

# MASTER'S THESIS

Course code: **BE304E-2 23V**

Name: **Navdeep Singh & Lars Lien**

---

## Ethical Hacking as a Risk Management tool in Organizations

---

Date: **23.05.2023**

Total number of pages: **80**

## Acknowledgments

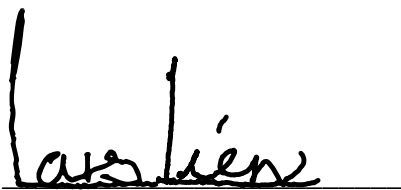
This master's thesis marks the end of our studies in the Master of Science in Business (MSc) program, specializing in business administration at Nord University's School of Business. Our focus has been on the fascinating and growing topic of cybersecurity. The idea for this thesis came about during a meeting with our professor, Anatoli Bourmistrov, who presented us with a clear challenge. We seized the opportunity to explore the unique topic of ethical hacking and how it can be used as a risk management tool in organizations. This was a new and unfamiliar subject for us, and we learned a lot about the exciting and valuable aspects of the cybersecurity industry.

Working on this thesis has been a highly educational process, both professionally and personally. Working for an extended period on such a complex task has taught us a lot. We have managed to maintain our spirits even when frustrated and have taken great joy and pride in our progress.

We want to thank our informants, who gave us unique information and made this thesis possible. We want to thank Nord University for two exciting and challenging years. Thanks to our master supervisor Olga Iermolenko for the valuable guidance and support. Working with you has been a joy, and we highly appreciate it.

Finally, we would like to thank our families, friends, and loved ones.

**Bodø, May 2023**



Lars Lien



Navdeep Singh

## Abstract

This master thesis is based on empirical evidence regarding cyber security and ethical hacking. The data are collected through five informants. The thesis' primary objective is to answer the question, "How can ethical hacking be used as a risk management tool in organizations?". The thesis uses institutional theory, the COSO, and NIST frameworks to answer this question. We find through our informants that the majority of organizations in Norway, especially small and mediums sized are in dire need of cyber security. With regulations such as DORA on the way, it's only a matter of time before security testing will become a requirement. Ethical hacking is an effective way to conduct real-life scenarios and test a company's system. As of now, ethical hacking is an expensive service not prioritized by most companies. In conclusion, it can be used as a risk management tool with the right prioritization and budget allocations.

**Keywords:** Risk management, Cybersecurity, Ethical Hacking, Institutional Theory, COSO, Hacking, Strategy, DORA, TIBER

## Sammendrag

Vi lever i dag i en verden der digitalisering og teknologisk fremgang preger store deler av vår hverdag. Selskap har blitt større og mer avhengige av teknologiske verktøy, noe som har gjort det lettere å bli utsatt for cyberangrep. Eksternt press fra regulatoriske og normative aktører har økt, der organisasjoner må tilpasse sine handlinger og valg for å tilfredsstille ulike interessenter. Denne oppgaven jobber mot å belyse temaene risikostyring og etisk hacking. Det gjøres ved å besvare problemstillingen «*How can ethical hacking be used as a risk management tool in organizations?*». Det er gjennomført fem kvalitative intervjuer for å besvare spørsmålet. I tillegg er det laget to forskningsspørsmål med hver sin delkonklusjon.

Det første spørsmålet handler om fordeler og utfordringer ved en implementering av etisk hacking. Ved bruk av Institutional Theory ser forskningsspørsmålet på hvilke regulatoriske, normative og kulturelle oppfatninger som påvirker organisasjoners evne til å forberede og endre seg i takt med nye trusler og utfordringer. Etisk hacking kan brukes som et verktøy til å forbedre sikkerhetstiltak innen organisasjoner, samt for å tilfredsstille eksterne tiltak, reguleringer og forventninger. Derimot er det også utfordringer knyttet til etisk hacking, hvorav begrenset tilgang til etiske hackere og økt etterspørsel av sikkerhetstesting kan skape en ubalanse.

Forskningsspørsmål nummer to fokuserer på hvordan organisasjoner kan implementere etisk hacking i sin organisasjon. For å svare på dette spørsmålet presenteres positive og negative sider med etisk hacking, med et søkelys på implementering ved bruk av to teoretiske rammeverk, COSO og NIST. Våre informanter forteller at en implementering av etisk hacking vil være positivt for de fleste bedrifter, men, ikke alle bedrifter jobber mot å være sikre, der noen kun fokuserer på daglig drift. En implementering av etisk hacking krever spesialisert kunnskap og mye ressurser. Dette kan gjøres enklere ved bruk av gode prosedyrer og retningslinjer innen risikostyring.

Det gjennomgående temaet i vårt diskusjonskapittel er at det er positivt for organisasjoner å implementere etisk hacking som et risikostyringsverktøy. Vi konkluderer dermed at etisk *kan* bli brukt som et risikostyringsverktøy i bedrifter. Det har dog sine utfordringer; det er tidskrevende og kostbart, samt ikke noe organisasjoner har som hovedfokus. Dette bidrar til at etisk hacking ikke er spesielt utbredt i mindre organisasjoner.

# Table of Contents

- 1.0 Introduction ..... 3
  - 1.1 Topic and Motivation ..... 3
  - 1.2 Research Questions ..... 5
  - 1.3 Ethical Hacking: What is known, and what needs knowing? ..... 6
  - 1.4 Literature Review ..... 9
  - 1.5 Research Gap..... 11
- 2.0 Theoretical Framework ..... 12
  - 2.1 What is Risk? ..... 13
  - 2.2 Institutional Theory ..... 15
  - 2.3 COSO Enterprise Risk Management..... 17
  - 2.4 NIST ..... 22
  - 2.5 Cyber Resilience Frameworks ..... 24
  - 2.6 Integrating NIST with COSO..... 26
  - 2.7 ISO 27001 & 27005 ..... 28
  - 2.8 Chapter Conclusion ..... 29
- 3.0 Methodology ..... 31
  - 3.1 Chosen Methodology ..... 31
  - 3.2 Research Design ..... 32
  - 3.3 Planning and Data Collection..... 33
  - 3.4 Case Descriptions ..... 35
    - 3.4.1 Interview Objects ..... 36
  - 3.5 Data Analysis Method ..... 38
  - 3.6 Ethical Considerations..... 39
  - 3.8 Chapter Conclusion ..... 41
- 4.0 Empirical Findings ..... 42
  - 4.1 Ethical Hacking Findings ..... 42
  - 4.2 Risk Management Findings..... 49
  - 4.3 Cyber Security Findings..... 53
  - 4.4 Other Interesting Findings..... 56
  - 4.5 Chapter Conclusion ..... 57
- 5.0 Analysis and Discussion..... 58
  - 5.1 Benefits and challenges ..... 58
  - 5.2 Integrating Ethical Hacking ..... 65
  - 5.3 Ethical Hacking as a Risk Management Tool in Organizations?..... 70
- 6.0 Conclusion..... 72
  - 6.1 Limitations and Theoretical Implications ..... 73
  - 6.2 Future Research..... 73
- References/Literature ..... 74
- Appendix ..... 78
  - Interview Guide 1 ..... 78
  - Interview Guide 2..... 79
  
- Table 1: Overview of Ethical Hacking Characteristics ..... 8
- Table 2: Overview of Informants ..... 35
- Table 3: Benefits and Challenges with Ethical Hacking..... 63
  
- Figure 1: COSO ERM Cube..... 18
- Figure 2: Theoretical Framework Illustration ..... 30

# Glossary

Terms	Definition
<b>Black Hat</b>	A black hat is an individual who engages in malicious hacking activities, exploiting vulnerabilities in systems and networks for personal gain, financial profit, or other harmful purposes.
<b>Blue Team</b>	The Blue Team is a group of cybersecurity professionals responsible for defending an organization's digital assets, networks, and systems against cyber-attacks.
<b>Bug-Bounty Hunting</b>	Bug bounty hunting is a practice where individuals or groups are rewarded for discovering and reporting security vulnerabilities in computer systems or software applications.
<b>Cyber Security</b>	Cyber security protects digital assets, including computers, networks, and data, from unauthorized access, theft, or damage caused by cyber-attacks.
<b>DORA</b>	DORA ( <i>The Digital Operational Resilience Act</i> ) is a proposed regulatory framework by the European Union to strengthen the cybersecurity and digital resilience of financial institutions and service providers.
<b>Ethical Hacking</b>	Ethical hacking is intentionally probing computer systems and networks to identify vulnerabilities and weaknesses, intending to strengthen security measures rather than exploit them for malicious purposes.
<b>Grey Hat</b>	A grey hat is an individual who engages in hacking activities that may be technically illegal but are generally not malicious, often exposing vulnerabilities to the public or affected organizations.
<b>NIST</b>	NIST ( <i>National Institute of Standards and Technology</i> ) is a framework with guidelines, standards, and best practices designed to help organizations manage and reduce cybersecurity risk.
<b>Pen-Test</b>	A Penetration test (pen test) is a simulated cyber-attack conducted by security professionals to evaluate the security

	posture of an organization's digital assets and identify vulnerabilities in specifically targeted systems.
<b>Purple Team</b>	The Purple Team is a group of cybersecurity professionals that combines the efforts of both Red and Blue Teams to improve an organization's security posture through collaborative testing and evaluation.
<b>Red Team</b>	The Red Team is a group of cybersecurity professionals who simulate real-world cyber-attacks on an organization's digital assets, networks, and systems to identify vulnerabilities and assess security measures. In comparison to a pen-test, red teaming brings a broader and more comprehensive approach.
<b>TIBER-EU</b>	TIBER-EU ( <i>Threat Intelligence-Based Ethical Red Teaming for the European Union</i> ) is a framework that enables European financial institutions to conduct controlled red teaming tests to assess their cybersecurity posture and resilience against cyber-attacks.
<b>White Hat</b>	A white hat is an ethical hacker who uses their skills to identify and report vulnerabilities in computer systems and networks, often working with the affected organizations to improve security.
<b>White Team</b>	The White Team is a group of cybersecurity professionals who oversee and coordinate the efforts of Red and Blue Teams during security exercises, ensuring the rules of engagement are followed and objectives are met.

## **1.0 Introduction**

The introduction chapter will focus on introducing the main concepts in our research. Furthermore, we will address the particular topic of choice and our motivations. In the remainder of this chapter, we will briefly describe specific terms used throughout this research paper and conduct a literature review on the existing literature connected to the topic.

### ***1.1 Topic and Motivation***

This research will focus on the topics of risk management and cyber security, with the main focus on Ethical Hacking. The term “Ethical Hacking” is relatively new but has gained momentum in recent years (Nicholson, 2019). As the internet impacts more of our everyday lives, our personal data and valuables are being exposed to uncertainties.

Our motivation for this research comes from the growing importance of cyber security and the uncertainty surrounding the safety of our data and resources. As more of our professional and personal lives connect to the internet, protecting against cyber threats and ensuring the integrity and security of the systems and technologies become important.

We want to look further into alternative cyber-improving techniques, such as Ethical Hacking, to see what benefits it can bring to an organization. The practice involves identifying and fixing vulnerabilities in current systems or improving their networks' overall resilience and security. In addition, we want to look at the risk of using such services and how companies address these risks. For example, does ethical hacking reduce the risk and help companies prepare for cyber threats? Our ultimate motivation for the research is to raise awareness and understanding of these critical issues and encourage individuals and organizations to take proactive steps to improve their cyber security.

In recent decades, the world has witnessed a significant increase in digitalization, dramatically transforming our daily lives. Digital solutions have created new opportunities for organizational growth but have also expanded the markets susceptible to external exploitation.

As recently as in 2019, one of Norway’s largest energy and raw materials companies was exposed to a significant cyber-attack. The company was Norsk Hydro, valued as the second largest company in Norway. The cyber-attack has been stated to be comprehensive and affected large parts of their operating activities globally. In later time, the company came out publicly, addressing the costs related to the data breach reaching upwards of eight hundred



million kroner in damages. In the aftermath of the incident, Norsk Hydro was forced to take serious actions to recover and improve its cyber security and re-structured its security management entirely (Hydro, 2019).

In 2020, another cyber-attack was targeted towards Stortinget. The cyber-attack created major implications for government members, where the opposing hackers gained access to sensitive information (Stortinget, 2020). A similar data breach at Stortinget occurred the following year, in 2021, through a breach in their Information and communication systems (ICT Systems). This incident affected several organizations due to the data breach being in the commonly used tool of Microsoft Exchange (Stortinget, 2021).

Each year, millions of dollars are lost in cyber security breaches among organizations, with costs related to response and recovery increasing in parallel. In 2022 alone, the average total cost of data breaches accumulated to 4.35 million USD, rising by 2.6% from the previous year. In 2022, IBM published their *Cost of a data breach Report* highlighting organizations and their current cyber security state. The report includes data from 550 organizations worldwide in critical industries such as finance, healthcare, and energy. The average cost related to data breaches in critical infrastructure organizations was 4.82 million USD, 1 million more than the average in other industries (IBM, 2022). This shows the growing importance of cyber security and the sheer scope of organizations prone to cyber risks.

With technology evolving at an unprecedented pace, it is critical to ask whether organizations are keeping up with digital change and taking the necessary steps to prepare for new uncertainties and risks. For example, among the 550 organizations studied, 45% of all breaches were cloud-based breaches. In addition, approximately 83% of the studied organizations had more than one data breach, ultimately leading to an increase in the price of their services (IBM, 2022).

As the use of the internet increases by the day, industries are becoming aware of the importance of cyber security and the ability to respond accordingly to cyber-attacks. As a result, cybercriminal activities are increasing rapidly, making cyber security a topic of growing importance (Humayun et al., 2020). Furthermore, the increasing use of information and communication technologies (ICT) in various organizations and industries has made the world more efficient and interactive.

On the other hand, enriching new technology and smarter solutions has reinforced our dependencies on ICT systems, which may never be completely safe and secure. This makes the topic of cyber security a matter of global interest and importance (Christen et al., 2020).

As cyber security is being portrayed more in the media, cyber-attack incidents in Norway and global reports on data breaches serve as a wake-up call for individuals, organizations, and governments worldwide about the critical importance of cyber security and risk management. The threats posed by malicious hackers or cyber actors are real and constant, and the consequences of a successful attack can be devastating, both financially and reputationally. As such, it is crucial that we explore and understand how ethical hacking can be leveraged as a risk management tool to help organizations proactively identify and address potential vulnerabilities. Furthermore, by studying the topics of cyber security and risk management, we can equip ourselves with the knowledge and skills needed to mitigate the risks associated with cyber threats. In doing so, we protect our interests and contribute to a broader agenda of promoting safer and more secure digital landscapes for individuals and organizations.

## ***1.2 Research Questions***

Cybersecurity is one of the most pressing challenges for organizations in the age we live in today. To protect their data and reduce risks from attacks with ill intent, they need to adopt adequate security measures and strategies, one of them being *ethical hacking*. The primary focus of this thesis' will be to explore how ethical hacking can be used as a tool to reduce risk in organizations. To explore this, we have chosen to address one main research question and two sub-questions. The main research question is:

*“How can Ethical Hacking be used as a Risk Management tool in Organizations?”*

The following sub-questions are:

- 1. What are the benefits and challenges of ethical hacking for organizations?*
- 2. How can ethical hacking be integrated into the risk management framework of an organization?*

### ***1.3 Ethical Hacking: What is known, and what needs knowing?***

Hacking has, throughout the years, been understood differently. Traditionally, hacking was referred to as “*radical programmers who aggressively explored creative solutions to problems*” (Radziwill et al., 2015, p. 1). However, in recent times, hacking has been divided into different categories. The two main categories are ***black and white hats, and a distinguished difference between them is their purpose and motivation*** (Radziwill et al., 2015).

Black hat is a term generally stereotyped for describing malicious hackers driven by the purpose of breaking into unauthorized computers and gaining access to systems and valuable data (Falk, 2014). In other words, black hats can be considered as *the bad guys*, utilizing their skillset and techniques with intentions to cause harm and discomfort. Their focus lies on breaking into or violating the system integrity of technological infrastructure, with the intent to either leak, destroy or use vital data and cause harm (Prasad, 2014).

On the other side of the spectrum, white hats, also known as ethical hackers, use their hacking abilities for proactive and security-improving purposes. White hat hackers are security professionals who utilize their skillset and knowledge within the field of hacking to locate weaknesses and implement countermeasures (Prasad, 2014). White hat hackers work towards finding security flaws and bugs within organizations: They provide a service of reporting and consulting organizations to make the correct and necessary adjustments to keep their information systems secure (Jagnarine, 2005).

Alongside these categories of different types of hackers, ***grey hats*** should also be mentioned. A grey hat hacker can be considered someone who operates between the ethical boundaries of a white hat and a black hat hacker. An example of an activity a grey hat hacker may take part in is ***Bug-Bounty hunting***, which is a practice where groups or individuals are rewarded for discovering and reporting security vulnerabilities in computer systems or software applications at their initiative or spare time (Walshe & Simpson, 2020).

Bug-bounty hunters are often compensated by companies or organizations as a way to encourage individuals to report vulnerabilities before they can be exposed to exploitation by malicious hackers. Grey hat hackers generally utilize similar hacking techniques as black hat hackers but differ in the purpose of their actions. Grey hats usually inform organizations of their security issues rather than exploitation (Walshe & Simpson, 2020).

The term Ethical hacking gets questioned when it comes to morals and ethics. However, in most contexts, the term is created to differentiate between lawful behavior and criminality and to be able to distinguish between acts toward the greater good versus acts intended for personal gain, crime, and harm (Harper et al., 2022).

Ethical hacking builds upon the principles of providing simulated cyber security tests, also known as *penetration testing*. Penetration tests or pen-tests can be defined as

“... a legal or authorized attempt to locate and successfully exploit computer systems for the purpose of making those systems more secure” (Engebretson, 2013, p. 1).

Pen-testing is done in controlled environments and consists of different teams with specially designated tasks in the testing phase. In these types of simulated cyber security tests, the different teams include groups of individuals that design, develop, manage, and participate in the testing. Penetration testing is a process where various teams have roles and responsibilities in completing the tests. Based on the role of the different teams conducting penetration testing, different colors are assigned to them to identify their roles (Yamin et al., 2020).

The team that designs and controls the overall assessment of the testing goes by the name *white team*. Their main objective is to ensure procedures and guidelines are followed by all parties involved. The white team has an administrative role and is usually the organization hosting the pen-test or a third-party organization (TIBER-NO, 2022)

Pen-testing and red teaming are two terms that overlap in many ways. Red teaming can be considered a form of pen-testing. In a penetration test, there are two main teams with designated tasks to defend and attack the given security system. The attacking team goes by the name of a *red team*, whose responsibilities lie in identifying and exploiting potential vulnerabilities in the exercising environment. The defending team gets referred to as the *blue team*, which acts as an active defense against the opposition team. Their primary responsibilities lie in identifying and patching potential vulnerabilities that can be exploited by the red team (Yamin et al., 2020).

Pen-testing is a practice that focuses on isolating a specific system within an organization with the intent of identifying vulnerabilities that may be exploited by malicious hackers. The scope is usually relatively narrow and precise, with clear guidelines and restrictions on what you can and cannot do. A penetration test can, for example, test as narrowly as a specific IP address or webpage (Engebretson, 2013).

On the other hand, red teaming is a more sophisticated and real-world-like test. The test scope usually prompts for a larger playing field and enables ethical hackers to be more creative and adaptable to different situations. Furthermore, red team testing often requires more resources due to in-depth planning and execution (TIBER-NO, 2022). To illustrate the various aspects of ethical hacking and penetration testing practices, we have created the following table. The table contains an overview of individuals and groups which take part in ethical hacking practices and links them up with various characteristics of their roles and responsibilities.

	<b>White hats</b>	<b>Grey hats</b>	<b>Black hats</b>	<b>Red Team</b>	<b>White Team</b>	<b>Blue Team</b>
<b>Professionals</b>	x	x		x	x	x
<b>Malicious</b>			x			
<b>Individuals</b>	x	x	x			
<b>Teams /Groups</b>				x	x	x
<b>Administrative</b>					x	
<b>Offensive</b>	x	x	x	x		
<b>Defensive</b>						x

Table 1: Overview of Ethical Hacking Characteristics

#### ***1.4 Literature Review***

To better understand the topic of ethical hacking and risk management, we have conducted a literature review. A literature review aims to analyze existing research concerning a particular research question. In the literature review, we searched for the three topics of ***Ethical Hacking, Cyber / Cybersecurity, and Risk Management*** to gain knowledge from available literature and to find potential research gaps.

Cyber security is a term used broadly and has no clear definition. As the word “cyber” covers the internet and digital world, “cybersecurity” is not a specific term and covers a broad area. Cybersecurity is an ever-evolving concept and is in rapid change. Craigen et al. (2014) state that cybersecurity is not static but an evolving, dynamic, multilevel ecosystem where people, laws, rules, regulations, innovation, and interactions happen, all influenced by its users (Lien & Singh, 2022).

Ethical hacking is a commonly misunderstood term, creating some uncertainty and questions to be answered. For example, how can possibly the act of hacking be done ethically? Ethical hacking can be explained as a cyber-security-improving service that is provided by either internal or external security vendors. The need for these types of services is often determined by organizational management. When organizations make decisions regarding the defense of their systems, the two critical factors of costs and their impact on the organization should be considered (Fielder et al., 2016).

Such decisions are commonly made by individuals delegated with responsibilities in the fields of security or information technology. Most commonly, the decisions are in the hands of chief information security officers, depending on the organizational structure. However, regarding investment decisions, statistics reveal insufficient funding and strict budgets allotted for improving security and technological infrastructure. There seems to be a shared understanding of what improved cybersecurity may bring to an organization in terms of value. However, a lack of appropriate actions taken towards it is still prominent (Fielder et al., 2016).

Ethics can be understood as the code or way in which an individual should live, work, and treat others (Kozhuharova et al., 2022). The question left to be answered is whether ethical hackers always act ethically? In the recent literature by Kozhuharova et al. (2022), the ethical aspects surrounding ethical hacking are presented, where different perspectives and views get discussed. In addition, some interesting discussions surround agendas, such as what information is important to share with the organization, what information may be lucrative to keep on to and keep a secret, and how ethical hackers find a balance between the two (Lien & Singh, 2022).

Ethical hacking is considered a method of improving security, but what value it brings to an organization and related costs are challenging to measure. In the research done by Wallingford et al. and Nicholson in 2019, the value of ethical hacking is discussed. The growing threats posed by hacking, insecure supply chains, and government regulations create a pressing need for organizations to prioritize cyber security. In addition, pen testing is discussed to be a valuable risk management tool that can help organizations repair weaknesses in their networks and reinforce system security against potential attacks.

Although ethical hacking has limitations in its modeling and measurement, it should be a part of a layered security approach, which may include automatizing tools, internal audits, cyber insurance, and cyber security training. Ethical hacking is highlighted to bring significant value to organizations as a tool to prevent or mitigate the impact of potential data breaches. However, if critically evaluated, the value ethical hacking brings to an organization is to some extent dependent on their current situation and their level of cyber security (Wallingford et al., 2019).

Wallingford et al., (2019) states that economics and cyber security is an emerging field of research. It helps management make informed decisions about risks connected to their advanced computing technologies and systems. Threats and risks are constantly emerging in new ways, especially in the digital world. Nicholson (2019) writes that businesses are now required to do whatever they can to cope with new risks. He writes that hackers and digital fraud are becoming more dynamic, up-to-date, and smarter. E-mails with legitimate email addresses or fake info that is almost impossible to spot.

## ***1.5 Research Gap***

After reviewing the available literature on the topics of cyber security, ethical hacking, and risk management, we found a diverse selection of literature. On cyber security, we found many different and interesting perspectives on the topic, showing its diversity and constant evolution. The research on this topic is growing due to cyber security being a relevant and ever-so-important subject moving forward in the digital era. However, when it comes to there being a research gap in cyber security, it depends on certain aspects of the topic, such as specific methods such as ethical hacking.

In comparison to cyber security, the topic of ethical hacking is less of a known practice. Literature connected to ethical hacking has grown in the last few years but cannot be compared with the vast growth of cyber security. When we first started with our research on cyber security and risk management, the term ethical hacking was unknown to us, which motivated us to look further into the literature. The literature on ethical hacking addresses its core principles and highlights the potential benefits of utilizing the practice. But on the other hand, the term still is little known to organizations, and it can be used as one of many tools for improving security. The ethical hacking literature highlights and discusses the value of such a practice, but to what extent organizations capitalize on this is less known.

The research gaps can be connected back to our motivation for studying the phenomenon of ethical hacking as a risk management tool. We believe that there are many new and interesting practices and tools out there that are less known, which can be used to bring value to organizations. However, there seems to be a lack of willingness to explore and learn about new and creative ways to improve security, especially in such a rapidly growing digital era. In our research, we would like to explore further into the challenges and benefits connected to ethical hacking practices and how organizations can implement such tools into their risk management frameworks.



## **2.0 Theoretical Framework**

The following chapter presents the theoretical framework for this thesis. This chapter aims to provide a comprehensive overview of risk management and its key concepts. We will discuss the origins and development of risk management, focusing on COSO, as well as risk management's main principles, approaches, and institutional theory. This will provide a solid foundation for the analysis and discussion presented in later chapters. Before writing this chapter, we reviewed the relevant literature to learn how risk management and ethical hacking work.

Risk management is essential for understanding and managing uncertainty in various contexts. Providing a structured approach to identifying, assessing, and mitigating risks helps organizations make informed decisions and achieve their objectives. We will particularly see if risk management frameworks need to be updated regarding cyber security. Risk and risk management are continuously updated and in touch with technological advancements, meaning the theoretical concepts has to be updated to some degree. In this thesis, we will mainly apply risk management to analyze our research problem and provide valuable insights into ethical hacking (Moeller, 2011).

The theoretical chapter starts with an introduction to risk, especially the risk management framework COSO. It also introduces cyber security frameworks, such as NIST and the two ISO standards 27001 & 27005. Finally, institutional theory is presented as the leading theory of this thesis.

## ***2.1 What is Risk?***

Even though risk is a widespread word that is used a lot, its ambiguity and vagueness make the question “What is risk?” hard to answer. In literature, the question of “what is risk” is less important than understanding and knowing the impact of risks; and what can one do with these risks? It’s argued that we live in a society with more risks than earlier, but studies show that humans interact with risks more and are more informed through the internet and social interactions (Power, 2004).

Risk refers to the probability of an event occurring and its potential impact on an individual or organization. The concept of risk has evolved rapidly, with roots in ancient civilizations. As civilizations advanced, risk became intertwined with economic activities and general decision-making processes (Moeller, 2011). Other literature suggests that risk management was something concerning the insurance business only. Based on this approach, every individual or organization purchasing insurance uses a risk-based approach (Moeller, 2011; Power, 2009).

As every company is becoming increasingly digital, especially after Covid-19, employees started to work from home, using digital workspace even more. This provided a more negligible risk for companies in terms of Covid-19 but, at the same time, a higher risk because of employees working from unsecure locations. (Moeller, 2011; Power, 2004)

The connection between risk management and cyber security is an increasing subject, especially as organizations become more reliant on digital systems and networks. Malicious cyber-attacks pose a threat to the company’s confidentiality and integrity. A successful cyber-attack may cause the company financial loss, damage to reputation, and operational disturbances. A proactive and well-thought strategy to manage cyber risk is essential to avoid this. This will help the company with resource allocation and minimize the impact of a successful attack (Power, 2004, 2009; Review et al., 2020).

In recent time, risk management, IT, and the economy have merged, and the awareness of cyber-attacks has followed with it. Organizations have recognized that cyber risk is not only an IT issue but something that affects everyone in the company. As every employee works digitally, sharper, and in-tune security culture is essential. Ethical hacking can be part of risk minimization, but there are other necessary steps to take as well (Bourmistrov, 2022; Moeller, 2011).

It's crucial to broaden our understanding of risk, especially when considering the potential consequences that may arise after the event of a risk. For example, in cyber security, one thing to consider is "what can we lose, and how will it matter?". For instance, if a hospital is hacked, the loss of personal information may occur, which is a dire consequence. Although the probability of this happening might be low, the consequence is high, requiring attention.

In conclusion, risk is a fundamental part of the organization. Risk has evolved over time, and frameworks like COSO ERM emerged from this. Cybersecurity has become a crucial part of an organizations risk management and is a topic that requires time and attention. Whatever method is used, risk should always be identified and understood before making decisions (Moeller, 2011).

Although the term risk management is commonly used; no single comprehensive definition accurately encompasses its entirety. Traditionally, risks were connected to terms such as *hazard risks*, *control risks*, and *opportunity risks*. However, the terms can lead positively and negatively, as risk is not inherently negative. The central aspect of risk management involves assessing the spectrum of potential risk responses and selecting the most fitting one for each situation (Hopkin, 2018).

Risks come in many forms and have different outcomes. Many of the responses connected to risks are automatic, depending on the types of risks in our personal and professional lives. Risks related to adverse effects go by the term *hazard risks*. They are closely related to issues such as health and safety and damage to infrastructure, IT services, and business dependencies. Hazard risks can disrupt normal operations within organizations, leading to increased costs and poor publicity and reputation. Hazard risks can also be closely related to fraud, theft, and represented cyber-attacks. This is especially true for organizations that handle cash and significant numbers of financial transactions (Hopkin, 2018).

In addition to hazard risks, organizations can be exposed to *control risks*. Control risks can generally be distinguished as risks related to controlling the environment within your organization. Control risks are associated with the unknown and are sometimes called uncertainty risks, making them difficult to map and quantify. These risks can be linked to project management, such as testing organizations' cyber security and safety protocols. One can argue that even though organizations assess and prepare, cyber-attacks are still highly uncertain (Hopkin, 2018).

As well as hazard and control risks, there are risks related to gaining positive outcomes. These types of risks are referred to as *opportunity risks*. Opportunity risks relate to the relationship between risks and returns, where the purpose lies in taking actions to achieve positive outcomes. For instance, investing in cyber security testing for your organization can yield positive results, such as enhanced control and insight into your organization's cyber resilience. However, by neglecting to seize such opportunities, organizations may be less prepared to manage potential threats (Hopkin, 2018).

## ***2.2 Institutional Theory***

Institutional theory is a sociological perspective that explains how organizations are influenced by external institutions and the environment in which they operate. The theory explains that organizations are shaped not only by market forces but also by a combination of social and cultural factors such as values, beliefs, laws, and regulations. Different types of institutions emit these types of external factors, which ultimately have a say in how organizations are shaped. Institutional theory is based on the idea that organizations strive for legitimacy and social acceptance in their institutional environment (Scott, 2008).

We believe institutional theory provides some exciting and beneficial viewpoints to our research. The theory offers a framework for understanding how organizations conform to social norms and external expectations in their decision-making. When looking at the rapidly growing importance and severity of cyber security, it becomes even more interesting to look into how organizations react and implement new security and risk management practices and how they do it following their competitors. This theory can be explained through three main institutional pillars, which can shape organizations in the way they react and respond to adversity.

In the research done by DiMaggio and Powell (1983), they seek to discuss and understand organizational isomorphism, which emphasizes organizations gradually being forced to resemble each other, given the same environments and circumstances. According to their research, institutional theory is built upon three main pillars of influence. These are coercive or, more recently known as *regulative*, *normative*, mimetic, or *cultural-cognitive*. These pillars can be conceptualized through the example of grocery stores, which comply with governmental regulations and customer expectations while mimicking each other's behavior, such as engaging in price wars to survive in a highly competitive market.

Regulative institutions refer to formal rules and regulations, such as laws, policies, and standards governing organizational behavior. Regulatory institutions provide clear guidelines for organizations to operate within, usually voluntary, or sometimes mandatory. These types of institutions create legal and administrative constraints that organizations must comply with to avoid potential sanctions and penalties. Some examples of this can be guidelines on how to report on sustainability practices or cyber security measures. By having these guidelines and regulations, organizations gain a sense of motivation to comply, not only to avoid sanctions but also to gain legitimacy and social acceptance (Dubey et al., 2017).

Normative institutions refer to the values, beliefs, and norms widely shared and accepted within a society. These institutions establish what may be considered “appropriate behavior” and guide organizations in their decision-making processes. They are usually closely connected to the expectations of the shareholders of organizations, being the employees, regulators, and investors. Some important expectations include social norms, ethical standards, and a code of conduct (DiMaggio & Powell, 1983). Organizations are regularly exposed to normative institutions, particularly large organizations expected to act according to established standards. For instance, companies with substantial customer bases face heightened expectations from stakeholders regarding their reporting practices, security protocols, and ethical behavior (Dubey et al., 2017).

Cultural-cognitive institutions can be challenging to define, with different understandings of the term. However, the essence of cultural-cognitive institutions focuses on beliefs of preferred ways of making decisions and carrying out actions. These are based on deeply embedded cultural and social norms that shape individuals' and organizations' behavior. These behaviors can be how organizations are structured, interact with stakeholders, and make decisions. Cultural-cognitive institutions highlight various ways to manage decision-making processes and “best practices” one can follow. Usually, so-called best practices originate from organizations that have gained legitimacy and social acceptance through their actions, which opens opportunities for imitation. Uncertainty in the environment of an organization can force replication and approval of a better practice to pursue. However, when organizational technologies are poorly understood, goals are too ambiguous, or the environment is uncertain, organizations tend to model themselves to other organizations (DiMaggio & Powell, 1983).

The institutional theory focuses on the three pillars of regulatory, normative, and cultural-cognitive institutions, which influence organizations' decision-making processes. We believe that institutional theory can be used to critically evaluate various aspects of organizational behavior and how they react and respond to external factors. Using institutional theory, we will focus on highlighting the growing importance of cyber security and look at different factors that alter how organizations manage and prepare for cyber threats. We plan on further analyzing empirical data to connect our findings to the three pillars of institutions.

In recent years, sustainability reporting has gained momentum due to increasing stakeholder expectations and legal requirements (Dubey et al., 2017). As a result, sustainability reporting has ever since been portrayed as being a good practice, giving organizations legitimacy and a better reputation. This has led to the hope that a similar trend will emerge in cybersecurity, as it's becoming a similar level of importance and priority.

### ***2.3 COSO Enterprise Risk Management***

The COSO framework is a comprehensive guide to managing risks. The framework was first introduced in 1992 as a response to the lack of consistent understanding of the term risk management among business professionals. The purpose of the initial internal control framework was to help organizations achieve their objectives by providing structural approaches to managing risks and improving the effectiveness of internal controls (Moeller, 2011).

The internal control framework was later updated in 2013 to the COSO Enterprise Risk Management framework, which focuses on managing risks at all levels of an enterprise. Compared to the updated version of COSO ERM, the enterprise risk management framework takes a more comprehensive approach to managing risks. COSO ERM considers not only the daily activities of an organization but also those related to strategic decisions and external factors. ERM aims to identify, assess, and manage all potential risks an organization may encounter, including those that might arise from their actions. The framework can be used to identify and prioritize risks, develop effective risk management strategies, and ensure that risks are managed in a coordinated manner (Moeller, 2011).

We believe this framework fits our research well because it is well-established, adaptable, and well-tested. The field of ethical hacking and cyber security is changing fast, and adaptability is essential to stay updated on today's technology. A well-tested framework as a foundation is

therefore important when integrating new risk-mitigating methods with it. The framework can be used to identify the risks associated with cybersecurity and ethical hacking, as well as the impact of these. By applying COSO ERM to frameworks connected to cyber security, we can gain valuable information on how to mitigate risks related to new cyber threats. In addition, the framework is well-known. It's used passively or actively by most organizations, meaning the transition to a semi-new approach won't impact the companies' structure and workflow as much.

The COSO ERM framework can be illustrated through a three-dimensional cube consisting of various components that are integrated and form a holistic approach to enterprise risk management. The cube consists of eight horizontal risk component levels and four vertical columns representing an enterprise's strategic objectives. We will explain all eight elements; however, some are more relevant to our research question than others. Relevant components are described in further detail about ethical hacking and cyber security. The less relevant ones will not be explained in detail.

We've especially focused on components one, three, four, five, and eight. All of these are crucial points in the event of a cyber threat. Later in chapter two, these components will be integrated with a cyber security framework to show how COSO ERM can be optimized to tackle and mitigate cyber risks.

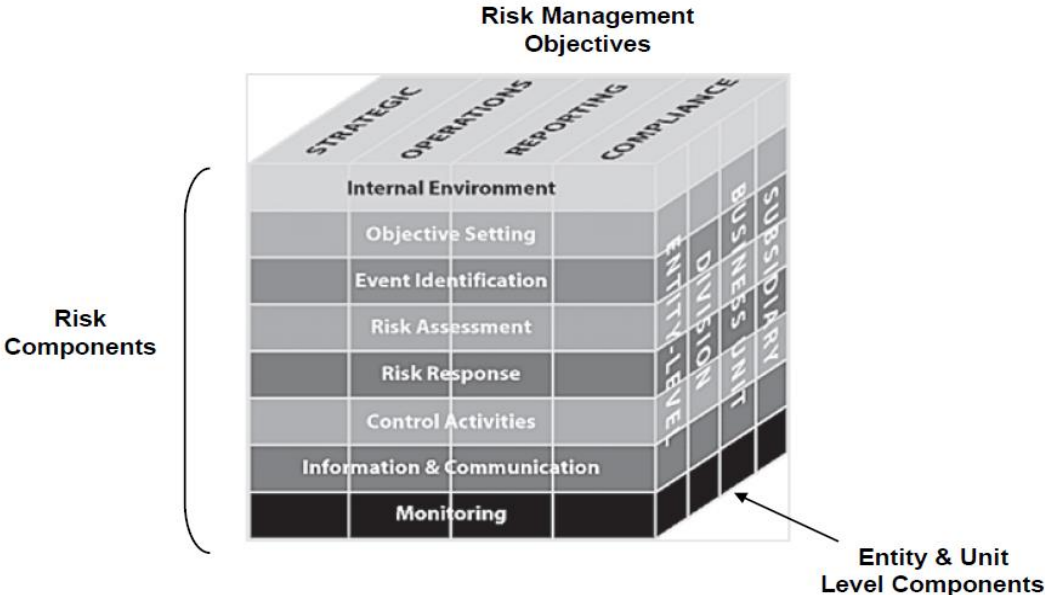


Figure 1: COSO ERM Cube

(Moeller, 2011, p. 55)

The first level of the cube is ***Internal Environment***, where the focus is on the culture and tone at the top of an organization. Some key elements within the internal environment are integrity, shared beliefs, ethical values, and attitude at the top of the organization. The internal environment in an organization is heavily decided by the internal culture and values, making these aspects important. Risk appetite is an element of the internal environment that emphasizes the amount of risk an enterprise is willing to accept in the pursuit of value. The internal environment is the first and arguably one of the most important aspects of the enterprise risk management process. The risk management process must be managed by individuals close enough to risk situations to understand various factors surrounding the risk and its implications (Moeller, 2011).

The second level of the cube is ***Objective Setting***, where the focus is on mapping the necessary objectives and practices that must be in place before managers can proceed with ERM processes. The objective setting emphasizes that the management must establish strategic objectives covering their operations, compliance, and reporting practices. The administration is also encouraged to align its risk management activities with its strategic objectives and risk appetite (Moeller, 2011).

***Event identification*** is the third level, where an enterprise should focus on identifying potential risks that could impact the organization's ability to achieve its goals. Event identification involves both internal and external risks. Examples of such potential risks are events affecting the external economy, environment, technology, and security. The ability to identify a risk event depends on how well the organization keeps up to date with risks while also monitoring existing risks. This is especially important in a fast-changing world with rapid technological advancements. An enterprise should be able to clearly define risks that are considered significant to monitor their state further (Moeller, 2011).

The fourth level in the framework is ***Risk Assessment***. It represents the core of the framework. Risk assessments involve analyzing and prioritizing identified risks based on their likelihood and impact. A key part of the risk assessment process is the consideration of potential inherent risks and residual risks. Inherent risks can be categorized as risks that, to some extent, will always exist within organizations. These types of risk arise from various sources such as operational, strategic, technological, size, and human factors. Technological and human factors can directly be connected to cyber security risks in terms of data breaches and unexpected errors. Residual risk, on the other hand, can be classified as risks that may



remain within the enterprise after management has responded to initial risks, threats, or countermeasures. As a result, organizations may take steps to reduce risk, but some inherent risks will always be present (Moeller, 2011; Sidwell & Hlavnicka, 2022).

The likelihood and impact of risks are also necessary to calculate the risk assessments. Likelihood refers to the probability of a risk event happening. It's often categorized into levels of risk. Risk estimation is easier to calculate, as one usually has value on certain items or systems. For example, if the likelihood of someone stealing customer data is high, the impact can be calculated based on *what* can be stolen. The calculation helps organizations decide how much resources to put into *risk response* and prevention (Moeller, 2011; Sidwell & Hlavnicka, 2022).

The fifth level of the ERM cube is **Risk Response**, which consists of four key elements: *avoidance, reduction, sharing, and acceptance*. After identifying significant risks, management must address the necessary steps to respond to various risks. *Avoidance* focuses on walking away from the risk or, as it states, avoiding it. The avoidance strategy is often complicated to implement as it's difficult to anticipate when one should walk away. The strategy strongly correlates with the organization's risk appetite, which can indicate what risks an organization is willing to take. The *reduction* strategy implicitly focuses on reducing the risk of certain events happening. An example of this may be to invest in cyber security testing to reduce the risk of your organization being exposed to successful cyber-attacks (Moeller, 2011; Sidwell & Hlavnicka, 2022).

The sharing risk strategy implies transferring or distributing some risks among other parties, typically through contracts, insurance, or cloud-based services. For example, purchasing insurance services, investing in funds, or making digital copies of information. Sharing risks can be an effective strategy for managing risks that are difficult to handle alone or for organizations that lack the necessary expertise. The last strategy focuses on *accepting* the identified risks. Many different types of risks approach enterprises, and in some cases, the best plan is to accept that some activities come with more significant risks. In general, management must find the best-suited strategy given their situation. Management should consider costs against the benefits of each potential risk and align these with the enterprise's overall risk appetite (Moeller, 2011; Sidwell & Hlavnicka, 2022).

The sixth level is ***Controlled Activities***, where the focus is on ensuring that the right controls and activities are present to carry out the appropriate risk responses and achieve the organization's objectives. Having identified the significant risks and the appropriate risk responses, management is responsible for the risk responses being carried out promptly and efficiently. The seventh level is ***Information and Communication***, where the importance of effectively sharing relevant information about risks and risk management activities across the organization is highlighted. This is an important level due to the importance of having everyone within the organization on board with the current state of their operations and what risks they are exposed to (Moeller, 2011).

The eighth and final level is **Monitoring**. This level emphasizes the importance of continuously monitoring and reassessing the effectiveness of the organization's risk management activities. This element is placed last in the framework due to its significance in assessing and determining all the different components of ERM and that they continue to work efficiently. In a risk management process, it is also something you do in the end. Monitoring is an ongoing process and is not something you start with; there has to be some foundation to monitor beforehand. Organizations should continuously evaluate and adjust their ERM framework as needed. While the cube presents a structural approach to ERM, it is not created to be a linear or a one-time process. Instead, the organization should view ERM as a dynamic, iterative process that changes alongside the organization's objectives and risk environment. A rapidly changing environment calls for rapid review and monitoring of risk (Moeller, 2011).

The framework provides a comprehensive and integrated approach to managing risk in relation to daily operations, but not so much when explicitly talking about risks connected to cyber security. In the past year alone, we have seen a significant increase in the number and impact of cyber-attacks (IBM, 2022). With COSO, its principles and guidelines can help organizations form a well-established foundation, while the frameworks flexibility allows organizations to adapt to different types of risks in a rapidly evolving digital era. The latter is especially important when we introduce NIST to connect these two frameworks together.

## **2.4 NIST**

This master's thesis focuses heavily on ethical hacking, cyber security, and risk management. Although there are few well-known theories and frameworks explaining cyber security, we will focus on one well-known framework and well-known terms. The first is the National Institute of Standards and Technology (NIST) framework. NIST is organized by five key functions and provides a comprehensive view of managing cybersecurity risk (NIST, 2023). The second one is the ISO standards 27001 and 27005. The 27000-series of ISO provides advanced and comprehensive guidance to cybersecurity. The ISO standard is also known to be one of the best standards organizations can get certified in (Standardization, 2023).

The NIST framework is a voluntary set of guidelines, standards, and best practices to help organizations manage and reduce cybersecurity risks. It's designed to fit organizations of all sizes using five core functions (NIST, 2023):

### **1. Identify**

When identifying the risks, understanding the risks, the systems data, and assets that need protection is vital. First, determine the critical operations that are indispensable for the organization to maintain function. Examples include customer data, websites, payment processing, and ensuring correct internal and external information. Onwards it's essential to understand the software and hardware of computers and inventory. These are frequently used as entry points. The policies, procedures, and organizational culture are also important to describe how to handle a possible cyber security breach.

### **2. Protect**

The second core concerns the *protection* of data and the appropriate implementation of systems to ensure the company's delivery of services. The framework emphasizes access management, protection of sensitive data, regular backups, device protection, and user training. The access controls are done by creating unique accounts, authenticating users, and restricting digital and physical access to devices. Organizations should always protect their sensitive data by encrypting it or authenticating the data on the sending and receiving end. The data should also be safely deleted when it's not needed. Lastly, all users and employees should be regularly trained to ensure continued preparedness.

### **3. Detect**

The *detection* phase is about implementing systems to identify events connected to cybersecurity. One of the main ways to detect is to prepare and test the system. Ethical hacking may be utilized here, along with processes and procedures to keep staff aware and updated. Controlling and monitoring information flow is important to record events such as changes to systems and accounts and know how the data is used. Lastly, it is very important to understand the impact a cybersecurity event can have on your organization and detect the possible damage it has done. Seeking professional help is often advised.

### **4. Respond**

The fourth function is *respond* and describes how to respond if a cybersecurity event is detected. Without a real plan on what to do if the incident occurs, it's difficult to respond appropriately. When responding to a cybersecurity event, preparedness is key; as companies cannot protect themselves 100%, it's better to know what to do when a breach happens. Planning, training, and testing throughout the company are vital elements to ensure appropriate responses. For example, using ethical hacking services helps organizations train on how to respond to cyber threats.

### **5. Recover**

After the four phases above are completed, the *recovery* phase begins. Appropriate programs and plans to recover any impaired or lost material are vital for any organization. Depending on the organization's size, they may have a responsibility to stakeholders and the media. Imagine a cybersecurity event at a bank where personal customer data got leaked to the public. The bank has to control the scenario and ensure stakeholders and the public that they have the attack under control. Failure to do so can cause irreplaceable damage to the bank's reputation and status.

## ***2.5 Cyber Resilience Frameworks***

Cybersecurity testing can be a complex and tedious process, where factors such as planning and mapping are essential for the safety of the organizations being tested. To gain better control and an overview of the activities being done, cyber resilience frameworks are created to monitor the testing environments. In our research, we will focus on two cyber resilience frameworks: ***TIBER-EU*** and ***DORA***.

To cope with uncertainties and possible scenarios of cyber threats in the financial markets, The European Bank came together with national central banks from around Europe to create a framework called ***TIBER-EU***. The framework was created in 2018 to measure European central banks' cyber resilience and adaptability to threats by carrying out thoroughly planned and monitored cyberattacks. TIBER-EU is a framework implemented by the majority of central banks around Europe with the intent of carrying out simulations and sharing results and data. In Norway, the framework is referred to as TIBER-NO, based on the TIBER-EU framework, where the difference lies in the country's rules and regulations (*TIBER, 2023*).

TIBER-EU stands for “*Threat Intelligence-Based Red Teaming*” and is a framework that measures financial sector firms' resilience against cyber threats. The framework challenges firms' core principles through realistic threat scenarios generated by quality threat intelligence providers. The framework implies methods of critical thinking and problem solving which involve simulating and evaluating the effectiveness of the organization's plans, processes, and systems. It is often used in cyber security and defense to identify vulnerabilities and weaknesses that might not be apparent within an organization (Lien & Singh, 2022).

TIBER aims to provide a realistic and objective assessment of an organization's resilience and ability to defend against potential threats and cyber-attacks. The framework also focuses on monitoring the red team's activities and whether or not they are conducted ethically and in accordance with the initial purpose. Ethical red teaming involves the use of ethical hacking techniques and other methods to test an organization's defenses. However, it is important to ensure that these activities are conducted responsibly and ethically (Lien & Singh, 2022).

In addition to the TIBER-EU framework, additional frameworks are in development to target smaller to medium firms and their cyber resilience. The Digital Operational Resilience Act, also called DORA, is a proposed framework that aims to improve the resilience of digital infrastructure and services around Europe. The proposed framework would introduce new requirements and regulations for operators of essential services, including telecommunications, energy, transport, and water, as well as digital infrastructure providers such as data centers and cloud service providers (DORA, 2022).

DORA applies to critical third parties which provide ICT (Information Communication Technologies)-related services to financial entities. The framework is proposed to ensure that essential services sectors can withstand and recover from digital disruptions, such as cyber-attacks, network failures, and data breaches. The framework would establish new regulations for the management of digital operational resilience, including the development of standards, the identification of risks, and the implementation of measures to address those risks. In addition, DORA can be utilized as a regulatory framework for digital operational resilience, with the intent that all firms need to ensure they can withstand, respond to, and recover from all types of ICT-related disruptions and threats (Lien & Singh, 2022).

In conclusion, TIBER and DORA play a crucial role in the research of ethical hacking as a risk management tool in organizations. Given the focus on cybersecurity and risk management in this thesis, both frameworks provide a comprehensive and structured approach addressing these concerns, with a specific emphasis on ethical hacking. Additionally, ISO standards serve as examples of best practice standards for cyber security in organizations, while the NIST framework offers guidance on how to protect data and essential information. By bringing together these four key elements, ethical hacking offers a powerful solution for addressing our research question.

## ***2.6 Integrating NIST with COSO***

Using the information previously provided about the COSO and NIST framework, we will attempt to integrate the NIST framework with COSO. Additionally, we will explain if the COSO framework is up to date or not when managing risks within cyber security. Integrating and using COSO to improve overall risk management strategies connected to cybersecurity is possible; however, the framework itself was not specifically designed for cybersecurity. Instead, the framework is intended as a general risk management and internal control.

The principles of the COSO framework can be implemented and applied to cybersecurity. The sphere of cybersecurity and the technology regarding it is advancing rapidly, and specific frameworks, such as the NIST framework, might be necessary to tackle this development. This framework provides detailed and specific guidance on how to manage and control risks connected to cybersecurity.

With that being said, COSO should not be ruled out completely. Its ways of managing risks can act as a solid foundation for companies in general, including cybersecurity. By integrating several frameworks into the risk management strategy, companies can stay up to date on “new” upcoming risks, such as technological risks, while still managing the traditional risks. Combining frameworks requires companies to be adaptive and set clear strategies to do this. This approach is possibly best suited for larger companies, as theoretical expertise combined with the ability to implement it can be an expensive affair. As stated in Chapter 2.3, we will focus on a selection of the COSO ERM components and combine them with NIST.

### **1. Internal environment**

As the internal environment focuses on internal culture and values, cybersecurity can be integrated by establishing a security culture and promoting security awareness. As COSO ERM states, this also includes a tone from the top management. This also includes establishing policies and procedures to show the importance of cyber security. Training employees to avoid possible risk events is important to mitigate risk further.

### **2. Event identification**

One of the most important aspects in COSO and NIST is identifying risk events. However, there is a distinct difference between how these two frameworks perceive this. NIST focuses on identifying an ongoing cyber-attack, while COSO aims to identify what risk events *may*

happen. Combing these two means the identification phase will be far more complicated, as there are whole different areas of risks connected to cyber security. Ethical hacking is a service that can be used to identify and *risk-assess* vulnerabilities in an organization's digital system. To improve and *respond* to these risks, the company needs someone working in IT. Identifying risks before they happen to help identify attacks is a good way to reduce risk, such as implementing systems that continually search for cyber-attacks.

### **3. Risk assessment and Risk response (Protect and Respond)**

The assessment of risks involves analyzing the identified risks and calculating their likelihood and impact. As with risk response, the risk assessments are often strategic elements already in place, allowing overlap when introducing cyber risks. NIST focuses more on the protection of existing data. This means that control over your systems helps mitigate risk.

The risk response involves the development of strategies to reduce and manage all forms of risks. The response mechanisms in NIST and COSO work similarly on a strategic level, although the execution is different. This component is relatively easily transferable to include cyber security, often because some systems are already in place, such as firewalls and incident response plans. Accompanied closely with *detection*, the reduction of risk is enhanced by more advanced *response* systems. The earlier a risk is detected, the faster a response arrives.

### **4. Monitoring**

The last phase is monitoring or recovery in NIST. NIST focuses on the recovery or identification of lost data after a cyber-attack, while COSO monitors the previous components. Implementing penetrating testing and ethical hacking is a way to monitor and test the systems. The two aspects can merge by conducting continuous cyber monitoring of new and traditional threats. By creating digital monitoring procedures, organizations can monitor a greater number of risks and rely on previous components to reduce them.

In summary, the COSO framework is not outdated in its sense; it's just not specified toward cybersecurity. The risk management procedures can and should still be used with a complementary addition of NIST. The chosen stages can be implemented with NIST without the use of too many resources, as several of the components already have procedures in place. This will ensure that companies stay adaptable and up to date on new emerging risks.



## ***2.7 ISO 27001 & 27005***

International Organization for Standardization, or ISO, is a worldwide base of national standards. The ISO-27000 series particularly focuses on cyber security and how to manage the risks connected to this. ISO-27001 is an international standard that provides a framework for establishing, implementing, maintaining, and continually improving an Information Security Management System, also known as ISMS. The 27001 series specifies the requirements for risk assessment, risk treatment, and risk management. When an organization adopts ISO-27001, it shows commitment to protecting their information (Calder & Gerrard, 2013)

ISO-27005, on the other hand, focuses specifically on risk management. It provides guidelines to identify, analyze, evaluate, and treat security risks. This is something the COSO and NIST framework also focuses on, just in different formulations. ISO 27005 is designed to help organizations develop a structured approach to risk management and risk-related information among stakeholders (Calder & Gerrard, 2013). As told by our informants, having ISO certification is one form of best practice as it's well-known and something other organizations can recognize.

Comparing the two standards, 27001 provides the overall framework. The series gives precise requirements to protect information and assets. 27005 focuses on specific risk management and how to deal with this strategically. This ISO is needed to complement ISO 27001 by providing specific guidance to the risk management associated with information security. Together they play a crucial role in helping organizations protect their information against malicious cyber-attacks.

## ***2.8 Chapter Conclusion***

In conclusion, risk is a fundamental concept that plays a critical role in organizations' processes connected to making decisions. Risks can be considered in everything we do, with it referring to the probability of an event occurring and its potential impact on an individual or organization. Alongside risks, various factors can alter organizations and their behavior. Institutional theory suggests that several external institutions influence organizations and shape them through norms, values, laws, regulations, and good practices.

While organizations are affected by external factors, internal control, and risk management dictates how organizations identify and respond to uncertainty and risks. The risk management framework of COSO provides organizations with comprehensive and integrated approaches to identifying and managing their risks. To accommodate the framework's lack of focus on cyber security, we incorporate the framework of NIST. We did this because the framework provides good guidance on how to manage cyber security risks, while COSO ERM provides a broader approach to managing risks across an organization. We believe the two frameworks can create a better foundation for organizations to work from and provide a new and up-to-date approach to managing risks and cyber threats.

We discuss the role of cyber resilience frameworks and ISO standards to further strengthen our reasoning for using Institutional Theory and the risk management and cyber security frameworks of COSO and NIST. The frameworks of TIBER and DORA can both be connected to risk management and cyber security. More importantly, they count as being good practices and impactful for organizations. ISO standards are gradually becoming more important and sort after and, in many industries, required by regulators.

To illustrate the theoretical elements discussed in this chapter, we have created a model that aims to help readers understand the relationship between different concepts and frameworks presented.

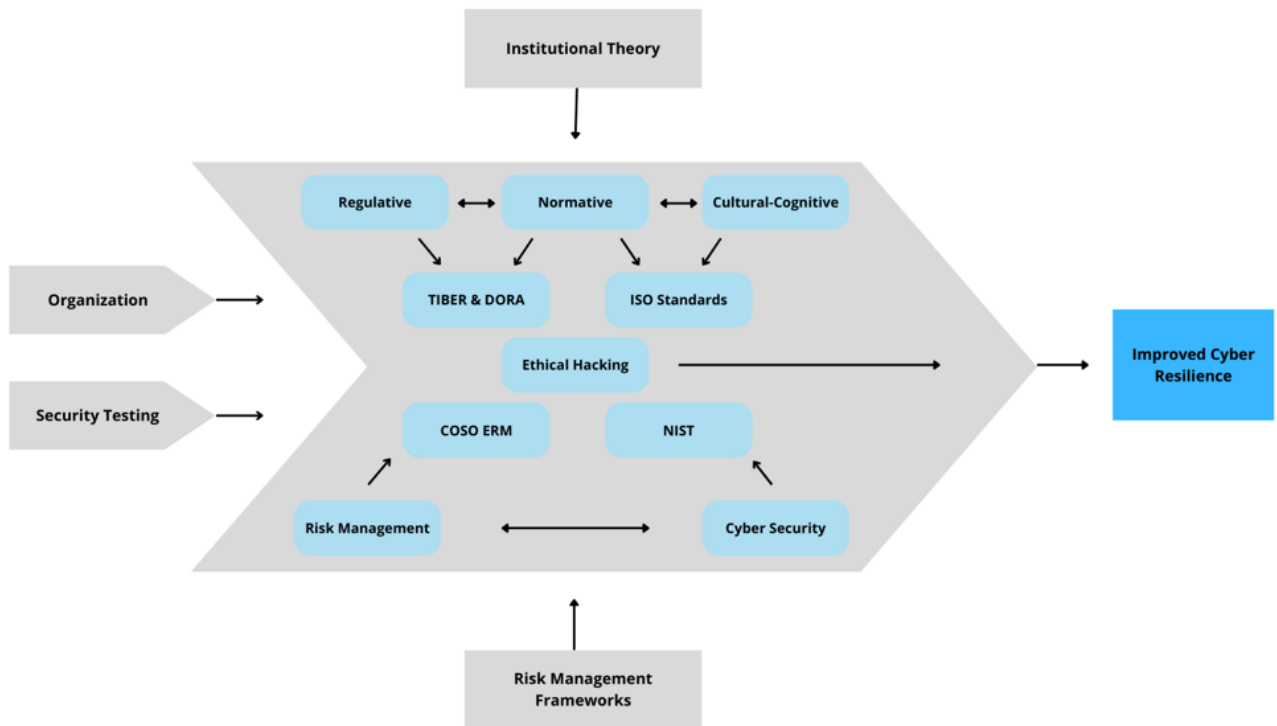


Figure 2: Theoretical Framework Illustration

The illustration is a process model, showing how cyber security and ethical hacking is a dynamic process, not a static situation. It shows the interconnections between institutional theory, ethical hacking, and risk management frameworks. Central to our research is the three pillars of institutional theory, which underpins the model. We position ethical hacking as a valuable risk management tool for organizations and emphasize the need for its integration into organizational frameworks. To fully capture the complexity of this relationship, we draw lines between ethical hacking, risk management, and cyber security, while incorporating the frameworks NIST and COSO. The model is a dynamic illustration of how ethical hacking can be implemented in organizations.

To contextualize institutional theory within the model, our analysis focuses on the regulatory, normative, and cultural cognitive institutions and their impact on organizations. To understand the relationship between institutional theory and ethical hacking, we have integrated the cyber resilience frameworks of TIBER, DORA, and ISO, which are connected to these different institutions. By doing so, we can examine how these frameworks align with institutional theory and contribute to our understanding of the role of ethical hacking in risk management and cyber security.

### **3.0 Methodology**

A rich and comprehensive research is needed to study how ethical hacking can be used as a risk management tool in organizations. The methodology chapter shows how we answer our problem statement, “*How can ethical hacking be used as a risk management tool in organizations?*”. The chapter also introduces our five informants. Chapter three will end with a conclusion and a short summary. In addition, the chapter will address how reliable and valid our data is.

#### ***3.1 Chosen Methodology***

The term “methodology” comes from Greek *methodos* and means to follow a specific path towards a goal. (Johannessen et al., 2020). The research in methodology is primarily divided into two different areas, the qualitative and the quantitative. Qualitative methods focus on collecting nonnumerical data through observations or perceptions. The data is often collected through in-depth interviews of a group or one individual. Qualitative data collection is used to gain a deep understanding of the experiences, knowledge, and motivations of the ones studied. Quantitative data collection focuses on data that can be analyzed using statistical methods. The data is collected with surveys or questionnaires and aims to generalize, not achieve depth (Johannessen et al., 2020).

We have chosen to use qualitative data collection as the primary data source. We want to achieve an in-depth understanding of risk management and ethical hacking, which cannot be gained through quantitative data. The objective of this master thesis is to acquire more knowledge about a topic becoming more and more relevant; that’s why qualitative methods were chosen (Johannessen et al., 2020; Yin, 2018).

The advantages of interviews are many, especially when we want to get in-depth information about their field of work, their personal angle towards cyber security, and the risk within this field. It allows us to get much richer data. Experiences, perceptions, and complex answers are also easier to obtain through interviews. The semi-structured gives us flexibility, which means we can adapt our follow-up questions based on the participants' responses. The goal is to have a natural and open conversation, which can lead to unexpected insights. The loose and informal conversation provides a personalized experience, allowing us to talk about sensitive information if need be. Interviews and speech increase the validity of our thesis. It helps us ensure that we are accurately capturing the participant's perspectives. Overall, qualitative

interviews provide rich and detailed information on complex phenomena that cannot be captured by quantitative surveys alone (Johannessen et al., 2020; Yin, 2018).

However, it does have its limitations. The data can be complex and time-consuming to plan, conduct, transcribe, and analyze. If the data collected does not give well-founded answers, it takes time to perform a new interview. To solve this problem, we asked and got confirmation from our informants that we could send them an e-mail if we had additional questions. The interviews only cover a small amount of people, focusing on individual experiences and educational knowledge. There is always a possibility that the informants may respond with answers we want to hear. Not only is this unlikely, but we can validate the data answers through secondary theoretical research and ask other informants the same questions to see if they give somewhat the same answer. We asked everyone some of the same questions to ensure our data's validity, for example: "Do you think the Norwegian industry is prepared for several and more advanced hacking attempts?".

### ***3.2 Research Design***

There exists almost an infinite amount of different research designs which fit different purposes. Johannessen et al. (2020) write that research design is how research is conducted. In qualitative research, it's essential that every aspect of the case is explained.

We are conducting a single case study on "*ethical hacking*" because we do not compare two cases against each other or draw parallel lines between them. A single case study is appropriate when studying one or several cases separately. We are conducting several interviews to gain knowledge about a specific subject, not to compare opposites and acquire an answer that way. Yin (2018) writes that there are five single-case rationales: critical, unusual, common, revelatory, or longitudinal. These rationales also connect with the theory chapter, as it's a crucial part of our thesis. Our problem statement relies on it being an exploratory case study. Meaning we want to explain why or how some condition came to be; additionally, our research question intends to study a phenomenon (Yin, 2018). The case is exploratory because there is little to no research on this exact phenomenon. Most of the data provided is collected from experts, buyers, or sellers of ethical hacking services.

Reliability is a term used to describe how consistently a method measures something. The study is considered reliable if the same results can be consistently achieved by using the same methods under the same circumstances. The goal of reliability is to minimize errors and biases in a study (Yin, 2018). For example, if someone were to ask our informants the same questions as us, they should get somewhat the same answer. The answer will not be the same word by word, but the thesis conclusion should be the same. Validity is how accurate the research is compared to what it's intended to measure.

To achieve reliability, we asked the informants for some of the same answers and expected the same results. As we conducted a semi-structured interview, it's natural not to achieve the exact same results from every question. The pre-set questions were answered with similar answers by all informants. We concluded that the comparable data was mostly the same, with some variations of viewpoints and experiences. As our research is exploratory, we wanted quite a bit of general information about cyber security, risk management, and ethical hacking. In addition, all informants provided specific and general information, giving the data a high validity.

### ***3.3 Planning and Data Collection***

We conducted qualitative research in the form of interviews. We wanted to talk to someone with different experiences in cyber security and risk management. They don't have to be in a leadership position, but the ones working with risk management often have a connection with the management. We based our selection of informants based on a set of criteria, split into three groups of people. Johannessen et al. (2020) write that criteria-based selection means only the ones fulfilling these criteria are chosen. This narrows down our search and gives us people with the specific knowledge we are after. The groups were, first, someone who offered services connected to ethical hacking and cyber testing. They sell their services to companies wanting to test their security systems. Secondly, someone who overviews the process and is informed about the risks. This individual often has a continuous connection with their team and the company buying the services. Thirdly, we wanted to talk to someone who *buys* these services, like a bank or other financial institutions. To conduct our research, what companies we got a hold of was not too important. It will suffice if they have experience with cyber security and risk management. Companies with specific expertise in these fields are often medium to large-sized companies and not small local ones.

Before we started to contact possible informants, we had to plan the data collection. We wanted to conduct interviews in a semi-structured format. This means we first create an interview guide with a base of questions to start the conversation and to fall back on. The semi-structured format allows us to ask follow-up questions during the interview (Johannessen et al., 2020). The informants were found through either a professor at the University or by simply sending e-mails to people of interest. Some answered, and some didn't, as expected. The interviews were done physically or digitally, whatever suited the informant best. We wanted the interview to be physical, if possible. We think the conversational flow is better this way.

Onwards, we filled out a "SIKT personvern" document. It contains information about how we will store and process the data we collect. It is used to protect the informant's privacy and ensure we process sensitive and private information correctly. The informants were informed about their option to be anonymous or not. One of them opted to be anonymous; therefore, we are making all the informants anonymous.

Our questioning partly explains this, as we did not want our informants to discuss confidential or sensitive information. This line of questioning gave us a more personal angle to questions. It was important for us that the informants felt comfortable to get honest and quality answers. The interviews were recorded, allowing us to focus on the conversation and removing the need to write notes during the interview. This allows us to analyze the speech deeply and not jump to conclusions.

When conducting the interviews, we prepared 15-23 questions beforehand, plus planned small talk at the beginning. We sent the interview guide to all informants in advance. The guide was not identical to all informants, as we altered it with consideration to their role and education. We did not prepare any sub-questions, as we wanted to keep the interview loose. The estimated time was around 1 hour, but we wanted the informants to set aside at least 1 hour and 30 minutes in case they provided a lot of interesting information or if we had any technical problems. So, we wanted to get some general information about cyber security and more specific information about ethical hacking.

Additionally, we wanted to get information about how the ethical hacking process works. The informants were willing to answer all our questions. They provided a lot of useful information, especially about how the relationship between supplier and buyer works, the

procedures concerning security, and what “*hackers*” can and cannot do when testing the security system.

### 3.4 Case Descriptions

This subchapter will describe our cases. Primarily a description of who they are, what they do, and why we chose to talk to them. How we analyzed the collected data will be described in depth later in chapter three. We have decided to interview five people to get an in-depth understanding of our phenomenon. All of them either work or have significant experience within the field of cyber security. It’s important to mention that none of our interview objects talk directly on behalf of their respective company, which will be presented in chapter four. Their assignments and tasks are work-related, but their opinions are personal and based on experience. We opted to make all of the informants anonymous because one out of five wanted to be anonymous. We did this to make it as comparable as possible and protect the one who wanted to be anonymous.

<b>Name</b>	<b>Company</b>	<b>Role</b>	<b>Experience</b>	<b>Field</b>	<b>Duration</b>
<b>Karoline</b>	A national bank	Technical Advisor	13 Years	Security and Risk	1hr 7 min
<b>Simen</b>	Professional service company, one of the big four	Manager	5 Years	Red-Teaming	1hr 16 min
<b>Julia</b>	Security service provider	Head of IT-Department	7 Years	Ethical Hacking	1hr 5 min
<b>Aleksander</b>	Security service provider & university	Advisor / Associate Professor	10 years	Cyber Security	1hr 14 min
<b>Jens</b>	Large Scandinavian Bank	Head of Technology Security Oversight	20 Years	Security and Banking	1hr

Table 2: Overview of Informants



### **3.4.1 Interview Objects**

#### **Karoline, A national bank**

Our first interview was with Karoline, who works at a national bank. She works as what we call “a middleman,” meaning she’s neither a provider nor a buyer. She provides guidance and has insight into what goes on between the *ethical hackers* and the *buyers*. She studied as an IT engineer and has significant experience in the field of cyber security. She has worked with cyber security for several years, alternating different jobs. Karoline works closely with the implementation and execution of the TIBER framework. The TIBER framework primarily targets large financial institutions like banks, which is what she has the most experience with.

During the interview, Karoline seemed eager and excited to talk to us. She was interested in the subject of cyber security and how ethical hacking can be used in organizations. The conversation was relaxed and informal, allowing all of us to talk freely and not rely on static questions as much.

#### **Simen, professional service company, one of the big four**

The second interview was with Simen, who works at one of the big four accounting companies in Oslo. He works in a team with “*ethical hackers*” and provides services where they test a client’s security system to an extent ranging from small to large. A small extent can be just looking at protocols and procedures at the company. While a large extent can be a red team test or a complete run-through of security systems. Simen has previously worked with security abroad. He has a lot of experience with “*Ethical hacking*” and security testing at organizations. Earlier and in his free time, Simen likes to explore new ways to exploit and test security systems and do bug bounty hunting.

The interview with Simen was exciting and fun. He was interested in our problem statement and thought we had a up and coming concept. He was happy to talk about his opinions of ethical hacking and how it can be implemented as a risk management tool. Being an “ethical hacker” himself, he helped us understand what organizations buy this service and what they expected to get out of it. He also explained how he and his team worked with security testing. The flow of our conversation was good, and the semi-structured interview was helpful for us. It allowed us to quickly ask follow-up questions without being bound to the questions we had

written down. This could have created an unnatural stop in our conversations, interrupting the flow.

### **Julia, security service provider**

The third interview was performed online over Microsoft Teams. Julia works at a security service provider located in Oslo. The company provides security services everywhere, from general security consulting to more advanced technical services such as red teaming and ethical hacking. She works in the technical part of the company and provides similar services as our informant Simen does. The main difference is that Julia delivers a broader and more specialized service. The company provides client services ranging from a complete analysis of a company's security to small-scale advisory jobs.

Like the other informants on the «supplier» side, Julia was also engaged and willing to talk about her job and the company's services. As Julia works as head of technical services, she has a broader overview of the services provided to customers. She told us even more about “selling” and “buying” the services. A common trait from the informants selling the services is how strict and in order the process is. There are several protocols and security measures to ensure the risk is as small as possible when hiring someone to test your system. This interview was on Microsoft Teams, but the conversational flow was still good. She seemed comfortable doing the interview online and was at work.

### **Aleksander, security service provider and university associate professor.**

The fourth informant was Aleksander. During the interview, the informant gave us reflected answers based on education and experience. Aleksander works in a company providing security testing and solutions but does not work with this on a daily basis. He has mainly experience with economics but has written a thesis about cyber security. The valuable insight about how these two subjects merge more and more was interesting. It provided unique modern views to our thesis. He also provided data on how ethical considerations should be taken care of when doing a cyber test, especially considering the employees.

In this thesis, Aleksander acts as an expert in the field of cyber security and ethical hacking and not a supplier or deliverer of cyber security services. The unique perspective from an expert without bias from either supplier or deliverer is important when discussing the empirical findings. The interview was done over Microsoft Teams, and the conversational flow was without interruptions.

### **Jens, large Scandinavian bank**

Jens works in a large Scandinavian bank as head of security technology oversight. He has around 20 years of experience in the field of cyber security and provided insights primarily based on risk management and the risk connected to the services of ethical hacking. The bank is comprehensive, and we were informed that cyber testing was done internally and externally. As the rest of the interview objects, Jens was eager and excited to talk about his field. With extensive knowledge, he provided insight into how risk is managed and considered when ordering services connected to cyber security. Jens works mostly in Teams and has a role in managing and overseeing these.

The interview was done over Microsoft Teams, as neither he nor we had time to travel and join a physical interview. The Teams meeting was completed without technical issues, and the conversational flow was good. Previously he has worked as an advisor within cyber security in other companies.

### ***3.5 Data Analysis Method***

The data analysis is perhaps the most crucial aspect of the methodology chapter. It involves a systematic and thorough examination of the data collected. The purpose of the analysis is to identify categories and answers which are meaningful to our master thesis. The analysis was done in a systematic order to make sure we didn't miss any important information. We started by listening to and transcribing the interviews. We chose to transcribe them word by word but left out any meaningless conversation, such as where we are from and today's weather.

Repetitive words, or words without meaning, were also left out. This was left out to make the selection of quotes easier. Onwards, after copying the original documents, we deleted any information without value to our four chosen themes: Risk management, Ethical hacking, Cyber security, and Other interesting finds.

We found that the risk management aspect is important to any company buying or selling security services. The informants told us that strict rules and regulations are in place to protect all parties participating in these tests. The risk of an ethical hacker doing a harmful act is very low, as the professionalism is extremely high. The findings around ethical hacking focus on how the service works, what they do, and whether they pose a risk. We're told that ethical hackers provide invaluable insight into the companies' security systems, possibly finding holes and entryways open to malicious hackers. The value of finding these can be high, as well as reducing cyber risk.

The cyber security findings focus on what cyber security is and how it works. How are companies using it, and how can it be improved? We wanted to acquire information about how well cyber security is implemented in Norwegian companies. And is it still a priority when companies have high expenses elsewhere? We also wanted to know how well-prepared companies are for specific cyber-attacks and if they know how to handle them. But, as our informants told us, most companies are very little or not at all prepared. The aspect of learning and sharing was also brought up. The informants told us companies often do not share information about attacks successfully reported because they are "high risk." The last category presents other interesting finds that don't "fit in" anywhere, such as companies' risk appetite.

This made it even easier to sort the transcription into usable quotes. To extract the quotes, we wanted to look more at, we created a color code system and marked the quotes appropriately. Both members of the thesis reviewed all the text to avoid missing any important information. All the sorting was done under a "low heel," meaning we highlighted *anything* with value. We wanted to make sure we didn't miss anything and rather exclude some of the highlighted quotes. The quotes will primarily be used in chapter four, where the empirical findings will be presented and explained.

### ***3.6 Ethical Considerations***

When conducting research, it's important to consider ethics. Ethics are, first and foremost, about the relationship between people and what we can and cannot do to each other. When conducting research with people, ethical questions and dilemmas may occur (Johannessen et al., 2020). This thesis won't go deep into research ethics, only touch upon the base guidelines. Discussing the ethical considerations in a thesis is essential if sensitive and personal data is

being processed, especially medical information and sensitive data that may harm individuals or companies. Because of the thesis' delicate topic, "cyber security," it's important to note that taking ethical considerations will only get you that far. If one does not think about who can hack a system and access the data, the ethics have not been considered in its whole. Of course, there is only so much one can do, especially without financial means and backing. But papers and papers supported by the public/private sector should consider their storage and data collection systems. As mentioned by our informants as an example, a hospital using a cheap, insecure cloud service to store personal data could have massive repercussions later on.

On the website "forskningsetikk.no," the national committee for research ethics explains three crucial points to ethics (Johannessen et al., 2020; Torp, 2023):

### **1. Informants' right to self-determination and autonomy**

Whoever participates or has participated in our research decides if they want to keep participating or not at any given moment. Their involvement should be voluntary; if they choose to withdraw from the study, it shouldn't have any negative consequences.

### **2. Researchers' duty to respect the informant's private life.**

As mentioned before, we gave our informants the opportunity to be anonymous. And even though their first name and workplace will be visible, no additional information such as e-mail, phone number, or date of birth. However, if the informants wanted to be anonymous, no information that could identify them would be visible.

### **3. Researchers' responsibility to avoid damage.**

The last point regards every research where humans are affected, especially medical research. It must be considered through every aspect of the research if it can harm anyone connected. Therefore, anyone participating must be exposed to as little burden as possible.

### ***3.8 Chapter Conclusion***

The empirical chapter is important to create a foundation for the thesis. It explains how we will prepare the writing and data collection and give the reader insight into who's been interviewed. We've conducted five interviews with people whom all gave unique and valuable insight into the questions we asked them. When we started the interviews, our knowledge about ethical hacking was limited. We thought it was a process unknown to many organizations, with risks connected to malpractice and opportunistic malicious hackers. We thought the service was only provided to large banks and financial institutions, such as DNB and Sparebank1, as explained in the previously mentioned TIBER framework.

We found that ethical hacking is a service used by many organizations, especially large ones. It is often part of a more extensive security test, where ethical hacking is an important real-life simulation. It was surprising to see how "normal" these tests are in larger organizations, while it's worrying to hear how little it is utilized in most smaller and medium organizations. Onwards, we learned that professionalism is very high, and the rules and regulations are also stringent.

This master thesis is exploratory and relies heavily on the data collected from interviews. The reason for this is that there are none, or extremely few studies like this one, yet. The combination of merging ethical hacking into risk management procedures is unique. The thesis can be used for educational purposes by showing how risk management and cyber security work together. As well as an eccentric view from five informants working in the field of cyber security.

## 4.0 Empirical Findings

The empirical chapter will present our findings from the conducted interviews. The data is from five interviews with individuals ranging from ethical hackers to specialists within the field of cybersecurity. The chapter presents our informants thoughts and reflections around the three main topics of questions asked: *ethical hacking*, *risk management* and *cyber security*. It is important to note that some of the quotes provided will overlap within the three categories, as well as some interesting findings that do “not fit anywhere”. The data is sorted with our two additional research questions in mind.

1. *What are the benefits and challenges of ethical hacking for organizations?*
2. *How can ethical hacking be integrated into the risk management framework of an organization?*

The ethical hacking category contains questions primarily regarding what ethical hacking is, how it is used and the difference between hacking and ethical hacking. The findings concerning risk management will show informants’ view on frameworks concerning risk management and cybersecurity and what risks ethical hackers pose to organizations. Cyber security was often answered as part of another question, as we had few specific questions regarding cybersecurity.

### 4.1 Ethical Hacking Findings

As our research focuses on ethical hacking and how it can be used as a risk management tool, we started by gathering different perspectives on what ethical hacking is and what distinctive differences there are between traditional hackers and so-called ethical hackers. Some of the responses were as follows:

*“The reasoning behind it becoming a term was that in the beginning they were typically divided into black hats and white hats, something that made the distinction between the terms wider because there has never been something like an unethical hacker. It has either been a hacker or an ethical hacker... It comes from the fact that black hats were actually conducting real attacks.”*

*(Interview Object 2, Simen)*

*“It is a relatively simple definition; ethical hacking is hacking you explicitly have been given permission to do. Everything else is truly illegal, whilst ethical hacking is something you are allowed to do. You have e permit saying that you are allowed to do this.”*

*(Interview Object 4, Aleksander)*

When asked about the origin of ethical hacking and the difference between *hackers* and *ethical hackers*, our informants generally provided the same answer. They point out that the past suggested a hacker is someone with malicious intent and aims to cause harm to individuals or organizations. On the other hand, ethical hackers are someone who’s been allowed to poke around and find security flaws in the system. The distinct difference can be hard to pinpoint, as both activities aspire to get inside a secure system. All of our informants agreed that ethical hacking requires a high level of trust and control. They think that the use of risk management systems, internal controls, and a high level of oversight help reduce the amount of risk an ethical hacker can pose to companies when testing their system.

The use of ethical hackers can directly mitigate risks in organizations by finding vulnerabilities otherwise found with malicious intent. As pointed out, the difference between hackers and ethical hackers lies in trust, professionalism, and strict guidelines to protect the parties included in security testing processes. The balance between trust and control is one of the most important aspects when hiring someone to do security testing, and defining what can and cannot be done is vastly important.

### **Difference between pen-testing and red-teaming**

When addressing the topic of Ethical Hacking, the terms *penetration testing* and *red teaming* are frequently used and may confuse many. So, we wanted to get a better understanding of the differences between these terms and got the following clarifications:

*“There is a very distinct difference between a penetration test and a red team test, right? Because a penetration test is strictly scoped. It's for a set of servers for an IP range for an application something like that. It has some hard boundaries for the tester.”*

*(Interview Object 5, Jens)*



*“Red teaming is initially more of a **can we get caught or not caught** type of scenario, where it is preferred not to be detected. People don’t know that there is testing being done, and it is usually done in way less of a scope. It is more like **how much mischief can you cause?**”*

*(Interview Object 2, Simen)*

*Yes, it happens sometimes. We use techniques to avoid it, but usually we agree on a budget and timeframe, meaning we don’t have infinite time to write the perfect malware. Sometimes the client has put a lot of effort into the defenses as well.*

*(Interview Object 3, Julia)*

In relation to the distinction between penetration testing and red teaming, our informants shared similar views. According to their perspectives, penetration testing is a more focused approach to ethical hacking that concentrates on testing and manipulating specific parts of a system. In contrast, red teaming is a more dynamic and realistic approach that simulates real-life scenarios. The primary differences between the two approaches center around the scope of ethical hackers’ operations and the extent to which they can tamper with specific systems and areas.

When penetration testing is done, several individuals in an organization are usually informed, and a notice is generally given in advance, meaning the company is prepared. This test is done to test a system of the managements choice, for example, the webpage. On the other hand, red teaming is known to very few individuals in the organization, and generally, no notice is given out beforehand, leaving the company unprepared. The aim is to find an access point into the system without getting caught. However, as stated by our informants, sometimes you do get caught. If you do get caught, it means the *defenders* have *detected* you. The detection can be due to detection systems or luck.

### **Shortage in security professionals and the requirements in terms of education and skills.**

To be able to provide ethical hacking services to expanding markets, the need for security professionals is essential. In recent years, we have seen rapid growth in technology, but have our educational institutions been able to keep up? In addition, is there a shortage of IT and security professionals, and how does this affect companies providing ethical hacking services? The following are some comments surrounding the concerns:

*“... but I believe that the biggest problem or a vital aspect of the solution is to be able to motivate and educate enough people for the industry and to do the specific job. Because this is the problem, we see that people with talent and knowledge is at such a shortage that even if companies want to solve problems, they still find themselves struggling in getting inn enough people to do the job.”*

*(Interview Object 2, Simen)*

*“We knew that there has been a need for security professionals, not only testers but in every aspect, it has been a notified crisis. “*

*(Interview Object 1, Karoline)*

Professional security testers are something organizations need, but there are too few of them. Our informants told us new regulations such as DORA and TIBER would increase the need for security testing while also increasing the demand for testers. Not all of these testers need to have the capability of performing ethical hacking; security consultants are also valuable resources. One can argue that a limited number of security testers increase the quality of each one as the training becomes more personalized and of higher quality. However, if the workload is too high, the quality of their work may decrease. In an ideal situation, there would be enough security testers and high-quality training for everyone.

*“It requires technical knowledge, being able to understand computers and programing ... The last part is that you need to have a certain approach to things where you are creative and like to a look at problems differently ... We usually call this a hacker mindset or an attacker mindset.”*

*(Interview Object 2, Simen)*

*“... And some concerns you can have when you're dealing, that's not just for penetration testing is that's dealing with consultancy in general such as say EY, PwC, all of these guys not pointing at anyone is that **we are lacking security professionals in this world**. And that means that these guys are in constant hiring mode.”*

When asked to comment on the concerns, our respondents had similar perspectives. They all point out that there is a lack of IT and security professionals and a need to motivate and encourage students to approach fields such as cyber security. In addition, the right individual for the job has to have certain personality traits and qualities to succeed, which amplifies the importance of motivating and encouraging the right people.

One of our informants even states that the lack of security professionals can lead to desperation and misjudgment in hiring processes among consultancies. This can ultimately impact the overall quality of the service provided.

But why should a hacker act ethically? As stated, there is a lack of security professionals in every way. The ethical aspect comes from a desire to do good, and the same skillset can most likely be used to *hack* with malicious intent and gain a larger profit this way. As one of our informants stated, professional hackers can make a living selling malware to others, mitigating their risk of getting caught. And if this is the case, how can the balance between trust and risk happen? The main reason is the risk of being caught when doing a security test, as it's done within secure conditions. Also, the payment for breaking the trust during a security test would have to be quite large for it to be worthwhile.

### **Vendors providing security testing.**

Following the previous findings section, we wanted to better understand the actors providing penetration testing and red team services. For example, is there a large supply of vendors providing such services, and are bigger vendors always better? These were the following responses:

*“There is a large market for it, and it has exploded in the last few years. I believe they are hiring as fast as they can, and they have enough to deal with.”*

*(Interview Object 1, Karoline)*

*“Yes, I believe so. Ever since I started working within the field, I have noticed a large growth already, and I do not see any reason for it stop anytime soon.”*

*(Interview Object 3, Julia)*

As stated by our informants, there is a market for ethical hacking, and several actors provide such a service. However, as mentioned above, DORA and TIBER will affect how many vendors are needed to fulfill the demand. The obvious solution to tackle this problem is to increase the number of people and companies providing such services. However, security testing is a sensitive service and is based on trust; smaller and newer companies could have a hard time entering the market. This is why companies such as PwC and EY are also starting to provide these services.

*“I can come up with many names but take into account that there can be many more, I don’t want to be biased. Watchcom, Defendable, Netsecurity, yes there are a lot of suppliers of these types of services.”*

*(Interview Object 3, Julia)*

*“That’s where we’re starting to look into the contract and that’s not just for security testing. That’s just dealing with security consultancy in general, right? Because there is a lack of security skills. So bigger just not necessarily mean better. And the reason why bigger tends to go with bigger is that there are some mutual understandings on the level of governance and reporting that is expected.”*

*(Interview Object 5, Jens)*

When asked about the availability of pen-tests and red teaming services, our informants gave us several vendors that provide such services, ranging from large to small and medium size actors. There seems to be a market for these types of security measures, where even larger companies that do not mainly focus on security have side departments such as PwC and their red teaming services. One of our informants shared their opinion on why bigger usually does not mean better. It was pointed out that a mutual understanding among big companies may be the driving factor for large companies choosing large vendors. With having many employees and endless business opportunities, it is not a given that you’ll be delegated the best and most experienced security professionals. Factors such as scope, who is available at the time, duration, and complexity must be considered.

### **Will increased demand influence the overall quality of the service?**

In our interviews, we were curious about whether and how the quality of pen-testing and red teaming would be affected by increased demand. Some of the informants found this question quite interesting, and their opinions came out as follows:

*“Not necessarily, it does not have to happen, but realistically I believe the quality might drop a little due to the larger firms having the greater talents and them being able to pay more. The smaller firms will not necessarily be able to compete with the same terms, which might result in them having less talent, doing a worse job.”*

*(Interview Object 2, Simen)*

*“It is a real concern. I do believe that it will happen, and it will be really interesting what effect newer regulations might have. Because these regulations have to be quite detailed for it to not affect the quality. But then again, this might create another issue that only the largest suppliers being able to meet the new regulations. Then you will end up creating exclusive supplier markets and potential monopoly situations.”*

*(Interview Object 1, Karoline)*

*“...on our part, we recruit what we can, and it is yet difficult to find people. We do not lower our quality on what we deliver, but if the market becomes increasingly larger it becomes even more difficult to find the right expertise, so it can well be imagined ending up that way. That there will be actors out there delivering a mediocre product.”*

*(Interview Object 3, Julia)*

*“It is not unimaginable that there will be standardizations on what tests that companies will run, and also their reports. You’ll probably be able to uncover the most basic things, but I believe ethical hackers need room for creativity, only then they are able to find loopholes ... It is clear that if things get standardized, the quality may deteriorate.”*

*(Interview Object 4, Aleksander)*

After being asked how the quality of these services would be affected by increased demand and supply, the informants had similar interpretations of the dilemma. They all believed in some deterioration of the overall quality due to the lack of security professionals and desperation among vendors. Once again, several factors contribute to larger companies having an advantage in acquiring talent. This is often due to their ability to offer better opportunities or sometimes provide higher compensation than their smaller counterparts. One of our informants made an interesting comment on the possibility of security testing being standardized in the future. This can significantly impact how security testing could be provided and may bring some complications for smaller vendors.

Overall, it is difficult to say anything specific about whether the quality will change. Our informants state that higher demand for services such as ethical hacking is inevitable. The guidelines and emerging companies can and should still uphold a standard while delivering a quality product. Standardization is not guaranteed to lessen the quality. Guidelines may be so thorough that it covers almost the entire spectrum of cyber testing, however, it’s something that has to be updated continuously.

## **4.2 Risk Management Findings**

This section addresses the empirical findings concerning risk management aspects of acquiring ethical hacking services. In addition, our informants provide valuable insight and viewpoints on the positive and negative sides of security testing and what risks they believe ethical hackers pose to their organization.

### **Does ethical hackers pose as a risk to the organization?**

Ethical hackers can be used as a tool for measuring the level of security within an organization. With this in mind, we wanted to gather different perspectives on what risks these security professionals pose to an organization. For example, are there risks for ethical hackers to act unethically? Do some vendors pose a greater risk than others? Are ethical hackers trusted? We also wanted to look at how these risks can be mitigated. The following are some interesting finds:

*“Of course, there is a risk for it to happen, but I would not even bother typing it down to be honest. They’re commercial and pretty serious suppliers due to the level being so high. If anyone found out, it would be the end of that company. ”*

*(Interview Object 1, Karoline)*

*“All it takes is one mistake, and your credibility is gone ... It is a profession, you risk losing your job, and you’ll never get that back. So I don’t see it as a significant risk, but if we take a step back and look at the overall risk of conducting these types of security tests, of course, there is a risk.”*

*(Interview Object 2, Simen)*

*“I think that concern usually comes from a lack of understanding of the business. I mean, there’s a risk in everything we do. There’s also a risk of having people coming in and tampering with our systems. ... There is the unintentional consequence of them doing something that kills the system, that’s always a risk. ”*

*(Interview Object 5, Jens)*

The informants talked about how some risks cannot be mitigated and will always be present. Such as the risk of ethical hackers poking around a system not meant to be poked around in. The risk of compromising an important system will always be present. In addition, the risk of personnel doing something they shouldn’t is always present, although, a very low risk. As one

of our informants pointed out, the risk of such events is so low that he almost would not write it up. This is due to high level of professionalism, and strict guidelines throughout the testing.

*“... Being dishonest when they had access to our vulnerable system, they will no longer exist as a company, right? So as a company, we also trust that they are very much in control of their employees ...”*

*(Interview Object 5, Jens)*

*“That being said, of course, you need to do proper third-party risk management. You need to do it right. You need to understand who you're dealing with, not just because of the risk of the companies stealing, but also from the risk of the company not actually having the competence that they claim they have.”*

*(Interview Object 5, Jens)*

After being asked about the risk of acquiring ethical hackers and their services, our informants highlighted similar perspectives on the importance of trusting and knowing the people you let inside your organization. Risks are present whenever organizations perform an action. Having security professionals test your security system is not an exception. The importance of knowing whom you are dealing with and having a mutual understanding of trust is important. Our informants also shared their opinions on security professionals and what organizations should expect from them. The level of professionalism and integrity that comes with large vendors makes it career-ending for their employees to act unethically and with malicious intent.

There are several specific risks connected to using the services of an ethical hacker. The informants talked about how an ethical hacker may have insufficient skills. Inadequate skilled ethical hackers may fail to identify vulnerabilities, keeping organizations exposed to cyberattacks. A similar risk connected to this is inexperienced ethical hackers unintentionally damaging existing systems inside the organization.

The informants also talked about how standardization of cyber security practices can lower the quality of tests. Adaptability and keeping up with the newest cyber-attack methods are essential to keep a high quality on the test. However, standardization of tests can also downgrade the quality of legal agreements. These agreements are crucial to set parameters and protect organizations and ethical hackers. A dispute between the parties can occur without a predefined scope and good structure of agreements.

Another risk our informants mentioned was a breach of confidentiality and insider threats. Although a very low risk, ethical hacking requires security professionals to access data and systems. There is a strict confidentiality standard, but there is always a risk of information leakage, both intentionally and unintentionally. Overall, a high level of trust is required.

### **What benefits can Ethical Hacking bring to an organization?**

When addressing the topic of risk management and cyber security, organizations usually seek to gain new insight and value. With this in mind, we wanted to gain different perspectives on what value ethical hackers bring to organizations and how they benefit in improving security and risk management measures. The following is some insight from our informants:

*“I do believe that ethical hackers, or security officials should be considered a valuable resource. If we link it to risk management, there are large varieties of risks with a lot of uncertainties. It can become subjective, difficult to quantify, what is the actual possibility of it happening? Then, security professionals are worth their weight in gold.”*

*(Interview Object 1, Karoline)*

*“We need to do penetration testing simply because we are required to do it, but also because we think it’s a good tool and the same for red-team testing, which has now become a requirement. But of course, it is something we’ve been doing before it was a requirement because they are good tools.”*

*(Interview Object 5, Jens)*

*“It brings value to a place like ours, right, because being a bank, we are very governance heavy ...”*

*(Interview Object 5, Jens)*

*“It’s relevant to test the system, in the sense one often finds things that can be better, one often finds holes. On the contrary, it is very resource demanding due to high costs for the organizations ordering such a service.”*

*(Interview Object 4, Aleksander)*

After being asked what value ethical hackers bring to an organization, our informants had encouraging opinions to share. From a resource perspective, ethical hackers seem to be of great value to organizations. They bring valuable insights and perspectives on challenging and important aspects of organizations.



In addition, ethical hackers usually bring a different mindset and passion for solving complex tasks, making them valuable resources for improving security. On the contrary, some of our informants mentioned the high costs related to ethical hacking services due to their complexity and the resources that must be allocated towards it. One of the specific benefits organizations get from the use of ethical hackers is improved cyber security. By simulating real-world attacks, ethical hackers can potentially expose security holes and help organizations plan and strategize how to improve security.

### **How does an organization react to being tested?**

Cyber testing can make company employees nervous or eager to see how well their cyber security is. We wanted to find out how employees and management reacted to being tested to see if they took any specific precautions.

*“It varies. I have experienced that normal employees do not care too much. Those who work in the security department, or in IT, can become a bit defensive. Often if we find a weakness, they become very involved in the discussions and rationalize the findings with “we are working with this” or, “we don’t have enough resources.”*

*(Interview Object 2, Simen)*

*“It depends, sometimes the employees are used to the testing. Sometimes the employees work extra hard to update and have everything ready before testing.”*

*(Interview Object 3, Julia)*

When asked how the organization reacts to being tested, our informants told us it was a large variation between companies. Some employees reacted with caution and made sure to complete every update, as well as dodging any phishing emails. Sometimes only one to a handful of people know about the tests, often connected to the red team test. Even though the employees sometimes do not know about the test, they can catch glitches or bugs in the system when it's being tested. We were told this is most often reported and indicates a good company security culture. Onwards, the informants talked about how IT and security departments sometimes make excuses regarding why there was a security breach in the first place and sometimes blame time or budgets. This shows us that organizations might not prioritize cyber security as much as they should. We expected a similar answer to what we got, but we didn't think that most of the companies are informed about tests besides the red-team tests.

### **4.3 Cyber Security Findings**

The growing importance of cyber security comes from several factors. When the informants were asked about this, the answers did not vary too much. However, some of them elaborated more than others. They all agreed that in the last five years or so, we have seen an explosion in cyber-attacks, and thus the need for better cyber security systems.

*“I think many companies saw an explosion in the focus on security information, not just cyber security. And, of course, the crisis in Ukraine is putting this on the top of the agenda on many boards level.”*

*(Interview Object 5, Jens)*

*“This does not mean that there aren’t a lot of companies doing good and sensible work, but we have to remember that most organizations do not operate to be secure.”*

*(Interview Object 4, Aleksander)*

*“It’s definitely something that is being taken much more seriously that it was ten years ago.”*

*(Interview Object 5, Jens)*

#### **The importance of detection and response to cyber-attacks**

When it comes to cyber security, the focus usually lies in ensuring your organization is ready and prepared in cases of cyber-attacks. As well as being able to prevent them from happening. With this in mind, we wanted to get insight into what other procedures organizations value and if factors such as detection and response are equally important as prevention. The following were our informants’ views.

*“A principle one talks about is building security in layers. Not one layer defending everything”*

*(Interview Object 3, Julia)*

*“It is not always about stopping it completely, but rather getting to know quickly when it happens, known as detection. Typically, if you’re good at detection you may get to know within 12-24 hours, but if you’re bad at detection, you may never find out.”*

*(Interview Object 2, Simen)*

*“I think there is a truth in the saying that its more important to prepare for what to do if something happens, rather than putting everything into preventing it from happening.”*

*(Interview Object 4, Aleksander)*

When asked about alternative focus areas and being able to cope with cyber-attacks, our informants shared some interesting perspectives. They emphasized building security in layers, meaning having multiple stages of security and defense mechanisms. This can be achieved through having independent monitoring functions within your organization, internal security testers, and external security professionals such as ethical hackers coming in and giving feedback on current security systems and controls. These functions prevent external hackers from gaining access to various systems while forcing them to breach multiple levels of security instead of just one.

Our informants shed light on the importance of preparing and responding correctly when cyber-attacks occur. Organizations can respond accordingly and save valuable resources and time by being well-prepared for cyber-attacks. The focus should not be on stopping the attacks entirely but rather on being prepared for **what** to do when they first occur. To better understand the importance of being able to detect and response, IBM shared in their report that there has been a decrease in time taken to identify and contain data breaches of 3.5% from 2021 to 2022, which gives us an indication that this is gaining attention among organizations (IBM, 2022). As discussed in NIST and COSO, prevention, assessment, and identification of risks are also important. If you can stop the attack from happening entirely, the company will save money and time.

### **Shearing of knowledge and security measures**

On the topic of cyber security, one of our informants shared their view on the lack of information sharing among organizations regarding security. The following was stated:

*“The information sharing, and information flow is becoming a huge problem. Security measures comes in the way of sharing information. It has become unsecure to share information about security.”*

*(Interview Object 4, Aleksander)*

Prior to this, we had a shared understanding of security information being classified as sensitive information, but we would believe organizations would be more open in sharing aspects of what they do to educate each other. As our informant stated, information flow and sharing become increasingly difficult to share due to security measures and risks playing a part. It becomes more of a risk in the sense that organizations might fear their information sharing may lead to them being more vulnerable and exposed to cyber threats. That it becomes unsecure to share information about security in cases of this being used for the wrong purposes.

On the other hand, sharing could be argued to be a helpful tool, especially when it comes to communicating and learning from each other's experiences. If information flow and sharing were less of a taboo topic, organizations could benefit in many ways. For example, if this is from learning from each other's mistakes or implementing certain aspects or security controls that are proven effective, organizations could gain a shared value.

### **Norwegian cyber security compared to European countries.**

Cybersecurity is a growing topic of importance both globally and among organizations. Prior to interviewing our informants, we had a general understanding of Norway being a country that heavily focuses on cyber security due to our national reserves and resources. With this in mind, we wanted to get our informants' perspectives on how Norway is doing as of now compared to other European countries. The following were their thoughts:

*“Yes, the impression I’ve got is that large companies in Norway are becoming more mature. They are no longer in the starting phase. Medium sized companies are starting to scratch their heads and begin to think about it, while small companies either does not have enough resources, or not enough insight.”*

*(Interview Object 2, Simen)*

*“I think other places in Europe are starting to become better, but I think firms in Norway don’t realize how exposed they are.”*

*(Interview Object 2, Simen)*

Our informants shared their opinion on the maturity level of organizations in Norway and that they are becoming more mature and aware of the risks and benefits. Cyber security is becoming more important daily, especially as technology evolves. Large organizations seem to have the severity of the risks that come with poor cyber security, while small to medium size organizations are catching on. Some explanations for SMEs being slower to act on the agenda may be due to financial restrictions or a lack of understanding of the topic. Cyber security could be perceived as an unnecessary hurdle for smaller firms as thoughts such as “*Who would do anything to us? We're just a small firm minding our own business*” would be present. This type of ignorance is exactly why we should be worried because organizations do not realize how exposed they really are to external threats.

#### ***4.4 Other Interesting Findings***

##### **Risk appetite and monitoring**

When addressing the topic of risk management, we have got familiar with certain terminologies, such as risk appetite and monitoring, which tells us something about the level of risk an organization is willing to accept in pursuit of value (Moeller, 2011). Our informants brought these terms to our attention, which showed us that organizations have various parameters in place to measure risks. For example, our informants stated the following:

*“One of the most complex tasks we have is trying to measure risk, testing the risk. What is the probability of this happening, and what would be the impact? What is our risk appetite?”*

*(Interview Object 5, Jens)*

Our informant reflects on the complexity of measuring risks and mentions the importance of assessing factors such as probability, impact, and risk appetite. Risk appetite emphasizes the basic idea that every manager or collectively an enterprise should have some level of appetite for risks. Some may prefer risky ventures promising high returns, while others prefer lower risk for a lower reward. Risk appetite may give us a better understanding of an organization and its maturity in addressing risks. Hand in hand with risk appetite, our informant mentions the impact ethical hacking may have as a tool for monitoring risks:

*“I see huge value in this. Yet another control and as a monitoring and assurance testing tool.”*

*(Interview Object 5, Jens)*

Risk monitoring addresses the focus on the ongoing processes of identifying, assessing, and responding to risks and the possibility of certain risks occurring (Moeller, 2011). Together, risk appetite and risk monitoring are key components of effective risk management. By defining and monitoring their risk appetite, organizations can better understand and manage the risks they face and make informed decisions on how much risk to accept in their pursuit of value.

#### ***4.5 Chapter Conclusion***

Chapter four presents the empirical findings gathered from the five conducted interviews in a transparent way. The findings are separated into three categories based on the two sub-research questions and the main research question. The quotes presented are discussed and talked about before further addressing a selection of them in chapter five. The discussing in chapter four helps us analyze further in chapter five.

## **5.0 Analysis and Discussion**

This chapter will focus on analyzing the empirical data from chapter four and link it to our theoretical framework presented earlier in the thesis. Additionally, the chapter will address the following two sub-research questions:

- *What are the benefits and challenges of ethical hacking for organizations?*
- *How can ethical hacking be integrated into the risk management framework of an organization?*

Here, we will present sub-conclusions that will be further developed in the next chapter to form the conclusion for our thesis. Finally, as our main research question is “*How can Ethical Hacking be used as a Risk Management tool in organizations?*” we will examine relevant theory and empirical data collection gathered from our informants.

We have chosen two sub-research questions that we believe are relevant to the thesis and the main research question. The questions in this section will be supported by the findings from chapter four and tied to the theory in chapter two. Ultimately, these questions will guide the conclusion.

### ***5.1 Benefits and challenges***

The first research question we will answer is, “*What are the benefits and challenges of ethical hacking for organizations?*”. We believe that by looking at the benefits and challenges of ethical hacking and connecting it to institutional theory, we can better interpret its value to organizations.

Ethical hacking is a relatively unknown term among the general population, but in the realm of cyber security, it has its reputation of being a valuable tool for managing risks. Risk management has always been at the top of the agenda for many organizations, and with the increasing variety of risks emerging, it has not changed its role. When trying to express the value of what ethical hackers bring to organizations, our informant working for a national bank had the following words of encouragement:

*“I do believe that ethical hackers, or security officials should be considered a valuable resource. If we link it to risk management, there are large varieties of risks with a lot of uncertainties. It can become subjective, difficult to quantify, what is the actual possibility of it happening? Then, security professionals are worth their weight in gold.”*

*(Interview Object 1, Karoline)*

In a digital era where new cyber risks always emerge, having the right tools and procedures is crucial. The demand for security professionals is increasing by the day, with their skillsets and knowledge being of great value to organizations. Primarily, ethical hackers bring value to an organization in the way they think and their creativity when solving complex tasks. Hackers with malicious intent share some of the same characteristics and traits as ethical hackers, making countermeasures essential. Ethical hackers serve as an additional security measure in an already established security environment but can also benefit less mature organizations. The main essence lies in creating multiple layers of security.

*“A principle one talks about is building security in layers. Not one layer defending everything”*

*(Interview Object 3, Julia)*

Additionally, ethical hackers can bring several benefits to an organization when addressing the topics of stakeholder expectations, legitimacy, and social acceptance. Organizations are prone to external forces and regulations shaping and dictating their activities and decisions. When looking at security testing, you can draw comparisons from sustainability reporting and what impact it has had on organizations. Sustainability reporting is, as security testing, a growing topic of importance among stakeholders. What we have in recent years seen an explosion in the number of organizations reporting on sustainability, which is a result of external regulatory requirements, regulations, and shareholder expectations (Dubey et al., 2017). This is something we expect will happen to security testing.

In institutional theory, many concepts overlap with security testing and ethical hacking practices. As previously presented in the theory chapter, we address the cyber resilience frameworks of TIBER and DORA. Both frameworks emphasize security-improving practices and work in line with regulations and industry standards. Although TIBER is not a requirement by law, it is interpreted as a good practice among financial institutions and



central banks. The framework has been adopted in thirteen countries across Europe, including Norway, where its focus is on building joint expertise and experience (*TIBER*, 2023).

As institutional theory explains, regulative institutions directly impact organizations through regulations, policies, and standards (DiMaggio & Powell, 1983), which fall within the field of security testing. With many European countries adopting the practice of using TIBER and ethical hackers, they gain legitimacy and social acceptance because they work proactively towards solving a problem that may have serious negative effects in the future. Countries adopting such practices illustrate that organizations gradually gravitate towards and, at some point, resemble each other. This is highlighted in the research done by DiMaggio and Powell (1983) on institutional isomorphism, where uncertainty provokes mimetic behavior among organizations.

Another good practice we see reoccurring among organizations is the implementation of ISO standards. Implementing these standards benefits organizations by showing commitment and compliance with internationally recognized good practices (*ISO Strategy 2030*, 2021). The use of ISO standards in cyber security will have a positive effect on customer satisfaction and legal compliance, where some customers will value suppliers that demonstrate adherence to internationally recognized standards. In this context, cyber-attacks and data breaches tend to happen unexpectedly, emphasizing the importance of being versatile and prepared for uncertainty. Ethical hacking is beneficial because it is recognized as a good tool, and organizations acknowledge it as a practice of value.

With there being good practices organizations adopt from each other, external and internal pressure from stakeholders shape organizational behavior as a whole. As institutional theory suggests, there are normative institutions that establish what may be considered appropriate behavior and guide organizations in their decision-making. Stakeholders may impose specific requirements or demands, such as security and penetration testing, which makes ethical hackers in high demand and of great value. Our informant representing a large Scandinavian bank stated the following when asked about why they do penetration testing:

*“We need to do penetration testing simply because we are required to do it, but also because we think it’s a good tool and the same for red-team testing, which has now become a requirement. But of course, it is something we’ve been doing before it was a requirement because they are good tools. ”*

*(Interview Object 5, Jens)*

Ethical hacking is a practice that requires comprehensive and strategic planning and, in many cases, can be costly for organizations. With the framework of DORA and its focus on security testing among small to medium enterprises, we expect an overall increase in security testing. This makes regulations even stricter and opens possibilities for more standardized services and affects the organization in how they carry out tasks and procedures, forcing them to adapt to change. Our informant brought up these particular concerns:

*“It is a real concern. I do believe that it will happen, and it will be really interesting what effect newer regulations might have. Because these regulations have to be quite detailed for it to not affect the quality. But then again, this might create another issue that only the largest suppliers are able to meet the new regulations. Then you will end up creating exclusive supplier markets and potential monopoly situations.”*

*(Interview Object 1, Karoline)*

As of today, ethical hacking is a strict practice carried out by several parties (Yamin et al., 2020), which makes it a resource demanding service with high costs. With the emergence of the cyber resilience framework of DORA, we can expect an increase in demand after security testing due to the majority of small to medium size businesses being affected. This will result in there being too high of a demand after security testing that the supplying vendors cannot fulfill. This leaves us with the concern of organizations out there needing security testing that are simply unable to get the security professionals they need.

Ethical hacking is a practice that heavily relies on creativity and the ability of problem-solving, where the potential of standardization can be challenging. This practice today is somewhat standardized because certain measures and procedures are mandatory and cannot be tampered with. Security officials will have to adjust and adapt to new practices and regulations, which will impact their services.

To confirm our suspicions, one of our informants shared their views on what impact the framework of DORA may have in the market of security testing.

*“It is one of my biggest concerns with DORA as a whole. It will come as a shock for many organizations. It will be a positive thing for the suppliers and will create large demand if not dealt with correctly. Because, if there is one thing there is a shortage of today, it’s in security professionals ... It is already a large shortage here, and all of a sudden it may triple or even quadruple.”*

*(Interview Object 1, Karoline)*

Although with the concern of the demand skyrocketing with the addition of DORA, not all our informants shared the same views.

If one were to standardize ethical hacking services, they could become more affordable to the companies affected by DORA. By selling “packages” of security testing with standardized content price and testing, they can still comply with regulations and use ethical hacking as a tool to mitigate risk. These packages would most likely be delivered by public companies to control the price and could create a difference in quality between the private and public markets. However, as mentioned, standardization would mean the services require a certain amount of testing to be done, leaving the company with at least some degree of security testing.

Despite the challenge of ethical hacking becoming a fully standardized practice, the biggest challenge suppliers face is the lack of security professionals, which forces suppliers to be in a state of constant hiring. There has been a notified shortage of ethical hackers for quite some time, where the industry hasn’t been able to meet the desired need for security professionals. This is because of a lack of motivating and engaging with individuals interested in information technology and security. Several of our informants had similar perspectives on this agenda.

*“... but I believe that the biggest problem or a vital aspect of the solution is to be able to motivate and educate enough people for the industry and to do the specific job. Because this is the problem, we see that people with talent and knowledge is at such a shortage that even if companies want to solve problems, they still find themselves struggling in getting inn enough people to do the job.”*

*(Interview Object 2, Simen)*

This concern is challenging to address, where motivating and encouraging individuals toward a specific career path can be difficult. Although there are many ways to go about this, the main focus should be on motivation in terms of highlighting the importance of cyber security and the consequences surrounding cyber-attacks. This can ensure that individuals eventually go in the direction of cyber security.

To illustrate the benefits and challenges connected to ethical hacking, we have created the following table.

	<b>Benefits</b>	<b>Challenge</b>
<b>Improving Cyber Security</b>	X	
<b>Meet Regulations</b>	X	X
<b>Legitimacy and Social Acceptance</b>	X	
<b>“Good Practice”</b>	X	
<b>High Costs</b>		X
<b>Increased Demand</b>	X	X
<b>Supply of Security Professionals</b>		X
<b>Standardization</b>	X	X
<b>Risk Management</b>	X	X

Table 3: Benefits and Challenges with Ethical Hacking

There are several benefits to the practice of ethical hacking, where organizations can improve their security measures while also being able to meet regulatory, normative, and cultural-cognitive institutional demands (DiMaggio & Powell, 1983). When it comes to ethical hacking, there is no “one” main benefit that stands out, but rather a bundle of benefits that can propel an organization into becoming more secure and better prepared for cyber-attacks. Management in organizations may argue that security is a vital aspect of their business, but we must remember that not all companies operate to be safe. Financial performance and reputation are some of the most important aspects of an organization, but what value do these things hold when they are not properly protected against external threats? This is where ethical hacking excels in bringing value to organizations by helping organizations identify vulnerabilities and assist in protecting valuable assets.

With that being said, there are yet some challenges that cannot be overlooked. First, ethical hacking is an expensive practice to implement in organizations. It requires extensive planning and preparation, where several parties must be involved in the process, generating high costs and resource allocation. Secondly, with the emergence of cyber resilience frameworks such as TIBER and DORA, the supplier will be prone to large demands, which creates monopoly markets and organizations being unable to get extensive security testing done on their systems. This makes room for malicious cyber-attacks to occur, especially when it comes to organizations that are in desperate need. Lastly, cyber security and information technology industries are in desperate need of security professionals. This challenge, in particular, stands in the way of ethical hacking being supplied in accordance with the increased demand.

When looking at the benefits and challenges of ethical hacking, we conclude that there are more benefits to the security testing practice than challenges. Even though the challenges presented can seem difficult to handle, they are very manageable. Furthermore, if the public and private sectors come together and combat the potential increasing demand, a larger number of organizations can benefit from the great security practice of ethical hacking.

## ***5.2 Integrating Ethical Hacking***

The second research question will answer “*How can ethical hacking be integrated into the risk management framework of an organization?*”. In detail, this sub-chapter will discuss and see if ethical hacking and cyber security testing fit into traditional risk management frameworks, in our case, COSO. We will look into the positive and negative sides before answering the question.

Technological advancements have developed at a rapid pace over the last years producing other arenas where risks may occur. Using ethical hacking as a risk management tool, companies can simulate real-world attacks and test specific systems to see how their security holds up. Our informants state that ethical hacking helps companies stay updated and adaptable. Ethical hackers must stay up to date on new ways to hack into a system, thus helping companies. The system can therefore be up to date by other means than just scheduled updates.

As stated earlier in this thesis and by our informants, there is a rapid increase in cyber-attacks, and companies need to prepare what to do when facing these new threats (IBM, 2022; Saravanan & Bama, 2019). Cyber risk management frameworks must address both the technical and human aspects of the framework. However, COSO does not take the technical parts into account, leaving organizations vulnerable to certain aspects of risk. For example, although the NIST framework is well-known and provides quality guidelines for managers and employees, it does not explicitly mention the implications of using this combined with the risk management ecosystem. Furthermore, none of the frameworks provide guidance on how companies can justify their spending on cybersecurity or traditional risk management (Lee, 2021).

As companies try to quantify and identify new risks, it’s hard to pinpoint what these are without trained personnel. An employee in a risk management team might know everything about traditional risks, how to handle them, identify them, and use resources most efficiently. Furthermore, our findings indicate that cyber risks are often something that cannot be “guessed”, as it needs educated or experienced employees with specific skills. However, current risk management systems can be used to manage risk. Therefore, the new employees should train the existing personnel in working within risk as this reduces costs while

providing valuable insights and learning from each other (Lee, 2021; Moeller, 2011; NIST, 2023).

*“I see huge value in this. Yet another control and as a monitoring and assurance testing tool.”*

*(Interview Object 5, Jens)*

Implementing ethical hacking services into the organization is not something that’s done once and then never again. The digital age is constantly evolving, and hacking attempts are no different. In fact, updating digital systems may open for easier access to it, as it’s not gone through extensive testing or rushed into the market (Akram & Ping, 2020). And sometimes, old vulnerabilities lay dormant, not being discovered for years. Therefore, performing cyber security tests internally and externally regularly is essential to keep systems secure (Saravanan & Bama, 2019). In addition to keeping systems secure and updated, it helps companies train for real-world events. They must react and follow procedures to detect and respond to attacks. An example made by our informants was a hacker entering a system, shutting employees out. When employees went to see what procedures to follow, it was all on a now blocked digital server. These types of scenarios are something that companies can discover when using ethical hackers. The evaluation of security policies, test of response plans and raising awareness are all benefits from ethical hacking services (NIST, 2023).

As one of our informants pointed out, they often perform penetration testing and get into the system relatively easily. Organizations that had not had extensive security testing before and only relied on in-house competence. The reactions when ethical hackers told companies they were inside the system varied, but in general, it was “Oh, what do we do now?” meaning they weren’t prepared for such an event. Some want the ethical hackers to continue, others want to stop, this should also be defined in a contract.

*“Yeah, several times. The other end is often not used to this situation and becomes very stressed, saying, “What do we do now?”. If they panic, it’s necessary to step in and give some guidance.”*

*(Interview Object 1, Julie)*

By continuing the test, one increases the chance of mistakenly compromising the system, especially if the company has little or no plans on how to restore this system. This is always a risk when performing ethical hacking. When this happens, it's important to remember the human aspect inside the organization. The one responsible, maybe even proud of their IT system, may see their work fall apart, worried the company might not see their value anymore. This is a positive and negative side of using ethical hacking in organizations. On the positive side, the company will learn a lot from this event. By sharing it throughout the company, one can raise awareness and build a security culture. On the negative side, the workload after such events can be massive for small and medium organizations, especially if the IT team is small (Moeller, 2011; NIST, 2023).

*“You have to take care of your employees. Also, you have to be aware on how the experience feels for the employees.”*

*“Ethical hacking buys a condition report, giving one loads to work on after it is completed”*  
*(Interview Object 4, Aleksander)*

*“It's a balance of being pleased with your own work, and also have empathy for the ones receiving the report with documented flaws”*  
*(Interview object 1, Simen)*

Ethical hacking can sometimes be projected as a quick fix to an organization's security issues. It's, in fact, part of a larger costly security test that takes time and effort from both the company providing security services and the company buying these services. Firms without a comprehensive security system or that are using ethical hackers for the first time often receive several notes. As mentioned above and provided by our informants, a report is provided after buying ethical hacking services, where they do not actually fix the security problems without it being stated in the contract or agreed upon.

Even though ethical hacking provides several benefits when implemented in the organization, it's part of an extensive implementation that affects the company as a whole. As discussed, regulations and laws may require companies to implement security testing of some sort, meaning the demand will rise.



A rise in demand without more suppliers will lead to increased prices, making security testing even more unavailable for companies. As mentioned by our informants, it's not cheap and takes quite a long time to implement and test the system.

*“Large companies are on their way, medium companies are thinking about it, and small companies does not have enough insight, or high enough money”*

*(Interview Object 2, Simen)*

*“It is a risk minimizing tool when finding the errors, or at least a much more informed picture of internal risk. The risk control comes after the service is done, sometimes with suggestions on how to improve their cyber security”*

*(Interview Object 4, Aleksander)*

The second sub-research question, *“How can ethical hacking be implemented into an organization?”* will be divided into how small, medium, and large organizations are able to implement ethical hacking, where some will overlap. We assume all medium and large-sized companies have a strategy or framework in place to manage risk in different ways. Even though most companies don't specifically use the COSO framework, they tend to have guidelines connected to risk management touching upon the framework. One of the first important steps before implementing ethical hacking in any business is to assess their current cyber security.

In a quote mentioned by one of our informants, they said small organizations are not thinking about cyber security yet. They either don't have the knowledge or the budget to do this. Also, why would, for example, a local butcher shop think about cyber security? Most of these small organizations do not have cyber security as a goal, they are only trying to achieve profit from their business and live off it. These small organizations may not have the need for extensive security testing, but as the transition over to digital systems advances, some security testing is needed.

Small companies are often not in need of comprehensive ethical hacking, as they do not have a large cyber security system. If we use a local butcher shop as an example, the shop may have digital inventory lists and a registry for purchases and payments. However, these companies rarely use in-house accountants, meaning their financial information is located under a different company. Small companies should still implement security testing into their risk management, as digital risks might still be their most significant risk. If their system is hacked, it could serve as an access point to other networks, as it is all connected. As ethical hacking is an effective way to get a clear and good overview of your cyber security, small businesses should implement and conduct this routinely. The implementation of ethical hacking could cost a small firm quite a bit, but a thorough security check will keep the company's cyber security up to date (Moeller, 2011; NIST, 2023).

*“This does not mean that there aren't a lot of companies doing good and sensible work, but we have to remember that most organizations do not operate to be secure.”*

*(Interview Object 4, Aleksander)*

Medium sized companies are recognized as businesses with below 100 employees and small and medium-sized companies account for 99% percent of all companies in Norway (NHO, 2021), creating an extreme amount of possible cyber security demand. Medium companies have many more digital systems, including financial aspects such as accounting, salary, and personal employee information. In addition, they often have unique applications and networks. Both large and medium companies should have an extensive risk management strategy and their own IT department. Implementing ethical hacking into the organization would have to be done by extensive research and assessment of their current cyber security to see where ethical hacking should be performed for maximum value. As with small firms, the cost of implementing such a service would cost quite a bit, but it is a necessary step to reduce cyber risk. A large company holds mostly the same principles as a medium company, just in increased size. It will have more assets to protect but generally a sophisticated IT department, as well as guidelines and procedures connected to cyber security and risk management.

*“Ethical hacking reports on the immediate status. We tell them we found this and that, which may help them get a better budget, or priority focus on the most important security issues”*

*(Interview Object 2, Simen)*

*“We cannot tell companies how to run their risk management procedures. They own all the risk.”*

*(Interview Object 1, Karoline)*

How a company can implement ethical hacking is based on its size, industry area, number of employees, and how much they are digitalized. As mentioned, a butcher will not have the same need for ethical hacking as a hospital or a bank. The larger the firm, the more assets are covered under cyber security, making ethical hacking cost and take more time. However, a well-executed risk management strategy and a professional IT department can make the implementation more manageable and less resource demanding.

### ***5.3 Ethical Hacking as a Risk Management Tool in Organizations?***

As presented previously in this chapter, we have analyzed and discussed the two sub-research questions “*What are the benefits and challenges of ethical hacking for organizations?*” and “*How can ethical hacking be integrated into the risk management framework of an organization?*”. After answering these two sub-questions, we can with certainty say that ethical hacking can be used as a risk management tool in organizations.

Organizations constantly face external pressure. Laws and regulations will dictate the future of cyber security. Even if cyber security frameworks like TIBER is used in Norway and looked at as a valuable tool, it’s not required by law. This is where DORA comes in and will make a huge difference. It’s a framework that affects all small and medium-sized businesses, which account for 99% percent of companies in Norway (NHO, 2021). The question will then change from “*Do we need security testing?*”, to “*How much do we need to spend on security testing?*”. This is where ethical hackers can be used as a risk management tool in organizations, precisely to test security measures and give feedback on findings and points of improvement.

To use ethical hacking as a risk management tool, it’s important to look at what existing risk frameworks organizations already have in place. A variation of risk management practices that can be found in COSO is often used, as it is comprehensive and covers almost all elements of risks, except specific cyber security risks. By using the NIST framework to manage these specific risks, we see an opportunity to implement ethical hacking into the risk management framework. Using this approach may be critical for organizations that want or are required to assess and test their cyber security (Moeller, 2011; NIST, 2023).

When the world was introduced to sustainability reporting, companies were still unprepared. It was looked upon as another task costing money without obvious positive side effects. Fast forward to 2023, sustainability reporting is something all stock-listed companies have to report on. It is only a matter of time before the same happens with cyber security. Not only will such a practice be required by law, but external forces can create noise inside organizations. As an organization, it's their responsibility to keep stakeholders satisfied and follow social norms to avoid being excluded and discredited as serious actors (Dubey et al., 2017). Again, we see that ethical hacking is a great risk management tool.

## 6.0 Conclusion

Our thesis aims to see if ethical hacking can be used as a risk management tool in organizations. The thesis is an exploratory qualitative study based primarily on five interviews, and in addition, we use relevant theoretical frameworks. To answer the problem statement, we've asked two research questions. The main problem statement was answered with the conclusion that ethical hacking can be used as a risk management tool. It's a benefit for organizations now as the world is becoming even more digital and may become a requirement later. However, it can be a costly and resource-demanding service. Companies with a well-established risk management strategy, such as COSO or a variant of COSO, can reduce resource use.

Based on our research, it is clear that cyber security is a critical and increasingly important topic that demands attention. The media coverage of cyber scandals has shed light on this issue's urgency and brought it to the forefront of public interest. As a result, we believe that stricter security requirements will soon be established, making the role of ethical hackers even more valuable. When we initially started our research on ethical hacking, it was limited to available data. The topic is relatively new and in a constantly evolving field. We have perceived the subject to be somewhat unknown to the general public but rather familiar among personnel in the security industry, which has given us confidence that the topic is spreading in suitable industries.

Throughout history, hacking has always been associated with negative connotations. Hackers have been portrayed as malicious individuals seeking to cause chaos and destruction. However, the term "hacker" has become less ambiguous with the rapid advancements in technology and security. As we furthered our knowledge within the field, we discovered that hackers can be utilized to improve security measures in organizations.

As demonstrated in figure 2 and supported by our informants, ethical hacking can improve cyber resilience in organizations by being a dynamic risk management process. It can be leveraged as a regulatory tool to comply with future security testing requirements outlined by DORA and TIBER, as well as meet stakeholder expectations. Our informants noted that it is only a matter of time before cyber security testing becomes mandatory for almost every business, underscoring the importance of having skilled and competent security professionals, including ethical hackers.

## ***6.1 Limitations and Theoretical Implications***

The purpose of this research was to shed light on risk management, cybersecurity, and ethical hacking. This thesis contributes to the theoretical understanding of ethical hacking and its potential as a risk management tool in organizations. The thesis considers NIST and COSO frameworks while comparing them to informants' perspectives. This research can act as an information guide to organizations regarding the practical implications. It can also be a viewpoint for companies considering ethical hacking and cyber security services.

One significant limitation of this thesis is the lack of similar research on the topic, which limited our ability to compare and contrast findings with existing literature. In this study, we relied on information provided by our informants and general knowledge about cybersecurity and ethical hacking. However, the unique perspectives and insight each informant provided proved valuable in filling this gap in knowledge. Our informants expressed a shared enthusiasm for ethical hacking, which they see as a growing field that will become increasingly important in the coming years. They also highlighted the fact that many organizations are ill-prepared for cyber-attacks, underlining the need for the implementation of cyber risk frameworks. While our informants were eager to discuss the topics of cyber security and risk management, the limitation of discussing only non-confidential information during the interviews restricted the information we were able to extract.

Another limitation of this study was the difficulty in finding informants who had implemented specific cybersecurity and risk management procedures in their organization, which could have provided us with more detailed and practical insight. Despite efforts to reach out to companies, the limited timeframe and lack of responses posed a challenge.

## ***6.2 Future Research***

It is fascinating to see how important cyber security is and what an impact ethical hacking can make. It would be interesting to see if ethical hacking can be used as a risk management tool and how it's used explicitly in organizations today. Looking at how cyber security evolves with risk management would also be exciting to follow. It's a term that will change a lot in the coming years and will probably be affected by laws and regulations at some point. A study showing how an organization tried but failed to implement ethical hacking would be instructive. However, it proved challenging to find such a case with the time limitation of a master's thesis.

## References/Literature

### Litteraturliste

- Akram, J., & Ping, L. (2020). How to build a vulnerability benchmark to overcome cyber security attacks. *IET Information Security*, 14(1), 60-71. <https://doi.org/10.1049/iet-ifs.2018.5647>
- Bourmistrov, A. (2022). *Topic 1. COSO Framework*. Canvas. <https://nord.instructure.com/>
- Calder, A., & Gerrard, L. (2013). THE ISO/IEC 27000 FAMILY OF INFORMATION SECURITY STANDARDS. In (2 ed., pp. 12). United Kingdom: IT Governance Publishing.
- Christen, M., Gordijn, B., & Loi, M. (2020). *The ethics of cybersecurity*. Springer Nature.
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American sociological review*, 147-160.
- DORA. (2022, 28 November 2022). *The Digital Operational Resilience Act (DORA)*. Cyber Risk GmbH. Retrieved 17.12.2022 from <https://www.digital-operational-resilience-act.com/>
- Dubey, R., Gunasekaran, A., Childe, S. J., Papadopoulos, T., Hazen, B., Giannakis, M., & Roubaud, D. (2017). Examining the effect of external pressures and organizational culture on shaping performance measurement systems (PMS) for sustainability benchmarking: Some empirical findings. *International Journal of Production Economics*, 193, 63-76.
- Engelbreton, P. (2013). *The basics of hacking and penetration testing: ethical hacking and penetration testing made easy*. Elsevier.
- Falk, C. (2014). Gray hat hacking: morally black and white. *Gray Hat Hacking: Morally Black and White*.
- Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., & Smeraldi, F. (2016). Decision support approaches for cyber security investment. *Decision support systems*, 86, 13-23.
- Harper, A., Linn, R., Sims, S., Baucom, M., Fernandez, D., Tejada, H., & Frost, M. (2022). *Gray hat hacking: the ethical hacker's handbook*. McGraw-Hill Education.
- Hopkin, P. (2018). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Kogan Page Publishers.

- Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, 45, 3171-3189.
- Hydro, N. (2019, October 14, 2020). *Cyberangrep på Hydro*. Retrieved April 22 from <https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/>
- IBM. (2022). *Cost of a data breach 2022*. I. Corporation. <https://www.ibm.com/reports/data-breach>
- ISO Strategy 2030. (2021). <https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100364.pdf>
- Jagnarine, A. A. (2005). The Role of White Hat Hackers in Information Security.
- Johannessen, A., Christoffersen, L., & Tuftte, P. A. (2020). *Forkningsmetode for økonomisk-administrative fag* (Vol. 4). Abstrakt Forlag AS.
- Kozhuharova, D., Kirov, A., & Al-Shargabi, Z. (2022). Ethics in Cybersecurity. What Are the Challenges We Need to Be Aware of and How to Handle Them? In *Cybersecurity of Digital Service Chains* (pp. 202-221). Springer, Cham.
- Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, 64(5), 659-671. <https://doi.org/10.1016/j.bushor.2021.02.022>
- Lien, L., & Singh, N. (2022). *Ethical hacking, how can hacking be put to good use?* (Vol. Master of Science in Business) [Project Assignment, Dynamic MCS]. Nord University.
- Moeller, R. R. (2011). *COSO Enterprise Risk Management : Establishing Effective Governance, Risk, and Compliance Processes* (2 ed.). John Wiley & Sons, Incorporated. <http://ebookcentral.proquest.com/lib/nord/detail.action?docID=697656>
- NHO. (2021). *Fakta om små og mellomstore bedrifter (SMB)*. NHO. Retrieved 15.03.2023 from <https://www.nho.no/tema/sma-og-mellomstore-bedrifter/artikler/sma-og-mellomstore-bedrifter-smb/>
- Nicholson, S. (2019). How ethical hacking can protect organisations from a greater threat. *Computer Fraud & Security*, 2019(5), 15-19.
- NIST. (2023). *NIST Cybersecurity Framework*. National Institute of Standards and Technology. Retrieved 29.03.2023 from <https://www.nist.gov/cyberframework/getting-started/quick-start-guide>
- Power, M. (2004). The risk management of everything. *The Journal of Risk Finance*. <https://www.emerald.com/insight/content/doi/10.1108/eb023001/full/html>



- Power, M. (2009). The risk management of nothing. *Accounting, organizations and society*, 34(6-7), 849-855.
- Prasad, S. T. (2014). Ethical hacking and types of hackers. *International Journal of Emerging Technology in Computer Science & Electronics*, 11(2), 24-27.
- Radziwill, N., Romano, J., Shorter, D., & Benton, M. (2015). The Ethics of Hacking: Should It Be Taught? *arXiv preprint arXiv:1512.02707*.
- Review, H. B., Kaplan, R. S., Rice, C., Tetlock, P. E., & Schoemaker, P. J. H. (2020). Ch. 1: Managing Risks: A New Framework. In. United States: Harvard Business Review Press. <https://ebookcentral-proquest-com.ezproxy.nord.no/lib/nord/reader.action?pq-origsite=primo&ppg=12&docID=5829113>
- Saravanan, A., & Bama, S. S. (2019). A Review on Cyber Security and the Fifth Generation Cyberattacks. *Oriental journal of computer science and technology*, 12(2), 50-56. <https://doi.org/10.13005/ojst12.02.04>
- Scott, W. R. (2008). Approaching adulthood: the maturing of institutional theory. *Theory and society*, 37, 427-442.
- Sidwell, J., & Hlavnicka, P. (2022). COSO Evolution ERM Frameworks. In. United States: Business Expert Press. <https://ebookcentral-proquest-com.ezproxy.nord.no/lib/nord/reader.action?pq-origsite=primo&ppg=28&docID=29441122>
- Standardization, I. O. f. (2023). *ISO / IEC 27001 and related standards*. Retrieved 29.03.2023 from <https://www.iso.org/isoiec-27001-information-security.html>
- Stortinget. (2020, September 9, 2020). *IT-angrep mot Stortinget*. Retrieved April 22 from <https://stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Pressemeldingsarkiv/2019-2020/it-angrep-mot-stortinget/>
- Stortinget. (2021, March 10, 2021). *Stortinget utsatt for IT-angrep*. Retrieved April 22 from <https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Pressemeldingsarkiv/2020-2021/stortinget-utsatt-for-it-angrep/>
- TIBER. (2023). Norges Bank. Retrieved 06.03.2023 from <https://www.norges-bank.no/tema/finansiell-stabilitet/Forebygging/tiber>
- TIBER-NO. (2022). *TIBER-NO, Implementeringsveiledning*. <https://www.norges-bank.no/contentassets/67dfddb1ef9b4f8ea6e64bb3ed005471/tiber-no-implementeringsveiledning-v1.0.1b.pdf?v=11/24/2022144949>
- Torp, I. S. (2023). *De Nasjonale Forskningsetiske komiteene*. Retrieved 02.03.2023 from <https://www.forskningsetikk.no/>

- Wallingford, J., Peshwa, M., & Kelly, D. (2019). Towards understanding the value of ethical hacking. International Conference on Cyber Warfare and Security,
- Walshe, T., & Simpson, A. (2020). An empirical study of bug bounty programs. 2020 IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF),
- Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, 88, 101636.
- Yin, R. K. (2018). *Case study research and applications : design and methods* (Sixth edition. ed.). SAGE.

## Appendix

### *Interview Guide 1*

General cyber security and ethical hacking interview guide.

#### **Spørsmål:**

De første minuttene vil bli brukt til “småprat”, slik at du blir litt bedre kjent med oss, og vi litt bedre kjent med deg.

Kan du fortelle litt om din stilling?
Hva går din arbeidshverdag ut på?
Er du kjent med begrepet ethical hacking?
Hva slags rolle har ethical hackers i dagens samfunn?
Har ethical hackers en rolle i din bedrift?
Kjenner du til noen aktører som tilbyr slike tjenester?
Er du kjent med begrepet risk management?
Kan du forklare hvordan din bedrift bruker risikostyring på et generelt nivå? (Interne kontroller, prosedyrer og lignende)
Hvor stor risiko mener du at ethical hackers utgjør?
Hvordan vil du si at å leie inn ethical hackers kan være med på å forsterke eller forverre risikostyring i en organisasjon?
Kan du kort forklare hva TIBER-EU rammeverket er, og formålet bak det?
Om mulig, kan du forklare prosessen til en bedrift, og deres ansettelse av en ethical hacker? (Hvorfor, hvordan og hva)
Hvilken rolle spiller ethical hackers i et slikt rammeverk?
Ligger det til grunn noen retningslinjer for valg av de riktige etiske hackerne?
Vi har tidligere blitt informert om et kommende rammeverk med navn DORA (Implementert nå?), kan du kort forklare oss hva det går ut på?
Hva slags innvirkning vil et rammeverk som DORA ha på etterspørselen etter ethical hackers og deres tjenester?

Tror du kravene for å kunne tilby “ethical hacking services” vil bli strammere enn før?
Hvilke krav har vi i dag til slike tjenester? Hva slags bakgrunn / erfaring ser man etter blant ethical hackers?
Tror du Norges næringsliv er forberedt på en tid med flere forsøk på hacking og digitale «scams»? (Om ja, hvorfor – Om nei, hvorfor ikke)
Er det noe du føler du ikke har fått sagt?

Til slutt tar vi gjerne imot spørsmål fra deg, om det er noe du lurer på. Disse spørsmålene kan være rettet mot intervjuet, eller personlige spørsmål til oss.

## *Interview Guide 2*

Risk management interview guide.

### **Spørsmål:**

De første minuttene vil bli brukt til “småprat”, slik at du blir litt bedre kjent med oss, og vi litt bedre kjent med deg.

Kan du fortelle litt om din stilling?
Kan du fortelle kort om hva din avhandling gikk ut på?
Hva går din arbeidshverdag ut på?
Kan du forklare hvordan begrepet Cyber Security har endret seg de siste årene?
Hvordan var fokuset på cyber Security før i forhold til fokuset nå?
Er du kjent med begrepet ethical hacking?
Hva slags rolle har ethical hackers i dagens samfunn?
Hva slags rolle tror du ethical hackers vil ha i samfunnet og i bedrifter fremover?
Kjenner du til noen aktører som tilbyr slike tjenester?
Er du kjent med begrepet risk management?
Kan du forklare hvordan risikostyring kan kombineres med etisk hacking?
Hvor stor risiko mener du at ethical hackers utgjør?

Hvordan vil du si at å leie inn ethical hackers kan være med på å forsterke eller forverre risikostyring i en organisasjon?
Hvorfor / hvorfor ikke tror du risikostyring og teorier / rammeverk knyttet til dette er utdatert? (Ift. Cyber Security)
Hvordan har risikoen til bedrifter endret seg fra fysisk risiko, til en digital risiko?
Tror du tjenester som ethical hacking kan bli brukt mot sin hensikt? Hvordan?
Kan du gi dine synspunkter på om en økt etterspørsel etter ethical hackers gjøre kvaliteten dårligere, og dermed risikoen ved bruk av dem større?
Hvordan tror du etisk hacking kan bli brukt som et verktøy innen risikostyring?
Tror du kravene for å kunne tilby “ethical hacking services” vil bli strammere enn før?
Tror du Norges næringsliv er forberedt på en tid med flere forsøk på hacking og digitale «scams»? (Om ja, hvorfor – Om nei, hvorfor ikke)
Er det noe du føler du ikke har fått sagt?

Til slutt tar vi gjerne imot spørsmål fra deg, om det er noe du lurer på. Disse spørsmålene kan være rettet mot intervjuet, eller personlige spørsmål til oss.