

Master Degree Project



Information Asset Accountability in practice: information owner's perspective

A qualitative case study

Elaheh Aalinejad

Supervisor: Martin Lundgren
Examiner: Marcus Nohlberg

Master Degree Project (120 ECTS) in Informatics
with a specialization in data Science/
Privacy, Information, and Cyber Security
30 ECTS
Spring term 2022

ABSTRACT

Information plays an essential role in supporting an organization's business; this information encounters any business's technology, people, and process aspects. In contrast, each aspect can risk an organization's information assets. Information traceability and accountability can play a significant role in controlling and protecting information assets. When individuals *perceive* accountability for each modification or change, they will behave systematically in their activities because they can expect their actions to impact others. *A sense of information accountability increases the likelihood that people think about their behaviors in daily processes.* However, if the accountability mechanism is insufficient, it can cause conflicts between information owners and employees.

Previous works are based on the theories to increase the sense of information accountability and have efficient mechanisms. Moreover, improvement of the accountability mechanism is a concern because researchers rely on laboratory results, which is not enough to develop and have a systematic mechanism. Therefore, existing theories and explanations of information accountability tend to be unclear in practice.

This study presents a qualitative case study focusing on information asset accountability among information owners and finding the practical tools and techniques to enforce the accountability. Data collection is carried out through ten semi-structured interviews among information owners who directly own information and make decisions related to classified information and controlling access levels. The interview questions were based on the increasing information asset accountability to reveal the influential factors that must be addressed. Data analysis discloses information owners' requirements to increase the sense of accountability in an organization when it comes to information asset accountability.

Key findings seem to be applying proper tools and processes such as verification and traceability to strengthen the information asset accountability within organizations. It also reveals the employee's awareness and training to understand the information handling and processes. Employees get involved with *processes* by receiving training, clarifying their accountability expectations within information assets, and acknowledging the importance of their actions to secure critical information. The study's contribution provides an insight into the information accountability mechanism to identify the enforcement requirement from the information owner's perspective. Based on the result of the study, it can raise the significance of accountability and traceability mechanisms to the information owners and provide input to maximize their information asset's security level within the organization.

Keywords: sense of accountability, information asset accountability, information owner, accountability theory.

Table of Contents

- 1 Introduction.....1**
- 2 Background3**
 - 2.1 What is accountability?3**
 - 2.1.1 Accountability theory3
 - 2.1.2 Accountability and responsibility.....4
 - 2.1.3 Accountability for information security4
- 3 Problem area.....6**
 - 3.1 Problem background and related work.....6**
 - 3.2 Research question7**
 - 3.3 Aim7**
 - 3.4 Contribution7**
 - 3.5 Delimitation7**
- 4 Method9**
 - 4.1 Planning9**
 - 4.1.1 Case selection10
 - 4.1.2 Data collection method.....13
 - 4.1.3 Data analysis method.....13
 - 4.1.4 Ethical aspects14
 - 4.1.5 Threats to validity.....15
 - 4.2 Data collection.....16**
 - 4.2.1 Interview guide17
 - 4.2.2 Invitation email.....18
 - 4.2.3 Interview session.....18
 - 4.3 Data analysis.....19**
 - 4.3.1 Analysis of qualitative interviews.....20
- 5 Results.....24**
 - 5.1 Results from qualitative content analysis.....24**
 - 5.1.1 Verification.....24
 - 5.1.2 Traceability25
 - 5.1.3 Processes.....26
- 6 Discussion28**

6.1 Current and previous research	28
6.2 Method, analysis, and results.....	29
6.3 Ethical and societal aspects	29
7 <i>Conclusion</i>	31
7.1 Future work	31
<i>References</i>	32
<i>Appendix A: Interview guide</i>	37
<i>Appendix B: Interview invitation</i>	39

1 Introduction

Accountability provides a way to achieve compliance with regulations that enable mechanisms such as security, privacy, and transparency (Felici, Koulouris, and Pearson 2013) designed to protect information assets (Information that contains value to the organizations, such as intellectual properties (Stevens et al., 2005)). Traceability relates the objects of transparency to the goals of accountability, disclosures about a system, or records created by a system. In other words, holding *system owners, designers, developers, and operators of a computer system* responsible for its behavior, ultimately evaluating it (Kroll, 2021). For example, implementing accountability in a network that includes sensitive information means that the data flow in the network can be recorded and tracked, which keeps the network users accountable for their actions. Along with some appropriate punishment or rules in the real world, it prevents several attacks from happening. Accountability can increase trust in the network, which can be assessed from an accountability point of view (Ma, Wu, and Ge 2020).

Lack of adequate accountability and transparency can cause disputes between parties, such as information owners and IT providers (Techapanupreeda et al., 2014). For instance, a lack of access control methods for employees in database systems (when employees have more access than their roles demand) can lead to a risk of access policy violation and a significant security concern within organizations (Vance, lowry, and Eggett, 2015). Such as when individuals have access rights to illegally modify and insert temporary information into a database for their benefit and finally change the data back to the original state to keep the database integrity. Due to inaccurate access control policies, information owners might become victims of misusing data by criminals (Chen, Farn, and Tsai 2003).

When people know that they must justify their behavior to the other party, the need for a 'sense' of accountability increases; *the sense of having accountability increases the likelihood that people think about their behaviors on daily processes* (Vance, lowry, and Eggett 2015). A study by Vance, lowry, and Eggett (2015) designed an artifact to increase the *perception of accountability* (the *sense of accountability that arises in decision-making and judgment* (see section 2.1.1)). Four components from the *accountability theory* were applied in their study to enhance the sense of accountability: *identifiability, awareness of monitoring, the expectation of evaluation, and social presence awareness*. Overman and Schillemans (2022) recently studied the effects of accountability on end-users' behavior, but they found a lack of knowledge on when individuals feel more accountable. Hall, Frink, and Buckley (2017) are concerned that most studies about individuals' sense of accountability are based on the laboratory result but not within organizations in practice. Even though the accountability theory and components exist in information systems, it is unclear what can impact the increasing sense of end-user's accountability in practice. Therefore, a knowledge gap between accountability mechanisms and increasing information asset accountability can be visible. This study focuses on the accountability mechanism *to understand the methods and tools that can increase the sense of information accountability among information owners in practice*. The

accountability theory will determine the relationship between the importance of information accountability and individuals in information systems.

This thesis work is structured as follows: Chapter two: provides literature reviews - which describe the principal and related concepts. Chapter three: presents the problem area, background, the research question, aim, contribution, and delimitation of the study. Chapter four: the method includes planning, data collection, and analysis. Chapter five: explains the results from this study with some selected feedback from respondents. Chapter six: discusses the previous research and the thesis work and limitations. In addition, it includes the method, data collection analysis, results, and ethical and societal aspects. Finally, the last chapter concludes the study based on the thesis work analysis, answers to the research question, and future work.

2 Background

Chapter two provides an overview of the thesis study background and related concepts to give more insight into the research area. This chapter helps to understand the concepts used in this thesis work, accountability definition, accountability theory, accountability and responsibility, and accountability for security.

2.1 What is accountability?

Accountability refers to holding someone responsible for their actions and results and focusing on the consequences of a given decision. Therefore, information accountability is intended to oblige one party to explain, justify, and be responsible for using the other party's information, according to Gajanayake, Iannella, and Sahama (2011). Another definition of accountability is the ability that focuses on each user's actions performed on a system and traces the activities (Gunduz & Das, 2018; Åhlfeldt, Spagnoletti, and Sindre, 2007).

Bovens (2014) categorized the use of accountability into two concepts: *virtue* and *mechanism*. Accountability as a *virtue* has a willingness of the person to accept responsibility and a positive feature that a person is eager to take responsibility for tasks such as traits in government agencies, firms, and public officials. However, accountability as a *mechanism* is considered a process that individuals can explain their actions to the other parties who have the right to proceed with judgment on the activities as if there are any consequences of an individual's actions. In addition, accountability as a mechanism has a potential obligation to trace actions and report negative or positive outcomes. Vance, Lowry, and Eggett (2015) presented that corporate governance must have mechanisms to promote accountability (it is a key to corporate governance to have an accountability mechanism in place). These organizational mechanisms are typically seen between employees and managers to perform a relationship for an honest evaluation and monitoring.

2.1.1 Accountability theory

Accountability theory is about the feeling of responsibility that arises in the process of decision-making and judgment. Thus, when people understand that they must justify their behavior to the other party, the need for being accountable increases. This theory explains how perceived accountability impacts an individual's behavior, increasing the likelihood that people think about their behaviors and the organization's processes. Moreover, this theory was developed by Lerner and Tetlock (1999) from the beginning (Vance, lowry, and Eggett, 2015). Amankwa, Loock, and Kritzing (2022) found that a combination of accountability theory components can significantly influence people's attitudes to compliance with information security policy. Below are explained the components and the definitions with some examples:

Identifiability means that a person understands that their actions can impact a group. When an end user's login information appears on a system, it gives the

individuation feeling and increases information accountability to the user (Wong et al., 2021). Moreover, when people perform their behaviors with identification, they are most probably involved in systematic processing to ensure that they perform activities and behaviors and are willing to be responsible. In contrast, individuals are less motivated to take responsibility for consequences in a systematic process if they are not identified. (Eargle, Vance, and Lowry, 2013).

The expectation of evaluation can happen when an individual's beliefs are evaluated and assessed by others, resulting in consequences—for example, internal or external audits within organizations. According to Griffith (1993), to have evaluation awareness, individuals first must understand that their actions might be monitored and observed (indirectly or directly) by others.

Awareness of monitoring refers to tracing and recording users' behavior and activities (Wong et al., 2021). Organizations evaluate individuals' behaviors by monitoring which people must be aware of and responsible for their actions. A solution for the end-users' awareness would be applying a user interface design to understand the monitoring of critical information (Eargle, Vance, and Lowry, 2013).

Social presence refers to the awareness of the individuals to understand that some other users are in the systems too. This factor affects the user's behavior while thinking someone else is on the other side and creates a feeling of responsibility (Mohr, Cuijpers, and Lehman 2011). According to Vance, Lowry, and Eggett 2015, Guerin (1986) found from more than two hundred fifty studies that individuals change their behavior with the passive presence of others, mainly when the observer's behavior cannot be monitored.

2.1.2 Accountability and responsibility

Individuals can be *held accountable* if they are morally or functionally *responsible* for an action or behavior. If anything wrong or harmful happens due to the consequences of that action or behavior, the responsible person does not have any excuse for the destructive act. In other words, when a person is held responsible for an activity, that person is also accountable for the consequences of the action (Bivins, 2006).

2.1.3 Accountability for information security

A model has been proposed by Lin, Zou, and Wang (2010) to indicate the relationship between accountability and information security. They argued that *authentication, authorization, encryption, auditing, and availability are provided to protect information assets*. Without protection, information traceability would not be possible, and people would not take responsibility for their actions. Therefore, the end-user must identify itself with an authentication method while accessing the information asset. Hence, the end-user must have been authorized by information owners, which helps keep track of logs and modifications.

Authentication is the process of authenticating individuals. In this process, the security system checks whether the user's information matches in a database. Different authentication methods include username and password, smart cards, or biometric methods. They allow users to access the system differently (Lal, Prasad, and Farik, 2016). *Authorization* verifies and identifies the authenticated information unit with the access level; the authenticated users and group members can access multiple systems. Finally, the system logs collect with the accountability process to keep track of all logins (Lal, Prasad, and Farik 2016).

Knowing that *authentication* verifies the individual's identity and *authorization* preserves authority for the roles and responsibilities; if there is no verification and approval, there will be no traceability and accountability (Lin, Zou, and Wang 2010).

Moreover, an accountability mechanism can be established when security controls are in place. An accountability mechanism allows information owners to disclose end-users' identities using authentication methods (when needed) (Lin, Zou, and Wang 2010). *Identity* refers to the answer to the question "who I am" and who can have access to sensitive information (Nach & Lejeune, 2010). In other words, by applying an accountability mechanism, information owners must be able to identify end-user before accessing any critical information. Azhar (2015) argued that identity and access management are essential in several businesses. The accountability mechanism reveals the *roles*; it refers to who has been authorized to change or modify information. Moreover, accountability can disclose *responsibilities* by showing who has been involved in data and is responsible for them. Finally, accountability discloses the *outcomes* of monitoring systems to reveal end-users' actions (Lin, Zou, and Wang 2010).

To summarize, implementing accountability mechanisms can disclose identities, which can be applied when there is a serious issue, or something is incorrect in a system (Bender et al., 2007). For example, in an electronic healthcare system, accurate information must be accessible to improve patients' clinical records (Vimalachandran et al., 2016); if the information or records are incorrect, the outcomes of the monitoring system can disclose the individual's actions to track the logs and find the problem.

3 Problem area

Accountability is an essential part of all societies, and without having it, people would act individually without considering the consequences imposed by others. Organizations would also have challenges working efficiently with information assets without accountability. Moreover, in the past, several political issues have been connected to the failures in accountability (Hall, Frink, and Buckley 2017). Even though Overman and Schillemans (2022) concluded that an appropriate accountability mechanism could be effective if the end-user is aware of any future evaluations but is not clear which situations can hold the individual accountable. By having accountability theory and the components to increase information accountability, the problem of holding individuals to be responsible remains.

3.1 Problem background and related work

In a model proposed by Vance, Lowry, and Eggett (2015) to avoid access policy violations, the literature argued that user interface design could impact employee accountability. They used *accountability theory components* to test their hypothesis and argued that this mediation exists because of *identifiability, evaluation expectation, awareness of monitoring, and social presence*. By increasing end-users' accountability, the intention for access policy violation decreases. They tested their model using a factorial survey method. They concluded that the user interface design solution complements the efforts of the current traditional information security tools and mechanisms to mitigate access policy violations. Furthermore, they argued that increasing the information accountability decreases the end-users' interest in committing access policy violations. Although this study was based on the theory and they tested their model, eventually, they called for another research to create a more sophisticated design artifact to increase the information accountability within organizations.

Another research by Okike et al. (2015) concerned the lack of accountability; they examined the impact of accountability in the private sector in Nigeria. According to their finding, the weakness of applying accountability in practice is not about the lack of corporate governance structure but the enforcement mechanisms. The establishment of corporate governance must be appropriate to the organizations. However, their finding was to implement enforcement mechanisms but did not clarify end-users' requirements to perform it.

Amankwa, Loock, and Kritzinger (2022) studied the effects of having information accountability on information security policy compliance. They found that a combination of accountability theory components (identifiability, expectation of evaluation, awareness of monitoring, social presence) could significantly influence people's attitudes to compliance with information security policy. Moreover, this study is limited to solving compliance issues rather than participants' experiences concerning the increasing information asset accountability.

The recent study by Overman and Schillemans (2022) focused on accountability in the public sector; they argued that the effect of the accountability mechanism

on end-users' behavior depends on the individual's acceptance of the information owner's right. End-users change their behavior when there is an evaluation in the future from information owners. Moreover, an appropriate accountability mechanism confirms end-users' perceptions about their *role*, the information owner's *perceived authority*, and of course, the content of *the accountability mechanism*. However, the study lacks other aspects of accountability "in which situations can hold individuals accountable."

3.2 Research question

The study aims to understand the sense of information asset accountability from the information owners' perspective. The findings would provide insight into the information owner's opinions regarding accountability mechanisms and their responsibility in their daily work to answer the following research question:

RQ: What can enforce individuals in practice to have a sense of accountability for their actions regarding their information assets?

3.3 Aim

Reflecting on the problem area and background, this study aims to provide insight into the components of accountability theory in practice and understand the enforcement mechanisms to increase the sense of information accountability in organizations.

Due to the limited literature on *information asset accountability in practice*, this study is motivated to explore information owners' requirements on accountability mechanisms in practice and fill in the lack of knowledge between accountability theory and holding end-users accountable for information assets. Furthermore, understanding in practice would help determine the gap (if there is any) between the information owner's requirement and accountability mechanisms.

3.4 Contribution

The study's contribution is to provide input for the future to strengthen the understanding of accountability enforcement mechanisms to increase information accountability within organizations.

3.5 Delimitation

This thesis study intends not to provide any solution to accountability theory and the increasing sense of accountability. Moreover, it is not intended to provide a list of requirements from participants but to better understand them according to the previous research in scientific literature.

This study has limited accountability as a *mechanism* for having a potential obligation to trace actions and report negative or positive consequences. However, this also provides a way to achieve compliance with regulations that

enable mechanisms such as security, privacy, and transparency, designed to protect information assets. Therefore, this study limits the accountability mechanisms on the *information assets*, and all actions and behaviors discussed in this study are related to information assets too.

Furthermore, the theory that has been limited in this study is *accountability theory* to understand the accountability mechanism and sense of accountability among individuals since the theory aims to perceive accountability.

4 Method

In this chapter, the research methodology is presented. To best address the research question, this study has applied a *qualitative method* focusing on aspects such as motives, opinions, and attitudes that cannot be quantified (Queirós, Faria, and Almeida, 2017). Therefore, quantitative methods (aiming to develop models and theories) do not apply to this thesis work (Berndtsson et al., 2007). Furthermore, when the research question in thesis work is concerned with increasing knowledge, it follows a qualitative research method (Berndtsson et al., 2007).

The research area in this study is in a particular organization with its setup to get the insider's perspective to answer the research question (Berndtsson et al., 2007; Recker, 2013). Thus, a case study as the research approach was selected for this study, as it is widely used within information security (Hedström et al., 2011) and can follow an in-depth exploration of a phenomenon in an organization (Berndtsson et al., 2007). Most qualitative methods use *qualitative interviews* as data collection method to explore topics *in-depth*, and this method is getting more popular in information system research (Iyamu, 2018)

By conducting interviews, more questions can be answered, and there will be the benefit of asking follow-up questions to gather rich information (Iyamu, 2018). In contrast, in a questionnaire survey, often the time is too short, and there will be no chance for discussions and follow-up questions (Brinkmann, 2013).

Figure 2 shows the *research methodology* adopted in the qualitative case study (Bengtsson, 2016). There are three main steps to answer the research question: *planning, data collection, and data analysis*.

4.1 Planning

The planning refers to clarifying what the aim of the study is, as well as *who* and *how* it is going to be achieved. As mentioned in section 3.3, this study aims to understand the accountability mechanism and what can increase the sense of accountability in practice.

The qualitative research method has been selected to have individual opinions to answer the research question. Conducting semi-structured interviews (section 4.2.1) would help to get people's ideas about the sense of accountability within organizations and increase it according to their experiences. Based on Bengtsson (2016), the research planning process can be inductive or deductive. This study will look for predetermined and existing subjects by evaluating principles to answer the research question; therefore, this study has applied deductive reasoning based on the description from Bengtsson (2016).

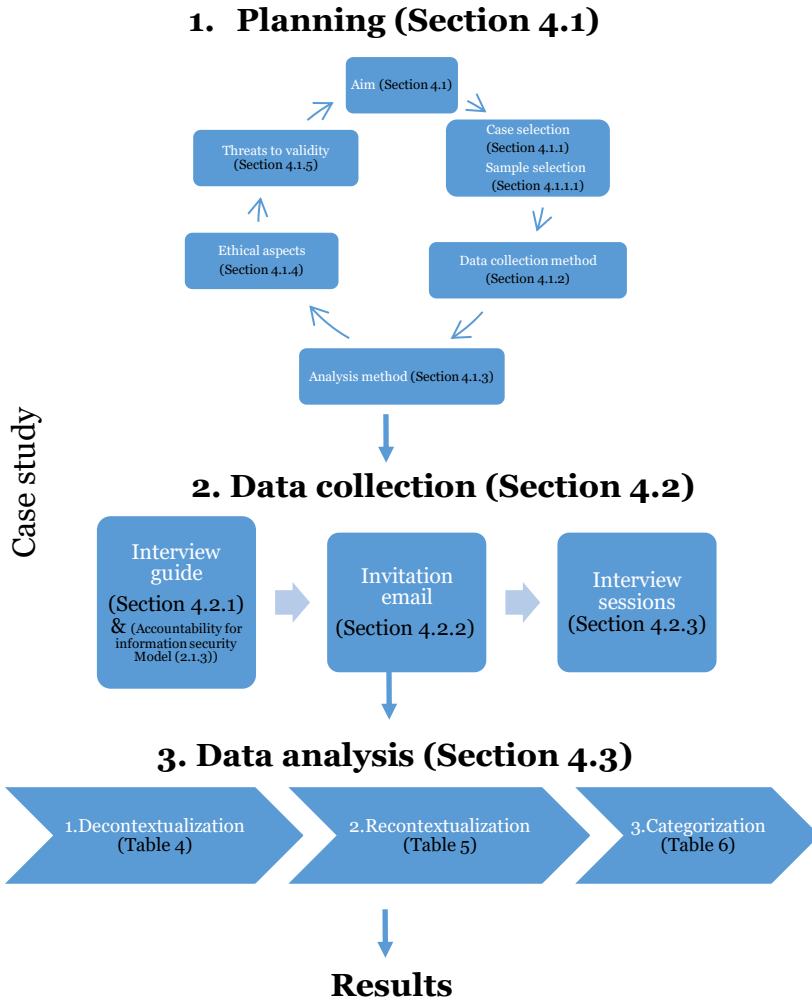


Figure 2. Research methodology adapted from Bengtsson (2016)

Below is explained case selection in more detail; moreover, the sample selection for the interview sessions is presented in detail.

4.1.1 Case selection

This study uses a case study as a research method to study a specific phenomenon arising from a particular entity. An interpretive approach aims to understand people in their natural settings and their own words. Moreover, an interpretive case study uses data collection and qualitative analysis methods (Stockdale and Standing, 2006). The choice of the current case study was according to the research from Vance, Lowry, and Eggett (2015), as this study is based on the model they proposed to enhance the sense of accountability in information systems.

The results would be better by including and conducting multiple case studies. However, the case study selected is single due to the limited resources and time concerns. Nevertheless, the case study company (a private company from Stockholm municipality) was established by a few people with some development ideas. Due to the high-paced growing company within a few years (around nine hundred employees so far), thus, the company is mature enough to have policies, processes, and documentation in place. Therefore, it was interesting to understand the information owner's opinions about their requirements for increasing the sense of accountability among employees regarding the information assets. Thus, this company was ultimately selected for the current thesis work. Table 1 illustrates the operation areas in the present case study and some examples of the responsibilities in each department.

Operation area	Responsibilities/examples
Finance and Human Resources (HR)	<i>Finance:</i> transactions within the company, invoices, project controlling, accounting, salary, treasury, legal <i>HR:</i> Onboarding, offboarding, training, employee contracts, company events, facilities
Sales	Prospecting, defining customer requirements, handling sales issues, customer support
Information Technology (IT)	Infrastructure, network, hardware and software, IT inventory asset management, phone and configurations, backups, company website, technical support
Business Development	Business plans and exploring new business opportunities, researching and planning for new markets, providing strategies to increase revenue, finding new market opportunities
Operations	Logistics, production planning, demand planning, manufacturing order, sourcing, supply chain
Research and Development	Product development, designing, prototyping, testing, programming

Table 1. Operation areas and examples of responsibilities in the case study in Stockholm municipality were taken from participants during the interview sessions.

Finance and human resources handled sensitive information such as transactions, salaries, legal, and employment contracts. They have some documents and processes, such as a code of conduct, the signature of authorities, and the financial process.

The sales department mainly works on customer requirements and handles customer problems. This department had the sales and marketing processes as documents.

The Information Technology (IT) department was involved in three areas, technical support, information security, and IT infrastructure. Moreover, the company had several policies and documents connected to the IT department, such as information security policy, IT management, and incident management. However, the company has been allocated a low budget to implement the

information security policies; therefore, according to the security manager, there were not enough people and tools to have proper methods for all the systems.

Business developments are a new group within the organization that is growing based on the organization's requirements. However, they only had a fundamental document for their processes.

The operations department has a lot of logistics, planning, manufacturing, and sourcing tasks. The documentation for each area was available but not updated.

The research and development department is the company's heart that develops the product according to the customer specifications, new technology, and new market. The documentation for product development and designing was available but not updated.

Moreover, most end-users were unaware of the concept of accountability and traceability, according to the participants in the interviews; this raises the question of whether the awareness is too simply taken for granted.

4.1.1.1 Sample selection

The focus of this study is information owners' opinions; therefore, the people selected for the interview were the information owners who have been working closely with sensitive information in the company. Multiple respondents from the same company who work in different departments have been invited to ensure adequate reliability in this study. Additionally, they have various years of experience and backgrounds at the same company. Ten information owners for the interviews were selected according to their years of experience in the company. This sample selection would help to have better results than fewer experienced employees, as shown in Table 2. Moreover, the selected participant's experiences in the same company are between four to nine years.

Department	Identity	Years of experience in the company
Finance & Human resources	#1	8
	#2	6
	#3	4
Sales	#4	9
	#5	7
Information Technology (IT)	#6	6
	#7	8
Business Development	#8	4
	#9	6
Operations	#10	7

Table 2. Overview of interviewee's title and departments.

4.1.2 Data collection method

Interviews as a data collection method were conducted in this study. *In this section, interview design and practical procedures for interviews were explained.*

4.1.2.1 Qualitative Interview

Semi-structured interviews were used to achieve an in-depth understanding of the research (Evans, 2017, Iyamu, 2018). This kind of interview consists of several key questions that allow the interviewer or respondents to pursue an idea or response in depth (Gill et al., 2008). Moreover, interviews were conducted to gather participants' experiences and insights (Busetto, Wick, and Gumbinger 2020). Another thing is understanding if the interview is relevant for the study (Brinkmann, 2013). The interview is open-ended, and the interviewees can discuss the topic more (Galletta, 2013), and there is more chance to get rich data (Iyamu, 2018). Moreover, this method is relevant for the study because of the openness feature to make the subject accessible and flexible for the interviewees; therefore, it can apply employees' individual experiences.

A model from Lin, Zou, and Wang (2010) was selected to design the interview questions. This model is suitable for this study because it defines relations between accountability and security. According to the model, there will be no traceability and accountability if there is no information security. On the other hand, when the security methods are in place, accountability can disclose *identity, roles, outcomes, and responsibilities* (see section 2.1.3). Therefore, the interview questions were designed according to *accountability for information security* (Appendix A).

4.1.3 Data analysis method

Qualitative content analysis (QCA) is used in this study to perform the content analysis. Applying the systematic text analysis method in qualitative text analysis maintains the strengths of content analysis, such as validity and reliability criteria for developing qualitative procedures (Prasad, 2019). In addition, this method can record the objects via tapes, notes, and documents (Mayring, 2019; Puppis, 2019). However, according to Sutton and Austin (2015), transcribing is challenging because what has been spoken must be written to be analyzed. Therefore, this study has been applied to be able to record voices and take notes to document the interview sections. According to Prasad (2019), content analysis definitions belong to approaches that come from impressionistic, interpretive, and intuitive to a systematic textual and strict analysis, a combined group of approaches.

In this thesis work, to conduct a qualitative content analysis, three relevant steps must be considered according to Bengtsson (2016); *decontextualization, recontextualization, and categorization.*

Decontextualization identifies *meaning units* taken from the transcribed information, including the code (Table 4). The process is deductive, so the coding list has been prepared before analysis. These codes are predefined codes taken

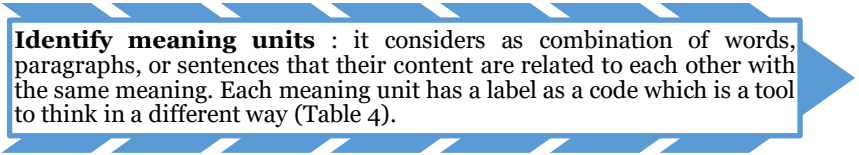
from the model (Section 2.1.3); the codes are identity, roles, outcomes, and responsibilities.

Recontextualization refers to re-reading and checking if the content is covered with all aspects of the aim of the study. In other words, it should be excluded unimportant content if they are not related to the study (Table 5).

Categorizing is the third step that mainly refers to the content and can be considered an expression of the open range in the text. In other words, it identifies homogeneous groups and often contains several subcategories to strengthen the richness of the content description. Themes and categories are identified at this level. A theme would be a thread of the main part of the sentence through condensed meaning units, codes, or categories (Table 6).

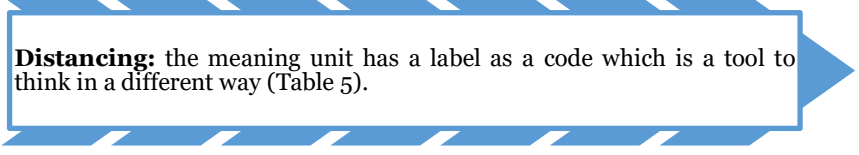
Figure 3 illustrates the steps in more detail.

Stage 1. *Decontextualization*



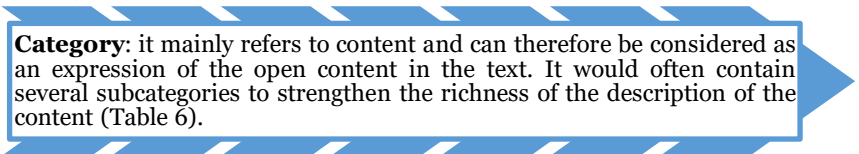
Identify meaning units : it considers as combination of words, paragraphs, or sentences that their content are related to each other with the same meaning. Each meaning unit has a label as a code which is a tool to think in a different way (Table 4).

Stage 2. *Recontextualization*



Distancing: the meaning unit has a label as a code which is a tool to think in a different way (Table 5).

Stage 3. *Categorization*



Category: it mainly refers to content and can therefore be considered as an expression of the open content in the text. It would often contain several subcategories to strengthen the richness of the description of the content (Table 6).

Figure 3. Qualitative Content Analysis steps adapted from Bengtsson (2016)

4.1.4 Ethical aspects

An ethical approach must be considered during the research process. This study has applied the approach from Allmark et al. (2009) to ensure the ethical aspects.

The participants had the right to *consent* when they understood the *purpose* of the study and the reason they had been selected for the study. They also informed that they could *withdraw from the case study* at any time during the interviews and change their decision if they did not want to participate. Moreover, it has been informed that the company's names and participants are *anonymous*, and their *recorded interview* sections are held *confidential* and *removed* after

transcribing. In addition, during the interview, only *relevant information* was discussed and asked. Information has been transcribed and asked for accuracy from the participants to ensure they are without *falsification*.

4.1.5 Threats to validity

According to Bengtsson (2016), *credibility*, *dependability*, *transferability*, and *confirmability* are the concepts created by Lincoln and Guba (1985) to check the possible threats of qualitative research.

Credibility refers to validity checking the data analysis procedures (Bengtsson, 2016). This study presents the analysis, results, discussions, and conclusions transparently. Two external people tested the interview session and questions to ensure they were understandable. Moreover, interviews have been scheduled once per day to avoid errors. For example, tiredness would impact misunderstandings; if the tiredness and misunderstandings happen, the notes cannot be reliable.

Additionally, critical points such as research area and method and interview questions are communicated with the course supervisor and examiner to ensure the quality and trustworthiness of the thesis work. Two master's students and two external engineers reviewed the thesis work for feedback. Moreover, it has been asked the participants to review and evaluate the research results to confirm the content of the transcriptions.

Dependability refers to reliability in checking the stability of the information and decisions during analysis (Bengtsson, 2016). The data collection and analysis process should state clearly to ensure the quality of the research (Lakshmi & Mohideen, 2013), such as research design, data gathering, and methodologies (Chapter 4).

Transferability means if the results of the research can be applied to other groups or not. In qualitative studies, sometimes the results are impossible to replicate because the information comes from a specific case or context (Bengtsson, 2016). In this case, the study is in a specific organization, and information owners are the participants; in the case of doing this study in another company, the results would be different or the same as the current study. All the choices and decisions during the research should be clearly explained, even any problems or limitations that might impact the results (Chapter 6).

Confirmability refers to the neutrality or objectivity of the information (Bengtsson, 2016). To deal with this, problem background and related research can help to understand if the results or findings have not been followed or affected by participants' particular positions or the researcher's preferences. Therefore, this study has reviewed related works (Section 3.1) to compare the results.

4.2 Data collection

The data collection method selected in this thesis work is the qualitative semi-structured interview. The interview guide and interview questions have been designed (Section 4.2.1). In addition, invitation emails were prepared and sent out to the participants via email (Section 4.2.2), and the interview sessions were conducted via Zoom meeting chat (Section 4.2.3).

The following strategies have been followed to conduct qualitative interviews (Berndtsson et al., 2007):

Selecting relevant interviewees is one of the steps that must be considered. In this thesis work, information owners were the target for better results and respondents' answers (Section 4.1.1.1). It would have different results than this if the participants were not having experiences of ownership of information assets. Therefore, ten information owners who accepted the interview invitations within the organization represented as follows: *three from finance, one from operations, two from sales, two from business development, and two from the IT department were involved in this study.*

Planning and structuring the interview flow during the sessions were performed (Section 4.2.1). The interview sessions were scheduled to be conducted in thirty minutes. If the follow-up questions were long, it was considered to prolong the meeting, but not more than forty-five minutes it has been communicated during the interview session to be clear about the schedule. Moreover, an interview guide has been performed with an introduction to familiarize the subject and warm up the interview session in the beginning. After that, the interview questions started, followed by some follow-up questions in some interview sections.

The interview session agenda was prepared and sent out with an invitation email to the respondents (Appendix B).

Collecting and structuring of the interview replies have been done during the interview by taking the notes and sending them to the participants for confirmation the day after the session (Section 4.2.3).

Recording interviews have been done for some of the interviews by asking for consent before the interview session. As a result, three of them accepted to record the interview and delete them after transcribing and completing the project. Regarding the sessions without recording, the notes were taken during the discussions (Section 4.2.3).

Confidentiality of files has been considered regarding the transcribed notes and recorded voices. This subject was communicated to respondents at the beginning of the interviews (Section 4.2.3).

Handling transcripts of notes was performed one of two days after the interview session and sent it the interviewees to allow the comments to correct misinterpretations.

The logistics for conducting interview sessions were selected to be conducted via Zoom meeting chat; therefore, respondents could select their location where they felt more comfortable.

Anonymity for the organization and respondents' names were considered. The participants were identified indirectly with a code number such as R#1; this was communicated to respondents before they accepted to participate in this thesis work. This strategy helped respondents to be transparent and answer the questions without considering any work-related consequences.

4.2.1 Interview guide

The interview guide should be defined as a list of questions to direct the conversation toward the research question during the interview sessions (Kallio et al., 2016). The questions should have consisted of the main theme (the theme in this thesis work is accountability mechanism), which contains the research subject, and the follow-up questions that each respondent would be questioned on each main theme (Appendix A). The order of the main themes has been recommended to be progressive to start the conversations as a warm-up to create a comfortable and relaxed environment (Kallio et al., 2016). In addition, the interview questions were explained to give some background to the respondents. Follow-up questions can be beneficial to increase the consistency of the interview subject. After each question, it was expected to have a follow-up question to explain more in detail. The technique used for follow-up questions was to continue the discussion with interviewees to run interviews to get rich information. For example, "Do you have experience with any of the techniques that hold you accountable?" or "What can improve this technique?".

A model influenced the sample questions, and concepts explained in section 2.1.3 to conduct the interview questions. There were four concepts in the model that accountability can disclose when a harmful action occurs: the user's *identity*, the authorized *roles* to have access to information, the *responsibilities* of individuals who can modify or change the information, and the *outcomes* from the monitoring such as systems, network, files. Four sections were defined for each concept with the main question. Each question includes a sample follow-up question according to the participant's discussions to get proper answers to the research question.

Below is the summary of the interview guide with some examples. Appendix A is the complete interview guide and sample questions.

Introduction questions, the purpose of these questions was to warm up the interview session and make them comfortable with the interview, inform them of the subject and interview process, and get consent relevant to the handling and documentation of the information from the interviews (name, voice recording). For example, "Is it okay if I record the interview?".

Section related to the identity includes question number 1 and follow-up question.

Section related to the authority and roles includes question number 2 and follow-up question.

Section related to the responsibilities includes question number 3 and follow-up question.

Section related to the outcomes from monitoring includes question number 4 and the follow-up question.

End questions, the purpose of these questions is to round off the interview session, ensure that all sections have been answered sufficiently, and allow the respondents to add more information before concluding the session. For example, “Is there anything else you think is important to add to this thesis work?”.

4.2.2 Invitation email

An invitation email (Appendix B) and a presentation were provided to prepare for the interview. The invitation email included the introduction, purpose of the interview, schedule, and the week number for the interviewees' availability. Ten out of fifteen accepted the invitation to participate. The interviews were scheduled for thirty minutes via Zoom meeting chat, but in some of them, the discussions were longer. Table 3 shows the details for the dates and duration of the interviews.

Respondent ID	Date	Duration (minutes)
R#1	2022-03-01	32
R#2	2022-03-03	30
R#3	2022-03-07	25
R#4	2022-03-11	36
R#5	2022-03-14	40
R#6	2022-03-16	35
R#7	2022-03-17	26
R#8	2022-03-18	38
R#9	2022-03-23	42
R#10	2022-03-29	45

Table 3. Interview schedules

4.2.3 Interview session

The interviews were scheduled upon the person's availability; they were conducted via Zoom video chat; thus, there was no location issue, and

respondents could select the interview session where they felt more comfortable. It is also expected that the employees answer the questions without considering any advantages or disadvantages and impact on their employee status.

The interviews started with a presentation; the first part of the interview was followed by an overview of the introduction to the research area and the defined goals. Then, the selection group and the reason for selecting the specific users for the interview were described; the model and the concepts introduced and explained accountability mechanism and the features that information security can impact accountability. Eventually, the discussion and questions started according to the method in four concepts mentioned in section 2.1.3: *identity, roles, outcomes, and responsibility*.

During the interview, the interviewee explained the questions by bringing up some real examples from the current information they were working on. The examples could help them to think about this kind of circumstances and understand more about the criticality of the information asset.

At the beginning of the interviews, it has been asked for consent if they can allow for recording voice and transcribing the notes. Three out of ten agreed to record the voices and delete them after completing the project, and the rest agreed to take notes and transcribe them. Therefore, no recording of the voices was not a problem for this thesis since it agreed to take the notes instead. Moreover, the files agreed to keep confidential until they are completely erased. Once the transcriptions were ready, they were sent to the respondent. Six of them were quick to respond and checked the transcribed notes, but for the rest, follow-up emails needed to ask for their feedback. After three weeks, the transcriptions were validated by participants.

4.3 Data analysis

The collected information from the interviews was presented in chapter 5, and qualitative content analysis has been applied in a structured way (Oates 2006).

A complete reading of the interview transcriptions has been completed to collect the information. Participants were offered to review the transcript materials due to the validity of the information. Therefore, the material was sent to them to validate and be used in thesis work. In addition, a data reduction was performed regarding the information that is repeating and irrelevant information.

According to Turner 2010 researchers must determine some areas of the phenomenon from previous knowledge before starting the interview (Turner, 2010). Therefore, the relevant information was categorized into four predefined codes: *identity, roles, outcomes, and responsibilities* based on the model (Section 2.1.3) and interview sessions (Lin, Zou, and Wang 2010). Section 4.3.1 explains the analysis of qualitative interviews in more detail.

4.3.1 Analysis of qualitative interviews

The transcribed texts were read several times to codify the information collected to analyze the interview data. The analysis process started with the read-throughs of the transcribed material. By considering the four concepts that have been applied to interview questions (*predefined codes*: identity, roles, responsibility, and outcomes), these codes were assigned to the participant's answers and aimed to help determine the lacking area of knowledge about accountability mechanisms, and how they are impacting information assets. Read-throughs confirmed that there are no materials left without codes. Afterward, the predefined codes were reviewed to define the appropriate *new codes* with the definitions (Table 5). For example, one of the predefined codes called identity could get a new code as '*authentication and verification method*' for identifications of end-user. Another example of the predefined code is *outcomes*; the new code allocated for it was '*auditing*'; this code was applied when the end-user feels that any activities can impact others and there are always other users involved in the system. The new codes were *authentication and verification methods*, *training and tracking awareness*, *system logs*, and *auditing*.

The next step was finding examples of meaning units according to the new codes. Table 4 contains examples with the assigned codes. These codes are the tools to think differently. Then, at this step, the new codes should be categorized into smaller groups if possible. Categories mainly refer to content and can therefore be considered an expression of the *open* content in the text. The common categories were defined for different codes, *verification*, *traceability*, and *processes* (Table 6). These categories were relevant for this study to answer the research question because they follow the same goal in accountability theory (section 2.1.1). Verification refers to *identifiability*; traceability tracks actions refer to *awareness of monitoring*, and processes are the instructions to understand the organizational expectations and regulations, which refers to the *expectation of evaluation and social presence* (Table 5).

Moreover, according to Shouran, Priyambodo, and Ashari (2019), organizations should have employee training and awareness to prevent potential risks to critical information. In addition, Suduc, Bîzoi, and Filip (2010) presented a need for an internal audit of information system security in any organization. By including employees in the audit process, they can be aware of the sensitivity of the information they have access to and how important it is to protect it (Tankard, 2015). This involvement can eventually lead to a more mature culture in an organization within the information security area (Nel & Drevin, 2019).

After defining the categories, they were reviewed to find the appropriate themes. The theme is used as an element and attribute to organize a group of repeating ideas, and it helps researchers to answer the study question. (Vaismoradi et al. 2016). As a result, two themes were identified in this thesis work, technical and non-technical aspects (Table 6). For example, verification and traceability could combine in a group because they were technical requirements. On the other hand, processes that refer to documentation and training could get a non-technical group.

In summary, four codes, three categories, and two themes were found during the QCA process. Below the codes, meaning units, categories, and themes are presented in more detail.

4.3.1.1 Meaning unit

Table 4 shows examples of meaning units after analyzing collected information from interviews. Each line has a condensed meaning unit and a code number; The codes are explained in table 5 in more detail.

Code number	Meaning unit	Condensed meaning unit
C1	<i>".... authentication for sensitive information, especially when they are critical., personal information needs extra protection such as being password-protected while the files are in the cloud and everyone in a specific department can view it" (R#8).</i>	Protection for sensitive information
C3	<i>"..... the logs are not there to look and see who has modified the file..."(R#4).</i>	Tracking system
C4	<i>".....end-user should expect this kind of auditing from IT or internal audits because we know about internal or external audits in the organization, but it looks like we are not aware and responsible for it. (R#10).</i>	Evaluation process
C2	<i>"When I am sharing information, especially critical and confidential information, I put an extra password to ensure that the information is not accessible to other people because not everyone in the same department should have access to all information, and this makes me unsure about if everyone takes the responsibility of the modifications afterward. I think training people is required to ensure that they understand and take responsibility for any changes.... (R#1).</i>	End-users' knowledge

Table 4. Meaning unit examples and code IDs

4.3.1.2 Coding

The coding was performed from the information collected from qualitative interviews, which were based on the meaning unit table. Each code includes its description and a code number to distinguish and add the codes to each meaning unit (Table 5).

Code	Descriptions	Code number
Authentication and verification methods	This applies when a user must be identified to access the system.	C1
Training and awareness of tracking	This code applies when an end-user expects to be questioned by others for any actions and activities in the system.	C2
System logs	It refers to the feeling of monitoring and evaluation by others in the organization.	C3
Auditing	It applies when the end-user feels that any information modifications and activities can impact others, and there are always other users involved in the system.	C4

Table 5. Codes and descriptions

4.3.1.3 Categories

After analyzing the collected data from qualitative content analysis, three categories have been identified: *verification*, *traceability*, and *processes* (Table 6).

Verification refers to the lack of authentication and verification methods in which the end user is concerned about access control violations. Sensitive and critical information needs to be protected from unauthorized access. Verification methods must be liable to the information owners to ensure organization confidentiality, integrity, and availability principles. For example, the end-user should be identified while logging into the system and take responsibility for the actions. These methods hold the end-user to be accountable.

Traceability refers to tracing information from beginning to end. The information owner should be able to identify and track any actions or modifications of other users. Of course, end-users should be aware of the system logs in case of auditing, which gives them a feeling of responsibility.

Processes are the third category that has been identified from collected materials. This category relates to end-users' awareness of processes, such as auditing and tracking information. By putting processes in place, employees can be aware of the monitoring, increasing the feeling of responsibility for modifying the sensitive information they might have access to. Moreover, this can increase liability and trust for the information owners within organizations.

4.3.1.4 Themes

Two themes emerged after analyzing data from interview materials, technical and non-technical. One theme included two categories, and the other included only one category.

Table 6 shows the themes and categories of each part.

Theme	Technical		Non-technical	
Category	Verification	Traceability	Processes	
Code	Authentication and verification methods	System logs	Auditing	Training and awareness of tracking
Meaning unit condensed	Protection for sensitive information	Tracking system	Evaluation process	User's knowledge

Table 6. Categories and themes

The primary theme relates to the *technical* issues that potentially can be a problem within organizations. This theme refers to the technical point of information security methods that must be addressed. This theme includes verification and identification of end-user to prevent unauthorized access. Considering this, when end-users perceive that the system demands verifications before accessing sensitive information, they become responsive to any organization's activities. Moreover, traceability systems will inform end-users that their actions can be monitored to find the records and logs when harmful actions happen. Thus, technical aspects increase the end-users' accountability to ensure data is secure from unauthorized access.

The second theme is *non-technical*, which refers to the general organizational processes, such as audit, monitoring, and awareness. This theme also impacts end-users' behavior; when internal and external audits are in place, employees feel responsive about their daily work and modification of sensitive information. Additionally, the training of employees prepares them to expect audit and tracking data and be accountable for their behaviors.

5 Results

This chapter presented results from the qualitative content analysis (section 4.3).

5.1 Results from qualitative content analysis

Two Themes and three categories have been identified from qualitative interview materials (Table 6). The results are presented below according to the categories: *verification, traceability, and processes*.

5.1.1 Verification

The first category that has been defined from the interview materials is *verification*. During the interview, the information owner's ideas and opinions on interview questions (*what makes them feel more accountable when they are going to have access to their information assets*) were more around information security methods, such as trustable authentication. Respondents R#8 and R#1 said they needed a secure authentication method. This method can be one of the first requirements for them to feel more accountable for handling critical information. Handling information with extra protection would highlight the need to increase the sense of accountability.

"[...] authentication for sensitive information, especially when they are critical [...]" (R#8).

Moreover, all the respondents described controlling methods on critical information from the beginning when they created the information. Therefore, they believe that identifying end-users gives the feeling that they should be aware of the consequences of the actions. On the other hand, in case of harm, information owners can identify the end-users and activities.

There was a follow-up question about *any techniques or methods that can help increase the sense of accountability*; participants had some experiences with multi-factor authentication and discussed the tool's benefits and simplicity. According to R#3 and R#6, the tools can ensure that verifications are secure with identified end-users. They argued that having this technique will remind them about their responsibilities related to critical information. Participant R#3 believes that even though this frustrates end-users, it can enhance information accountability and security. R#3 also mentioned that it could be challenging for employees and information owners to perform it, but it becomes an identification key after a while. For example, assume that when someone wants to purchase online, the transaction cannot be confirmed if the end-users' device (phone) does not verify the identity. This example can be helpful for the end-user to understand the information asset and the consequences of actions to be accountable.

"[...] I would recommend having it as an authentication tool, which can hold us accountable for what we have access to and remind us about our actions. I know it will be a bit frustrating for end-users [...]. (R#3).

Here is the summary of the discussion on the verification category. According to the information owners, information protection demands *verification* methods to declare the end-user's identity. Therefore, this can increase the accountability for the end-user to be responsible for their actions and behaviors. Thus, tools and techniques were recommended to improve end-users' attention to information asset accountability as an enforcement mechanism, such as multi-factor authentication.

5.1.2 Traceability

The next category is *traceability*. Some of the controlling methods discussed in this part can increase their accountability within the organization. For example, most of the information owners mentioned that tracking end-users' actions needed in harmful situations must be informed to the employees about the logs. This awareness can be beneficial in increasing the sense of accountability among employees. When end-user believe that monitoring and tracking critical information can happen in case of harm, they will be more careful about the actions and ensure that modifications are according to their responsibilities.

It has been discussed about company audits and having records. R#1, R10, and R#2 described that apart from handling information correctly, an organization's audit requires records that evidence any activity. Thus, it demands the end-users' awareness to expect the audit and evaluation, which can increase the sense of information accountability. R#3 and R#8 commented that having a system to collect the logs and record and, on the other hand, having a label to inform end-user regarding the sensitivity of data would help to enhance users' attention and hold them accountable for their actions.

R#10 added an interesting comment that most end-users are unaware of the accountability and traceability concepts, which is a problem.

"[...] end-user should expect this kind of auditing from IT or internal audits because we know about internal or external audits in the organization, but it looks like we are not aware and responsible for it" [...] " (R#10).

Respondents R#2 and R#1 discussed information classification and labeling in their daily work and suggested highlighting the confidentiality label to increase attention to accountability, such as watermarking confidential information when critical information is printed. This technique can increase the end-users accountability for taking care of the printed information. Moreover, R#4 mentioned that adding some security codes for the confidential information would be another option to inform end-users if they need to print out the document or not, and this can be tracked and avoid end-users' unnecessary hard copies.

"I think this is an excellent idea to have information labeling and understand the type of information while sharing.....and once the critical information is printed, it should be watermarked that is confidential. That would be helpful, which brings us responsibility feeling" (R#2).

In addition, information owners demand awareness for employees to understand the information assets and consequences of actions (R#2, R#6, R#1, R#5). They believe that if end-user be aware of the outcomes of modifying or removing any information, and someone can monitor their actions, they can think before they act while they have access to critical information.

Therefore, another aspect that information owners identified as an improvement for the accountability mechanism has *traceability* in place, making it easier for the information owners to track the modifications, which can be another aspect of increasing end-user's accountability.

5.1.3 Processes

The last category in this study has been defined as *processes*. Information owners are being discussed repeatedly during the interview sessions to know what organizations expect them to take care of and what actions are being tracked or audited. In addition, internal and external audit demands processes for employees to be aware of evaluation. Respondents conclude that end-users should be aware of these processes and responsible for any information changes. Respondent R#10 confirmed that they have audit processes but was unsure if everyone is aware and accountable for their activities and precisely knew information handling.

"[...] to make sure that everyone is responsible for the information, I can see that is required to be aware of audit processes" (R#10).

R#6 and R#2 discussed having training sessions for the end-users to understand the consequences of actions in information integrity. They mentioned that proper training often is needed for employees to remind their responsibilities and introduce new policies or processes within the organization.

"[...] not every user knows what to expect to use. Every quarter to have the training to improve and make it a habit for them" (R#6).

In follow-up questions, the information owners believe that having awareness and training for employees will teach them to behave and take responsibility for their actions. R#1 and R#5 mentioned the same idea.

"[...] I think training people is required to ensure that they understand and take responsibility for any changes[...]" (R#1).

In one of the follow-up questions, it has been discussed what can change for individuals once they are aware of processes; it has been mentioned that awareness of company expectations is always helpful to understand the importance of the behaviors and actions. It has been suggested that some examples and consequences can effectively understand the information assets and their impact on organizations.

"[...] using examples during the training would make sense of the consequences of the wrong actions" (R#3).

One of the recommendations in follow-up questions was about information management and the organization's scalability. Once the organization scales up, the problem arises; therefore, the processes need to be improved to adjust to new requirements and, at the same time, inform information owners and employees about the process changes.

"Always clear instructions and processes work better. [...].... When the processes are being changed, employees must be informed and take their responsibilities, either is a new process or old, and it must be informed "
(R#8).

It has been discussed about the reliability of the employees and how people can trust each other when they share critical information. Half of the respondents (R#7, R#1, R#3, R#5, and R#8) commented that with proper company awareness and training, increasing accountability. They believe that most people do not take their responsibilities seriously without training and awareness, which can be trouble for the information owners.

"When end-users knew about the organization's expectations, mostly the actions can be more reliable than when they are not aware"(R#7).

The other respondents discussed the benefits of training and awareness. They commented that end-users could ask their questions and clarify them during the training sessions; therefore, training can increase the trust between information owners and other employees regarding critical information.

"[...] training sessions would be more beneficial when they are open discussions too. This can help people to ask questions on how they should interact with critical information and eventually be reliable for the organization (R#4)."

Therefore, training end-users to be aware of *organizational audit* and *monitoring processes* became another aspect for information owners to increase accountability within organizations. Furthermore, apart from having training, it is essential that it is relevant and involves the participants in asking questions and discussing for a better understanding of the subject.

6 Discussion

This chapter is dedicated to discussing the current work and comparison with previous research. Moreover, the study limitations and ethical and societal aspects are discussed.

6.1 Current and previous research

While there has been previous research on what should be done to increase the sense of accountability, they have focused on theory more than practice (Amankwa, Looock, and Kritzinger (2022); Lerner and Tetlock (1999); Vance, Lowry, and Eggett (2015)). It is reasonable to argue that the components of accountability theory can increase the sense of accountability among individuals. These components of accountability theory give additional insights into performing accountability mechanisms and can help develop tools and techniques to benefit organizations. For example, two respondents (R#3 and R#8) pointed to the potential benefits of verification and traceability techniques such as software. While not explicitly mentioning software as an option, R#3 suggested that additional enforcement could be achieved with some form of tools such as multi-factor authentication. Based on these insights, perhaps the most obvious is that people need some enforcement mechanisms in workflow and the inherent design of tools to support accountability.

Moreover, awareness and training of the end-users to understand what organizations expect from them were another insight to enhance accountability among individuals. For instance, five respondents (R#8, R#2, R#4, R#6, and R#9) pointed to proper awareness and training to understand organizational expectations such as monitoring, tracking, information labeling, audits, which increases the trust between information owners and employees. Additionally, R#4 emphasizes that training should follow the discussions and real examples to be reasonable. Based on this perception, organizations probably need relevant training and awareness as employee assignments to increase information accountability. Therefore, the expected result from this study would increase the attention to accountability mechanisms within organizations to review their tools and techniques within the information security area.

This study has focused on the accountability mechanism to understand the methods and tools that can increase the sense of information accountability among individuals in practice. From the finding in this study, information owners are looking forward to having structured accountability mechanisms in place to achieve reliability and controllability of the information assets, especially when they have critical information. According to the finding of this study, *verification* and *traceability* aspects should be considered to achieve reliability. A study was conducted in a private organization in Nigeria, where the findings showed that they lack enforcement mechanisms to have efficient accountability. Moreover, another aspect is *processes* and *employee awareness* that impact organizational accountability effectiveness. This aspect can reflect the issue of the organization's documentation, policies, and processes that must be considered. According to Overman and Schillemans (2022), an *appropriate accountability mechanism* confirms end-users' perceptions about their role and

accountability content. These can be another common finding which indicates that an organization's processes should be adjusted to increase the sense of accountability.

Furthermore, the current and previous research results have some common findings with the processes and mechanisms regarding technical perspectives. On the other hand, this thesis work has been done in Sweden with different cultures and ways of working. Nevertheless, to some extent, they have common findings that can validate the result of the current research.

6.2 Method, analysis, and results

According to Berndtsson et al. (2007), the study could have potential limitations. This study has been limited to a single case study because of time and resource limitations. Of course, the results would be better by including and conducting multiple case studies. To deal with this problem, the case study and participants were selected accurately and relevant to the thesis work subject as described in section 4.1.1.1 (Berndtsson et al., 2007).

Semi-structured interview as data collection has been conducted in this research to have discussion sessions and collect more information. However, having lots of information also means that during the interview sections, sometimes it trails off into the subjects that may not be important for the thesis work to reach the research goal, such as participants complaining about the organizational policies or processes. This information can impact the results. An interview guide (Appendix A) with some sample follow-up questions was designed to avoid discussion about unrelated subjects. Moreover, the schedule for the interview session was limited to 30-45 minutes to be clear about relevant discussions. Participants were also expected to answer the questions without considering any advantages or disadvantages and impacts on their employee status. If the respondents do not consider it, that will change the study result if they were not following this idea. Therefore, it can be different if the same interview is conducted in another case study or with other participants.

6.3 Ethical and societal aspects

The ethical and societal aspects of this thesis work are presented in this section. This study conducted interview sessions in a company to provide the participants with insights into the research area. Anonymity has been applied in this case study, and this has been agreed with participants. When dealing with anonymous interviews, the interviewee's information must be protected and cannot identify their company. Therefore, the transcribed information is unavailable in the report.

The General Data Protection Regulation (GDPR) terms are not applicable since their personal information and the details are irrelevant to this thesis work. At the beginning of the interview agreed with the participants not to use any names from the company and participants. It also asked for consent if they could allow recording of the voices to evaluate the results better. After transcribing, recorded files were erased to protect the information and inform the participants.

Qualitative interviews have been deemed to understand what can increase the sense of accountability among individuals and hold them accountable for information assets. Hence, the findings from this study come from people's opinions, which would be the reason to be used by others without any social impact. Researchers could perhaps use the results of the thesis work to understand the basics of information accountability requirements from the information owners' perspective.

Moreover, the previous study highlighted a need for an enforcement mechanism that does not explicitly point out technical issues. Another research argues for an appropriate accountability mechanism, but the question of where and when the end-user can be accountable is unclear. Hence, there are issues related to the techniques and processes within accountability. By increasing the knowledge and understanding of these concepts, perhaps the thesis work can help IT providers and information owners redirect some of their focus to the more intangible aspects of information accountability.

7 Conclusion

Chapter seven presented the conclusion and future work of the research. The study aimed to understand the practical tools and techniques to increase individual information asset accountability.

The findings of this study provide several exciting aspects to holding individuals accountable. *First, authentication and verification* methods are required to increase a sense of accountability because they can hold end-users responsible for their actions. *Second, traceability* is another finding that information owners expect to control end-users' activities when needed; they should feel that someone else can be impacted by their activities to increase their sense of accountability. Finally, the last finding from this study was that information owners expressed awareness for employees to understand the *processes* and be aware of the organization's expectations in audit and monitoring.

Considering the finding from this thesis to answer the research question on “*What can enforce individuals in practice to have a sense of accountability regarding their actions?*” it demands information security methods, tools, documentation, training, and awareness to enhance end-user accountability. Perhaps, these are part of the requirements to establish an effective accountability mechanism within an organization.

7.1 Future work

This study adopted a qualitative research approach. The findings from one case study should be considered as this study contributes to understanding accountability enforcement mechanisms and a sense of accountability by utilizing practical insights into the subject matter. Follow-up research is suggested to enhance this basic understanding and to test the proposed categories and their relationships with other organizations. It is recommended to include different roles, such as leadership and management team, in follow-up studies to investigate if there is any gap between the information owners and top management perspective. Once the foundation for increasing accountability is established, one can suggest the appropriate approaches, tools, and techniques for adopting and implementing an effective accountability mechanism.

References

Allmark, P., Boote, J., Chambers, E., Clarke, A., McDonnell, A., Thompson, A., & Tod, A. M. (2009). Ethical issues in the use of in-depth interviews: literature review and discussion. *Research Ethics*, 5(2), 48-54.

Amankwa, E., Look, M., & Kritzinger, E. (2022). The determinants of an information security policy compliance culture in organisations: the combined effects of organisational and behavioural factors. *Information & Computer Security*.

Azhar, I. (2015). The Interaction Between Artificial Intelligence and Identity & Access Management: An Empirical study. Ishaq Azhar Mohammed," THE INTERACTION BETWEEN ARTIFICIAL INTELLIGENCE AND IDENTITY & ACCESS MANAGEMENT: AN EMPIRICAL STUDY", *International Journal of Creative Research Thoughts (IJCRT)*, ISSN, 2320-2882.

Bender, A., Spring, N., Levin, D., & Bhattacharjee, B. (2007). Accountability as a Service. *SRUTI*, 7, 1-6.

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus open*, 2, 8-14.

Berntsson, M., Hansson, J., Olsson, B., & Lundell, B. (2007). Thesis projects: a guide for students in computer science and information systems. Springer Science & Business Media.

Fitzpatrick, K., & Bronstein, C. (Eds.). (2006). *Ethics in public relations: Responsible advocacy*. Sage Publications.

Bovens, M. (2014). Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism. In *Accountability and European governance* (pp. 28-49). Routledge.

Brinkmann, S. (2013). *Qualitative interviewing*. Oxford university press.

Busetto, L., Wick, W., & Gumbinger, C. (2020). How to use and assess qualitative research methods. *Neurological Research and practice*, 2(1), 1-10.

Chen, H. H., Farn, K. J., & Tsai, D. R. (2003, October). Achieving database accountability and traceability using the bitemporal relation. In *IEEE 37th Annual 2003 International Carnahan Conference on Security Technology, 2003. Proceedings.* (pp. 151-156). IEEE.

Eargle, D., Vance, A., & Lowry, P. B. (2013, December). How moral intensity and impulsivity moderate the influence of accountability on access policy violations in information systems. In *Seventh Workshop on Information Security and Privacy*.

Elachgar, H., & Regragui, B. (2012, September). Information Security, new approach. In Second International Conference on the Innovative Computing Technology (INTECH 2012) (pp. 51-56). IEEE.

Evans, C., & Lewis, J. (2018). Analysing semi-structured interviews using thematic analysis: Exploring voluntary civic participation among adults.

Felici, M., Koulouris, T., & Pearson, S. (2013, December). Accountability for data governance in cloud ecosystems. In 2013 IEEE 5th International Conference on Cloud Computing Technology and Science (Vol. 2, pp. 327-332). IEEE.

Gajanayake, R., Iannella, R., & Sahama, T. (2011). Sharing with care: An information accountability perspective. *IEEE Internet Computing*, 15(4), 31-38.

Galletta, A. (2013). 2. The Semi-Structured Interview as a Repertoire of Possibilities. In *Mastering the Semi-Structured Interview and Beyond* (pp. 45-72). New York University Press.

Griffith, T. L. (1993). Monitoring and performance: A comparison of computer and supervisor monitoring 1. *Journal of applied social psychology*, 23(7), 549-572.

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British dental journal*, 204(6), 291-295.

Guerin, B. (1986). Mere presence effects in humans: A review. *Journal of experimental social psychology*, 22(1), 38-77.

Gunduz, M. Z., & Das, R. (2018, September). Analysis of cyber-attacks on smart grid applications. In 2018 International Conference on Artificial Intelligence and Data Processing (IDAP) (pp. 1-5). IEEE.

Hall, A. T., Frink, D. D., & Buckley, M. R. (2017). An accountability account: A review and synthesis of the theoretical and empirical research on felt accountability. *Journal of Organizational Behavior*, 38(2), 204-224.

Iyamu, T. (2018). Collecting qualitative data for information systems studies: The reality in practice. *Education and Information Technologies*, 23(5), 2249-2264.

Jarvenpaa, S. L., & Staples, D. S. (2001). Exploring perceptions of organizational ownership of information and expertise. *Journal of management information systems*, 18(1), 151-183.

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing*, 72(12), 2954-2965.

Kroll, J. A. (2021, March). Outlining traceability: A principle for operationalizing accountability in computing systems. In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (pp. 758-771).

Lakshmi, S., & Mohideen, M. A. (2013). Issues in reliability and validity of research. *International journal of management research and reviews*, 3(4), 275-282.

Lal, N. A., Prasad, S., & Farik, M. (2016). A review of authentication methods. *vol. 5*, 246-249.

Lerner, J. S., & Tetlock, P. E. (1999). Accounting for the effects of accountability. *Psychological bulletin*, 125(2), 255.

Lin, K. J., Zou, J., & Wang, Y. (2010, April). Accountability computing for e-society. In *2010 24th IEEE international Conference on Advanced information Networking and Applications* (pp. 34-41). IEEE.

Ma, Y., Wu, Y., & Ge, J. (2020). *Accountability and Privacy in Network Security* (pp. 1-140). Springer.

Mezmir, E. A. (2020). Qualitative data analysis: An overview of data reduction, data display, and interpretation. *Research on humanities and social sciences*, 10(21), 15-27.

Mezmir, E. A. (2020). Qualitative data analysis: An overview of data reduction, data display, and interpretation. *Research on humanities and social sciences*, 10(21), 15-27.

Mohr, D., Cuijpers, P., & Lehman, K. (2011). Supportive accountability: a model for providing human support to enhance adherence to eHealth interventions. *Journal of medical Internet research*, 13(1), e1602.

Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security*.

Oates, B. J. (2006). *Quantitative data analysis. Researching information systems and computing*, London; Thousand Oaks, Calif: SAGE Publications, 245-265.

Okike, E., Adegbite, E., Nakpodia, F., & Adegbite, S. (2015). A review of Nigeria's internal and external influences on corporate governance and financial. Okike, E., Adegbite, E., Nakpodia, F. & Adegbite, S. (2015), "A review of internal and external influences on corporate governance and financial accountability in Nigeria", *International Journal of Business Governance and Ethics*, 10(2), 165-185.

Overman, S., & Schillemans, T. (2022). Toward a public administration theory of felt accountability. *Public Administration Review*, 82(1), 12-22.

Puppis, M. (2019). Analyzing talk and text I: Qualitative content analysis. In *The Palgrave handbook of methods for media policy research* (pp. 367-384). Palgrave Macmillan, Cham.

Prasad, B. D. (2019). Qualitative content analysis: Why is it still a path less taken?. SSOAR-Social Science Open Access Repository.

Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European journal of education studies*.

Rashid, Y., Rashid, A., Warraich, M. A., Sabir, S. S., & Waseem, A. (2019). Case study method: A step-by-step guide for business researchers. *International journal of qualitative methods*, 18, 1609406919862424.

Recker, J. (2013). *Scientific research in information systems: a beginner's guide*. Berlin: Springer.

Shouran, Z., Priyambodo, T., & Ashari, A. (2019). Information System Security: Human Aspects. *International journal of scientific & technology research*, 8(03), 111-115.

Stockdale, R., & Standing, C. (2006). An interpretive approach to evaluating information systems: A content, context, process framework. *European journal of operational research*, 173(3), 1090-1102.

Stevens, J. F., Caralli, R. A., & Willke, B. J. (2005). Information asset profiling. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Sutton, J., & Austin, Z. (2015). Qualitative research: Data collection, analysis, and management. *The Canadian journal of hospital pharmacy*, 68(3), 226.

Tankard, C. (2015). Data classification—the foundation of information security. *Network Security*, 2015(5), 8-11.

Techapanupreeda, C., Chokngamwong, R., Thammarat, C., & Kungpisdan, S. (2014, September). Accountability in internet transactions revisited. In *2014 14th International Symposium on Communications and Information Technologies (ISCIT)* (pp. 378-382). IEEE.

Vaismoradi, M., Jones, J., Turunen, H., & Snelgrove, S. (2016). Theme development in qualitative content analysis and thematic analysis.

Vance, A., Lowry, P.B. and Eggett, D., 2015. Increasing Accountability Through User-Interface Design Artifacts. *MIS quarterly*, 39(2), pp.345-366.

Vimalachandran, P., Wang, H., Zhang, Y., Heyward, B., & Whittaker, F. (2016, December). Ensuring data integrity in electronic health records: a quality health

care implication. In 2016 International Conference on Orange Technologies (ICOT) (pp. 20-27). IEEE.

Wong, C. W., Wong, C. Y., Boon-Itt, S., & Tang, A. K. (2021). Strategies for building environmental transparency and accountability. *Sustainability*, 13(16), 9116.

Åhlfeldt, R. M., Spagnoletti, P., & Sindre, G. (2007, May). Improving the information security model by using TFI. In IFIP International Information Security Conference (pp. 73-84). Springer, Boston, MA.

Appendix A: Interview guide

Introduction questions:

Is it okay if I record the interview?

This interview aims to understand how accountability mechanisms can be applied in practice within an organization to increase the accountability perception level from the information owner's perspective.

All questions focus on the information accountability related to the information assets that you own and work with it on a daily basis.

I will present a PowerPoint to make it easier to follow the questions.

But before we start:

Are you working with critical information every day?

Do you feel accountable regarding the critical information that you have access to?

Section related to the identity

Question 1: What makes you feel accountable in the first place when you want to have access to your sensitive information?

Follow-up question

Do you think there are some techniques that you can recommend?

Do you have experience with any of them?

Section related to the authority and roles

Question 2: What kind of controls are you expecting to hold you accountable for your actions/behavior?

Follow-up question

Can you tell me about one of them and how that can affect you?

Section related to the responsibilities

Question 3: What kind of information or processes do you need to perceive accountability?

Follow-up question

Do you have any process in your mind that can hold you accountable?

Can you explain in detail what happens when you know these information or processes?

Section related to the outcomes from monitoring

Question 4: What is your requirement while handling information and collaborating with other users to be accountable?

Follow-up question

Do you grant the permissions to other users according to their responsibilities?

When you share critical information with other users, what behaviors can you expect from them?

What do you think makes the end-users' behavior to be reliable?

End questions - These questions aim to round off the interview session, ensure that all sections have been answered sufficiently, and allow the respondents to add more information before concluding the session.

Is there anything else that you want to add?

Do you have any other recommendations or thoughts to help the thesis work?

I will complete the notes from this interview which will be shared with you as soon as it is ready. When you receive my email, please review them and reply to me with your feedback.

Is it okay to keep the notes in a confidential file while using them for the thesis work?

Appendix B: Interview invitation

Hi there,

I am a master's student in Informatics specializing in Data Science/Privacy, Information, and Cyber Security. The study aims to understand the enforcement mechanisms to increase the sense of information asset accountability in organizations.

I would like to invite you for this interview to get your input and experience regarding sensitive information to discuss information accountability and the access control strategies within your organization; this would help to improve the organizational information security models.

The schedule for the interview is as follows:

Overview of the subject

Selection of respondents

Introduce the model and theory

Interview questions

Discussion

The interview would take around 20 minutes, but I will book 30 minutes in case you need to discuss more things. Do you have any time to participate within three weeks (weeks: 9,10,11,12)?

I would appreciate it if you could participate.

Best Regards, Elaheh Aalinejad