usually results in vague and incomplete answers that are difficult to code (Fowler 2014).

However, there are risks associated with closed questions as well, one of which is the possibility that none of the provided answer alternatives represents the answer a questionee wants to provide (Fowler 2014). This is dealt with by providing the “other” alternative, where a questionee can provide their own answer. With that said, there are many other factors to take into consideration when creating such questionnaires to avoid problems, such factors are systematically addressed in this survey, some of which are described in the following sections.

---

\(^2\) The Association of Local Government Denmark: https://www.kl.dk/english/

\(^3\) The Association of Finnish Municipalities: https://www.localfinland.fi/

\(^4\) The Icelandic Association of Local Authorities: https://www.samband.is/english/

\(^5\) Kommuneforlaget AS: https://www.kf.no/

\(^6\) The Swedish Association of Local Authorities and Regions: https://skr.se/tjanster/englishpages
The second set of questions consists of open questions in order to take advantage of the benefits provided by this question type. The first and most obvious advantage is acquiring unanticipated answers by letting the respondents describe their preferences and expectations in their own words (Fowler 2014). This is of great interest particularly because of the aforementioned gap between the practice and research communities (Norman 2010). The second advantage—which addresses an intrinsic problem of closed questions—is not imposing existing views on the participants and not allowing assumptions to guide them away from reality (Fowler 2014). The third advantage of having open questions is to avoid making participants frustrated, which can happen as a result of not being able to express their own views as they see them (Fowler 2014).

Utilizing both closed questions for the first set of questions and open questions for the second set of questions provides the ability to establish a common understanding of the general aim and tone of the survey among participants. This is done to ensure that participants have the same general overview of the survey, and is referred to as standardization. Further measures are taken in this study to ensure standardization and are presented in the following sections.

4.3 Standardization

It is important for a survey to ensure that all questionees will interpret questions the same way, otherwise, they will be answering—what to them are—different questions, which results in unreliable data (Berndtsson, Hansson, Lundell & Olsson 2008). This is known as standardization and it is of high importance for a questionnaire to be standardized and tested before a survey is carried out (Fowler 2014). This problem is mitigated through term definitions and exemplification, i.e., defining terms used in questions and answers that may bear different meanings to different respondents, which should ensure that all questionees come to the same understanding of a particular question or answer (Fowler 2014). Furthermore, redundant parenthetical information is provided to respondents throughout the questionnaire to ensure that their interpretations of questions and answers are the way they were intended correctly and fully.

A multinational survey that encompasses countries with different official languages introduces a risk of misinterpreting questions written in a non-native language (Fowler 2014). This is dealt with by professional proof-reading and translation into five Nordic languages to eliminate language as a variable in the understanding of the survey. The last measure undertaken before sending out survey invitations is pilot testing, which is done iteratively and systematically in this study both before and after the translation as described in the Pretesting section.

4.4 Instrumentation

One clear advantage of using an online questionnaire is being able to reach a large number of organizations with limited means (Berndtsson et al. 2008). However, many other advantages are rarely possible with other methods of data collection. Such is the ability to complete a questionnaire later, which is important in this context as some questions may require checking records or consulting with others at the organization (Fowler 2014). Additionally, not all questions apply to all respondents, e.g., organizations that do not currently have ISAT for end-users will not be able to answer questions about current methods—as none exists (Fowler 2014). This is dealt with through questionnaire logic—also known as conditions, where respondents are shown questions based on previous answers. Another advantage is the inclusion of a linear progress bar with a completion percentage indicator, which gives the respondents an overview of the questionnaire as a whole and has been shown to reduce the number of non-answers—especially with the
inclusion of the percentage indicators (Couper, Traugott & Lamias 2001; Li, Liu, Ji & You 2021). Although other progress bar techniques that yield a higher completion rate exist, a linear progress bar, i.e., shows the actual survey progress, is used as it is the most ethical method (Villar, Callegaro & Yang 2013). In order to further increase participation, participants are assigned tokens, based on which reminders will be sent out, and said tokens are embedded into invitation links (Crawford, Couper & Lamias, 2001). The survey instrument used in this study is LimeSurvey\footnote{LimeSurvey: https://www.limesurvey.org/}, for its high customizability and functionality in such a survey and for meeting all requirements set in this research methodology.

4.5 Questionnaire Validity and Reliability

In a self-administered online questionnaire, numerous factors threaten the validity and reliability of provided answers. While validity is defined as what is actually measured in contrast to what is intended to be measured, reliability is defined as the accuracy of the measurement and robustness of the measurement method (Berndtsson et al. 2008). In this work, validity and reliability threats are discussed throughout the Methodology section. However, further threats are provided in this section, followed by solutions to increase the validity and reliability of the collected data and by extension this work as a whole.

Bias is a major issue in this type of questionnaire and can result in respondents shaping their answers to satisfy the survey administrator, which results in unreliable data that is unrepresentative of reality (Fowler 2014). In this study two techniques, which are known for reducing this form of bias, are employed to deal with this issue. The first technique is presenting answer alternatives in random order, by leveraging a function in the questionnaire instrument. The second technique is the use of neutral wording that is free of judgment and opinion; in order to avoid guiding respondents in one way or the other without the mention of any specific ISAT programs (Fowler 2014).

Besides asking respondents the same questions, it is vital to ensure that a question means the same to all respondents. Otherwise, questionees will be answering—what to them are—different questions (Fowler 2014). To deal with this potential issue, general terms that are widely understood are used, which is important even if the respondents are well-educated on the subject (Fowler 2014). In order to make questions even clearer, terms are defined and exemplified where it is appropriate, and the kind of an appropriate answer is communicated to the respondent throughout the questionnaire with explanations of what answer alternatives exactly mean.

The use of general and easy-to-understand terms without any specific newly developed end-user ISAT programs has two more rationales to avoid two potential issues. The first is to avoid what is known as the First Order of Ignorance—lack of knowledge, which refers to the participants not knowing enough about the subject to understand terms commonly used in the research community (Armour 2000). The second rationale is to avoid what is known as the Second Order of Ignorance—lack of awareness, which refers to the participants not knowing enough about the subject to know what they can know (Armour 2000). This is of great concern especially in online questionnaires, due to the survey designer not knowing the individuals who can potentially participate in the questionnaire (Fowler 2014).
As this study is set out to cover municipalities in five countries an issue of language barriers becomes of concern, as it introduces a risk of respondents misinterpreting questions (Fowler 2014). However, the questionnaire is written first in English and then professionally translated into five additional languages—Danish, Finnish, Icelandic, Norwegian, and Swedish—by TransPerfect to further ensure respondents’ correct interpretations of questions.

Compound questions, i.e., questions with multiple question elements, are confusing to questionees and result in unreliable data. This is caused by merging two or more questions into one, and a questionee may have different answers to the different questions that make up a compound question (Fowler 2014). This is eliminated by ensuring that each question asks the questionees about one particular thing, irrelative of the simplicity of said thing.

Furthermore, assumptions in questions have a similar effect to compound questions, as they merge two elements, with the difference of not even allowing the respondent to provide an answer to the subject of the assumption. This happens when a question imposes an opinion on respondents, while simultaneously asking about something else starting from said assumption. However, it is likely that not all respondents have the same opinion, and not all their opinions are known (Fowler 2014). Therefore, the logic function of the online survey instrument is leveraged to tailor questions to participants based on their previous answers and not on assumptions.

Besides allowing participants to pause and continue with the questionnaire at a later time, the survey gives participants the ability to correct previous answers for the duration of the survey. This is done to ensure response correctness and avoid incorrect answers caused by honest mistakes, lack of knowledge, or poor information recollection (Fowler 2014).

Another issue of an online self-administered questionnaire is low response rate as participants motivation tends to be low (Berndtsson et al. 2008), which is dealt with—among other previously presented techniques—through providing respondents with information regarding the potential benefits of participation (Fowler 2014), i.e., the importance of a good understanding of the organizational perspective on information awareness training amongst researchers to tailor future programs to correspond with the acquired knowledge about organizational needs.

### 4.6 Ethics

Fowler (2014, p. 144) states that “researchers have an ethical responsibility to all those who participate in their projects” and in this study, multiple steps and measures are taken to ensure the ethical responsibility involved. As this study includes a survey, the most important ethical aspect that should be addressed first is informed consent (Fowler 2014; Wohlin et al. 2012). Participants in this study are under no circumstances to partake in the survey before receiving, understanding, and consenting to the information and rules provided to them. Said information includes the person carrying out the study and the research supervisor and their contact details. Further, participants are provided with information about the reason for the study and collection of data, the approximated time and the deadline for participating in the survey, and which organization is the study carried out for—the University of Skövde in this case. Rules of the data collection include voluntary participation, total anonymity, destruction of data at the end of the study, and no publishing of the complete data set.

Other important rules that participants are informed about include not collecting any personal information, only the researcher has access to the responses, participants are free to skip any
questions they do not want to answer, and not participating has no consequences (Wohlin et al. 2012). Furthermore, survey data is encrypted both under transmission and in storage, answer alternatives are randomized to minimize bias, no assumptions or judgments are made in any question, and general unguiding wording is used for all questions (Fowler 2014). Additionally, participants are provided with a guarantee that the collected data is not manipulated or misrepresented in any way, shape, or form.

Participants are also made aware of the ways and rules of the instrumentation, where participants can start the survey whenever they want within the allowed duration, they can stop the survey whenever they want, they can pause the survey whenever they want, they can complete a paused survey whenever they want within the allowed duration, and they can delete their answers entirely if they change their mind about participating.

4.7 Pretesting

In order to ensure the validity and reliability of the survey—and by extension the quality of collected data and this study as a whole—it is important to carry out rigorous testing of the questionnaire before deploying it (Fowler 2014). Firstly, a draft is established and then checked against the previous sections and adjusted accordingly. Secondly, the questionnaire is presented to the research supervisor, who gives feedback on the questionnaire, which is then adjusted accordingly. Thirdly, using the survey instrument the questionnaire is presented to a non-IT professional focus group of two individuals—one of which is a statistics expert—who give feedback on the questionnaire, which is then adjusted accordingly. Fourthly, using the instrument the questionnaire is presented to an IT-professional in person, who answers the questionnaire while thinking aloud and gives feedback at the end. Fifthly, the questionnaire is sent out through the survey instrument to seven individuals from different countries with different IT-proficiency, who give feedback, which is then incorporated into the questionnaire. Sixthly, the logic function of the questionnaire is tested to ensure correct behavior. These steps are revisited at least three times and the questionnaire is revised until all feedback is positive, and only then is the survey deemed ready to be sent out. Throughout the pretesting process, answer timings were logged, to be then communicated to the actual participants in the invitations.

4.8 Analysis

Analyzing the collected data in this study consists of two parts, as it combines both closed and open questions. The first set of questions is statistically analyzed, while the second set of questions is thematically analyzed. Although the steps of these analysis methods are similar, there are distinct differences. While statistical analysis tends to be a linear process, thematic analysis is an inherently nonlinear and iterative process (Creswell & Clark 2018).

4.8.1 Statistical Analysis

The first set of questions in the survey divides the participants into three groups, which are (a) municipalities that currently have ISAT, (b) municipalities that have had ISAT in the past, and (c) municipalities that have never had ISAT. Categorical descriptive statistical analysis is applied to the collected answers to the first set of questions. This provides the ability to use estimation—an inferential statistical technique—in combination with sample proportions as the best single estimates or point estimates of the true population proportions to interpret relevant data (Burdess 2010). Furthermore, having the same sampled population as the target population in this study
means that statistical inference can be used to reach conclusions about the target population based on the sampled population (Daniel & Cross 2018).

Therefore, three questions about the collected data are answered, the first question is (i) How representative the estimated proportions are of the true proportions of the target population—a measure of confidence, the second question is (ii) “What is the most typical value?”—a measure of central tendency, and the third questions is (iii) “How typical is it?”—a measure of dispersion (Burdess 2010, p. 20; Daniel & Cross 2018).

The statistical analysis begins with presenting statistical standardizations—summaries—of the responses in the form of percentages with the corresponding standard errors given by the following equation (Burdess 2010; Daniel & Cross 2018):

$$
\sigma_{\hat{p}} = \frac{2}{\sqrt{N}} \frac{\hat{p} q}{n} \frac{(N - n)}{(N - 1)} + \frac{2}{n} \frac{\hat{p} (1 - \hat{p}) (N - n)}{(N - 1)}
$$

Here, $\sigma_{\hat{p}}$ is the standard error of the percentage $\hat{p}$, $\hat{p}$ is the proportion of a sample of a population, $q$ is the probability of failure, and $n$ is the sample size. FPC is the finite population correction, where $N$ is the population size—number of Nordic municipalities. Utilizing the standard error, the confidence interval—“probabilistic estimate of the true population mean or proportion based on the data sample”—is calculated (Rea & Parker 2014, p. 312). The confidence interval for a proportion is calculated using the following formula (Daniel & Cross 2018):

$$
CI = \hat{p} \pm z_{(1 - \alpha/n)} \times \sigma_{\hat{p}}
$$

$$
CI = \hat{p} \pm z_{(1 - \alpha/n)} \frac{2 \hat{p} (1 - \hat{p}) (N - n)}{n}
$$

Here, $CI$ is the confidence interval and $z_{(1 - \alpha/n)}$ is the reliability coefficient—a standard normal random variable that defines the number of standard errors, within which lie 95% of all possible values of a point estimate $\hat{p}$. In this study, the chosen $\alpha$ value is 0.05 with a corresponding 0.95 confidence level, which has an associated reliability factor of $z_{(1 - \alpha/n)} = 1.96$. This combination of values is chosen as it is one of the “most frequently used” in research (Daniel & Cross 2018, p. 167).

Categorical data in this study are either nominal or ordinal. Nominal data has no built-in order of categories, this means that means and medians cannot be calculated. However, the modal category (mode) can be calculated and is used to answer the second question (ii), and is defined as the category with the largest number of individuals—municipalities in this case (Burdess 2010). Ordinal data has some generally agreed on order, which is decided on by giving the categories sequential numerical values when performing the analysis. This provides the ability to calculate the median, which answers the second question (ii). This is done according to the following formula (Burdess 2010):

$$
Med(x) = 0.5 \times (n + 1)
$$

Here, $Med(x)$ is the median of the dataset and $n$ is the number of values in the sample data. This formula is only applicable for a dataset with an odd number of values $n$. For even-numbered
datasets, the median is the mean of the two values at the middle of the dataset, but the mean of ordinal data cannot be calculated. This is simply solved by taking the lower of the two values at the middle of the dataset—omitting the +1—as shown below (University of Guelph n.d.):

\[ \text{Med}(x) = \frac{n}{2} \]

The third question (iii) is answered by calculating the variation ratio for nominal data. This is done using the following formula (Burdess 2010):

\[ VR = 1 - \frac{f_{\text{mode}}}{n} \]

Here, \( f_{\text{mode}} \) is the occurrence frequency of the mode category in the dataset—the number of participants whose answer is or included the mode category. The variation ratio reveals how dispersed the dataset is, where the greater the variation ratio is—the closer to 1, the more dispersed the data are across the categories. By extension, the lower the variation ratio is—closer to 0, the less spread the data are across the categories (Burdess 2010; Daniel & Cross 2018).

Answering the third question (iii) for ordinal data involves calculating the interquartile range, which is the middle 50% of the dataset, by subtracting the first quartile from the third quartile. The first quartile is the middle of the first half of the data, while the third quartile is the middle of the second half of the data—25% and 75% respectively (Burdess 2010; Daniel & Cross 2018). By extension, the second quartile is the middle point of the dataset, which is the median—50%.

The first and third quartiles and the interquartile range are calculated using the following formulas (Daniel & Cross 2018):

\[ Q_1 = \frac{n + 1}{4} \]
\[ Q_3 = 3 \times \frac{(n + 1)}{4} \]
\[ IQR = Q_3 - Q_1 \]

Here, \( Q_1 \) is the first quartile, \( Q_3 \) is the third quartile, \( IQR \) is the interquartile range, and \( n \) is the number of values in the dataset. As this formula is used in combination with ordinal data, there is a possibility that in some cases \( (n + 1) \) may not be evenly divisible by 4, in which case the lower of the two nearest values—natural number—in the dataset is chosen. This is the same technique used to mitigate a similar issue with the median as suggested by the University of Guelph (n.d.). The interquartile range is an indicator of the amount of variability in the middle half of the dataset, i.e., the lower the \( IQR \) is, the lower the variability is, and by contrast the higher the \( IQR \) is, the higher the variability is (Daniel & Cross 2018). However, the \( IQR \) itself is relative to the range of the complete dataset. Therefore, comparing the two ranges presents more meaningful and valuable information about the dataset than just presenting the \( IQR \) alone. The range is calculated using the following formula (Daniel & Cross 2018):

\[ R = x_L - x_S \]
Here, R is the range, \( x_L \) is the largest value, and \( x_S \) is the smallest value in the dataset. Comparing the IQR and R in this study is done by calculating the percentage of R that IQR represents, and is done using the following formula (Daniel & Cross 2018):

\[
IRR = \left(1 - \frac{IQR}{R}\right) \times 100
\]

Here, IRR is the percentage ratio of the interquartile range to the range of the entire dataset. This formula provides the percentage of R that IQR represents, where the higher the IRR is the less the variability in the dataset is.

4.8.2 Thematic Analysis

The second part of the survey consists of open questions, which results in free text that is subject to thematic analysis—also known as thematic coding. Thematic coding is defined as a “method for identifying, analyzing and reporting patterns (themes) within data” (Braun & Clarke 2006, p. 79). Flick (2014) describes thematic analysis as a data categorization strategy, which involves segmenting, categorizing, summarizing, and reconstructing data to highlight important aspects within the data (Flick 2014). A theme is a construct that captures an important concept about the data in relation to the research question and defines a pattern of sorts within a data set. Said patterns or themes can be extracted using one of two ways, inductive or deductive (Braun & Clarke 2006). This study utilizes a deductive approach, which has district characteristics deemed important for this study. The deductive approach—also known as top-down or theoretical—is characterized by the themes being strongly linked to the research question and the analysis being analyst-driven rather than data-driven (Braun & Clarke 2006). This is deemed appropriate for this study as the research question is clearly identified before the analysis process, which requires coding for a specific research question.

With that said, there are guidelines for thematic analysis in general and, for a theoretical approach in particular. A theoretical or deductive approach for thematic analysis requires “engagement with the literature prior to the analysis” (Braun & Clarke 2006, p. 86). This is achieved through the Background section. Generally, thematic analysis is—as mentioned before—an iterative nonlinear process that is recursive and requires flexibility and performing steps gradually through repetitions (Braun & Clarke 2006). Saldana states that even the identified codes themselves may be subject to change through iteration and that a thematic analysis should at least go through two iterations—or cycles (Saldana 2016). Furthermore, note-making—a part of the first step in thematic analysis—consists of three levels, where the first level is “what the text says”, which is just noting the text at face value. The second level is “what the text does” which is a description of the text that starts the reflection process. The third and final level of note-making is “what the text means in relation to your question” which is to extract relevant data for the research question of this work and to be included in the review (Jesson, Matheson & Lacey 2021, p. 59).

Braun and Clarke (2006) provide an outline of thematic analysis through six phases that are followed in this study. These six phases of thematic analysis are listed and described below.

“Familiarizing yourself with your data”, refers to the process of reading the data multiple times and making notes (Braun & Clarke 2006, p. 87). However, reading is not the only process to be
iterated in this step, since note-making is an iterative process with three levels as mentioned before (Jesson, Matheson & Lacey 2021).

“Generating initial codes”, refers to the activity of systematically identifying attributes that are interesting for the research question throughout the dataset and combining relevant data (Braun & Clarke 2006, p. 88).

“Searching for themes”, this phase entails combining all previously generated codes into potential themes and gathering data relevant to all potential themes (Braun & Clarke 2006, p. 89).

“Reviewing themes”, this phase involves two levels, where it begins by ensuring that the drafted themes work with the data extracts or notes—level one. The second level of this phase includes checking the validity of the drafted themes against the whole dataset (Braun & Clarke 2006, p. 91).

“Defining and naming themes”, this phase involves defining and refining the previously identified themes and describing what aspects of the dataset each theme captures (Braun & Clarke 2006, p. 92).

“Producing the report”, this phase includes the final analysis of data extracts, identifying data examples that best represent each theme, and relating the analysis to the research question, as well as presenting the analysis in a scholarly report (Braun & Clarke 2006, p. 93).

4.9 Analysis Validity and Reliability
This section presents the potential threats to the validity and reliability of the analysis, followed by measures taken to mitigate said threats and assure the quality of the analysis.

4.9.1 Statistical Analysis
There will always be some amount of variation between the true population proportions and the sample proportions. However, some measures can be taken to minimize said variation, which ensure the validity of the analysis (Berndtsson et al. 2008; Burdess 2010; Daniel & Cross 2018).

The randomness of the sample is an essential condition for the analysis to be meaningful and representative of the true population proportions (Daniel & Cross 2018). In this study, all members of the target population are invited to voluntarily participate in the survey, which introduces an element of randomness to the sample.

Another important factor that must be met is for the sampling distribution of the sampling proportions to be normal. Daniel & Cross (2018) state that when the sample size $n$ is large, “the distribution of sample proportions is approximately normally distributed”. There are two conditions that have to be met in order to consider a sample large enough and by virtue, the sample means to be approximately normally distributed, the two conditions are (Daniel & Cross 2018, p. 151):

$$np > 5 \land n(1 - p) > 5$$
Here, $n$ is the sample size and $p$ is the true population proportion. With that said, the true population proportion is unbeknownst, hence this study. However, the central limit theorem allows sampling from a population with an unknown distribution, while guaranteeing approximately the same sampling distribution of the sample mean if the sampling is applied to a normally distributed population. This is true so long as the sample size is large enough, and a sample size of 30 is considered to be satisfactory to the central limit theorem (Daniel & Cross 2018).

When sampling without replacement, independence becomes an issue as the sampling procedure affects any subsequent samplings by changing the population. This, however, can be avoided by following the 10% condition, that is, a sample should not exceed 10% of the total population (Bock n.d.). In this study the total sampled population is $N = 1123$ and a sample size of $n = 112$ or less meets the 10% condition.

The three aforementioned conditions of randomness, normality, and independence are considered to be met by first examining the collected data and trying to identify any patterns that might affect the randomness of the sample. This examination of the data should at least identify any issues regarding the randomness of the sample. To meet the second and third conditions the sample size has to fall in a specific range within the sampled population, these conditions are summarized as follows:

$$30 \leq n \land n \leq \frac{N}{10}$$

Meeting these conditions while having a sampled population that is the same as the target population provides the ability to confidently use statistical inference and reach conclusions based on the sample data collected through the survey (Daniel & Cross 2018). However, some questions in the survey apply to small numbers of participants, which breaches the foretasted conditions by having a sample $n$ of less than 30. In this case, the following conditions are applied to the data subset to check if the normality assumption holds or not (De Veaux, Velleman & Bock 2017):

$$n q \geq 10 \land n \hat{p} \geq 10$$
$$n (1 - \hat{p}) \geq 10 \land n \hat{p} \geq 10$$

In this case, the normality assumption falls and the distribution is assumed to be binomial, where Wilson score interval is calculated and the confidence interval is given by the following formula (Wilson 2012):

$$CI = \hat{p} + z(1 - a/n)^2/2n \pm z(1 - a / 2n)^{1/2} \sqrt{\hat{p}(1 - \hat{p}) / n + z(1 - a / 2n)^2 / 4n^2}$$

Additionally, the first question to be answered through the statistical analysis identifies the confidence interval of the proportions of the dataset in relation to the sampled population with a 95% confidence level. This step ensures that the proportions observed through the survey are representative of the sampled population with a 95% confidence level.

Another important validity factor related to data representation is not being misleading. This can happen for example with column plots, where values presented on the $y$-axis do not display the whole range, which can even happen with automated tools (Berndtsson et al. 2008). Therefore,
data representation in this study is done carefully to prevent misinterpretation and deception and to ensure a common correct understanding among readers.

4.9.2 Thematic Analysis

There are several pitfalls that should be avoided when performing thematic analysis for said analysis to not be poor (Braun & Clarke 2006). A great risk is not actually analyzing the data, which can stem from not interpreting data extracts sufficiently. Data extracts should be analyzed and not just taken at face value, i.e., the analysis should go beyond what the extracted data is and interpret it in relation to the research question (Braun & Clarke 2006).

Although there is no clear definition of what constitutes a theme, simply converting the questions used to acquire the dataset does not allow for deep analysis. This is true due to the fact that a thematic analysis spans the whole dataset in order to identify interesting patterns in relation to the research question (Braun & Clarke 2006).

Another pitfall is the failure of encompassing the majority of the dataset in the identified themes. This occurs when the identified themes are decoupled from the dataset or when sufficient thematic examples from the data are not provided or not existent. The result of such poorly constructed thematic analysis is an unconvincing and anecdotal analysis—where a few weak phenomena are “reified” into inaccurate themes or patterns (Braun & Clarke 2006, p. 95).

Furthermore, a mismatch between the dataset and the analysis results in a weak analysis that is built on unfounded claims, where the data either does not support the analytical claims or completely contradicts them. Consistency between the collected data and any analytical claims made about said data prevents this problem. Therefore, considering alternative interpretations of the dataset is essential in the process of performing an accurate thematic analysis (Braun & Clarke 2006). Another mismatch that will result in a failure, is between analytical claims and the research question. Therefore, an accurate thematic analysis should be consistent with the theoretical setting of the study and should be related to and address the research question (Braun & Clarke 2006).

Additionally, any good analysis should always clarify the way it was carried out and any assumptions that are made as a starting point or taken under the analysis and the rationale behind said assumptions (Braun & Clarke 2006).
5 Results and Analysis

An invitation to the survey—shown in Figure A-1 under Appendix A—was sent out on a Sunday evening and two weeks later a reminder—shown in Figure A-2 under Appendix A—was sent out to municipalities that had not participated yet. Thereafter, the survey, which is presented in Appendix A (Figure A-4 to Figure A-17), was available for one more week, making the period of data collection three whole weeks. This resulted in 96 respondents covering 136 Nordic municipalities as several municipalities can have a joint IT-department. The majority of the responses came from Swedish municipalities and the spread of the results is shown in Table 1.

<table>
<thead>
<tr>
<th>Country</th>
<th>Total number of municipalities</th>
<th>Number of responses</th>
<th>Number of municipalities covered</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denmark</td>
<td>98</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>Finland</td>
<td>310</td>
<td>6</td>
<td>14</td>
</tr>
<tr>
<td>Iceland</td>
<td>69</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>Norway</td>
<td>356</td>
<td>10</td>
<td>23</td>
</tr>
<tr>
<td>Sweden</td>
<td>290</td>
<td>70</td>
<td>89</td>
</tr>
<tr>
<td>Total</td>
<td>1123</td>
<td>96</td>
<td>136</td>
</tr>
</tbody>
</table>

Table 1 - Spread and coverage of survey responses (the author’s own table).

This yielded a set of results that are more representative of Swedish municipalities than the rest of the Nordic municipalities, which means that it should be interpreted as such. The reason for this spread is uncertain but it might be contributed to Swedish municipalities knowing about the institute where this study is carried out, thus trusting the source of the survey more than the rest of the Nordic municipalities.

5.1 Closed Questions

After the three weeks data collection period, the data were downloaded from the survey instrument directly into SPSS 27. SPSS was used to calculate frequencies for the first set of questions because it preserved the logic of the survey, where participants were asked questions based on their previous answers. Then a custom Python program was developed and used to calculate the proportion and the standard error, margin of error, and confidence interval of each proportion with a confidence level of 95% along with further statistical tests for both nominal and ordinal data according to the formulas presented in section 4. All participants were asked whether they currently offer ISAT or not and those who answered that they do not currently offer training were asked if they have offered it in the past and if they were planning to offer it in the future. Table 2 shows the results of these questions, where over 70% of respondents answered that they offer ISAT and of those municipalities that do not offer it 50% have offered it in the past and over 96% are planning to offer it in the future. This shows that the majority of Nordic municipalities are aware of the importance of ISAT for end-users in relation to the information security of their organizations as a whole.

<table>
<thead>
<tr>
<th>Answer</th>
<th>Proportion</th>
<th>Standard error</th>
<th>Confidence interval</th>
<th>Modal</th>
<th>Variation ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes – currently</td>
<td>70.83%</td>
<td>4.43</td>
<td>62.13, 79.53</td>
<td>X</td>
<td>0.29</td>
</tr>
<tr>
<td>No – currently</td>
<td>29.16%</td>
<td>4.43</td>
<td>20.46, 37.86</td>
<td>X</td>
<td>0.29</td>
</tr>
<tr>
<td>Yes – in the past</td>
<td>50%</td>
<td>9.33</td>
<td>31.70, 68.29</td>
<td>X</td>
<td>0.5</td>
</tr>
<tr>
<td>No – in the past</td>
<td>50%</td>
<td>9.33</td>
<td>31.70, 68.29</td>
<td>X</td>
<td>0.5</td>
</tr>
<tr>
<td>Yes – in the future</td>
<td>96.42%</td>
<td>3.46</td>
<td>82.28, 99.36</td>
<td>X</td>
<td>0.03</td>
</tr>
<tr>
<td>No – in the future</td>
<td>3.57%</td>
<td>3.46</td>
<td>0.633, 17.71</td>
<td>X</td>
<td>0.03</td>
</tr>
</tbody>
</table>

Table 2 - Results of questions about offering ISAT (the author’s own table).
Participants who currently offer ISAT or have offered training in the past were asked about the training deployment period—the number of years they have been offering or offered training. The results of these questions are shown in Figure 3 with a deeper data presentation provided in Table 3.

<table>
<thead>
<tr>
<th>State</th>
<th>Modal</th>
<th>Median</th>
<th>R</th>
<th>IQR</th>
<th>IRRP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Currently offering</td>
<td>1 – 3 years</td>
<td>1 – 3 years</td>
<td>Less than 1 year → More than 5 years</td>
<td>Less than 1 year</td>
<td>67</td>
</tr>
<tr>
<td>Offered in the past</td>
<td>Less than 1 year &amp; 1 – 3 years</td>
<td>Less than 1 year</td>
<td>1 – 3 years</td>
<td>Less than 1 year</td>
<td>100</td>
</tr>
</tbody>
</table>

Table 3 - ISAT deployment period (the author’s own table).

Looking at the proportions from Figure 3 reveals an interesting observation, which is that municipalities that have offered training in the past did so for at most 3 years, whereas municipalities that currently offer training are included in the whole range of between less than one year and more than five years. This means that municipalities that offer training for over three years are more likely to continue doing so.

When asked about the general attitude of their trainees, the participants reported mostly positive attitude followed by indifferent and very low percentages of negative attitude. This was the case for both municipalities that currently offer training and municipalities that have offered training in the past as shown in Table 4. This can help greatly in sustaining training in municipalities as user attitude, compliance, and acceptance are of major concern in relation to ISAT for end-users (Bada, Sasse & Nurse 2015; Siponen, Mahmood & Pahnila 2014).

<table>
<thead>
<tr>
<th>Answer</th>
<th>Proportion</th>
<th>Standard error</th>
<th>Confidence interval</th>
<th>Modal</th>
<th>Variation ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Positive – currently</td>
<td>61.76%</td>
<td>5.714</td>
<td>50.56, 72.96</td>
<td>X</td>
<td>0.38</td>
</tr>
<tr>
<td>Indifferent – currently</td>
<td>32.35%</td>
<td>5.501</td>
<td>21.57, 43.13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negative – currently</td>
<td>1.47%</td>
<td>1.415</td>
<td>0.260, 7.871</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Positive – in the past</td>
<td>64.28%</td>
<td>12.73</td>
<td>38.76, 83.65</td>
<td>X</td>
<td>0.35</td>
</tr>
<tr>
<td>Indifferent – in the past</td>
<td>28.57%</td>
<td>12</td>
<td>11.72, 54.64</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Negative – in the past</td>
<td>0%</td>
<td>0</td>
<td>0.0, 21.53</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4 - Attitude of trainees towards ISAT (the author’s own table).
All participants were asked if they classify, classified, or will be classifying ISAT as mandatory for their users and their answers were significantly spread out across the available alternatives—yes, partially, and no—as seen in Table 5. This reveals the existence of conflicting views amongst participants—especially those currently offering training. There is no obvious reason for why such a conflict in views exists, but an educated assumption can be the difficulty of finding the right balance between persuading and mandating users to participate in training activities. However, the literature is quite clear about the importance of persuading users and enriching their understanding of the importance of training and what it contributes to them and their organizations (Bada, Sasse & Nurse 2015; Desman 2003; Siponen, Mahmood & Pahnila 2014; Wolf, Haworth & Pietron 2011).

<table>
<thead>
<tr>
<th>Answer</th>
<th>Proportion</th>
<th>Standard error</th>
<th>Confidence interval</th>
<th>Modal</th>
<th>Variation ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes – currently</td>
<td>33.82%</td>
<td>5.56</td>
<td>22.91, 44.72</td>
<td>X</td>
<td>0.64</td>
</tr>
<tr>
<td>Partially - currently</td>
<td>30.88%</td>
<td>5.43</td>
<td>20.23, 41.53</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No – currently</td>
<td>35.29%</td>
<td>5.61</td>
<td>24.27, 46.30</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Yes – in the past         | 14.28%     | 9.29           | 4.009, 39.94        | X     | 0.5             |
| Partially – in the past   | 50%        | 13.28          | 26.79, 73.20        |       |                 |
| No – in the past          | 35.71%     | 12.73          | 16.34, 61.23        | X     | 0.5             |

| Yes – in the future       | 37.03%     | 9.18           | 19.03, 55.03        | X     | 0.62            |
| Partially – in the future | 37.03%     | 9.18           | 19.03, 55.03        | X     | 0.62            |
| No – in the future        | 11.11%     | 5.97           | 3.851, 28.05        |       |                 |

Table 5 - Results of question about whether training is mandatory or not (the author’s own table).

Two further questions applied to all participants the first was whether municipalities enforce, enforced, or will enforce secure user behavior based on the training, and the second question applied if the answer to the first was either “yes” or “partially” and it asked the participants about the methods of enforcing secure user behavior. Results of the first question are presented in Table 6 and the results of the second question are presented in Figure 4.

<table>
<thead>
<tr>
<th>Answer</th>
<th>Proportion</th>
<th>Standard error</th>
<th>Confidence interval</th>
<th>Modal</th>
<th>Variation ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes – currently</td>
<td>51.47%</td>
<td>5.87</td>
<td>39.95, 62.98</td>
<td>X</td>
<td>0.48</td>
</tr>
<tr>
<td>Partially - currently</td>
<td>36.76%</td>
<td>5.66</td>
<td>25.65, 47.87</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No – currently</td>
<td>11.76%</td>
<td>3.78</td>
<td>6.083, 21.53</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Yes – in the past         | 42.85%     | 13.14          | 21.38, 67.40        | X     | 0.57            |
| Partially – in the past   | 28.57%     | 12             | 11.72, 54.64        |       |                 |
| No – in the past          | 28.57%     | 12             | 11.72, 54.64        |       |                 |

| Yes – in the future       | 40.74%     | 9.34           | 22.42, 59.05        | X     | 0.59            |
| Partially – in the future | 11.11%     | 5.97           | 3.851, 28.05        |       |                 |
| No – in the future        | 0%         | 0              | 6.938, 12.45        |       |                 |

Table 6 - Enforcing secure user behavior based on ISAT (the author’s own table).

In the question presented in Table 6 participants could choose one of the alternatives and all alternatives that applied in the question presented in Figure 4 with the possibility of providing their own answer as “other” if none of the alternatives applied or another that applied did not exist in the provided list. The majority of respondents answered “yes” to enforcing secure user behavior followed by “partially”, which is in line with what the literature suggests (Bada, Sasse & Nurse 2015; Wolf, Haworth & Pietron 2011).
Observing Figure 4 reveals that respondents who answered “yes” or “partially” to enforcing secure user behavior mostly see all presented methods to be effective.

![Methods of enforcing secure user behavior](image)

Figure 4 - Methods of enforcing secure user behavior (participants could chose more than one alternative) (the author’s own figure).

This is backed by research as well, where using one method of enforcement is considered good, and combining several methods is regarded as optimal (Bada, Sasse & Nurse 2015; Wolf, Hawthor & Pietron 2011). Further statistical details about the question regarding enforcement of secure user behavior are shown in Table 7.

<table>
<thead>
<tr>
<th>Answer</th>
<th>Proportion</th>
<th>Standard error</th>
<th>Confidence interval</th>
<th>Modal</th>
<th>Variation ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware – currently</td>
<td>45%</td>
<td>6.251</td>
<td>32.74, 57.25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software - currently</td>
<td>50%</td>
<td>6.282</td>
<td>37.68, 62.31</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Written – currently</td>
<td>58.33%</td>
<td>6.195</td>
<td>46.19, 70.47</td>
<td>X</td>
<td>0.41</td>
</tr>
<tr>
<td>Other – currently</td>
<td>5%</td>
<td>2.738</td>
<td>1.714, 13.70</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware – in the past</td>
<td>20%</td>
<td>12.59</td>
<td>5.668, 50.98</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software – in the past</td>
<td>70%</td>
<td>14.43</td>
<td>39.67, 89.22</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Written – in the past</td>
<td>90%</td>
<td>9.448</td>
<td>59.58, 98.21</td>
<td>X</td>
<td>0.09</td>
</tr>
<tr>
<td>Other – in the past</td>
<td>10%</td>
<td>9.448</td>
<td>1.787, 40.41</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware – in the future</td>
<td>78.57%</td>
<td>10.9</td>
<td>52.41, 92.42</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software – in the future</td>
<td>64.28%</td>
<td>12.73</td>
<td>38.76, 83.65</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Written – in the future</td>
<td>85.71%</td>
<td>9.297</td>
<td>60.05, 95.99</td>
<td>X</td>
<td>0.14</td>
</tr>
<tr>
<td>Other – in the future</td>
<td>14.28%</td>
<td>9.297</td>
<td>4.009, 39.94</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 7 - Methods of enforcing secure user behavior (participants could chose more than one alternative) (the author’s own table).

Municipalities that have offered ISAT in the past but do not anymore were asked about the reasons behind stopping the training. In this question, participants were able to choose multiple reasons and even provided reasons of their own. The reasons are presented in Figure 5 with respective proportions and Table 8 presents deeper statistical details.

<table>
<thead>
<tr>
<th>Answer</th>
<th>Proportion</th>
<th>Standard error</th>
<th>Confidence interval</th>
<th>Modal</th>
<th>Variation ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>42.85</td>
<td>13.14</td>
<td>21.58, 67.40</td>
<td>X</td>
<td>0.57</td>
</tr>
<tr>
<td>No need to train other users</td>
<td>7.142</td>
<td>6.843</td>
<td>1.272, 31.46</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Logistics</td>
<td>35.71</td>
<td>12.73</td>
<td>16.34, 61.23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User resentment</td>
<td>14.28</td>
<td>9.297</td>
<td>4.009, 39.94</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training results were not satisfied</td>
<td>21.42</td>
<td>10.9</td>
<td>7.571, 47.58</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>21.42</td>
<td>10.9</td>
<td>7.571, 47.58</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 8 - Reasons for stopping ISAT (participants could chose more than one alternative) (the author’s own table).
The majority of participants who chose the “other” option gave managerial resentment as a reason for stopping the training and the rest who chose “other” stated that it was a temporary stop and that they are planning to start the training again. Managerial acceptance and support of ISAT is mentioned extensively in both the early and recent research literature and is considered essential in the success of ISAT campaigns (Ghafir et al. 2018; Siponen 2001; Siponen, Mahmood & Pahnila 2014). Figure 5 shows that training cost and logistics are the most cited reasons for stopping training, which relates to the previous point of managers being on board with ISAT and their willingness to invest in it and provide the required resources. This is followed by unsatisfactory training results, which can be related to existing training programs not being supported by empirical data (Al-Daeef, Basir & Saudi 2017; Alshaikh, Maynard, Ahmad & Chang 2018; Kävrestad & Nohlberg 2020c; Siponen & Willison 2009).

![Figure 5 - Reasons for stopping ISAT](attachment:figure5.png)

Participants who answered that they currently offer ISAT were asked multiple questions to further understand the current state of training in Nordic municipalities. Table 9 presents the results of a question about the origin of the training programs used at Nordic municipalities that currently offer ISAT, where the answer alternatives were either yes or no meaning that it is either developed in-house or not. Reading the results reveals that the majority of participants who offer training do so using programs that are not developed in-house. This means that such programs and frameworks are likely to be fallible due to them being too general and generic without much attention paid to the different and unique security needs and requirements of different organizations (Siponen & Willison 2009).

<table>
<thead>
<tr>
<th>Answer</th>
<th>Proportion</th>
<th>Standard error</th>
<th>Confidence interval</th>
<th>Modal</th>
<th>Variation ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes – developed in-house</td>
<td>35.29%</td>
<td>5.61</td>
<td>24.27, 46.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>64.7%</td>
<td>5.61</td>
<td>53.69, 75.72</td>
<td>X</td>
<td>0.35</td>
</tr>
</tbody>
</table>

Table 9 - Results of the question about whether the training programs used in Nordic municipalities are developed in-house or not (the author’s own table).
Furthermore, Figure 6 shows the results of a question about the content of the training, where participants could choose one out of four alternatives. These alternatives are: (i) all potential information security threats that end-users can be vulnerable to, (ii) only the threats that have the greatest impact on the information assets of the organization, (iii) only the threats that are most likely to occur regardless of their impact severity, and (iv) only the threats that are most likely to occur and have the greatest impact on the information assets of the organization. From Figure 6 an observation is that most participants include information about all potential information security threats that end-users can be vulnerable to in their ISAT. However, the literature advises against such practices and emphasizes the importance of the training content being concise and relevant to the users. Simply, storming users about all potential threats can result in undesired outcomes and possibly orientate users in the wrong direction because they tend to ignore irrelevant and too frequent information. This in combination with the users not being information security experts can lead to them ignoring important information just to be able to cope with the amount of information they are provided (Al-Daeef, Basir & Saudi 2017; Desman 2003; Kävrestad & Nohlberg 2020c; Siponen 2001).

Participants who answered that they provide ISAT to their users were asked two questions about users covered by the training. The first question was “Does the ISAT at your organization cover all IT users?” and the second question was “Does your organization offer ISAT for new employees as a part of their organizational introduction or orientation?”. The results from these two questions are presented in Table 10, where the majority of participating Nordic municipalities provide training to all of their users and new employees as part of onboarding. Although the majority of users are covered, researchers emphasize the importance of covering all users of IT (Bada, Sasse...
The lack of training for some users can be—at least partially—attributed to the idea that only small parts of the training are relevant to all users, while the rest of the training should target specific groups of users. This can be dealt with by deploying relevant or context-aware training and providing trainees with the ability to—at least partially—skip parts of the training that are seen as irrelevant, especially repetitive information (Kävrestad & Nohlberg 2020c).

Those participants who offer ISAT but not to all their users were asked about which user groups they offer training to and why only said groups. Table 11 shows that the majority of the participants offer training to both IT-departments and non-IT-departments.

Table 12 reveals that the most reported reasons for not offering training to all users in participant Nordic municipalities are cost and logistics. Training can be particularly expensive and difficult to encompass all users when it is instructor lead or in the form of presentations. However, other methods of training delivery can cover large numbers of users without requiring huge resources, such as articles, videos, online training, and context-aware embedded training (Al-Daeef, Basir & Saudi 2017; Ghafir et al. 2018; Kävrestad & Nohlberg 2020c).

Respondents who reported that they currently provide ISAT were asked about the frequency of training and as shown in Figure 7 the most predominant training frequency is once a year followed by less than once a year. This can have major implications and undesirable consequences as new attacks and viruses are not scheduled, which means that it is of great importance to keep users up-to-date on the latest and current security concerns and issues (Desman 2003). Furthermore, a study that aimed to measure user behavior and compliance with password policy showed that after four different interventions spanning six weeks the user compliance percentage rose from 44% to 60%, which implies that repetition is key to influence user behavior and ensure compliance (Wolf, H wast & Pietron 2011). Another study examining how well users retained training information after a period of one week using various training methods found that in the best-case scenario 64% of participants were successful in the test that followed the initial training by one week (Kumaraguru et al. 2007). Context-aware training takes the ISAT frequency to another level, where
it emphasizes that training should be a part of everyday tasks and does not need to be scheduled, where users go about their normal work activities and if the system detects a situation that warrants training or warning of sorts it provides it to the user right then and there (Ghafir et al. 2018; Kävrestad & Nohlberg 2020c). Providing training once a year—or less frequently for that matter—is considered to be inadequate as most users will most likely not be able to retain acquired knowledge for such a long period, which should be the main goal of ISAT in order to be effective

![Frequency of ISAT](image)

Figure 7 - Frequency of ISAT (the author's own figure).

Moreover, a question regarding the delivery methods of ISAT was asked to participants who currently offer training. Respondents were given six answer alternatives with an additional “other” alternative with the ability to provide their own methods. Respondents were asked to choose all alternatives that applied to them below is a list of the alternatives with clarification of what was meant with them:

- Oral informative (e.g., presentations, lectures)
- Written informative (e.g., articles, emails, manuals)
- Simulation or embedded (e.g., leverages existing systems to simulate attacks, e.g., phishing emails)
- Online (e.g., online test, videos, courses)
- Gamified (e.g., game-based training)
- Promotional (e.g., announcements, pop-ups, desktop backgrounds)
- Other
Figure 8 details the results from this question, where the most predominantly used training delivery method is online followed by oral informative, which slightly surpasses written informative. Online training has been shown to be an effective training method and it costs relatively very little, which explains the popularity of this method amongst respondents (Al-Daeef, Basir & Saudi 2017). Oral informative training is popular because it has been shown time and again to be effective, however, it is high-cost, and covering a large number of users is very time-consuming. The high cost of oral informative training in combination with its popularity can partially explain that almost 40% of respondents who currently offer ISAT do not cover all their users (Al-Daeef, Basir & Saudi 2017). A study that aimed to measure user behavior and compliance with password policy using four different training delivery methods showed that oral informative training in the form of a presentation was by far the most effective method in comparison to the three other methods (Wolf, Haworth & Pietron 2011). Written informative training is very popular and is used extensively in both the public and private sectors and has been proven to increase the trainees’ knowledge about information security (Al-Daeef, Basir & Saudi 2017).

![Delivery methods of ISAT](image_url)

Figure 8 - Delivery methods of ISAT (participants could chose more than one alternative) (the author’s own figure).
5.1.1 Dispersion

In this study two ways of measuring data dispersion were deployed. IRRP was used to measure dispersion in ordinal data, where no notable values were found. However, using variation ratio as a measure of dispersion in nominal data the two following cases of interest were observed:

i. Participants’ answers to the question of classifying ISAT as mandatory (Table 5). The reason for the data dispersion is unclear, but an educated guess can be the challenges associated with balancing between persuading and mandating users to participate in ISAT. However, this issue is settled in the literature. Research has shown that persuasion is better than mandating or scaring users into participating in ISAT. The reason is to minimize intrusiveness and presenting training as beneficial and not as a chore (Bada, Sasse & Nurse 2015; Desman 2003; Siponen, Mahmood & Pahnila 2014).

ii. Participants’ answers to the question of enforcing secure user behavior based in ISAT (Table 6). The reason for this dispersion can be partially explained by the answer alternatives that were provided to participants. The answer alternatives for this question were "yes", "partially", and "no" and the majority of participants answered using the first two. Yet, a relatively considerable minority answered no, thereby conflicting with recommendations in the literature. Research into the area is clear on the importance of secure behavior enforcement mechanisms (Wolf, Haworth & Pietron 2011).

5.2 Open Questions

The second set of questions contained open questions, which were asked to all participants to capture the perspective of all participating Nordic municipalities in their own words regarding the ideal state of ISAT. This set consisted of four questions, which were analyzed using thematic content analysis. The first question focused on key design factors of ISAT and the results of this question are presented in Table 13. The identified themes are presented with their relevant categories, which are aspects that were mentioned by respondents, alongside the number of times each category was mentioned. Reading the results from this question reveals that respondents desire frequent yet time-effective training programs, which relates to the need for a low-cost training solution that is available for users to take at their own pace. Further observations are the need for such a training program to contain relevant information that is concise and easy to understand while covering the majority of users and being—at least—partially compulsory.

<table>
<thead>
<tr>
<th>Theme</th>
<th>Category</th>
<th>Number of mentions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content related</td>
<td>Awareness increasing</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Concision</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Layman language</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Relevance</td>
<td>26</td>
</tr>
<tr>
<td>Financial</td>
<td>Cost effectiveness</td>
<td>12</td>
</tr>
<tr>
<td>Logistics</td>
<td>Availability</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Feedback</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Compliance monitoring</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Integration with existing systems</td>
<td>4</td>
</tr>
<tr>
<td>Time</td>
<td>Training frequency</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>Time effectiveness</td>
<td>23</td>
</tr>
<tr>
<td>User related</td>
<td>Compulsoriness</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Ease</td>
<td>23</td>
</tr>
<tr>
<td></td>
<td>Inclusiveness</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>User friendly</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 13 - ISAT key design factors (the author’s own table).
The second question regarded ISAT delivery methods, where participants were asked to describe the ideal training delivery methods for their municipalities. The results of this question are presented in Table 14, where videos and articles are the two most preferred methods of delivering training to users. An interesting observation that confirms to the literature is the popularity of written and oral informative training delivery methods, which is not surprising as these have been proven to be effective (Al-Daeef, Basir & Saudi 2017; Wolf, Haworth & Pietron 2011). Although the simulation delivery method is only mentioned three times it is considered a valid theme because it reveals that Nordic municipalities are aware of such new training methods. Furthermore, just one mention of context-aware training warrants a separate theme due to the fact of this method being currently in development (Ghafir et al. 2018; Kävrestad & Nohlberg 2020c). This reveals that some Nordic municipalities are—at least—considering the use of state-of-the-art techniques in ISAT for end-users.

<table>
<thead>
<tr>
<th>Theme</th>
<th>Category</th>
<th>Number of mentions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded</td>
<td>Context-aware programs</td>
<td>1</td>
</tr>
<tr>
<td>Online</td>
<td>Tests</td>
<td>21</td>
</tr>
<tr>
<td></td>
<td>Videos</td>
<td>51</td>
</tr>
<tr>
<td>Oral informative</td>
<td>Presentations</td>
<td>19</td>
</tr>
<tr>
<td>Simulation</td>
<td>Guided scenarios</td>
<td>3</td>
</tr>
<tr>
<td>Written information</td>
<td>Emails</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Articles</td>
<td>45</td>
</tr>
</tbody>
</table>

Table 14 - ISAT delivery methods (the author’s own table).

Thereafter, participants were asked about the ISAT content that is best fitting to their municipalities as can be seen in Table 15. The most predominant themes are accepted behavior, importance of security, and legislation surrounding information security. This means that the most important content as seen by the respondents is simple behavioral rules to influence the behavior of users while making them aware of why such rules are important and what consequences ignoring these rules may lead to, which is in line with what is proposed in the literature (Bada, Sasse & Nurse 2015; Desman 2003; Kävrestad & Nohlberg 2020c).

<table>
<thead>
<tr>
<th>Theme</th>
<th>Category</th>
<th>Number of mentions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Behavioral</td>
<td>Accepted secure behavior</td>
<td>46</td>
</tr>
<tr>
<td>Importance</td>
<td>Security importance</td>
<td>19</td>
</tr>
<tr>
<td>Legal</td>
<td>Legislation</td>
<td>13</td>
</tr>
<tr>
<td>Organizational</td>
<td>Incident routines</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Risk management</td>
<td>6</td>
</tr>
<tr>
<td>Password</td>
<td>Password</td>
<td>7</td>
</tr>
<tr>
<td>Social engineering</td>
<td>Email phishing</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Other phishing</td>
<td>5</td>
</tr>
</tbody>
</table>

Table 15 - ISAT content (the author’s own table).

Lastly, participants were asked about key goals and expected results of ISAT, and their results are presented in Table 16, where the most important goal and expected results of the training are improved user knowledge followed by improved user behavior, fewer incidents, and lastly improved security according to the respondents. The reasoning is that having the main goal as improved user behavior and knowledge leads to fewer incidents, which in its turn should result in better overall information security in the organization.

<table>
<thead>
<tr>
<th>Theme</th>
<th>Category</th>
<th>Number of mentions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization related</td>
<td>Improved security</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>Fewer incidents</td>
<td>20</td>
</tr>
<tr>
<td>User related</td>
<td>Improved behavior</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>Improved knowledge</td>
<td>48</td>
</tr>
</tbody>
</table>

Table 16 - ISAT key goals and expected results (the author’s own table).
5.3 Results Validity and Reliability

The target population of this study is Nordic municipalities and the results of this study presented in section 5 are indicative of this population and generalizing these results to other populations is fallible and beyond the scope of what this study is set to achieve.

The results of the survey were mostly from Swedish municipalities, which may have been caused by this study being carried out in a Swedish university. This results in the findings of this study being more representative of Swedish municipalities than other Nordic municipalities. Therefore, the results of this study should be interpreted in this context.

Self-reporting in online questionnaires may cause results to be somewhat unreliable for various reasons, especially when addressing sensitive issues such as information security (Fowler 2014). However, in this study such validity threats were systematically and thoroughly addressed, as described in section 4.5.

This survey covered 96 participants encompassing just over 12% of all Nordic municipalities, which is common for online surveys (Sauermann & Roach 2013). Although 12% is not representative of all Nordic municipalities, in this study statistical methods described in sections 4.8 and 4.9 were applied to the collected data in order to measure the margins of error and confidence intervals of the proportions as presented in section 5 with a 95% confidence level.
6 Conclusion

This study investigated the preferences and expectations of Nordic municipalities in regards to end-user ISAT. An online survey was developed and sent out to all Nordic municipalities, where 96 respondents participated in the survey covering 136 of the 1123 Nordic municipalities. The survey was anonymous and consisted of two sets of questions, where the first was closed questions and examined the current state of ISAT in Nordic municipalities, and the second was open questions that examined the ideal ISAT design as seen by Nordic municipalities. The first set of questions was statistically analyzed using various statistical tests, while thematic content analysis was applied to the second set of questions. Several observations of interest were made, some of which conformed to the literature where others did not, and of those practices that did not conform to the literature some even contradicted the ideal design of ISAT as seen by the participants themselves. Furthermore, participants provided answers that proved their knowledge and understanding of recent research developments in the field of ISAT, yet these developments are not widely adopted in the participating Nordic municipalities. This may indicate the existence of a gap between the researcher and practitioner communities, which hinders innovation and adoption of these developments in the real-world as described by Norman (2010).

Some of the most interesting observations made using the first set of questions in this study regarding the current state of ISAT in the participating Nordic municipalities are mentioned below:

- Participating Nordic municipalities are well aware of the importance and impact of ISAT.
- Over 70% of respondents currently offer ISAT for their employees.
- Of those participants who do not currently offer ISAT, over 96% are planning to do so.
- One to three years is the predominant period that ISAT have been offered among both municipalities that currently offer and municipalities that have previously offered ISAT.
- Participants reported mostly positive user attitude towards ISAT followed by indifferent with zero to very few percentiles of negative attitude.
- Cost and logistics of ISAT are the most cited reasons for stopping ISAT in municipalities that have previously offered it.
- The majority of participants who currently offer ISAT cover all their users and those who do not cite cost and logistics as the most predominant reasons for not doing so.
- Municipalities currently offering ISAT mostly do so annually or less frequently.
- The most cited ISAT delivery methods currently deployed among participants are oral informative, online, and written informative.
The second set of questions provided insight into what is seen as the ideal state for ISAT by participants. Observations made using this set of questions are presented below:

- According to participants ISAT should be frequent yet time effective, come at a low cost, and be highly available—preferably on-demand. It should be relevant, concise, and easy to understand, while covering at the minimum the majority of users and being at least partially compulsory.
- ISAT should be available in a variety of delivery methods including online, written informative, oral informative, simulation, and context-aware training.
- The content of ISAT should highlight accepted secure user behavior, the importance of information security for both the organization and the users, and the legal aspects of information security.
- The goals and expectations of ISAT as seen by the participants include improved user knowledge, improved user behavior, fewer incidents, and improved overall security.
7 Discussion

The main contribution of this study is a deeper understanding of the preferences and expectations of Nordic municipalities in regards to ISAT. To that end this area should be investigated further on a larger scale—preferably globally. This can lead to a wider understanding of ISAT in production environments in the whole world. Furthermore, this study encompasses organizations in the public sector, and a natural continuation to this can be applying a similar research to the private sector. These ideas can possibly lead to researching the differences between the public and private sectors on a global scale in relation to ISAT.

The survey results show that over 85% of participants’ municipalities either currently deploy or have deployed ISAT in the past, which reveals that Nordic municipalities know the importance of ISAT with regards to the overall information security of the organization. Recent developments in ISAT constitute another aspect that participants are aware of, yet these developments are not being used in production. Furthermore, over 36% of participants reported not covering all user and the majority of those cited cost and logistics as the main reasons for not covering all users.

The participants largely reported that ISAT should include simple rules of behavior that indicate to users what is acceptable secure behavior and why it is important, with the end goal of influencing user behavior. This is in line with the literature as such rules give users a sense of control and ultimately yields greater acceptance among them (Bada, Sasse & Nurse 2015). Another observation made through the survey results was that participants mostly cited relevance and ease of absorption as important features of an ideal training and that high frequency reoccurring training is greatly valued. Although these characteristics of what is perceived as ideal ISAT by the participants is in line with the literature (Kävrestad & Nohlberg 2020c), it is clear that said characteristics are not being implemented by the participants.

Additionally, the results from this study show that participants are well aware of the importance of ISAT and the recent developments and research in the field along with the recommendations and observations that results from said research. Moreover, the ideal preferences and expectations of ISAT as seen by the participants mostly conform to the research. However, the current state of affairs as described by participants differ from both their own ideal design and the literature, which may suggest a gap between research and practice.

The most unexpected result of the survey is that gamified training methods were not mentioned at all as a part of ideal ISAT design, even though these methods are very praised by researchers. This may seem arbitrary due to the amount of research supporting the use of gamified training methods. Taking a closer look at this issue reveals underlying problems with gamified training methods. Most research on gamification of ISAT tends to be short term, meaning that research on the long-term viability and effects of ISAT gamification is scarce (Gjertsen, Gjære, Bartnes & Flores 2017). Another potential issue with gamification is that the competitive nature of games may turn some individuals off who would have participated in the training otherwise leading to less participation (Gjertsen, Gjære, Bartnes & Flores 2017). Gjertsen, Gjære, Bartnes and Flores go on to conclude that “there are no concrete evidence that can actually show if gamification will improve the security awareness and training process” (Gjertsen, Gjære, Bartnes & Flores 2017). Furthermore, Baxter, Holderness and Wood found in their study that gamification of ISAT has almost no improvements other than for those who are already gamers and that the same group is unsatisfied with the gamified side of ISAT (Baxter, Holderness & Wood 2015). This is supported
by Buell, Cai and Sandino who found that gamification of ISAT does not attract new participants or motivative employees to train (Buell, Cai & Sandino 2019). This is concerning because most of the literature on the subject suggests that gamification is positive and encouraged. This highlights the gap between research on one side and practice on the other. This is due to the tendency of research being abstract and not directly applicable to production. This may lead to recommendations in the literature that do not stand in the real-world (Norman 2010).

7.1 Ethical Aspects of Scientific Research

This section provides insight into some ethical aspects and the transparency of this study by reflecting on the study as a whole and pointing out important factors to keep in mind.

7.1.1 Ethics

As this work involved collecting data from human subjects it entailed a great ethical responsibility this is clearly and transparently discussed in section 4.6. The human subjects were made aware of all their rights regarding all stages of this study. Furthermore, presenting and interpreting the survey responses was carried out with utmost care in order to ensure the ethnicity of this study. In short, ethical aspects of all the steps carried out before, during, and after this study were considered and reflected on extensively and carefully.

7.1.2 Validity and Reliability

The validity and reliability of the methodology design, results, analysis, and conclusion is transparently discussed at every step of the way throughout the report along with the numerous measures taken to ensure them. This doesn’t mean that this study is flawless as discussed in section 5.3. A few shortcomings exist mainly in the response distribution among the Nordic municipalities and have to be taken into account when interpreting the findings of this study.

7.1.3 Bias

Bias can be a major issue in research to, so much so, that it may render certain projects unusable. However, in this study bias was avoided to the best extent possible. The questionnaire was designed to be unassuming and non-leading so that participants could voice their opinions based on their own experiences and expertise rather than underlying biases. Furthermore, interpreting the survey results and writing this report was impartial and unaffected as the author stands to gain nothing irrespective of the results and findings of this study.

7.1.4 Generalizability

This study addresses the perspective and expectations of Nordic municipalities, where the sampled population allows for generalizing these results to the target population. This is ensured through statistical measures that are presented in section 4.8.1 and further validated in section 4.9.1. Therefore, the results obtained in this study are generalizable to the target population with a confidence level of 95%. This is transparently presented in the 5.1 section, where every proportion is accompanied with its respective margin of error and confidence interval.

7.1.5 Reproducibility

The method and procedures deployed in this thesis are communicated clearly and comprehensively throughout this report. This includes tools, instruments, equations, and steps of research background, design, and analysis to name a few. This ensures that this study is reproduceable and
that a similar study will have similar results. These measures further strengthen the validity and reliability of this study.

7.1.6 Honesty

Science discourages taking reports at face value and cherishes investigation and scrutinization of evidence-based research in order to guarantee quality. In this study honesty was taken seriously by not manipulating or shifting any facts, results, or findings. This study was presented in a public arena to peers and superiors who scrutinized it and then it was defended and held up. This goes to safeguard the honesty presented in this study.

7.1.7 Trustworthiness

The subjects discussed above are indicative of the level of trustworthiness this study carries. Ethical issues are addressed systematically throughout the whole report, which reflects the level of special care that was put into ensuring the ethnicity of this work. The validity and reliability are discussed and presented transparently throughout the study. Additionally, bias is countered and reduced systematically and transparently in this report. The scope to which the results and finding of this study extent is communicated clearly multiple times to ensure the prevention of misinterpretations. The reproducibility of this study was considered and ensured at every step of the way to further support its validity, reliability, honesty, and trustworthiness. Honesty is also discussed in order to present the measures that were taken to ensure the honest and correct portrayal of facts, results, and findings, which highlights the trustworthiness of this work.

7.2 Societal Aspects

As discussed in section 2.6 the information security strategies of all Nordic countries stress the importance of making the whole of society aware of information security risks and even take a step further by including such training into the education system. This goes to show the societal impact information security risks have. This is only realized when information security is considered a national security issue and it is of importance to the society as a whole. The value and contribution of this study goes beyond answering the research question and achieving objectives. The societal awareness raised by addressing the subject area at hand is probably the most important and valuable contribution brought forward by this study. As 70% of participants answered that they currently offer ISAT is good in a way, but it has serious implications in other ways. The remaining 30% is of great concern for multiple reasons.

As mentioned, information security risks are considered to be a national security issue rather than a technical one. This is further clarified when the infrastructure that is supported by information systems is taken into account as an accessible target for adversaries. In today’s society information systems go well beyond simply baring information to become critical infrastructure. Realizing this and acting accordingly with prompt a more aware society and encourage investments into protecting this indispensable infrastructure.

7.3 Future Work

For Nordic municipalities to be well aware of the importance of ISAT and the recent developments in the field yet not covering all users and not making use of the recent developments may be caused by the inefficiency of some of the ISAT methods used today, such as oral informative training, which is highly costly and impractical with large numbers of users (Al-Daeef, Basir &
Another possible reason is the nature of research developments being abstract and not directly applicable to practice (Norman 2010). Ultimately this is beyond the scope of this study and is an interesting idea that warrants further investigation.

The reasons for not implementing what is considered to be ideal design of ISAT by the participants themselves lays outside the context of this study and it makes for an interesting idea for future work. Moreover, simulation and embedded ISAT methods were mentioned very few times as a part of ideal ISAT design. This conflicts with the literature, as these methods have been proven to work efficiently with promising results (Al-Daeef, Basir & Saudi 2017; Ghafir et al. 2018; Kumaraguru et al. 2007; Kävrestad & Nohlberg 2020c). However, the reasons behind this are beyond the reach of this study.

The conflict between what is seen as ideal ISAT be the participants and what they deploy today may indicate the existence of a gap between researchers and practitioners. This gap should be further investigated, and if the problem is proven and formalized, future research can contribute to bridging said gap. Gamified methods were not mentioned at all as a part of ideal ISAT design, yet they are very praised by researchers. This conflict must be further investigated from new angles with an open mind.
References


41


43


Appendix A – The Survey

Hello,

My name is Aoua Al Salek and I am a final year bachelor student at the University of Skövde in Sweden. As a part of any final year project I am doing an anonymized survey on the preferences and expectations of Nordic municipalities in regards to information security awareness training for users and employees.

I can be reached all days of the week between 07:00AM and 23:00PM at aoua.al.salek@his.se or +46704751375. Please do not hesitate to get in touch and ask any questions about the survey and the research project in whole.

My project supervisor is Joakim Kjærvestad and he can be reached at joakim.kjaervestad@his.se. You are welcome to contact him for any further questions regarding the project.

The reason for this study is to understand the preferences and expectations of Nordic municipalities in regards to information security awareness training for their users. This will be helpful for future research and development of training methods that will ultimately result in better security in Nordic municipalities. The data collected in this survey is essential for the understanding of preferences and expectations of Nordic municipalities.

The collected data will be analyzed to identify trends and patterns in the preferences and expectations of Nordic municipalities in regards to information security awareness training.

The collected survey responses do not contain any identifying information and will not be shared with anyone. The data will be analyzed and a summary of the analysis will be included in my report.

I ask you kindly to participate in this survey as it will be of great help to my research and ultimately the information security of Nordic municipalities.

No questions in the survey are mandatory, and you can answer the question you want. The survey is available in 6 languages, Danish, English, Finnish, Icelandic, Norwegian, and Swedish.

It is preferable that the respondent is knowledgeable in the field of IT. However, the survey is written specifically with general widely understood terms so that it does not require much knowledge in the field.

To participate, please click on the link below.
https://survey.eu/4b4e9a2?locale=EN&lang=en

Best regards,
Aoua Al Salek

Figure A-1 - E-mail invitation.

Hello,

Recently I invited you to participate in a survey.

I note that you have not yet completed the survey, and wish to remind you that the survey is still available should you wish to take part.

My name is Aoua Al Salek and I am a final year bachelor student at the University of Skövde in Sweden. As a part of my final year project I am doing an anonymized survey on the preferences and expectations of Nordic municipalities in regards to information security awareness training for users and employees.

I can be reached all days of the week between 07:00AM and 23:00PM at aoua.al.salek@his.se or +46704751375. Please do not hesitate to get in touch and ask any questions about the survey and the research project in whole.

My project supervisor is Joakim Kjærvestad and he can be reached at joakim.kjaervestad@his.se. You are welcome to contact him for any further questions regarding the project.

The reason for this study is to understand the preferences and expectations of Nordic municipalities in regards to information security awareness training for their users. This will be helpful for future research and development of training methods that will ultimately result in better security in Nordic municipalities. The data collected in this survey is essential for the understanding of preferences and expectations of Nordic municipalities.

The collected data will be analyzed to identify trends and patterns in the preferences and expectations of Nordic municipalities in regards to information security awareness training.

The collected survey responses do not contain any identifying information and will not be shared with anyone. The data will be analyzed and a summary of the analysis will be included in my report.

I ask you kindly to participate in this survey as it will be of great help to my research and ultimately the information security of Nordic municipalities.

No questions in the survey are mandatory, and you can answer the question you want. The survey is available in 6 languages, Danish, English, Finnish, Icelandic, Norwegian, and Swedish.

It is preferable that the respondent is knowledgeable in the field of IT. However, the survey is written specifically with general widely understood terms so that it does not require much knowledge in the field.

To participate, please click on the link below.
https://survey.eu/4b4e9a2?locale=EN&lang=en

Best regards,
Aoua Al Salek

Figure A-2 - E-mail reminder.
Information Security Awareness Training

Survey on the preferences and expectations of Nordic municipalities in regards to information security awareness training.

Hello and welcome to this survey on the preferences and expectations of Nordic municipalities in regards to information security awareness training.

Introductory information:
• This survey is carried out by Aous Al Salek to collect data for a final year research project for a bachelor degree in information technology with a specialization in network and system administration at the University of Skövde. I can be reached all days of the week between 07:00AM and 23:00PM at aous.al.salek@his.se or +46729182126. You are welcome to ask any questions about the survey and the research project in whole.
• My project supervisor is Joakim Kåvrestad and he can be reached at joakim.kavrestad@his.se. You are welcome to contact him for any further questions regarding the project.
• The reason for this study is to understand the preferences and expectations of Nordic municipalities in regards to information security awareness training for their users. This will be helpful for future research and development of training methods that will ultimately result in better security in Nordic municipalities.
• The data collected in this survey is essential for the understanding of preferences and expectations of Nordic municipalities.
• The collected data will be analyzed to identify trends and patterns in the preferences and expectations of Nordic municipalities in regards to information security awareness training.

Guarantees and rules:
• Participation in the survey is voluntary.
• No personal information is collected.
• The data is anonymized.
• Only the researcher has access to the responses.
• Only statistical and thematic summaries of responses are published.
• Participants are free to skip any questions they do not want to answer.
• Not participating has no consequences.
• Survey data is to be destroyed at the end of the study.
• Survey data is encrypted both under transmission and in storage.
• Answer alternatives are randomized to minimize bias.
• No assumptions or judgements are made in any question.
• General non-guiding wording is used for all questions.
• Participants can start the survey whenever they want within the allowed duration.
• Participants can stop the survey whenever they want.
• Participants can pause the survey whenever they want.
• Participants can complete the survey whenever they want within the allowed duration.
• Collected data is not manipulated or misrepresented in any way, shape, or form.

Figure A-3 - First page of the survey.
Figure A-4 - A part of the survey questions.

Figure A-5 - A part of the survey questions.
Figure A-6 - A part of the survey questions.
<table>
<thead>
<tr>
<th>Question</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>How often do users receive information security awareness training?</td>
<td>- Daily&lt;br&gt;- Weekly&lt;br&gt;- Monthly&lt;br&gt;- Quarterly&lt;br&gt;- Semi-annually&lt;br&gt;- Annually&lt;br&gt;- Less frequently (e.g., with more than one year interval, or once)</td>
</tr>
<tr>
<td>What type of information is included in the training content?</td>
<td>- Only the threats that are most likely to occur regardless of their impact severity.&lt;br&gt;- Only the threats that have the greatest impact on the information assets of the organization.&lt;br&gt;- Only the threats that are most likely to occur and have the greatest impact on the information assets of the organization.&lt;br&gt;- All potential information security threats that end-users can be vulnerable to.</td>
</tr>
<tr>
<td>Does your organization offer information security awareness training for new employees as a part of their organizational introduction or orientation?</td>
<td>- No&lt;br&gt;- Yes</td>
</tr>
</tbody>
</table>
Figure A-8 - A part of the survey questions.
Figure A-9 - A part of the survey questions.

Figure A-10 - A part of the survey questions.
Figure A-11 - A part of the survey questions.
Figure A-12 - A part of the survey questions.

Figure A-13 - A part of the survey questions.
Figure A-14 - A part of the survey questions.

Figure A-15 - A part of the survey questions.
Please briefly answer the questions on this page irrespective of the status of information security awareness training at your organization (have/had/never have had) as seen best fit for your organization.

What are the most important key factors regarding the design of information security awareness training? (e.g., frequency, length, cost, users covered, being mandatory).

What is the information security awareness training delivery method or combination of methods that suits your organization the most?

What type of information should be included in the training content? (Generally speaking).

What are the key goals and expected results of deploying and using information security awareness training?

---

**Figure A-16 - A part of the survey questions.**

---

Thank you very much for your participation.

If you would like to receive a copy of the finished report in June, please email me at sous.ai.salek@his.sr.

**Figure A-17 - The closing page of the survey.**