Universiteit Leiden

ICT in Business and the Public Sector

A Research regarding how IT professionals conduct risk classification against ISO/IEC 27001 in the context of corporate environments

Name: Yun Wan
Student-no: 2251132

Date: 18/04/2023

1st supervisor: Dr. Olga Gadyatskaya
2nd supervisor: Dr. Eleftheria Makri

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)
Leiden University
Niels Bohrweg 1
2333 CA Leiden
The Netherlands

Acknowledgments

First of all, I want to express my deepest gratitude to my thesis supervisor, Olga Gadyatskaya, for her invaluable guidance and support throughout the entire research process. I could not have written this thesis without her help. I also could not have undertaken this journey without my internship company, which generously provided knowledge and resource for me to conduct this research.

I also would like to thank the participants who generously shared their time and experiences for my study. Without their contributions, this research would not have been possible.

I want to express my heartfelt gratitude to my parents for their constant love and support. Lastly, I want to send my special thanks to my partner, Jin. Your unwavering support and belief in me have given me the con dence to pursue my goals. I am grateful for having you by my side.

Abstract

0.1 Context

In today's digital age, cyber security is increasingly important in both business and daily life. As technology advances and more aspects of our businesses become digitized, e ective cyber security measures are essential [Barnard and Von Solms, 2000]. ISO/IEC is a widely recognized framework for managing an organization's information security. Its purpose is to establish, implement, maintain, and continually improve an organization's information security management system. ISO/IEC 27001 is often used to help organizations safeguard their information from various risks.

0.2 Problem

ISO/IEC 27001 speci es a set of requirements and controls that organizations should implement for their information security purposes. Risk classi cation represents a crucial stage in the process of conducting risk assessment with ISO/IEC 27001. However, ISO/IEC 27001 does not provide detailed guidelines on how to carry out risk classi cation. As an organization needs IT professionals to conduct ISO/IEC 27001 cyber security activities, the lack of clear guidelines can lead IT professionals to exercise their subjective judgment, which may result in inaccurate risk classi cation or biased risk assessment outcomes. Therefore, it is vital to investigate the factors that a ect IT professionals' judgment and the decision-making process they undertake when performing risk classi cation using ISO/IEC 27001.

0.3 Objective

IT professionals can utilize ISO/IEC 27001 for various cybersecurity activities, including obtaining certi cation, conducting risk assessments based on ISO/IEC 27001 standards, and implementing ISO/IEC 27001 guidelines. This study focuses primarily on the topic of risk classi cation, which encompasses activities related to ISO/IEC 27001 certi cation and maturity assessment, as mentioned earlier. The aim of this research is to investigate the decision-making processes used by ISO/IEC 27001 practitioners during the risk classi cation of certi cation and maturity assessment. The study also seeks to identify the factors that impact their decision-making.

0.4 Method

In this study, three steps were performed. Firstly, a background introduction was conducted to introduce the basic concepts of this research topic, such as ISO/IEC 27001, IT audit, risk assessment, maturity assessment, etc. Secondly, a literature review was performed to show the understanding of the current state of knowledge of the research topic and identify research gaps. Furthermore, a qualitative research method was applied, and thirteen interviews were conducted. The data were analyzed using grounded theory, and a model was generated as the result of this research. Overall, valuable insights into this research topic were provided, and areas for future research were highlighted.

0.5 Findings

This study examines four key aspects of ISO/IEC 27001, namely the decision-making processes involved in conducting risk classi cation in the audit and consulting elds, as well as the challenges and opportunities for improvement in these processes. A model based on existing research and expert interviews is developed to achieve this, which illustrates the factors that a ect risk classi cation and their associated decision-making processes.

Keyword: ISO/IEC 27001, risk assessment, risk classi cation, maturity assessment, impacting factors, decision-making process, risk assessment methods

Contents

0.1 Context v
0.2 Problem v
0.3 Objective v
0.4 Method vi
0.5 Findings vi

Contents vii

List of Figures xi

List of Tables xiii

1 Introduction 1
1.1 Research objective 2
1.2 Research questions 2
1.3 Research structure 2
1.4 Key de nitions 3

2 Background 5
2.1 ISO/IEC 27001 5
2.1.1 ISO 27000 series 5
2.1.2 Why ISO/IEC 27001 is needed 5
2.1.3 ISO/IEC 27001 framework 6
2.1.4 Adoption of ISO/IEC 27001 9
2.2 Risk classi cation 9

2.2.1 Risk management, risk assessment and risk classi cation 9
2.2.2 Risk classi cation models 12
2.3 Risk classi cation under enterprise context 17
2.3.1 Risk classi cation in audit eld 17
2.3.2 Risk classi cation in consulting eld 19

3 Related work 22
3.1 Security risk management professionals 22
3.1.1 Roles and responsibilities 22
3.1.2 Key skills and quali cations 23
3.1.3 Challenges faced by security risk management professionals 23
3.2 Decision making processes 24
3.2.1 Decision making process model 24
3.2.2 Decision making factors 26
3.3 Professional Judgment 26

4 Methodology 28
4.1 Research Strategy 28
4.2 Data Collection 29
4.2.1 Sampling 29
4.2.2 Interviews 29
4.2.3 Grounded theory 29

5 Results 31
5.1 Interviews Overview 31
5.2 Codes and Categories 32
5.3 Results of subquestions 33
5.3.1 Risk classi cation in auditing eld 33
5.3.2 Maturity level assessment in advisory eld 44
5.3.3 Di culties 45
5.3.4 Improvement 48

6 Models 52

6.1 Model of impacting factors 52

6.2 Model of factors ranking 54

6.3 Final Model 54

7 Discussion 57

7.1 Re ection of the results 57

7.2 Limitations of the research 58

8 Conclusions 59

8.1 Future work 60

Bibliography 62

9 Appendix 70

9.1 Appendix A: Semi-structured interview questions 70

9.2 Appendix B: Coding (sub)categories and concepts 72

List of Figures

2.1 Screenshot of Clauses of ISO/IEC 27001:2013 8

2.2 Screenshot of Annex A of ISO/IEC 27001:2013 8

2.3 ISO 31000 Risk assessment. Source: [Fazzino and Jones, 2021] 10

2.4 Example of qualitative risk assessment 12

2.5 Decomposition of Risk according to the FAIR framework and The Open Group taxonomy, source: [Ionita, 2013] 14

2.6 COBIT 5 Framework 15

2.7 Decomposition of Risk level (Exposure) according to the OWASP methodology, source: [Ionita, 2013] 16

2.8 Audit process ow 17

2.9 Cyber maturity assessments process. Source: [Centric, 2018] 20

2.10 Five levels of Capability Maturity Model. Source: [Welch et al., 2016] 21

3.1 Risk Rationalisation Flow. Source: [M'manga et al., 2019] 25

5.1 Proposition of participants in terms of skills 32

5.2 Company side factors 34

5.3 Practitioner's side factors 36

5.4 Control-related factors 37

5.5 Major nonconformities/Red ags 41

5.6 Minor nonconformity 42

5.7 Observations 43

5.8 Exceptions 44

5.9 Di culties 48

5.10 Improvements 51

6.1 Model of overview of impacting factor 53

6.2 Ranking 54

6.3 Model of risk classi cation against ISO/IEC 27001 55

List of Tables

1.1 Process of conducting research 2

2.1 Clauses regarding risk management of ISO/IEC 27001:2013 7
2.2 Area controls and controls amount of ISO/IEC 27001:2013 Annex A 7

4.1 Example of coding process 30

5.1 Overview of the interview experts 31
5.2 Number of codes for each interview 33

8.1 Process of conducting research 59

Chapter 1

Introduction

Cyber security has become a crucial topic in today's business landscape, as digitalization has become ubiquitous across almost all industries. Protecting information systems is of paramount importance, and one e ective approach to achieve this is by implementing cyber security policies or risk management frameworks. The ISO/IEC 27001 is a globally recognized standard for managing information security. It provides a comprehensive framework for organizations to establish, implement, maintain, and continually improve their information security management systems.

ISO/IEC 27001 standard outlines the necessary requirements for managing and safeguarding sensitive information. Its primary objective is to assist organizations of all sizes and types in managing the risks associated with their information assets and ensuring they are protected against diverse security threats. By adhering to the ISO/IEC 27001 standard, organizations can maintain a systematic and proactive approach to information security management. This can result in protecting valuable data assets, reducing security breaches, and avoiding negative nancial and reputational impacts.

ISO/IEC 27001 is widely applicable across various industries, including banking, healthcare, insurance, government, education, and manufacturing, among others. Additionally, the standard remains relevant for organizations that utilize emerging technologies such as cloud computing and mobile devices. Such organizations can leverage ISO/IEC 27001 to undertake several critical activities, such as certi cation, maturity assessment, gap analysis, implementation support, internal audit, training and awareness, as well as maintenance and improvement. This study primarily focuses on the cybersecurity activities of ISO/IEC certi cation and maturity assessment, which are predominantly carried out by ISO/IEC 27001 auditors and consultants, respectively. To enhance clarity, the professionals who perform ISO/IEC 27001-related activities will be referred to as ISO/IEC 27001 practitioners throughout this research if no further distinguishment is needed.

To certify or assess a company against ISO/IEC 27001, the ISO/IEC 27001 practitioners should rst gain an understanding of the company and have its information security policies, objectives, and scope de ned. Subsequently, audits or risk assessments will be conducted based on the de ned scope and content of ISO/IEC 27001. The risk assessment results will then be used to determine the outcome by the ISO/IEC 27001 practitioners.

To carry out some of these activities, it may be necessary to engage specialized cyber security organizations, particularly for certi cation, which typically requires the expertise of quali ed Certi cation Bodies, other activities such as maturity assessment and gap analysis may require assistance from cyber security consulting rms. Consider, for instance, a medium-sized company that wishes to obtain certi cation against ISO/IEC 27001 to expand its business opportunities.

The company approaches a Certi cation Body that provides certi cation services and employs ISO/IEC auditors. The Certi cation Body then provides the company with the ISO/IEC 27001 service, and the entire certi cation process lasts three years.

1.1 Research objective

It can be observed that while ISO/IEC 27001 is widely accepted and applied, its limitations in providing detailed guidelines for risk classi cation are acknowledged. Risk classi cation is considered to be a vital step in risk management, and clear guidelines are expected to be followed to ensure rigor. However, the lack of detailed approaches for conducting risk classi cation in a universal way within ISO/IEC 27001 means that practitioners can apply subjective judgment. Additionally, as human engagement is mandatory for risk assessment, the absence of such guidelines leaves room for subjectivity in the classi cation process.

In order to address the aforementioned issue, interviews were conducted with ISO/IEC practitioners possessing experience in certifying companies against ISO/IEC 27001, providing ISO/IEC 27001 consulting services featuring maturity level assessments, and assisting companies in implementing ISO/IEC 27001. The aim of this research was to comprehend the decision-making process utilized by ISO/IEC practitioners when classifying risks and to identify the factors that in uence their decision-making.

1.2 Research questions

To achieve the research objective, the research question, the subquestions, and expected result are formed as follows:

Table 1.1: Process of conducting research

No.	How do IT professionals conduct risk classi cation against ISO/IEC 27001 in the context of corporate enviroments
SQ 1	When certifying a company against the ISO/IEC 27001 standard, what factors contribute to evaluating security risk classi cation in the audit process?
SQ 2	when delivering advisory services, What factors contribute to the evaluation of maturity level classi cation
SQ 3	What do IT professionals perceive as the most challenging in the process of conducting ISO/IEC 27001 risk classi cation?
SQ 4	How can the process of ndings classifying be improved to minimize reliance on subjective professional judgment?
Result	A model of factors that impact the process of risk classi cation decision-making

1.3 Research structure

The thesis will be structured as follows:

Chapter number	Theme	Description
2	Background	Establish the basic concepts that will be used to understand the research
3	Related work	Present an overview of the existing research related to the research
4	Methodology	Address the methodology applied in this research
5	Result	Show the result of the interviews and data analysis
6	Model	Present the result by constructing models
7	Discussion	Explore the result, discuss models and future work
8	Conclusion	Conclude brie y the whole research

1.4 Key de nitions

Information risk management : Risk management is the process of identifying, assessing, and mitigating risks in a continuous, structured way to protect the organization's information from being exploited by other parties [Zammani and Razali, 2016].

Information risk assessment : Information security risk assessment is the process that enables the identi cation, evaluation and prioritization of potential risks based on speci c rules in the management practices of enterprises [Saleh and Alfantookh, 2011].

ISO/IEC 27001 : SO/IEC 27001 is a risk management framework that helps organizations to protect information systems. It is used to provide \a model for establishing, implementing, operating, monitoring, reviewing and improving on Information Security Management System". This standard can be applied by all sorts of organizations, pro t or non-pro t, commercial or public [ISO, 2013].

ISO/IEC 27001 Certi cation : ISO/IEC 27001 certi cation is a process where an independent and quali ed third party examines an organization's information security management system to see if it meets the requirements of ISO/IEC 27001. If the organization meets the requirements, it is quali ed to receive ISO/IEC 27001 certi cation, which is valid for three years [Lambo, 2006].

ISO/IEC 27001 Maturity assessment : ISO/IEC 27001 maturity assessment is a process to assess an organization's maturity level based on ISO/IEC 27001. Often time an independent and quali ed party conduct the assessment. They also evaluate the gaps between the organization's existing practices and requirement of the standard, and the results can be used to improve the organization's information security [Proença and Borbinha, 2018].

Chapter 2

Background

This chapter will introduce the background information of risk classi cation against ISO/IEC 27001. The rst section introduces the ISO/IEC 27001 and its adoption. The second section introduces risk classi cation, including the basic concepts and a few risk classi cation models with their impacting factors for making classi cation decisions, on top of it, the risk classi cation in ISO/IEC 27001 is discussed too. The third section introduces the processes of conducting ISO/IEC 27001 certi cation and maturity assessments.

2.1 ISO/IEC 27001

2.1.1 ISO 27000 series

ISO/IEC 27001 is the core standard among ISO/IEC 27000 series. The ISO 27000-Series, also known as "ISO 27 K" or the "ISO 27000 family", is a series of frameworks and standards developed speci cally for information security management systems [Meriah and Rabai, 2019].

The ISO/IEC 27000 series concept was rst proposed in 2005. In 2007, ISO/IEC 27002 was added to the ISO 27k family. Up to 2022, there were 19 standards in ISO 27000 family. Among all the ISO/IEC 27000 family, ISO/IEC 27002 serves as a guideline for implementation of ISO/IEC 27001 Annex A, it provides many details and is thus seen as useful for ISO/IEC 27001 [Kosutic, 2023].

2.1.2 Why ISO/IEC 27001 is needed

ISO/IEC 27001, known as \Information technology | Security techniques | Information security management systems | Requirements", is a risk management framework that helps organizations to protect information systems. It was jointly developed by International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), a leading international standards organization that develops and issues standards for the electronics and electronics-related technology sectors.

ISO/IEC 27001 is deemed the most well-known information security standard and the third most commonly held ISO certi cation [Culot et al., 2021]. The ISO/IEC 27001 standard is used to provide \ a model for establishing, implementing, operating, monitoring, reviewing and improving

on Information Security Management System". It is designed to help organizations to conduct risk management practices with a risk management approach. This standard can be applied by all sorts of organizations, pro t or non-pro t, commercial or public [ISO, 2013].

Three aspects of information are protected by ISO/IEC 27001: Con dentiality, Integrity and Availability. To achieve those goals, risk assessment has to be done to understand what are the potential risks, after that, risk mitigation and risk treatments are carried out to prevent the potential risks from happening [Kosutic, 2023].

ISO/IEC 27001 de nes a set of controls that organizations apply to protect information systems. Those controls are related to the aspects of organization issues, human resources, IT-related and physical security. Not all controls have to be implemented. Organizations can pick the controls that are applicable to them and those controls must be implemented [Leal, 2022].

Companies can bene t from implementing ISO/IEC 27001 for the following aspects. Firstly, complying with ISO/IEC 27001 helps organizations to comply with multiple laws, regulations and policies, such as data privacy. It is because implementing ISO/IEC 27001 can help organizations align with various legal requirements. Secondly, the main goal of ISO/IEC 27001 is to prevent cyber incidents, implementing ISO/IEC 27001 can prevent money and time loss from serious incidents happening. Thirdly, ISO/IEC 27001 can improve competitiveness, ISO/IEC 27001 is well-recognized within certain industries. Having ISO/IEC 27001 implemented can help build trust for businesses and increase competitiveness when certi cations are needed [Isms.online, 2022b, Kosutic, 2023].

2.1.3 ISO/IEC 27001 framework

There are three versions of ISO/IEC 27001 standards. They were published in 1995, 2013 and 2022 separately [ISO, 2023]. The version this research uses is the ISO/IEC 27001:2013, this is because when this research got started in March, 2022, the latest version was not published yet. So the ISO/IEC 27001 in this research refers to ISO/IEC 27001:2013, this applies also in later chapters.

The ISO/IEC 27001:2013 mainly consists of two sections: the Clauses and Annex A, which is a set of controls. The clauses are a series of provisions that provides speci c requirements and guidelines to conduct risk management. Organizations that intend to be certi ed against ISO/IEC 27001 are encouraged to adhere to these requirements and guidelines to guarantee the pro ciency of their information security management system. All the clauses are grouped into ten main sections, each of which discusses a di erent topic of information security management, such as leadership, planning, performance evaluation, etc [Kosutic, 2023]. The screenshot of part of Clauses can be found in gure 2.1, The list of all clauses can be found in table 2.1.

Like clauses, Annex A is a set of security controls and objectives that organizations can apply to ensure their information security management system works e ectively. The clauses of ISO/IEC 27001 represent the fundamental components of the ISO/IEC 27001 standard and outline the fundamental requirements. Annex A security controls and objectives serve as a supplementary resource to the requirements described in the primary clauses, o ering organizations supplementary guidance on the methods to safeguard their information systems and secure their information assets [Kosutic, 2016]. The screenshot of part of Annex A can be found in gure 2.2. The list of components of Annex A can be found in the table 2.2.

Clause Number	Clauses
4	Context of the organization
5	Leadership
6	Planning
7	Support
8	Operation
9	Performance evaluation
10	Improvement

Table 2.1: Clauses regarding risk management of ISO/IEC 27001:2013

Control Number	Controls	Control Amount
5	Information security policies	2
6	Organization of information security	7
7	Human resource security	6
8	Asset management	10
9	Access control	14
10	Cryptography	2
11	Physical and environmental security	15
12	Operations security	14
13	Communications security	7
14	System acquisition, development and maintenance	13
15	Supplier relationships	5
16	Information security incident management	7
17	Information security aspects of business continuity management	4
18	Compliance 8 Total Amount of Control	8
	Total Amount of Control	144

Table 2.2: Area controls and controls amount of ISO/IEC 27001:2013 Annex A

Figure 2.1: Screenshot of Clauses of ISO/IEC 27001:2013

Figure 2.2: Screenshot of Annex A of ISO/IEC 27001:2013

2.1.4 Adoption of ISO/IEC 27001

According to [Research, 2023], compared to 2021, cyber attacks has increased by 38% in 2022, the average amount of reported attack was reported as 1168 every week. Besides, the organization's information systems, such as migration to the cloud, and the legitimate tools organizations use are being seen as targets?]. Having a robust information system is necessary to protect organizations nowadays. Information Security Management System(ISMS) is a series of practices to protect organizations' information security [?]. Adopting an ISMS can bene t companies by enabling them to develop customized solutions to mitigate potential information system risks. Moreover, as the trend toward digitalization accelerates and information-critical processes generate a growing proportion of revenue, ISO/IEC 27001 assumes greater importance for companies seeking to secure their business operations [Cavusoglu et al., 2009]. Thus, adopting ISO/IEC 27001 helps establish appropriate personnel, processes, and technologies, fostering a proactive approach to security and risk management [Brenner, 2007].

In 2020, the successful adoption of ISO/IEC 27001 was observed among nearly 45,000 companies, re ecting an impressive growth rate of 22% [ISO, 2021, Podrecca et al., 2022]. Many well-established companies have chosen ISO/IEC 27001 to facilitate their information system security management, such as Apple, Amazon, etc [Culot et al., 2021, Podrecca et al., 2022].

Research also demonstrates that obtaining ISO/IEC 27001 certi cation can have an impact on the performance of companies, particularly with respect to pro tability, labor performance, and sales performance. The impact is associated with the degree of internationalization of the certi ed companies [Podrecca et al., 2022].

On top of a number of companies choosing to go through the full certi cation procedure to have themselves certi ed against ISO/IEC 27001, more companies try to reach a level that can be aligned with ISO/IEC 27001. For example, according to the estimation, in the UK, around 20-40% of large to medium-sized businesses have achieved a level of alignment with or are actively working towards ISO/IEC 27001 certi cation [Everett, 2011].

Similarly, in Germany, research shows that companies are willing to mention their business partners' ISO/IEC 27001 certi cation status on their websites. Studies also show that almost half of the certi ed companies are in the information and communication technology sector [Mirtsch et al., 2021], implying the high recognition level of ISO/IEC 27001 within the ICT industry.

Thus, certifying or conducting risk management against ISO/IEC 27001 can provide signi cant business value, particularly for companies whose information management systems are integral to their operations. This highlights the importance of obtaining a clear guideline for risk classi cation when utilizing ISO/IEC 27001.

2.2 Risk classi cation

2.2.1 Risk management, risk assessment and risk classi cation

Risk management

The goal of a risk management framework is to conduct risk management. Risk management is the process of identifying, assessing, and mitigating risks in a continuous, structured way to protect the organization's information from being exploited by other parties [Zammani and Razali, 2016].

Risk management often follows certain guidelines, which are presented as an information risk management framework. Plenty of risk management framework exists in both academic and business domains, famous framework publishers include National Institute of Standards and Technology (NIST), FAIR Institute, The MITRE Corporation, The American Institute of Certi ed Public Accountants (AICPA), the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), those publishers own one or multiple information risk management frameworks [Giuca et al., 2021]

Companies can decide to follow a speci c framework that suits their business goal the best, or follow multiple frameworks as long as they are capable of, or integrate frameworks or processes to better serve their business objectives, for example, integrating IT risk management framework with more general frameworks such as ISO 9001 for quality management system [Barafort et al., 2017].

To facilitate comprehension of the risk management and risk assessment process, the ISO/IEC 31000 framework is utilized in this chapter to illustrate as an example due to its simple and straightforward structure and universal applicability [ISO, 2018, Lalonde and Boiral, 2012]. ISO/IEC 31000 risk assessment process is shown in gure 2.3:

Figure 2.3: ISO 31000 Risk assessment. Source: [Fazzino and Jones, 2021]

Figure 2.3 shows the basic risk management process. When conducting risk assessment at an organization, the following steps usually will be undertaken. Step 1 often refers to understanding the organization's context before assessing risks. It can involve understanding the goals and objectives of this organization, its existing policies, criteria, etc. Step 2 is about risk assessment. This step includes (a) identifying the risks of this company, (b) analyzing estimation, such as considering the cause and consequences, and (c) evaluating risks, which means deciding which risks need to be treated and prioritizing the treatment. Step 3 is about risk treatment, the company should have solutions to mitigate identi ed risks. Step 4 is about risk acceptance. In ISO/IEC 31000, the mentioned steps can interact with internal communication and review all the time [PECB, 2015].

ISO/IEC 31000 describes the general process of risk management. In other risk management models, the steps above may be integrated, decomposed, or more steps are added. For example, ISO/IEC 27005 adds the satisfactory part on the base of ISO/IEC 31000 to facilitate decision-

making [Ferreira, 2020]. NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF) is another commonly used risk management framework published in 2018. The ve Core Functions of NIST CSF are identify, protect, detect, respond, and recover [Anderson, 2020]. The terms used in those two models are di erent, yet some risk management activities are overlapped and share similarities.

Risk assessment

Risk assessment is a part of risk management and is often regarded as the most important phase of the information risk management process [Zambon et al., 2011]. Risk assessment is often related to the computation of risk [Peltier, 2005]. According to [Elo et al., 1993], risk assessment refers to the process that combines the identi ed risk factors so that a risk measurement can be generated for each information technology domain. Risk assessment results are vital to the nal risk-related decisions.

According to [Peltier, 2005], the risk assessment consists of six steps: Asset De nition; Threat Identi cation; Determining the probability of Occurrence; Determining the impact of the Threat; Controls Recommended; Documentation. During the process of assessment, the factors, for example, business purpose, customers, resources such as money and personnel, procedures, etc, that can impact the assessment result are taken into account.

The methodology of assessing risks can be quantitative or qualitative. The following part will discuss more information on quantitative and qualitative approaches.

Risk classi cation

Risk classi cation aims at grouping risks based on a set of speci c attributes of the risks. Usually, those attributes include the risks' likelihood of occurrence and potential impact. By classifying the risks, organizations could know what risks should be prioritized rst and how to relocate the risk management resources [Curti et al., 2019].

The output of risk classi cation can be quantitative or qualitative. The quantitative risk assessment method uses numerical calculations to assess the probability of a potential risk event and its potential impact, such as statistic analysis, nancial loss calculation, probability calculations, etc. For example, the Factor Analysis of Information Risk (FAIR) is an information framework featuring its quantitative risk assessment method. It uses frequency and magnitude as axes, and then decomposes them further as measurable components [Maze, 2018].

Qualitative risk assessment is also frequently utilized for its simplicity. This approach applies judgment to some extent to evaluate and categorize the risks based on risk frequency and impact. The terms of classi cation can also be di erent. In many cases, the terms of"low, medium, high" are used. For example, The CIS and NIST cybersecurity frameworks apply various versions of terms to show cyber security risk levels, yet they can generally be described as"critical, high, medium, and low" levels of risk [Bocchino, 2022]. A visualization of qualitative risk assessment can be seen in gure 2.4:

Quantitative methods can also be translated into qualitative methods. For example, Common Vulnerability Scoring System(CVSS) is on a scale from 0-10, the scores can be mapped into the severity of risks, such as"no risk, low risk, medium risk, high risk, critical risk" , each term has a range of basic score [Bocchino, 2022].

Similarly, Risk Priority Number(RPN) is a risk classi cation method that uses the product

Figure 2.4: Example of qualitative risk assessment

of the severity, likelihood, and detection score to get numerical values [Peko et al., 2018]. Failure Modes and E ects Analysis (FMEA) applies the RPN method, using a speci c structure to list potential factors that impact a system and determine the levels of information risk [Liu et al., 2013].

Compared to the quantitative risk assessment method, the qualitative method is regarded as not "reliable" . According to [Cox Jr et al., 2005], qualitative risk assessment has a poor performance when there are a few large risks mixed with many small risks, in this case, the qualitative rating is likely to be unable to distinguish those two types of risks. This fact leaves a certain uncertainty about the accuracy of the qualitative risk assessment method.

As mentioned above, there are multiple risk classi cation frameworks and methods. Organizations can choose the one that suits them the best based on their business objective, and the desired level of detail.

2.2.2 Risk classi cation models

In the risk classi cation section, several factors that can impact the grading/classifying levels of information risks are mentioned but not discussed in depth. In this section, three well-recognized risk management models, the FAIR, COBIT 5, and OWASP are studied, and the factors in those models are discussed. Those models are selected for their extensive recognition within the industry and their comprehensive treatment of the factors that may impact decisions regarding risk classi cation. Through a detailed analysis of these models, this section aims to provide an understanding of the factors that in uence risk classi cation decisions in the context of information security.

FAIR

Factors Analysis of Information Risk (FAIR) is a framework describing the factors contributing to risks and the relationships between each risk. FAIR was developed in 2005 by Jack Jones, who is currently the chairman of The FAIR Institute [Jack Jones, 2022]. FAIR combines the FAIR taxonomy and statistical techniques, enabling the FAIR model to be used for quantitative risk assessment [The Open Group, 2019]. FAIR is regarded as one of the most popular models for

quantitative cybersecurity risk assessment"by applying algorithms of a set of quanti able risk factors [Wang et al., 2020].

The risk assessment process of FAIR can be divided into four phases: Identify Scenario Components; Evaluate Loss Event Frequency (LEF); Evaluate Probable Loss Magnitute (PLM) and Derive and Articulate Risk. The last step Derive and Articulate Risk can be illustrated as gure 2.5:

As the gure shows, the tree shape model shows six layers of factors that can impact risk classi cation. All the factors are divided by "Loss Magnitude" and "Loss Event Frequency" in the rst layer. In the loss magnitude section, factors such as"Access", "Cost" , "Timing" , "Remediation" are mentioned. In the "Loss Event Frequency" section, factors such as"Contact Frequency", "Control Strength" are mentioned. In total 43 factors are shown in this model.

Though FAIR is acclaimed for its good taxonomy, it is believed that it is not suitable for carrying out an organizational risk assessment. This is because the FAIR model focuses more on analyzing existing risks, which means it lacks interaction with the organization or projects to some degree. For example, it may have a limited understanding of the organization's objectives and strategy [Reciprocity, 2022]. As a result, FAIR may have limitations when being used in a business context.

COBIT 5 Framework

COBIT 5 is an information technology governance framework that was developed by Information System Audit and Control Association (ISACA) and the IT Governance Institute (ITGI). COBIT stands for Control Objectives for Information and Related Technology, it is often used to help organizations to meet their business objectives, to help them be compliant with regulations. The latest version of COBIT 5 was released in 2012 [Governance, 2023].

Compared to other risk management frameworks, COBIT 5 is more oriented towards enterprise and business needs. Unlike other frameworks that focus more on technical risk management, COBIT 5 considers the dynamics of the enterprise, making it a preferred choice for many commercial companies seeking to manage their information systems. ISO/IEC 27001 is often a requirement for commercial enterprises and is widely used. Thus, COBIT 5 is being introduced in this section due to its relevance in enterprise settings and its similarity with ISO/IEC 27001 in addressing business risk management [Bakkah2021, 2021, De Haes et al., 2013].

COBIT 5 is built on ve key principles, those 5 principles are: (a) Meeting the stakeholders; (b) Covering the enterprise end-to-end; (c) Applying a single integrated framework; (d) Enabling a holistic approach; (e) Separating governance from management [Jones, 2022]. The illustration of COBIT 5 Principles can be found in gure 2.6.

The COBIT 5 framework provides a series of enablers. Those enablers support the implementation of the COBIT 5 framework and in uence whether the IT governance and management will work. Those enablers are: (a) Principles, policies, and frameworks; (b) Processes; (c) Organizational structures; (d) Culture, ethics, and behavior; (e) Information; (f) Services, infrastructure, and applications; (g) People, skills, and competencies. Those enablers act as the resources that help organizations to align their IT operations with their business objectives, thus it also impacts the risk management of the organizations [Salman, 2017]. The illustration of COBIT 5 Enablers can be found in gure 2.6.

The COBIT 5 is welcomed by enterprises, yet it is believed that it is focusing more on developing Enterprise Governance at the expense of IT governance. This could lead to a gap between

Figure 2.5: Decomposition of Risk according to the FAIR framework and The Open Group taxonomy, source: [Ionita, 2013]

Enterprise Governance of IT and IT Management [de Meijer and Bruyndonckx, 2015].

(a) COBIT 5 Principles. Source: [Shobhit, 2019]

(b) COBIT 5 Enablers. Source: [Nugroho and Surendro, 2016]

Figure 2.6: COBIT 5 Framework

OWASP Risk Rating Methodology

The Open Web Application Security Project (OWASP) is a nonpro t foundation with the primary objective of enhancing software security. Although the organization is primarily geared towards software products, its framework provides an outline of the critical factors in uencing threat agent activities, business impact factors, and other related aspects, thus having a close relationship with enterprise-wide risk management. OWASP comprehensively depicts and decomposites potential risk factors that can be used for information systems [Ionita, 2013]. Figure 2.7 illustrates this decomposition.

The OWASP risk rating methodology comprises three key elements, the likelihood of exploitation, the impact of exploitation, and the resulting risk rating. The likelihood of exploitation component is grounded on an assessment of the threat agent, such as motivation and skill level, and the vulnerability factors such as ease of discovery, awareness The technical impact is gauged by examining the con dentiality , integrity , availability , and accountability of the data or system. The business impact contains nancial damage, reputation damage, etc. The risk rating is established through a fusion of the likelihood and impact assessments.

Compared to previous risk assessment frameworks, the OWASP framework places a greater emphasis on application software security [Wright, 2008]. As noted by [Gantz, 2014], OWASP includes a set of business factors that can assist organizations in developing comprehensive IT audit strategies to assess their customized applications and other commercial applications used by the organization.

In summary, from these three models, we can conclude that there are multiple factors that could impact the judgment of risk classi cation. For example, the soft factors such as the company's goals, structure as COBIT 5 depicted, and the technical factors such as the timing, detection or remediation measurements as FAIR described. Risk classi cation is a behavior conducted by risk management practitioners, which means practitioners can also have an impact on how to conduct risk classi cation. This viewpoint will be discussed in the next section.

Figure 2.7: Decomposition of Risk level (Exposure) according to the OWASP methodology, source: [Ionita, 2013]

2.3 Risk classification under enterprise context

2.3.1 Risk classification in audit field

Audit risk assessment process

According to a source in the company studied in this research, the audit process can be roughly illustrated in figure 2.8:

Figure 2.8: Audit process flow

As figure 2.8 shows, the process of auditing a company can be split into following steps:

- The first step is to accept the engagement. This step involves the activities that help to understand the clients to see if it is doable to accept the clients, such as client intake, client acceptance, specifically, relationship check and independence check, etc.
- The second step is winning the proposal. This step involves activities such as selecting the audit team, preparing a draft proposal, validating audit time, authorizing the proposal, etc.
- The third step is preparing the audit. In this step, the lead auditor should prepare 3-year audit programme, the audit plan, etc. In total, the whole audit process includes initial audit, the first and second surveillance audits and a recertification audit in the third year before expiration of certification.
- The fourth step is to conduct the audit. In this step, auditors should conduct stage 1 and stage 2 audit, as well as the first and second surveillance audits. The findings showed in the stage 1 audit can be improved in the stage 2 audit.
- The fifth step is to complete the plan. This step involves communicating the findings with clients, corrective actions to resolve the major nonconformities, certification decisions, etc.
- The last step is to maintain conformity. This step involves activities such as information changes, past performance reviews, measures when non-compliant.

It is noted that auditing a company against ISO/IEC standards is not a one-time event. The process takes three years and involves multiple rounds of audits. As a result, any history of repetitive nonconformities may a ect the auditors' nal decision on the risk classi cation and certi cation of the company.

Risk classi cation terminology

To certify a company against ISO/IEC 27001, practitioners must examine all applicable controls. Regarding the classi cation of ndings or risks in a company's information system, ISO 27001 does not specify whether to use a quantitative or qualitative approach. Instead, the standard requires that the company's chosen risk assessment method be "consistent and repeatable" [ISO27001guide, 2020].

ISO/IEC 27001 has its own terminology for classifying controls and ndings. The ndings or potential risks can be categorized into the following categories: conformity, nonconformity and observation. Nonconformity can be further classi ed as major nonconformity and minor nonconformity [Dougher, 2022]. This terminology comes with de nitions, yet without prescribed numeric formulas, so no speci ed quantitative method is required when using those terms.

Conformity means that the requirements are met. Nonconformity refers to a state in which an organization fails to ful ll what is required by the standard, nor the requirement nor the documentation [Kosutic, 2014].

Major nonconformity is a type of nonconformity that indicates the presence of a deviation from requirements that signi cantly impairs the ability of the management system to achieve its intended results. Major nonconformity may arise under the following circumstances:

- If there is substantial uncertainty regarding the e ectiveness of process control or the ability of products or services to meet speci ed requirements;
- The presence of several minor nonconformity related to the same requirement or issue may indicate a systemic failure, thereby qualifying as a major nonconformity.

Unlike major nonconformity, minor nonconformity refers to the fact that the nonconformity is present but it does not impede the ability of the management system to attain the desired outcomes.

Observation refers to the state in which a requirement is met, but room for improvement exists [Chopra et al., 2020].

Some examples of nonconformity can be: If an action is corrected and the standard asks to have records of this corrective action, yet the organization does not have corresponding records; The procedure requires the organization to use a speci c approach to conduct an action, but the organization uses a di erent approach to do it; The organization does not provide su cient output for its customers, yet the organization is expected to do so in terms of the contract it signed with customers [Kosutic, 2014].

[Control Union Certi cations, 2021] also describe the scenarios that should be considered as major nonconformity: If the issue is not compliant with the legal requirement, or a breach that a ects the subject of assessment to be able to accomplish its goals, for instance, such as when an organization deliberately conceals unfavorable evidence or fail to produce compliant products, processes, or services based on their performance, the issue at hand may require further scrutiny. Some other considerations include the omission of a whole section, for example, a lack of

completed risk assessment or risk management review, or an item may be regarded as signi cant and documented, but a lack of clear evidence exists to demonstrate its actual implementation [Certikit, 2020].

For minor nonconformity, examples include that the improvements have been made, but their evaluation has not been carried out with due diligence, or where regulatory measures and controls have been implemented, but they do not adhere to the documented process [Certikit, 2020].

An observation is inferior to minor nonconformity in terms of severity. An observation indicates the places where there are early signs of a minor nonconformity. For observation, if actions are not taken in a timely to treat this observation, it may lead to minor or major nonconformities at the later stage [Isms.online, 2022a].

The de nitions of major and minor nonconformity above partially describe how to distinguish these two types of nonconformity. Yet when it comes to reality, it may involve multiple practical issues that need more discussions and analysis by ISO/IEC 27001 practitioners. As [Hall, 2019] indicated, there are no universal and sophisticated guidelines on distinguishing major nonconformity, minor nonconformity, and observations if no quantitative risk method is used. This raises a question: to what extent is the control not compliant with the requirements? A major nonconformity indicates there is a signi cant deviation from the standard. A minor nonconformity means there may be one or multiple requirements the origination does not meet but in general, those issues do not a ect the operation of ISMS [Certikit, 2020]. It is worth a discussion about whether ISO/IEC practitioners always reach the same understanding of risk classi cation for ndings.

2.3.2 Risk classi cation in consulting eld

Risk assessment process in consulting eld

If a company has not implemented ISO/IEC 27001 standards, or it has been implemented but has not been certi ed, a maturity assessment, also commonly called a gap assessment, can be conducted against the standard to ensure that current practices are in compliance with the standard [Popa, 2018].

Maturity level assessment is part of the cyber security consulting service. Compared to the ISO/IEC 27001 certi cation process with rigorous guidelines, the consulting process of ISO/IEC 27001 is less strict. The process ow of the cyber maturity assessments process and relevant activities are illustrated in gure 2.9:

As [Centric, 2018] indicates, the cyber maturity assessments start with a series of questions in various forms, it is for the ISO/IEC 27001 practitioners to have a comprehensive image of the client's current security environment as well as the business goals.

After the phase of understanding and discovery, ISO/IEC 27001 practitioners will evaluate and analyze the present security position in comparison to the ideal state, speci cally, the business objectives, important systems, identi ed risks, and the e ectiveness of controls.

In the end of the assessment, the ISO/IEC 27001 practitioners will provide a report which contains maturity assessment result, suggested roadmap, ect based on their ndings.

As the ISO/IEC 27001 implementation is not strongly related to the topic of risk classi cations, in this research, we do not emphasize the process of ISO/IEC 27001 implementation.

Figure 2.9: Cyber maturity assessments process. Source: [Centric, 2018]

Maturity assessment scoring system

Di erent from certi cation, the standard and process of using ISO/IEC 27001 in the consultancy sector are di erent. Often cases, the consultancy sector presents the risk assessment results in a visualized way, one of the widely used approaches is to use the maturity model [Monda and Giorgino, 2014].

The maturity model is a model used to depict the level of maturity in an organization's performance [Khoshgoftar and Osman, 2009]. They identify and explore an organization's advantages and drawbacks and show benchmarking information [Abazi and Kõ, 2019]. Under information system context, the term "maturity" refers to the understanding of information systems and a tool to benchmark information in order to show future improvement [Lasrado et al., 2015, Mettler et al., 2010].

Multiple maturity models are being used, for instance, ISM3 (Information Security Management Maturity Model), SSE-CMM (System Security Engineering Capability Maturity Model), COBIT Maturity Model and NIST Maturity Model. One of the most popular maturity models is Capability Maturity Model developed by Software Engineering Institution (SEI) [Abazi and Kõ, 2019].

The Capability Maturity Model (CMM) was proposed after software developers experienced their ine ciency in managing the software process in 1980s. The current version of CMM results from multiple times of feedback and is used to see if a company has a mature IT environment [Paulk et al., 1993, Atoum and Otoom, 2017].

The capability Maturity Model consists of ve levels of maturity, with each level representing a di erent stage of organizational maturity and capability. As the gure 2.10 shows, those levels show process maturity from low to high.

Level 1 refers to the Initial, it is the lowest level of maturity. At this level, the process

Figure 2.10: Five levels of Capability Maturity Model. Source: [Welch et al., 2016]

is dynamic, unstable and poorly documented. Uncontrolled activities and events can happen frequently and bring uncertainty to the process.

Level 2 refers to Repeatable. At this level, processes are disciplined yet not rigorous, some results are consistent. Processes depend on familiar scenarios or environments. When the context differs from the familiar ones, the processes may become chaotic and messy.

Level 3 refers to the Defined. At this level, processes are more standardized, defined, and consistent. The processes at this level can be referred to and used by users to make them more capable of proceeding with processes.

Level 4 refers to Managed. At this level, processes are more under control. One characteristic of this process is that the processes can be measured and controlled using metrics. The process database is likely built up. The processes are predictable, and deviations can be noticed in time and corrected correspondingly.

Level 5 refers to Optimizing. At this level, the focus is continuously improving processes. An approach that can avoid deficiencies, recognize weaknesses and make improvements has been developed. The data is accessed to predict and analyze to get the best result.

In conclusion, this chapter focuses on introducing basic concepts of risk classification and understanding the decision-making process of security practitioners when conducting ISO/IEC 27001 risk assessment for enterprises. As this study mainly examines two security activities related to ISO/IEC 27001: certification in the audit field and maturity assessment in the consulting field, The research questions were formulated based on this information, with the first sub-question focusing on the certification process and its relation to the audit process, and the second sub-question focusing on the maturity assessment process and its relation to the consulting process. Further details on the study findings can be found in the Results chapter.

Chapter 3

Related work

This chapter presents a picture of the current state of knowledge on the role of professional judgment in decision-making by IT professionals. The discussion is divided into three parts. The first part focuses on the role of security risk management professionals, the second part discusses the general decision-making process, and the third part examines the role of professional judgment during risk assessment. By analyzing these three aspects, a picture of how IT professionals make decisions is shown, this is helpful for understanding how IT professionals make decisions when using ISO/IEC 27001 for certification or maturity assessment.

3.1 Security risk management professionals

3.1.1 Roles and responsibilities

Security risk management professionals include multiple roles and corresponding areas. For job titles, such as security manager, IT risk & security specialist, risk and compliance investigator, information security officer, security architect, loss control consultant, compliant consultant, IT auditor [Moramarco, 2018, Haney and Lutters, 2021] etc. Some of those jobs are internal positions of companies, such as risk manager, which evaluates and analyzes the company's risk situations. Some jobs, such as compliant consultants and IT auditors, are often positions provided by special companies that are qualified to provide information security consulting services or information management certifications to other organizations. In this research, because we mainly focus on information risk assessment against ISO/IEC 27001, the experts are mainly from qualified cyber security companies, such as ISO/IEC 27001 auditors, consultants and implementers.

IT auditing analyzes and examines an organization's IT systems, infrastructure, policies, procedures, and operational processes against recognized standards, and frameworks [Aditya et al., 2018]. By conducting IT auditing, a company could know if their existing IT controls work effectively to protect the company's assets, and align well with the company's goals and businesses [LeanIX, 2022].

IT auditing is conducted by IT auditors. IT auditors assess if the controls protect the organization and its assets well [LeanIX, 2022].

Another type of risk management professional providing cyber security services is the consultant. An IT consultant is a professional who helps customers with their technological projects.

Companies often hire IT, consultants for advice when deciding on a company's technology infrastructure [IndeedEditorialTeam, 2023]. For example, companies might come to IT consultants to ask for help with assessing their information maturity level against a specific framework, by doing so, the company can have a better view of how aligned the company is with the framework's requirements.

Framework implementation specialists help customers implement a specific framework, translating the framework's requirements into specific actions. By implementing a risk management framework, the company has a set of safeguards and controls against cyber attacks [Bakertilly, 2016].

3.1.2 Key skills and qualifications

To become a qualified risk management professional, [Haqaf and Koyuncu, 2018] identified twenty skills and categorized them into five groups: technical skills; project/process management skills; risk management skills; business skills; core information security skills. The research shows that, among those skills and groups, the project/process management skills, specifically, the ability of "understanding of information security issues from a management point-of-view"ranks the highest, followed by risk management skills in"identifying the best information security practices for risk management" and core information security skills in "designing information security systems". Interestingly, the study found that core information security skills were mentioned the most, while technical skills were mentioned the least among the twenty skills identified.

In a study by Parker and Brown (2019), thirty-three skills were identified and categorized into six groups. The largest proportion of skills, at 40%, fell under the category of technical skills. Specifically, skills such as"technical writing" , "design technical solutions and systems"and "vulnerability management" are seen as important. The second biggest share was attributed to interpersonal skills, including "communication" and "client service" . The remaining skills were grouped into business skills, such as"reporting and monitoring budgets", management skills, such as"developing security policies and procedures,"analytical skills, such as"assessing requirements," and finally, leadership skills.

[Vogel, 2016] examines the cyber security skills gap, concluding that gap can be reduced by providing individuals with more education and training. [Colley, 2007] holds a similar opinion, indicating that in 2007, around 41% of the total security budget went to education and training for personnel.

3.1.3 Challenges faced by security risk management professionals

[Morgan, 2002] indicates that the rapidly evolving threats have become one of the biggest challenges for security risk management professionals to face. More organized crimes and terrorist adaptations to the new technologies are showing up. The constantly evolving cyber threat makes it hard for professionals to always keep track. Professionals must regularly refresh their knowledge and skills to recognize and mitigate emerging threats effectively.

[Armando et al., 2015] believe there should be a balance between security management and accessibility. In many industries, such as schools and hospitals, students or patients use applications to access their data. The issue is that users may be frustrated remembering multiple complex logins [Saxena, 2004]. Robust security measures can help mitigate risks yet lead to a less user-friendly system. Thus, it is important for professionals to pay attention to strike a balance between security and accessibility.

[Jamshidi et al., 2018] points out that the more complex a technology is, the more di cult to identify and mitigate risks. If a large organization has multiple interconnected and dynamic systems, professionals will likely put more e ort into understanding the systems and conducting risk management e ectively. This challenge requires professionals to update their knowledge in a regular basis.

Security risk management professionals must comply with di erent regulations and navigate a complicated regulatory environment [Callen-Naviglia and James, 2018]. On the one hand, there are many laws, policies and regulations regarding data privacy, especially for an organization that is related to multiple business elds and has to obey multiple regulations, this can be challenging. On the other hand, researchers also argue that too many controls may have a negative impact on cyber security behaviors [Muckin and Fitch, 2014]. As not all controls may be appropriate for every distinct organizational environment, preventing organizations from failing to solve their particular issues e ectively [Marotta and Madnick, 2020].

Ethical issues can also exist in cyber security practice [Macnish and Van der Ham, 2020]. For cyber security professionals who provide cyber security services to other companies, bias and discrimination can be an issue. On the one hand, the new technologies, such as the use of automated, cognitive technologies and the use of data may increase the professionals' judgment bias or generate new biases [Lombardi et al., 2022]. On the other hand, cyber security professionals may rely on experience too much and do not clearly distinguish all the di erences between companies, which makes them may overlook each company's speci c and details cyber risks and vulnerabilities.

3.2 Decision making processes

3.2.1 Decision making process model

The decision-making process of cyber security management is strongly related to various information [Diesch et al., 2020]. Security analysts may nd it challenging to make decisions in an uncertain environment. [M'manga et al., 2019] has proposed a normative model that transfers ambiguity to certainty in cyber security decision-making process. The model is shown as gure 3.1:

Figure 3.1 shows the basic decision-making process for cyber security.

- The rst step is situation assessment. This step is to answer the question "how may a situation be understood?" The decision makers have to know knowledge of the situation, the a ordances of evidence, recognize the situational timeline and data correlation;
- The second step is goal formation. This step is to form the goals based on the understanding of the situation and identify the situations that prevent the realization of the goals;
- The third step is information needs assessment. This step answers the question "which information is relevant for decision-making?" In this step, the decision-makers have to identify the necessary information and move out redundant information
- The fourth step is information exploration. This step answers the question "where can additional decision-making information be sourced?" Decision-makers must explore possible alternatives if the information is unavailable. For example, ask for help from legal o cers and tax specialists.

Figure 3.1: Risk Rationalisation Flow. Source: [M'manga et al., 2019]

- The fth step is information limitations analysis. This step tries to answer the question "what remains unknown". The decision-makers need to identify important information gaps and analyze the possible consequences.
- The sixth step is options generation and analysis. This step tries to answer the question "what are the decision alternatives?" Decision-makers should identify the alternatives and their implications.
- The seventh step is options validation. This step answers the question "where could assumptions be incorrect?" In this step, it is important to know if there are any signs of uncertainty and if those uncertainties could impact the decision-making process. The impacting factors can be categorized into four groups: Environmental factors such as dynamic or still, consistent or inconsistent, complete information or incomplete information; Contextual factors such as time issue, complexity, and magnitude of the situation; Personal factors such as experience and training; and Information factors such as accurate, relevant speci c, unbiased, etc.
- The last step is option selection. In this step, the most knowledgeable and impartial option is chosen for the decision.

3.2.2 Decision making factors

[Oltramari et al., 2015] assessing cyber security risks is a process of multiple components involved. It is not only about hardware, and software, but also about environmental, and human factors.

[Diesch et al., 2020] identify the factors that impact information security. According to the importance of the factors to organizations' information security, the factors are ranked as vulnerability, resources, awareness, access control, physical security, infrastructure, risk, continuity, security management, organizational, CIA Triad and compliance & policy.

[Parsons et al., 2015] address the in uence of organizational information security culture on information security decisions making, pointing out that there is a positive correlation between information security decision-making and organizational information security culture.

[Shreeve et al., 2020] point out that the decision-makers must have the ability to risk thinking, that is "identifying risks, assessing their severity and prioritizing responses." The research shows that the plasticity of teams plays an important role in decision-making, which can relatively easily impact decision-making strategies.

Cyber security requirements are subject to the in uence of various stakeholders' priorities and determinations. In an organization, di erent roles are responsible for di erent risk management activities and tasks, for example, CISOs determine the risk prioritization. The research shows that the experts are a ected by their biases and experience when playing decision-making games, which cause them not well performed in the decision-making process [Shreeve et al., 2020].

[Hibshi et al., 2016] indicate that even though there are many guidance about how to secure systems, the security experts often do not fully comply with the guidance, they often use their prior knowledge and experience to conduct a risk assessment and identify the vulnerabilities.

Transparency and multi-stakeholder dialogue are deemed as important elements of cyber security [Stifel, 2017]. [UK, 2016] points out that establishing a line of communication between people responsible for the organization's security is signi cant. For example, a big cyber security project may involve multiple departments, it is not expected to see each department works solo or lack su cient communication, which could lead to inconsistency in the project. Having a xed contact person or regular communication may reduce this situation.

Besides, it is also important to establish external channels to communicate with business partners. Regular communication with business partners about cyber security can serve as a means for organizations to identify potential vulnerabilities, thereby allowing for collaborative e orts to address them. This engagement helps foster best practices that bene t both parties [Nagler, 2019].

3.3 Professional Judgment

Although there are numerous guidelines for risk assessment and classi cation, the professional judgment remains a factor that can result in varying opinions on risk classi cation. Professional judgment refers to the use of auditors' training, knowledge, and expertise to make decisions that comply with accounting and ethical standards [Auditor Forum, 2022].

[de Wit et al., 2021] reveals that security professionals' risk preferences and decision-making processes are signi cantly a ected by their individual characteristics, background, and experience.

Furthermore, organizational culture and the feasibility and constraints of security measures exert a heavy in uence on security professionals' decision-making processes. [Yazdipour et al., 2013] indicates that professional judgment constitutes an important element in information security risk classi cation, and can serve as a complementary approach to formal methods in the risk classi cation process. [Barber et al., 2010] has a similar opinion on professional judgment's value in information security risk management. It states that professional judgment can be used as a tool for organizations to manage their information risks.

[Vose, 2008] explores the drawbacks of expert judgment in risk management, the study posits that excessive usage of expert judgment can potentially result in errors and biases. It also argues that using formal methods and quantitative models are a good way to achieve reliable and e ective results than expert judgment in many cases.

[Morrell, 2013] indicates that the results of applying expert judgment are less e ective than using formal risk management methods in identifying and mitigating risks. Expert judgment is often impacted by personal factors and thus leads to bias. In comparison, formal methods are more objective and consistent for risk management. [Aven and Zio, 2014] holds similar opinions, indicating that formal methods generate a more robust risk management result than expert judgment.

More speci cally, using the maturity model can also be related to professional judgment. [Paulk et al., 1993] believes that the maturity model allows a certain extent of professional judgment since some key practices are intentionally vaguely stated for exibility. Though most risk management standards have speci ed detailed information for achieving quali ed results, professional judgment is still needed on many occasions. For example, the phrase "as appropriate" and \as necessary" are not explicitly de ned in key practices of the maturity model. In di erent companies or di erent projects in the same company, these two phrases may have di erent meanings.

[Paulk, 1999] summaries possible spots in every level that have to apply professional judgment. It also mentions that for goals when using the maturity model, the risk assessment team can usually nd 3-5 "alternate implementations" are applied. 10-15% of the key practices are interpreted and the assessment team has to discuss in detail if this interpretation is good or not.

In this case, we can conclude that professional judgment is applied when ISO/IEC 27001 practitioners conduct risk classi cation or evaluate a company's information system maturity level. Therefore, identifying the factors that contribute to making professional judgments is crucial.

Chapter 4

Methodology

This chapter outlines the methodology used in the research, starting with a discussion of the research strategy. Next, the method of data collection is introduced. The study followed a qualitative research approach, with grounded theory applied to process codes and generate concepts.

4.1 Research Strategy

The objective of this research is to investigate how ISO/IEC 27001 practitioners classify information risks or ndings, and what factors in uence their decision-making. As outlined in the Background chapter, no rigid framework exists to guild ISO/IEC 27001 practitioners in their risk classi cation assessment. To the best of our knowledge, this problem was not yet been fully studied. Consequently, the exercise of professional judgment is used for discretionary decision-making. In order to identify the key factors that in uence ISO/IEC 27001 practitioners' judgment and their utilization thereof, an exploratory research approach is deemed appropriate. This research methodology seeks to establish the "what" and "how" of the aforementioned factors. Upon analysis of the results, a model detailing the factors that impact IT experts' decision-making will be formulated.

According to [Lindlof and Taylor, 2017], qualitative researchers"seek to preserve and analyze the situated form, content, and experience of social action, rather than subject it to mathematical or other formal transformations" . [Frey, 1992] state that qualitative data can be analyzed and displayed as"critiques, and sometimes verbal reports". In this context, the interview method is chosen to conduct this research, as it allows for a good understanding of the study phenomenon in cases with limited knowledge about it [Gill et al., 2008]. Additionally, interviews can help guide participants to answer a speci c research question [Stuckey, 2013].

To answer the research question in detail, four subquestions are proposed. The rst two subquestions discuss professional judgment in two di erent sectors, the certi cation and advisory. The third question discusses the di culties of conducting risk classi cation using ISO/IEC 27001. The last subquestion discusses how to make the process more repeatable and reliable. The interviews will be semi-structured, with xed questions that will be adjusted and improved due to the following reasons: (a) the increasing understanding of the answers provided by experts, (b) the expertise of each participant, (c) and the time limit. The data will be analyzed using grounded theory methodology, and multiple coding techniques will be applied to generate the nal model.

The research is conducted in a commercial company that has a wide network of ISO/IEC 27001 practitioners. Due to the privacy needs, the name of the company and participants are anonymous. The interviews were conducted between March to September 2022.

4.2 Data Collection

4.2.1 Sampling

The data are collected via 13 interviews. In order to have a better view of how levels of risk ndings of the company's information security system are classi ed, the samples are selected from a group of ISO/IEC 27001 practitioners who have experience in applying or are familiar with ISO/IEC 27001.

All experts belong to one of three business divisions: certi cation, advisory, and implementation. Experts from the certi cation division are typically auditors responsible for certifying companies against ISO/IEC 27001. Experts from the advisory division are consultants who provide consulting services related to ISO/IEC 27001, with a particular focus on maturity assessment. Implementation experts, on the other hand, assist companies in implementing ISO/IEC 27001 controls and help them become quali ed for ISO/IEC 27001 certi cation. The participants of the interviews include (senior) associates, (senior) managers, directors, and partners. This range of roles is intended to provide a comprehensive perspective on the factors that could impact experts with varying levels of experience when evaluating the ndings of a company's information security system. This approach can help identify potential variations in how experts interpret and classify risk ndings, leading to a more thorough and accurate evaluation.

4.2.2 Interviews

The interviews are designed as semi-structured interviews. This method allows for exibility to accommodate new topics or better t the experts' unique situations. Moreover, open-ended questions allow experts to answer in their own words. This creates a wider range of possible answers.

The interviews are conducted virtually or physically. All the interviews are recorded after being given consent by experts. To reduce the mutual in uence, all interviews are conducted one-on-one. The interviews are transcribed using a tool calledDescript, and all transcripts are coded using a tool called Atlas.ti .

4.2.3 Grounded theory

The grounded theory is used to code the transcripts as grounded theory signi cantly impacts qualitative traditions [Walker and Myrick, 2006]. The grounded theory approach expects researchers to continually compare and categorize the data, and build relationships between the data [Tie et al., 2019].

In the grounded theory methodology, the process of coding is a crucial step in conducting research. According to [Corbin and Strauss, 1990], the coding process comprises three primary steps: Open Coding, Axial Coding, and Selective Coding. These steps are vital for analyzing qualitative data and identifying relevant themes and concepts.

The first stage of coding is open coding, where coders approach the data with an open mindset. This data is typically obtained from transcripts of interviews and is broken into smaller pieces, which are then labeled with descriptive codes.

Axial coding is the second stage of coding. In this phase the relationships and connections between codes needed to be explored. The codes should be aggregated into broader categories.

Selective coding is the last stage of coding. Here core categories are built. The generated core categories are developed from existing axial coding categories or new categories are summarised from other categories. The core categories integrate with each other and describe the relationship between them.

An example can be given to show the coding process. Below is a snippet of the transcript and added label:

"And then for example, or let's say a client is much smaller than the type of clients that you're used to #company_size_as_a_factor. It can be, you know, require an additional thought to, yeah, to be able to assess them."[Expert 13]

The three types of coding and coding processes in this research is shown as follows:

Table 4.1: Example of coding process

Process	Output	Example of output
Open coding	Concept	Company size
Axial coding	Subcategory	Company side factor
Selective coding	Category	Impacting factor

Chapter 5

Results

The previous chapter outlined the methodology employed in this research, including the use of qualitative research and interviews as the data collection method. This chapter presents the results of the interviews and coding. The rst section provides an overview of the interviews, while the second section presents the generated codes and categories. In the third section, the data mapping of codes and research subquestions is shown. Finally, a visualization of the research process is presented.

5.1 Interviews Overview

A total of 13 interviews were conducted for this research. All the participants were experts who had varying degrees of experience with or application of ISO/IEC 27001. The number of clients (companies) each expert dealt with varied based on their role and experience within the company.

Table 5.1: Overview of the interview experts

No.	Role	Job title	Experience	Answered subquestions
1	Consultant	Associate	2	2-4
2	Auditor and consultant	Associate	2	1-4
3	Auditor and consultant	Senior manager	5	1-4
4	Consultant	Manager	8	2-4
5	Auditor and consultant	Senior associate	2	1-4
6	Auditor, implementer and consultant	Senior associate	5	1-4
7	Auditor and consultant	Director	27	1-4
8	Implementer	Manager	7	3-4
9	Auditor and consultant	Senior manager	24	1-4
10	Auditor and consultant	Partner	20	1-4
11	Auditor and consultant	Director	12	1-4
12	Consultant	Senior manager	10	3-4
13	Auditor and consultant	Senior associate	3	1-4

As table 5.1 shows, the experts primarily have the roles of auditor, consultant and implementer. The job titles of the experts include Associate, Manager, Director, and Partner. The years of experience range from 2 years to 27 years, with a median of 7 and an average of 9.7 years.

Though participants work in their own departments, many of them have experience with di erent roles. Out of the thirteen people, nine have knowledge of both certifying and assessing a company's maturity level against ISO/IEC 27001. One participant has only experience with maturity assessment, while another has only experience with implementation. One participant has experience with auditing, implementation, and maturity assessment, and one participant has no experience with any of the above activities regarding ISO/IEC 27001 but had training on ISO/IEC 27001 certi cation, thus he is categorized in the certi cation sector. The illustration of their area of expertise is shown in gure 5.1:

Figure 5.1: Proposition of participants in terms of skills

Due to the travel restrictions imposed in response to the COVID-19 pandemic, eleven of the interviews were conducted online, while two were conducted in person. All the interviews were conducted in English, the initial questionnaire can be found in Appendix A. It is important to note that, due to the expertise of the experts and time constraints, the questions asked during each interview were slightly adjusted. The average duration of the interviews related to the research topic was 32 minutes ranging from 20 to 63 minutes.

5.2 Codes and Categories

In total, 660 codes are generated through 13 interviews with experts. Number of codes for each interview can be found in table 5.2.

After all initial codes were obtained, selective coding was conducted to group the codes into multiple concepts based on their correlations. Categories and subcategories were then generated based on the existing concepts. The full list of interview concepts and categories can be found in Appendix B.

The previous chapter presented the results of the codes generated from interviews. In this chapter, we will delve deeper into the codes and each subquestion. The rst section focuses on risk classi cation when using ISO/IEC 27001 for auditing, the second section discusses risk classi cation for maturity assessment, the third section addresses di culties, and the nal section explores potential improvements.

Table 5.2: Number of codes for each interview

No.	Number of codes
1	56
2	71
3	58
4	42
5	50
6	50
7	51
8	48
9	55
10	52
11	49
12	35
13	43

5.3 Results of subquestions

5.3.1 Risk classi cation in auditing eld

Impacting factors

Impacting factors: Company' context Based on the collected data through the interviews, it shows that the companies have the strongest and direct impact on ISO practitioners' decisions of risk classi cation. The company in this research can also refer to clients/customers who request to have ISO/IEC 27001 certi cation or be maturity assessed against ISO/IEC 27001.

The reason why the company context has the most signi cant impact is that each company's context varies, making it challenging to expect di erent companies to use the same benchmark. The size, infrastructure, and structure can di er greatly and have varying levels of complexity. These factors a ect the scope of the audit content, which, in turn, in uences the classi cation decision.

The factors that were mentioned most frequently during the interviews as having the most signi cant impact are the goals, size, type of the company, and company complexity such as the structure, infrastructure, and process . Those elements directly in uence the scope of the risk assessment. Not all controls of ISO/IEC 27001 need to be audited for a company; only applicable controls will be included in the scope. Unrelated controls will be excluded from the audit scope. It is not realistic to expect a small startup to have a mature information security system that's as robust as that of a large international bank, even if both aim to achieve ISO/IEC 27001 certi cation.

Take the company goal as an example. If a company's goal is to achieve certi cation in order to be sold or to align with a parent company, the controls that are included can vary according to the purpose, and as a result, the scope can be di erent. As an expert has indicated:

"You have an ISO certi cation with a certain purpose, and based on that purpose, the organization identi ed what is in scope, what is out scope, because you don't need to have all the domains and all the details." [Interview 10]

The motivation and attitude of a company towards obtaining ISO/IEC 27001 certi cation can impact the auditor's decision. A company with strong motivation to obtain ISO/IEC 27001

certi cation is more likely to invest su cient time, resources, and e ort to meet the requirements. Management is also more likely to raise awareness of the certi cation throughout the entire company, and the evidence provided to the ISO practitioners may be of higher quality. Conversely, companies with low motivation may invest less in the certi cation process. Moreover, motivated companies may conduct strict self-assessments and regularly examine their risk management. One indication of motivation is whether the certi cation process receives the attention of the company's management. Experts interviewed mentioned that whether a company's management values ISO/IEC 27001 certi cation can in uence the results of the risk evaluation:

"The reason was that there was not su cient attention from higher management and investment on that topic, and as such," [Expert 10]

The knowledge and capability of a company regarding information security can impact whether it can e ectively implement su cient security controls. For the controls that do not apply to the company, ISO/IEC practitioners will not take them into account to assess, it is the scope of the work, and also it is related to the statement of applicability.

"But like it's a three-year program normally that you go through, right? Like rst-year certi- cation, second-year surveillance, third-year surveillance before you go for an extension of your certi cation. And during the second and third year where you do these surveillance audits there, you also try to ensure that you cover at least the full set of controls that the customer has in place. But what's also important to realize is that not all AnnexA controls are necessarily applicable to a customer. That's why you also have the statement of applicability that you review. [Expert 3]

"Because there is also the statement of applicability that you get evidence that is not applicable to the environment that you are auditing, for instance, or something like that." [Expert 12]

In summary, the company side factors can be illustrated as gure 5.2:

Figure 5.2: Company side factors

Impacting factors: Practitioner's context There can be di erent opinions on the same nding depending on the situation of the ISO/IEC 27001 practitioners (auditors in this context). According to the interviews, a practitioner's personality, experience, and training are considered to be the most in uential factors a ecting their judgment. As an expert emphasize how training impacts their decisions on risk classi cation:

"However, once you have had, you know, the necessary training and exposure to the terms being used in practice, then yeah, it becomes quite familiar...We have like elaborate and regular trainings where they will discuss this kind of thing and we would, for example, look at examples and things

like that as part of our frequent training. We make sure that we understand how to make that judgment. and as I said together, like using examples and things like that, and discussing it with other colleagues where needed."[Expert 12]

As to personality, experts indicated that he tends to be more strict with risk classi cation as the approach he uses is to falsify everything until it is proved:

"So in my head, everything's already a nonconformity until proven and conformity... And if I see, okay, this is indeed su cient, then I will give the classi cation conformity, otherwise in my head it's a nonconformity and o cially there is no classi cation yet, but I do basically the other way around." [Expert 1]

"Eventually, like we'd make this decision with the audit team. So that'll be usually two or three people. And it just depends on, people will be more strict in that aspect."[Expert 5]

Experience plays an important role in risk classi cation. When practitioners get su cient experience, they develop a systematical and logical method to conduct risk management:

"experience is a big part of it. I think in the beginning, you know, it's more common to have those type of discussions with colleagues who are just starting out to help them make that professional judgment. But over time it becomes, you kind of become used to it because you've done it like a lot of times. [Expert 13]

Auditors' roles and duties can be relevant to the judgment. Auditors' roles are related to experience and the skills of making the most correct decisions. For example, if an auditor is a lead auditor, he/she is likely to be more decisive when confusing cases happen than inferior auditors do.

"It's not always the case that I should be right. because in the sacrication of duties within the team, sometimes the auditors also review the more detail, the documentatio1n"[Expert 9]

In addition, their technical knowledge and sensitivity/intuition to risks are also crucial. For instance, an auditor with strong technical knowledge might still be able to identify and recognize hidden risks even if the company has met all control requirements. Sensitivity is a factor that can impact the risk classi cation result. Practitioners with a good understanding of new concepts and the ability to identify risks that others may overlook are more likely to achieve accurate risk assessments. As an expert indicated:

"It could be very strict at the same time because you can have an auditor that actually has the sensibility to understand this control." [Expert 6]

In summary, the company side factors can be illustrated in gure 5.3:

Impacting factors: Controls variation Controls are implemented to protect the information system from attacks. However, if a control fails, it can create a risk. The way controls are presented can vary depending on the company's context, leading ISO/IEC 27001 practitioners to have di ering opinions on the same controls. During the interviews, six experts stated that if the initial control fails, they would check for replacement or compensating controls and evaluate their e ectiveness. One issue is that replacement controls may not be identical to the initial control, which leaves room for judgment on whether they can function as well as the initial control or to what extent. As a result, assessing the e ectiveness of replacement controls can be subjective.

An expert provided an example where an initial control requires a company to retain data for