An empirical study into how cyber security professionals deal with uncertainty in information security risk assessments

Understanding perceptual aspects and judgment operations

K. J. C. Hagenaars

Management of Technology
Technische Universiteit Delft

Cyber Risk Services
Deloitte

TU Delft

An empirical study into how cyber security professionals deal with uncertainty in information security risk assessments

Understanding perceptual aspects and judgment operations

by

K. J. C. (Kay) Hagenaars

Master thesis submitted to Delft University of Technology
in partial fulfilment to obtain the degree of Master of Science
in Management of Technology from the Faculty of Technology, Policy and Management

To be defended publicly on Monday October 21st, 2019 at 1:30 PM.

Student number:	4745442	
Project duration:	April, 2019 – October, 2019	
Thesis committee:	Prof. dr. M. J. G. (Michel) van Eeten,	TU Delft, Chair
	Dr. ir. W. (Wolter) Pieters,	TU Delft, First Supervisor
	Dr. M. P. G. (Maarten) Franssen,	TU Delft, Second Supervisor
	ir. K. V. M. (Kirsten) Meeuwisse,	Deloitte, External Supervisor

An electronic version of this thesis is available at http://repository.tudelft.nl/.

TU Delft Deloitte.

Preface

This thesis is the final work in fulfilment to obtain a master's degree in Management of Technology at Delft University of Technology. Skills and knowledge acquired from this Master program have been applied as part of the final assessment for the duration of this thesis.

The study has a socio–technical problem at the core that required the analysis of stakeholders and the technical processes involved to gain a better understanding of the underlying structures within the research domain. This research has contributed to the current body of knowledge by shedding light on the perceptual aspects of uncertainty and the judgment operations of cybersecurity professionals during information security risk assessments.

This particular topic is chosen based on personal experience from one of the cyber courses during the Master program. Tasked with the execution of an information security risk assessment, many questions about the technical process and people involved came to mind. In particular concerning the perception of uncertainty and how the judgment operations allow information security risk assessments to be executed. A thorough analysis of this process and the cybersecurity professionals involved provided me with the opportunity to gain insight into this complicated and dynamic domain. These professionals have to understand the organisational and environmental factors involved in a craft that is under constant pressure from the responsibility it carries for both the organisation and society. The research conducted has provided me with valuable learning experiences about this intriguing topic that is nested in the domain of Cyber Security.

The output from this thesis would not have been the same if it weren't for the people involved in this process. Therefore, I want to express my gratitude to all of them. For starters, I want to thank my supervisors from the university that have supported me throughout this research project. Wolter, I want to thank you for your time, patience and undivided attention that served my work with the feedback I needed. Maarten, I want to thank you for the philosophical and critical discussions which allowed me to reflect and improve my work. Michel, I want to thank you for your help in providing the tips and tricks needed for the correct structuring and writing of my thesis.

Secondly, I want to thank all my colleagues at Deloitte for their support and good times while working on this thesis. Specifically, I want to express my gratitude to Kirsten for her devotion, critical view and unconditional support throughout the different stages of this process. I'd like to thank all people involved from the Cyber graduate program for their time, insightful conversations and of course foosball games. Additionally, I want to thank the respondents, i.e. the cybersecurity professionals in question, who were involved and provided me with their time and knowledge. Without them, this research would not have been possible.

Finally, I want to thank my family and friends for their encouragements throughout this process. In particular I want to thank my girlfriend, Joëlle. Her patience, listening ears and motivational feedback have always provided me with the renewed energy to pursue my goals. Thank you.

Kay Hagenaars
Amersfoort, October 2019

Executive Summary

The current developments in the digitalised world see an increase in cybercrime which causes society to demand information security (IS). However, budget constraints and an increasingly tough economic climate forces organisations and governments to spend their financial resources most effectively to obtain their operational goals with minimum risk. Consequently, effective information security risk management (ISRM) is imperative to track and control the identified risks to informational assets. However, the fast evolution of the IS environment provides limited available information that can be used for IS risk assessments, creating incomplete knowledge of eventualities, dependencies and values about a system or phenomenon in the IS risk assessment. The limited available information consequently creates heavy reliance on the cybersecurity professional's interpretation and judgment of risks. However, little is known about the perceived uncertainty (the experienced inability to predict or identify something accurately from incomplete knowledge) and subsequent judgment operations of the cybersecurity professionals involved during IS risk assessments. Therefore this study set out to create an understanding for this gap in the current body of knowledge, guided by the following research question:

How do cybersecurity professionals deal with perceived uncertainty about their organisation's information security environment in a risk assessment?

To answer the research question, two guiding sub–questions are drafted to aid in answering the main research question:

SQ1: How do cybersecurity professionals perceive uncertainty about the organisation's information security environment in a risk assessment?

SQ2: How do cybersecurity professionals provide judgment under the perception of uncertainty about the organisation's information security environment?

The information security risk assessment domain

The ISRM practices allow risks that are associated with the organisation's IS environment to be identified and managed. The process of IS risk assessment plays a crucial role in the identification of these risks. This study adopts the ISO27005 IS risk assessment methodology, which forms the backdrop for examining the research questions.

This study conceptualises the IS environment based on the IS definition adopted from Cherdantseva and Hilton [14] who define it as: "the development and implementation of security mechanisms of all available types (technical, organisational, human–oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and consequently, information systems, where information is created, processed, stored, transmitted and destructed free from threats." This definition has three defining elements that allow the conceptualisation of the IS environment against the ISO27005 framework. These elements are: (1) the information and information systems of the organisation (within and outside its perimeters), which is referring to the assets of an organisation, (2) the threats that can harm the organisation's information and systems, referring to actors and factors that can have negative consequences to the organisational assets, and (3) the development and implementation of security mechanisms to keep information and information systems free from threats, referring to the controls available.These elements characterise the different steps of the ISO27005 methodology and subsequently aid in the interpretation of the IS environment. The combined set describes scenarios that allow the identification of risks. This conceptualisation is necessary to answer the research question with the theorised concepts. For further details, please refer to Chapters 2 and 3.

Conceptual framework

This research theorises two concepts that help interpret and explain the results to answer the research questions. The first concept is on perceived environmental uncertainty (PEU), which is used to analyse

the perceptual aspects of uncertainty (i.e., the experienced inability to estimate or identify something accurately from incomplete knowledge) with the cybersecurity professionals. The PEU theory knows three (3) types of uncertainty that can be perceived:

- **Effect uncertainty**: the perceived inability to predict the impact from possible events/changes in the IS environment for the organisation, relating to the nature, severity and timing of impact.
- **State uncertainty**: the perceived inability to make accurate probability estimates as well as the difficulties with grasping the interrelations between components and how they are changing within the IS environment.
- **Response uncertainty**: the perceived inability to predict the consequences from response options from strategies formulated for a threat in the IS environment.

The theory provides five factors that influence an individual's PEU, which are known as the sources of variability to the perceived uncertainty:

- The **complexity**: refers to the number of non-similar components and interrelations within an environment.
- The **dynamism**: refers to the changing factors and the emergence/disappearance of factors in the environment.
- The **individual cognitive characteristics**: refer to the ability to deal with ambiguity and uncertainty.
- The **availability of response options**: refers to the experience that one has in dealing with ambiguity and uncertainty.
- The **social expectations from the organisation**: the socialisation process of the organisation on the individual that influences how one deals with ambiguity and uncertainty.

The PEU theory helps to interpret and explain the perceived uncertainty about the IS environment which cybersecurity professionals might have. This theory provides the first pillar of the conceptual framework, allowing to delineate the factors that contribute to the perceived uncertainty and identifying the type of perceived uncertainty. This concept relates to SQ1.

The concept of judgment heuristics is used to understand the judgment operations from cybersecurity professionals when they perceive to be uncertain during the IS risk assessment. The conceptual framework theorises three (3) heuristics that are used to gain an understanding in the judgment operations:

- **Availability heuristic**: the judgment that is based on the cognitive ease by which instances of events comes to mind, allowing the judgment of plausibility and frequency.
- **Representativeness heuristic**: the judgment that is based on how representative/similar the subject under judgment is to a certain stereotype, allowing judgment of probabilities.
- **Selective accessibility model**: the judgment based on the hypothesised correctness and accuracy of information provided for the judgment problem.

The theorised concept is used as guidance for interpreting and explaining the judgment operations of cybersecurity professionals when under uncertainty during an IS risk assessment. This concept relates to SQ2.

The theorised concepts allow the examination against the backdrop of the IS risk assessment methodology from the ISO27005, for which a conceptualised description of the IS environment is provided above. This provides a research framework that consists out of seven (7) discrete steps (1.1 – 1.5 and 2.1 – 2.2) which consequently allows the comparison of respondent answers for different aspects of the IS risk assessment. The methodology is chosen due to its renowned status as an IS standard that encompasses all crucial aspects of an IS risk assessment.

Methodology

This research adopts an exploratory angle that aims at describing the 'how' of the research problem at a descriptive level. Consequently, an inductive research strategy is required to analyse the qualitative data from respondents with particular knowledge and skills (purposeful sample). In total, fifteen (15) semi–structured interviews were conducted with cybersecurity professionals that have a proven record of involvement with executing IS risk assessments on an organisational level.

The interviews are semi–structured by nature and guided by a rigorous interview script to complete all facets of the IS risk assessment as described by the ISO27005 methodology. The interview questions operationalise the concepts into relevant and identifiable questions that result in data suitable for analysis for the research questions.

All data were recorded and transcribed using an edited transcription method. The subsequent coding is guided by a coding scheme that allowed the researcher to identify elements from the theory in the data, thereby minimising the researcher bias in the coding process.

Results & Synthesis

The perception of uncertainty about the IS environment

The research results show two types of PEU are used to explain perceived uncertainty about the IS environment and their attributing factors:

State uncertainty

The type of state uncertainty is identified with the following IS risk assessment steps: (1.1) asset identification, (1.3) identification of existing controls, and (2.2) likelihood analysis.

The results show that the sources of variability that have a positive influence on the perception of state uncertainty in the identified steps are complexity and dynamism. The complexity dimension refers to the many non–similar components and number of interrelations between the organisation's general landscape of information and information systems. This complexity creates difficulties in assessing the interrelations within the organisation's IS environment. The dynamism dimension reflects on the changing nature of interrelations within the organisation's general landscape of information and information systems. This dynamism creates difficulties estimating changes/events in the organisation's IS landscape.

Effect uncertainty

The type of effect uncertainty is identified with the following IS risk assessment steps: (1.2) threat identification, (1.4) vulnerability identification, (1.5) CIA identification, and (2.1) business impact value analysis.

The results show that the sources of variability that have a positive influence on the perception of effect uncertainty are complexity and dynamism. The complexity reflects on the many interrelations and layers of the landscape of information and information systems in the organisation's IS environment. This complexity makes it difficult to assess how threats are relevant to the organisation, how information systems process information, and how the context needs to be incorporated to examine the impact. The dynamism dimension reflects on the changing and ever–evolving nature within the IS environment. Dynamism addresses the threat landscape that continuously evolves and incorporates new technologies, as well as the changing business contexts within the organisation. This dynamism creates difficulties in keeping track of all changes that can have an impact on the organisation.

The influence of the perceptual processes

The results show that the individual cognitive characteristics and the availability of response options are identified to have a negative influence on the perception of uncertainty about the IS environment. The respondents indicated not to perceive uncertainty based on their knowledge and experience on how to deal with ambiguity and uncertainty during the IS risk assessments. The social expectations were referenced by one respondent who referenced to a strong entrepreneurial spirit within the organisation. However, the influence on the perception of uncertainty could not be identified, resulting in undefined influence. The complexity and dynamism dimensions (i.e., the characteristics of the IS environment), as described above, have a positive on the perception of uncertainty. Please refer to Figure 1 for an overview of the conceptual model and associated findings for the PEU theory. Please note that

this conceptual model is from qualitative data from one sample of fifteen (15) respondents as part of exploratory research. Consequently, the model is a representation of the research findings without attributing quantitative meaning.

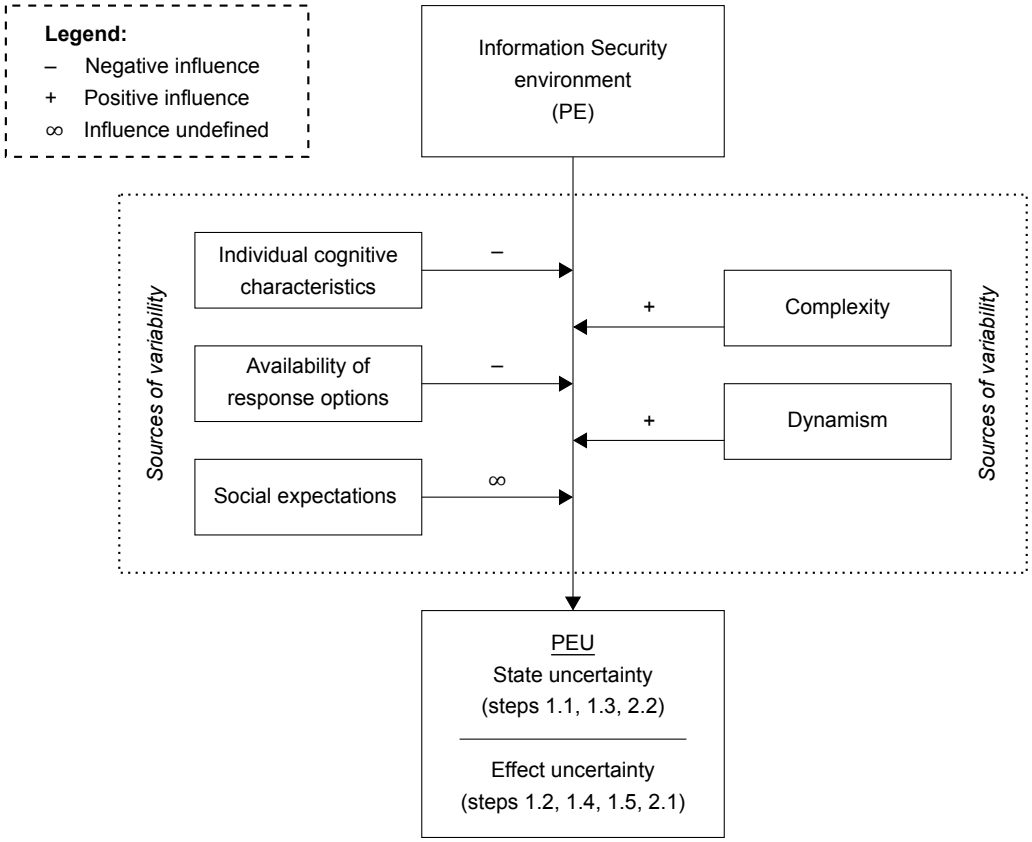


Figure 1: The conceptual model for the cybersecurity professional's perception of uncertainty about the IS environment in an IS risk assessment. Adapted from Downey et al. [20]

Relevant finding on the perception of uncertainty

Unfathomable uncertainty

Furthermore, a type of uncertainty that was not related to the theoretical concept of PEU was identified with the respondents in the vulnerability identification (step 1.4). Unfathomable uncertainty is has issues of integrality, where the identification of all vulnerabilities is unknown. Additionally, the identification of impact from all vulnerabilities is unknown. Thereby the perception of uncertainty is based on fundamental unknown–unknowns to the vulnerability identification process.

Identified factors for perception of uncertainty

The study has identified that shadow IT, the organisational structuring and innovation processes within the organisation are factors that contribute to the uncertainty perception of cybersecurity professionals in an IS risk assessment. They identify with both complexity and dynamism, the sources of variability that are identified to have a negative effect on the uncertainty perception of the cybersecurity professional.

Shadow IT refers to information and information systems that are in use in an organisation without the IS department knowing about it. The organisational structuring relates to the decentralised nature of the organisation. In this structuring, the IT and IS department is in a supporting role that could create a lack of overview and involvement with decentralised parts of the organisation. Furthermore, the innovation processes are identified as a factor for uncertainty. The innovation processes create complexity and dynamism within the organisation that contributes to the perceived uncertainty.

Judgment operations under uncertainty in the IS risk assessment

The theory on judgment heuristics is used to understand the judgment operations of the cybersecurity professional. The results show that the respondents referenced to all theorised heuristics in their answers:

Availability heuristic

The availability heuristic was referenced during the CIA identification (step 1.5) and the likelihood analysis (step 2.2). The results show that large events that are well imprinted in the mind are taken into account in providing estimates. Thereby allowing the ease by which something comes to mind to be incorporated in the IS risk assessment.

Representative heuristic

The representative heuristic is referenced during the CIA identification (step 1.5) and the likelihood analysis (2.2). The results show that scenarios and assets are actively compared to their similarities with stereotypical examples during the IS risk assessment, consequently allowing judgment.

Selective accessibility model

The selective accessibility model was referenced in four (4) out of the seven (7) steps from the IS risk assessment (step 1.1, 1.2, 2.1, 2.2). The results show that information that is provided, i.e. coming from third parties, is actively hypothesised as a suitable answer. Thereby assessing the correctness and accuracy applicable to their organisation's IS environment. The results also show that the respondents stayed close to the provided values during the IS risk assessment. Furthermore, the values from materialised incidents were used as a starting point to allow the respondents to provide value estimates.

Relevant findings for providing judgment

The judgment heuristics only explained parts of the answers provided by the respondents. Additional findings of the judgment operations could also be discovered. Often it was indicated by respondents that the final judgment call was not up to them, thereby not providing any insights into their judgment operations. However, these responses did show that the accountability structure within organisations is a way to deal with the perceived uncertainty. Furthermore, the respondents indicated to accept the uncertainty perceived and to rely on the security policy and philosophy. Thereby it was often referred that the paradigm shift from prevention to detection and response allowed them to deal with the uncertainty associated to the IS risk assessment steps. Finalising this subsection, it was also mentioned by respondents to incorporate the security awareness of the people involved that allowed them to provide judgment.

Conclusion

The objective of this research is to create an understanding in the perceptual aspect and judgment operations of cybersecurity professionals during an IS risk assessment. This objective is guided by the following research questions:

How do cybersecurity professionals deal with perceived uncertainty about their organisation's information security environment in a risk assessment?

SQ1: How do cybersecurity professionals perceive uncertainty about the organisation's information security environment in a risk assessment?

SQ2: How do cybersecurity professionals provide judgment under the perception of uncertainty about the organisation's information security environment?

The research questions are subsequently answered from the synthesised results. The study has shown that if uncertainty is perceived about the organisation's IS by cybersecurity professionals, both state and effect uncertainty could be identified in varying steps of the IS risk assessment. Factors that are attributed revolve around the complexity and dynamism, mostly introduced due to shadow IT, organisational structuring and innovation processes within the organisation. The results also show that

the respondents identify with judgment operations from the theory on judgment heuristics as a way to deal with the PEU. Thereby using the availability and representative heuristic, as well as the selective accessibility model in various steps of the IS risk assessments. Some of the respondents were hindered from elaborating on their judgment operations due to the accountability structure within the organisation, having business/risk owners make the final judgment call. Additionally, the cybersecurity professional deals with uncertainty due to the paradigm shift from prevention to detection and response. Finally, the cybersecurity professional also assesses the security awareness of the people involved to provide judgment.

Scientific, managerial and societal implications

This research contributes to the current body of knowledge by shedding the first light on the perceptual processes and judgment operations of cybersecurity professionals in an IS risk assessment. From a managerial perspective, organisations can use the results from this research to identify and treat potential factors that create difficulties in the estimates provided by their cybersecurity professionals. Additionally, the results suggest that a discussion on the ownership of risk and security in relation to the organisation's accountability structure needs to be sparked for the most effective protection of information, incorporating the views of specialists in the final judgment and decision–making. This discussion benefits the organisations from an economical perspective and adds value to society in the creation of a safer digital environment.

Contents

List of Figures

List of Tables

1 Introduction

The rapid expansion of electronic data processing and electronic business as well as the continuous growth of the Internet has transformed modern life [17, 35]. This rapid expansion provides opportunities and benefits to a globalised, interconnected and digital society. However, this digital freedom also offers criminals the opportunity to benefit from the wealth that data can provide nowadays by committing cybercrimes through networked technologies such as computers and the internet [35]. Cybercriminals have recognised the increased value of data because society manages many aspects on the Internet; criminals are consequently out to steal or compromise information to earn a payday [49]. This is supported by data that shows an increase in data breaches – "a compromise of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to protected data transmitted, stored or otherwise processed" [53] – that causes hundreds of millions of confidential or protected information records to be exposed. The United States alone experienced 1,244 million data breaches that resulted in the exposing of 446.52 million records in 2018 [66]. The protection of valuable information that is accessible through networked technologies consequently becomes a prevalent issue for all layers of the digital society [33].

Information–intensive organisations and governments are thus at risk due to the massive amounts of information they process, that is both of value to them as well as to cybercriminals. They thereby require informational assets to be protected from the adverse effects of cybercrime. This protection of information is often referred to as information security (IS). This research adopts the definition on information security from Cherdantseva and Hilton [14, p.37] who define it as: "the development and implementation of security mechanisms of all available types (technical, organisational, human–oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and consequently, information systems, where information is created, processed, stored, transmitted and destructed free from threats."

The current increase in cybercrime causes society to demand for IS. In combination with the increased dependency on networked technologies, many organisations and governments are pressured to invest in IS to protect their valuable information assets [70]. Drivers for investment are: regulatory obligations, experienced incidents and their consequences, organisational characteristics or reputation damages [16, 70]. However, budget constraints force organisations and governments to make though decisions on the IS expenditures [74] because the increasingly tough economic climate demands the financial resources to be spent most effectively to achieve operational goals with minimum risk [6]. Organisations and governments consequently need to identify and protect themselves from the risks imposed from the adversarial threats. They are thereby tracking and controlling the identified risks by deploying cost–effective information security risk management (ISRM) practices.

Crucial to ISRM is the risk assessment process, which aims at identifying, analysing and evaluating risks about the IS environment of an organisation. Different approaches and scales exist in executing IS risk assessments, and each of them has its advantages. However, indifferent of the approach and scale used, they all rely on input in the form of judgment from the risk assessor [56]. The need for this judgment in IS risk assessments is caused by the variability of future events, the incomplete knowledge about the IS environment, undiscovered vulnerabilities and unrecognised dependencies that could lead to unforeseen impact [56].

Consequently, IS risk assessments depend on the predictions/identifications from the risk assessor's judgment [61]. What is critical to this dependency is that the risk assessor might experience the inability to accurately predict/identify these values. This inability is defined as perceived uncertainty. However, the IS risk assessments still rely on this input, even though the risk assessor could perceive to be uncertain about its predictions/identifications. Therefore it is essential to understand how uncertainty about the IS environment is perceived and how subsequent judgment is provided during this perceived uncertainty.

This chapter further describes the research problem (Section 1.1), the research questions (Section 1.2), the relevance of this research (Section 1.3) and finally the thesis outline (Section 1.4).

1.1. Research problem

This research focuses on the IS risk assessment process, the risk assessor of interest in this research is the cybersecurity professional that executes the IS risk assessment. From this point on, the risk assessor is referred to as the cybersecurity professional.

Evident from the introduction is the increase in cybercrime and that society is feeling the ramifications. Consequently, IS is demanded that should prevent the negative consequences from the ever–increasingly digitalised world. The general perception is that organisations and governments are expected to protect society from risks associated with the possession and usage of information on individuals. This perception is underscored by the adoption of the European General Data Protection Rules (GDPR) in April of 2016 [22]. Additionally, it is in the organisations' and goverments' interest that intellectual property and other sensitive information is protected from the adverse effects of cybercriminals. Consequently, ISRM must be executed to deal with the risks associated with the protection of these informational assets.

What is however seen as a significant issue for the execution of effective ISRM is the fast evolution of the IS environment. This fast evolution creates limited available statistical information that can be used as objective data in IS risk assessments [8, 15, 60], and forces the use of judgment from cybersecurity professionals. Although the use of judgment is considered to be an integral and crucial part to IS risk assessments [54, 56], it underpins the lack of objective and accurate data that creates a dependency on the accurate predictions/identifications of cybersecurity professionals.

This dependency on the judgment from cybersecurity professionals is considered a limitation because it implies that the accuracy of estimates for IS risk assessments depends on the cybersecurity professional's beliefs, preferences and ability to process information [47, 61]. It can thus be argued that the perception of uncertainty about the IS environment will influence the cybersecurity professional's judgment. It is consequently pivotal to understand how cybersecurity professionals perceive uncertainty, allowing insight into the factors for their experiences and how this influences their perceptions.

Research into behavioural psychology shows that judgment can be guided by heuristics when experiencing uncertainty. The heuristic principle simplifies complex judgment operations, allowing the assessment of eventualities and the prediction of values. These heuristics can introduce biases in judgment because not all influencing factors from the original complex question are taken into consideration [69]. The judgment processes based on heuristics can subsequently cause suboptimal outcomes in IS risk assessments. Mersinas et al. [47] suggest that the ability of cybersecurity professionals to assess risks is more accurate than that of laypeople. However, this is only under the condition of perfect information.

When synthesising the observations from the above paragraphs, it is evident that the protection of information assets depends on the ability of cybersecurity professionals to provide accurate judgment. Consequently understanding the cybersecurity professional's perception of uncertainty about the IS environment, as well as the subsequent judgement operations provides new insights into the IS risk assessment process. This understanding allows scrutiny of the IS risk assessment processes, focussing on how cybersecurity professionals deal with perceived uncertainty about the IS environment.

1.1.1. Knowledge gap

The dependency on the judgment from cybersecurity professionals is a debated topic in the field of IS risk assessments, and several approaches to deal with this are discussed in the literature. Allodi and Massacci [1] provide a methodology on how the available statistical information from an organisation's Security Operation Center (SOC) can be leveraged to provide estimates in risk assessments, by–

passing judgment as much as possible. Feng and Li [23] have created a model that uses evidence theory to assess the validity of estimates provided through expert judgment, aiming at more accurate estimates for IS risk assessments. Also, Ryan et al. [60] demonstrated an approach to how expert judgment elicitation can be used in IS risk assessments.

Critical to the above depicted studies is that their focus is on dealing with the variability of future events and the incomplete knowledge about the IS environment in relation to the vulnerabilities and dependencies. However, they do not focus on the perception of uncertainty that cybersecurity professionals have when providing judgment about the IS environment. This perceptional aspect of uncertainty is crucial to the estimates provided from judgment because this will impact how the available information is supplemented with the cybersecurity professional's judgment.

The findings from Mersinas et al. [47] suggests that cybersecurity professionals are also prone to heuristics and biases in IS risk assessments. These findings are confirmed by other studies [7, 62]. The IS field is also steadily using theory on behavioural decision–making and judgment operations in other contexts, such as research in behavioural responses of users to security scenarios [58], in understanding risk perceptions on IS [72], as well as in leveraging system design with knowledge on user behaviour [25]. However, most of the research on decision–making concerns technical approaches to improve IS, which is underpinned by Pfleeger and Caputo [57] who actively promote research into heuristics and biases in the field of IS because this incorporates human behaviour into the cybersecurity technology and processes.

Based on the research problem in Section 1.1 and the short examination of the current body of knowledge on the topics, two research gaps are identified:

- The current research in the field of IS has mainly focussed on technical solutions that provide approaches to use judgment from cybersecurity professionals in IS risk assessments. However, the cybersecurity professional's perception of uncertainty about the IS environment prior to providing judgment is currently absent from the literature.
- The current literature suggests that cybersecurity professionals are also prone to heuristics and biases in assessing risks. Several studies have identified different heuristics and biases in user behaviour and risk perception. There is however no knowledge on the heuristics and biases in the IS risk assessment processes which focus on how cybersecurity professionals provide their judgment.

The two identified research gaps provide the opportunity to firstly understand the cybersecurity professional's perception of uncertainty about the IS environment in a risk assessment. Secondly, analysing how cybersecurity professionals provide judgment under their perceived uncertainty about the IS environment provides insight into the judgment operations during the IS risk assessments.

1.1.2. Research objective and deliverable

The research objective is to create an understanding into the way cybersecurity professionals deal with perceived uncertainty about the IS environment in a risk assessment. This understanding creates insight into the perceptual aspects and judgment operations that cybersecurity professionals go through in an IS risk assessment.

The deliverable of this research is a Master's Thesis as partial fulfilment of the requirements for the degree in Master of Science in Management of Technology from Delft University of Technology. The research is executed at an external party, Deloitte Risk Advisory B.V., which is located in Amsterdam, The Netherlands. The knowledge gained from this research project in the documented form of a Master's Thesis constitutes as the deliverable to Deloitte.

1.2. Research questions

This research project is exploratory because it aims at describing associations between different concepts that have not been researched before in this particular IS risk assessment context. The research intends to describe how cybersecurity professionals deal with perceived uncertainty about the IS environment in an IS risk assessment. The findings are presented at a descriptive level, understanding how uncertainty about the IS environment is perceived by the cybersecurity professional, as well as understanding how subsequent judgment is provided under this perception of uncertainty. Based on the problem statement from Section 1.1, the following research question is formulated:

Research question:
How do cybersecurity professionals deal with perceived uncertainty about their organisation's information security environment in a risk assessment?

The exploratory nature of this research project consequently demands a qualitative approach. The aim is to describe the 'how' in relation to the perception of uncertainty and the judgment operations. This research will start with a dissection of the research domain, the IS risk assessment; analysing the different aspects of the IS risk assessment process, conceptualising the IS environment and defining the interpretation of risk and their associated variables.

This approach is continued with a literature review that dives deeper into the theoretical concepts. The first theory that is explored is on perceived environmental uncertainty (PEU) from Gerloff et al. [26] and Milliken [50]. The theory on PEU is an organisational theory that identifies different types of uncertainty that one can experience about the environment, as well as sources of variability (i.e. the factors) to perceive this uncertainty. The theory on PEU is consequently used to interpret and explain the cybersecurity professional's perception of uncertainty about the IS environment. The interpretation is executed by analysing the data for identifiers that relate to the theory, allowing to understand the underlying structures of the different perceptual aspects of uncertainty.

The second theoretical concept that is explored is the theory on judgment heuristics from Mussweiler and Strack [52], Strack and Mussweiler [67] and Tversky and Kahneman [69]. This theory focuses on behavioural psychology, in particular judgment and decision–making. The theory is therefore used to interpret and explain the judgment operations from cybersecurity professionals who perceive uncertainty about the IS environment during a risk assessment.

Both theoretical concepts are elaborated upon and conceptualised into a conceptual framework that supports this research. Thereby the theories help explain and interpret the observations from cybersecurity professionals during IS risk assessment. This conceptual framework consequently guides the fundamental topics of interest to this research. Please refer to Chapter 3 for the conceptual framework. Based on the concepts that are used to study the main research questions, two sub–questions are devised:

SQ1: How do cybersecurity professionals perceive uncertainty about the organisation's information security environment in a risk assessment?

SQ2: How do cybersecurity professionals provide judgment under the perception of uncertainty about the organisation's information security environment?

The research questions are answered from qualitative empirical data that is collected through semi–structured interviews. Please refer to Chapter 4 for the complete methodological approach of this study.

Evident from Section 1.1 is that current research suggests that cybersecurity professionals are just as prone to heuristics and biases as laypeople, which could create suboptimal outcomes. By identifying if cybersecurity professionals perceive to be uncertain and consequently reference to employing heuristics in their judgment during IS risk assessments, possible biases can be combated to allow the most accurate estimates from judgment.

1.3. Relevance of the research

This section describes the scientific and societal relevance of this research, as well as the relationship with the Master of Science program.

1.3.1. Scientific relevance

This research will contribute to the current body of knowledge by providing insight into how cybersecurity professionals perceive uncertainty about the IS environment in a risk assessment. Additionally, this research aims at understanding how cybersecurity professionals subsequently deal with perceived uncertainty about the IS environment. These key variables are currently missing in the body of knowledge. Understanding these interacting variables creates insight into how the cybersecurity profes-

sional's judgment in an IS risk assessments comes about and will be a valuable feature in assessing the outcomes from assessments. Furthermore, it allows the previously mentioned technological solutions that develop methods to use judgment from cybersecurity professionals to reassess their models to improve accuracy.

1.3.2. Societal relevance

The discussion about underinvestment in IS is present for a while now with several suggestions to combat it [32, 59]. However, still extreme volumes of data breaches occur [66]. The relevance of accurate risk assessments to support IS decision–making is the foundation to combat the adverse consequences from cybercrime for society. Understanding how cybersecurity professionals deal with uncertainty in their judgment for IS risk assessments provides the opportunity to accurately interpret and use the predictions/identifications provided from a IS risk assessment. This IS risk assessment is the first step to ISRM, which if executed effectively, creates the most secure digital environment for organisations and government from which consequently all layers of the digital society will benefit.

1.4. Thesis outline

The section describes the outline of this thesis report. Chapter 2 describes the research domain for this thesis, which revolves around the IS risk assessment process. In Chapter 3, the theorised concepts are depicted, which amounts to a conceptual framework that is used to help interpret and explain the empirical findings. The methodology for this research is delineated in Chapter 4, elaborating on the research design, how the concepts are operationalised, the method for data collection and finally how the identification of theories is executed in the data analysis phase. The results of this research are depicted in Chapter 5, and the reader is provided with synthesised data that scrutinises the research problem in by synthesising the results in Chapter 6. The analysed results culminate in a conclusion in Chapter 7, answering the research questions and delineating a path of future research on this topic.

2

The Information Security Risk Assessment Domain

This chapter presents the domain of this research, the information security risk assessment domain in which the cybersecurity professional is required to provide judgment. Section 2.1 provides insight into the practices of information security risk management in order to keep an organisation's information protected. The research domain is further analysed in Section 2.2, which allows the conceptualisation of the information security environment in Section 2.3. The philosophy and associated premises about risk and the chosen methodology are delineated in Section 2.4. The chapter is finalised with a conclusion Section 2.5.

2.1. Information security risk management

To provide information security (IS), it is important to identify and manage the exposed risks of an organisation. This is commonly done using information security risk management (ISRM) practices, where risk management aims at the "coordinated activities to direct and control an organisation with regard to risk" [55]. Thereby the organisational needs regarding IS should align with the organisation's environment and enterprise risk management. The ISRM process should establish the external and internal context, and subsequently assess and treat the risk to an acceptable level [54]. ISACA [36, p. 85] defines ISRM as: "the process of identifying vulnerabilities and threats to the information resources used by an organisation in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level based on the value of the information resource to the organisation."

Two items of the above provided descriptions from ISACA [36] and the NEN [54] are highlighted. First, risk management is defined as a process; thereby it is ongoing and iterative in nature, which is due to the changes in the organisation's environment in which new threats and vulnerabilities can emerge every day from different sources within the environment. Second, the use of countermeasures/ treatment (often defined as controls) to manage risks are related to the value the information has to the organisation. Thereby a balance between productivity, effectiveness and costs is necessary for the information to be protected, i.e. the risk needs to be reduced to an acceptable level (value).

2.2. Information security risk assessment — ISO27005

Critical to the ISRM process is the IS risk assessment, the domain in which this research is conducted. Many different approaches and methodologies exist that support organisations in the execution of ISRM and their associated IS risk assessments. This study however confines itself to only one methodology that serves as the backdrop of this research domain. This approach allows the collection of comparable data because of the structured approach and accepted interpretation of nomenclature with this methodology. This restriction provides structure to the research and supports constructively answering the research questions.

The IS risk assessment methodology from the NEN [54], the ISO27005:2018 – Information security risk management, is chosen as backdrop for a variety of reasons: (1) the standard is often regarded as the industry's best practice, (2) the methodology is assessed to be the most complete and mature, (3) it is the only methodology that identifies business processes to be an informational asset to the organisation, and (4) it contains a description on how to conduct subjective knowledge–based probability and impact estimations [73]. Supported by this reasoning, this research benefits from adopting this methodology due to the widespread applicability and acceptance within the industry. Additionally, it supports business processes that span across an organisation's environment, which are considered relevant to this research. Please refer to the Figure 2.1 for an overview of the ISRM process as prescribed by the ISO27005 from the NEN [54].

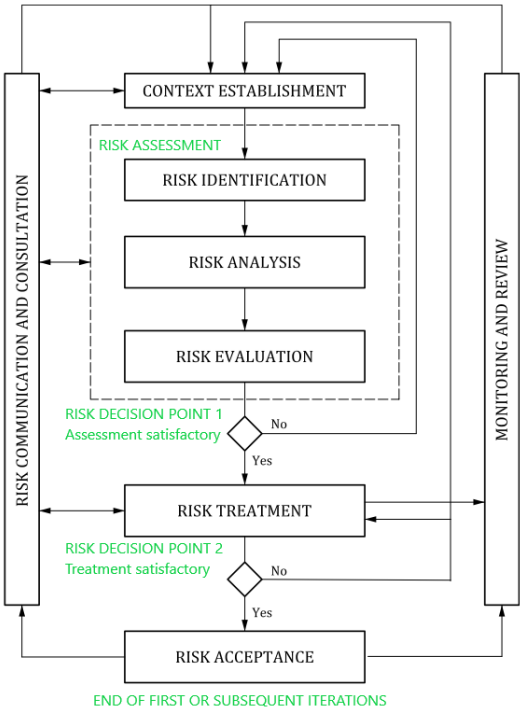


Figure 2.1: ISRM, adopted from NEN-ISO/IEC 27005:18 [54, p. 4]

2.2.1. The information security risk assessment subprocesses

In Figure 2.1, the IS risk assessment is indicated green with a dashed box surrounding three different subprocesses delineated by the methodology. The first subprocess in the IS risk assessment is the risk identification which aims at determining what could inflict potential loss and allows insight into how, why and where this loss can happen. The second subprocess is the risk analysis in which the input from the risk identification subprocess the construction of a scenario. For these scenarios, the impact of consequences and the likelihood of these consequences occurring are expressed. This expression of values for scenarios can be done using qualitative attributes that describe the magnitude, or using quantitative numerical scales. The final subprocess to the IS risk assessment is the risk evaluation. In this step, the outcomes from subprocess #2 (risk analysis) are evaluated against the acceptable values determined by the organisation. These "acceptable values" are determined in the context establishment process, which is a process prior to the risk assessment. In the context establishment process, criteria for the organisation's IS are defined such as the maximum risk that an organisation is willing to take or the maximum risk on a particular asset, i.e. the organisation's risk appetite. This context establishing process allows prioritising and effective decision–making during the risk evaluation subprocess, which consequently influences the risk treatment process that succeeds in the IS risk assessment process [54].

Each of the subprocesses knows several steps that further delineate the actions necessary from the cybersecurity professional to execute the IS risk assessment according to the ISO27005 norm. Please

refer to Table 2.1 for an overview of the different steps associated with the subprocesses. Please note that in the second column, “Step & Description”, the name of the steps are indicated in italic.

Table 2.1: IS risk assessment subprocesses and associated steps, adopted from NEN-ISO/IEC 27005:18 [54]

Subprocess	Steps & Description
1. Risk identification	1. The *identification of assets* allows an organisation to map anything that has value to an organisation, thus requiring protection. This mapping includes the information itself, but also the information systems that are used within the organisation. 2. Through *threat identification* all the possibilities of harm doing to assets are identified. This identification includes all threats, accidental and adversarial, within an organisation’s IS environment that can lead to a data breach. 3. The *identification of existing controls* maps their current working state in relation to the assets they need to protect from threats. Also, it avoids unnecessary work or costs when controls are duplicated. 4. The *identification of vulnerabilities* is necessary to determine if and how threats can exploit them which causes harm to the organisation’s assets. These can be identified from different areas, such as the organisation itself, processes and procedures, routines, personal, the physical environment, software and hardware of information sytems, IT configuration as well as dependencies on external parties. 5. By *identifying the CIA values* an information classification is assigned for the confidentiality, integrity or availability of the identified assets, determining the information value for these. This classification is often done using incident scenarios which describe how a threat exploits a vulnerability in an IS incident which results in harm to the asset. Such scenarios can result in a data breach where the confidentiality or integrity of an asset is compromised. Alternatively, it can result in a malicious attack that prevents services or assets from being available.
2. Risk analysis	1. By *assessing of consequences*, the business impact value can be expressed, e.g. financial losses and/or reputational damages. Important to this step is the valuation of assets that will determine the business impact value. 2. The *assessment of the likelihood* is necessary to determine the probability for the occurrence of a scenario incident which materialises in harm to the organisation. 3. Combining the assigned values for the likelihood of consequences occurring and the business impact value (the actual consequences to the organisation), the *level of risk is determined*.
3. Risk evaluation	The risk analysis outcome is evaluated against the accepted values determined in the context establishment process. Thereby providing input to the risk treatment process that is next in the ISRM process.

2.3. The information security environment

The organisation’s IS environment is mentioned a few times at this point and is a topic that needs clarification because it is a crucial element to this research. Therefore this section provides a conceptualisation of the IS environment based on the adopted definition on IS in relation to the chosen IS risk assessment methodology. First the definition of IS is dissected, which is subsequently synthesised with the IS risk assessment methodology.

This research adopts the definition on IS from Cherdantseva and Hilton [14] who define it as: “the development and implementation of security mechanisms of all available types (technical, organisational, human–oriented and legal) in order to keep information in all its locations (within and outside

the organisation's perimeter) and consequently, information systems, where information is created, processed, stored, transmitted and destructed free from threats." This definition has three defining elements that are itemised and analysed below in relation to the different steps of the IS risk assessment subprocesses from Table 2.1. The different elements from the definition are presented in italic:

1. The *information* and *information systems* of the *organisation (within and outside its perimeters)*. This element refers to the assets of an organisation in which information is created, processed, stored, transmitted and destructed. This element explicitly refers to an organisation's assets in the form of information and information systems/IT (as supporting assets) that are of value, and is thereby directly associated the first step in the IS asset identification. Also, this element is associated with the identification of CIA values, reflecting on the value of the information and information systems (assets) concerning the confidentiality, integrity and availability.
2. The *threats* that can harm the organisation's information and information systems. The element of threats explicitly refers to actors and factors that can have negative consequences on the organisational assets, relating to the step for the *identification of threats*.
3. The *development and implementation of security mechanisms* to keep the information and information systems free from threats. This element relates to the fourth and fifth step, the *identification of existing controls* and the *identification of vulnerabilities*, aiming at the implementation and development of security mechanisms of the organisation.

As can be seen above, all elements individually link to one or multiple steps of the risk identification subprocess. The combined elements allow the cybersecurity professional to determine the risk level in the risk analysis subprocess of the IS risk assessment as depicted by the ISO27005. This is done because the risk identification subprocess provides input on all elements to be synthesised in a scenario that allows the cybersecurity professional first to determine the business impact value to the organisation. Secondly, synthesis of all elements allows the cybersecurity professional to determine the probability that such an impact will happen, i.e. the likelihood of the impact as depicted by the scenario materialising. The combined values of step #1 and #2 of the provide input for step #3 of the risk analysis subprocess. Together with the risk evaluation, step #3 of the risk analysis can not be conceptualised as part of the IS environment because it uses input values to come to a risk level which is subsequently evaluated with the risk appetite.

Please refer to Table 2.2 for an overview of the selected risk assessment steps and their associated elements of the IS definition that provides this research with the conceptualisation of the IS environment.

Table 2.2: The risk assessment steps conceptualised for this research to identify PEU for the IS environment

Subprocess & Steps	**Relation with elements from the IS environment (element#)**
Risk identification	
1. Asset identification	The information and information systems of the organisation (withing and outside its perimeters). (#1)
2. Threat identification	The threats that can harm the organisation's information and information systems. (#2)
3. Identification of existing controls	The development and implementation of security mechanisms to keep the information and information systems free from threats. (#3)
4. Identification of vulnerabilities	The development and implementation of security mechanisms to keep the information and information systems free from threats. (#3)
5. Identification of consequences for CIA	The information and information systems of the organisation (withing and outside its perimeters). Reflecting the value of information in relation to the CIA. (#1)

Table 2.2: The risk assessment steps conceptualised for this research to identify PEU for the IS environment

Subprocess & Steps	Relation with elements from the IS environment (element#)
Risk analysis	
1. Analysis of consequences for business impact value	The synthesis of all elements provides a scenario that allows the cybersecurity professional to determine the business impact value. (#1-3)
2. Analysis of likelihood scenario materialising	The synthesis of all elements provides a scenario that allows the cybersecurity professional to assess the probability, i.e. the likelihood, of the impact to the organisation materialising. (#1-3)

2.4. How are risk and its variables to be interpreted

This research focuses on how cybersecurity professionals deal with perceived uncertainty about the IS environment in risk assessments. Consequently, it is important how risk and the associated variables are to be interpreted to understand the outcomes of the IS risk assessments in relation to the perceptual aspects and judgment operations.

The concept of risk is tricky because there exist many diverging conceptions. In the field of risk assessments, there is no consensus on fundamental concepts, making the perspective on definitions leading for the interpretation of outcomes from risk assessments [3, 4]. The interpretation of risk is thus determined by the risk assessment methodology [4]. Indifferent of the many existing conceptions of risk, this research conceptualises risk in accordance with the chosen risk assessment methodology from the NEN [54, p. 8], who describe risk as: *"a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event"*. From this definition Equation (2.1) can be derived from which the risk level is determined, as could be seen from Section 2.2.

$$risk = consequences \times likelihood \tag{2.1}$$

It is consequently important to specify the interpretation of the risk variables and the risk outcome. According to Aven [4], Equation (2.1) is characterised by consequences and uncertainties. The dimension of consequences relates to something that impacts something that is of value, i.e. informational assets of an organisation. The uncertainty dimension is depending on the knowledge of/available to a cybersecurity professional. This determines the interpretation of the risk equation's outcome as the expected value from consequences which are uncertain [4]. The consequences and uncertainties in this interpretation of risk are thus based on the knowledge of/available to the cybersecurity professional.

It is vital to make a clear distinction between objective uncertainty that is present in IS risk assessments, and uncertainty that can be perceived by cybersecurity professionals. Objective uncertainty that is inherently present in IS risk assessments is caused due to the variability in future events, as well as the incomplete knowledge about the IS environment in relation to the undiscovered vulnerabilities and unrecognised dependencies that could lead to unforeseen impact NEN [54], NIST [56]. In accordance with the characterisation from the definition of risk, the inherent objective uncertainty in IS risk assessments is consequently defined as the incomplete knowledge of eventualities, dependencies and values of a system or phenomena. This objective uncertainty is subsequently subject to the interpretation and ability to process information of the cybersecurity professional during its judgment operations.

The definition of risk, as described by the NEN [54], uses the expected value from materialised consequences as its outcome and subsequently allows risk indexation for decision–making [4]. This interpretation in quantitative approaches is subject to criticism because the relevance and usefulness are based on historical information and causal models. However, as indicated in Section 1.1, the fast changes in the IS environment creates limited available statistical information that can be used as input for the IS risk assessments. The qualitative approaches are argued to benefit from the identified risk interpretation because it allows a complete picture on risk situations concerning complexity, uncertainty and ambiguousness. This qualitative approach creates scenarios that rely on the expected value from

materialised consequences and thereby allows uncertainty characterisation and judgment processes to create more meaningful risk estimates [5].

2.4.1. Synthesising the risk concept in relation to the research domain's information security risk assessment methodology

What can be observed from the risk assessment processes as described by the ISO27005, is the relation to the definition and subsequent interpretation on risk throughout the assessment process. As prescribed by Aven and Renn [5], the ISO27005 methodology adopts a scenario–based approach that allows the incorporation of uncertainty and judgment processes into the risk assessment. In subprocesses #1 (risk identification) and #2 (risk analysis), there is a clear relation between the variables $consequences$ and $likelihood$ of Equation (2.1). The focus of these subprocesses is on the mapping of consequences and assigning likelihood values to events materialising, thereby determining the risk level associated with the scenario. The interpretation of the risk level outcomes is again in line with Aven [4], drawing conclusions on the expected value from materialised scenarios.

Distinct from this synthesis on risk is the presence of incomplete knowledge of eventualities, dependencies and values on a system or phenomenon (uncertainty) throughout the IS risk assessment process. Due to criticism towards quantitative risk assessments with a risk interpretation as defined by the NEN [54], the focus of this research domain will consequently shift to qualitative IS risk assessments based on the ISO27005. This allows a complete picture to risk situations with regard to how cybersecurity professional perceive uncertainty and consequently provide judgment.

2.5. Conclusion to the research domain

In order to keep an organisation's informational assets protected from harm, ISRM practices are necessary to identify and manage the risks to the organisation. This study focuses on the IS risk assessment as the research domain to provide answers to how cybersecurity professionals deal with perceived uncertainty about the organisation's IS environment. The ISO27005 IS risk assessment methodology is used as the backdrop against which the organisation's IS environment is conceptualised. This backdrop provides the opportunity to research the different aspects of the IS risk assessment process with theoretical concepts (described in Chapter 3) to create an understanding into the research problem; creating an understanding how uncertainty about the IS environment is perceived and subsequently judged (i.e. dealt with). The focus is on qualitative and semi–quantitative IS risk assessment approaches which allow the inclusion of uncertainty and judgment processes, providing the desired angle for this research question.

3

Conceptual Framework

This chapter presents the conceptual framework for this thesis that is applied to the research domain as depicted in Chapter 2. Different theories that relate to the research questions will be dissected and synthesised. Before diving into the theoretical concepts, the interpretation of uncertainty for this research is defined in Section 3.1. In Section 3.2 theory on the perception of uncertainty about an organisation's information security (IS) environment is dissected. Thereby depicting the theoretical guidance for answering sub–question 1. In Section 3.3 theory on providing judgment under perceived uncertainty is synthesised, aiding in answering sub–question 2. Finally, in Section 3.4 the research domain and the theoretical concepts are synthesised from which the conceptual framework is constructed that supports this research.

3.1. Uncertainty defined for this research

Before conceptualising the theories used for this research, the distinction between inherent objective uncertainty in IS risk assessments (as depicted in Section 2.4) and the perceived uncertainty of cybersecurity professionals is further delineated. Thereby allowing the reasoning behind the outset of this study is explained.

The concept of uncertainty has a rich history in which different branches, interpretations and conceptualisations exist. Extensive research started in the 17^{th} century, but to date depending on the field of science, still many taxonomies have different definitions for the same word [45, 68]. These conceptualisations are focused on the objective form of uncertainty, which could be present indifferent of the application in which the concept is used.

This research domain focuses on IS risk assessments where according to the chosen methodology, the concept of objective uncertainty (incomplete knowledge of eventualities, dependencies and values of a system or phenomena) is inherently present and is caused due to the variability in future events, as well as the incomplete knowledge about the IS environment in relation to the undiscovered vulnerabilities and unrecognised dependencies that could lead to unforeseen impact (see Section 2.4) [54, 56]. Although philosophical consensus on the objective uncertainty concept is hard to find, this research aligns with the applied setting, the IS risk assessment methodology as described by the NEN [54].

What is however critical to understand, is that the objective uncertainty concept as depicted above reflects on the inherent uncertainty present in IS risk assessments. It does not reflect on how this uncertainty is perceived by cybersecurity professionals from which they have to provide judgment. Thereby stipulating that the objective uncertainty present in IS risk assessments are an essential part for the outset to research how cybersecurity professionals perceive uncertainty. This perception of uncertainty in IS risk assessments is further conceptualised in Subsection 3.2.1 and forms the starting point of this conceptual framework in relation to the research questions.

3.2. Perceived environmental uncertainty

The theory on Perceived Environmental Uncertainty (PEU) is used to theorise the perception of uncertainty about an organisation's environment, more specifically, the organisation's IS environment over

which the cybersecurity professional can experience uncertainty. The theorised concept of PEU will thus play a central role in this research and is directly related to sub–question 1.

3.2.1. Perceived uncertainty

To understand how cybersecurity professionals experience uncertainty, the PEU theory is used to define perceived uncertainty. According to this theory, the perception (the experience) of uncertainty is determined by the individual. The perceived uncertainty explains how the relationship between the organisation and its organisational environment is perceived, which is known as PEU and can be experienced when environmental variables of the organisation's environment are synthesised [50].

Perceived uncertainty is consequently defined as: the individual's experienced inability to predict or identify something accurately because it perceives to be lacking information/knowledge to make accurate predictions, or because the individual feels unable to discriminate among informational sources [27, 50]. What is key to note from this definition, is the internalisation of the uncertainty concept that is based on incomplete knowledge/information as is defined in Section 3.1. It is consequently vital to understand the distinction between these types of uncertainty and that reference is made to either of these two forms explicitly by name (uncertainty or perceived uncertainty). Other conceptualisations of uncertainty that are available in the literature within different research domains on uncertainty are not part of this research's scope.

3.2.2. The perceived environment

The theory on PEU defines a perceived environment (PE) about which uncertainty can be experienced. First, the theory's definition of the PE and the relationship with the organisation's IS environment will be identified, after which the associated factors in the PE are described.

3.2.2.1. Linking the research domain to the perceived environment

The definition of environmental uncertainty suggests that the source of uncertainty resides in the organisation's external environment, i.e. outside the organisation its perimeters. However, this interpretation is often considered too broad [21, 48]. Milliken [50] argues that specifying the source over which uncertainty is experienced constitutes the environment. In the case of IS risk assessments, this amounts to the organisation's IS environment as the PE about which cybersecurity professionals can experience uncertainty.

The PE of the cybersecurity professional in IS risk assessments, the organisation's IS environment, is conceptualised based on the definition from Cherdantseva and Hilton [14] in Section 2.3. Consequently, the organisation's IS environment is conceptualised as: the environment of the organisation where information and information systems (within and outside the organisation's perimeters) are kept free from threats by developing and implementing security mechanisms. This conceptualisation allows the PEU theory to be used to gain an understanding of how cybersecurity professionals experience uncertainty in IS risk assessments.

3.2.2.2. Sources of variability in the perceived environment

There are different factors, or sources of variability, that are ascribed to perceived uncertainty about PE, relating to factors of the environment and to the individual who synthesises the variables in the environment.

Duncan [21] argues that the PE has two dimensions: complexity (C) and dynamism (D). The complexity dimension of the environment describes the similarities within it, i.e. the more components that are present, the more complex the environment can be perceived. The dynamism dimension refers to the changing nature of the environment, i.e. the perceived degree of change of environmental factors as well as the emergence of new environmental factors. Duncan [21] consequently argues that this will affect the perception of environmental uncertainty. Additionally, Duncan [21] and Lindsay and Rue [43] argue that the variance in PEU is determined more heavily by dynamism than complexity. The effects of dynamism and complexity can be illustrated as in the graph of Figure 3.1

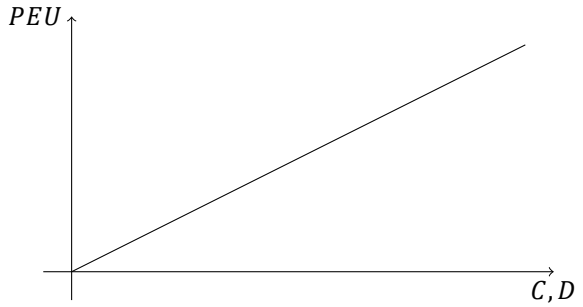


Figure 3.1: The effects of PE characteristics (C, D) on PEU [21]

The argument of Duncan [21] that the perceived uncertainty about the environment is determined by the PE's characteristics of dynamism and complexity is debated. Downey et al. [20] argues that PEU is not the direct effect of dynamism and complexity alone. Although the dimensions of the PE provide primary input, Downey et al. [20] illustrates that the mapping process — the reiterative process of sense–making about the environment (i.e. the synthesising of the PE's variables) — is determined by more than just the PE's characteristics.

Downey et al. [20] argues that the perceptual processes of the individual are more of a determinant factor of perceived uncertainty about the environment. The perceptual processes are depending on the individual cognitive characteristics, the behavioural response options available and the social expectations. The individual cognitive characteristics focus at how the individual deals with ambiguity, which subsequently determines how uncertainty is perceived. The behavioural response options refer to the variety of experiences available to the individual, which is argued to have an effect on the perceived uncertainty. The social expectations denote that the socialisation process of an organisation's influence on an individual's response to uncertainty [20].

3.2.3. The research model for perceived environmental uncertainty

By combining the sources of variability from Subsection 3.2.2, the perceived uncertainty from Subsection 3.2.1 about the IS environment can be synthesised into a research model. Please refer to Figure 3.2.

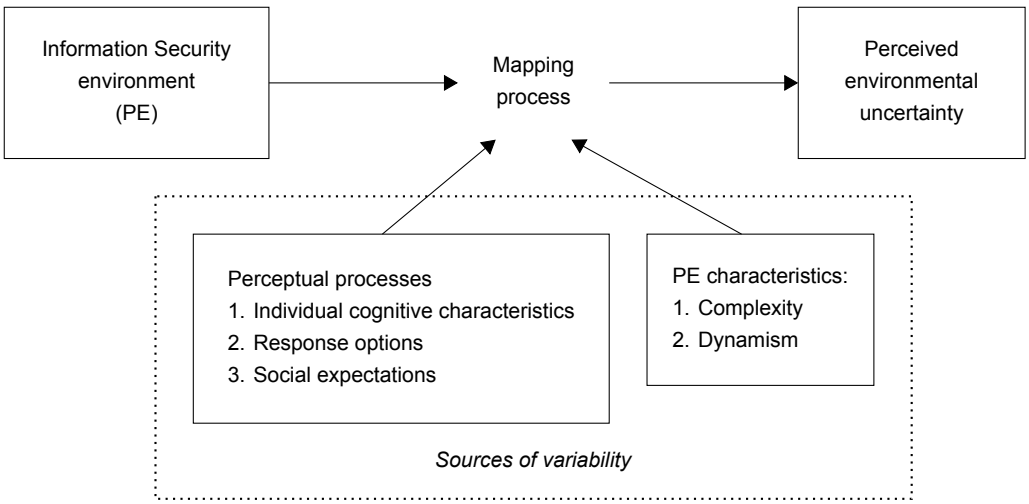


Figure 3.2: The research model for the identification of PEU, adapted from Downey et al. [20]

The research model, as depicted in Figure 3.2, shows that the mapping process results in PEU. However, what is not clear from the model of Downey et al. [20] is that the mapping process is essential to decision–making about the organisation's IS environment. The PEU of the organisational administrator is consequently a by–product from the mapping process that theoretically influences decision–making; this is an important side note.

The above depicted model in combination with the conceptualisation from the IS environment in relation to the IS risk assessment steps, depicted in Table 2.2, provides the first pillar of the conceptual framework to research PEU with cybersecurity professionals in an IS risk assessment. According to the research model, the IS environment will change per step of the IS risk assessment. The cybersecurity professional consequently starts a mapping process for the IS environment. This mapping process is according to theory influenced (moderated) by the characteristics of the IS environment, which will vary per step of the risk assessment, as well as by perceptual processes of the cybersecurity professional. By researching the indicated sources of variability per step of the IS risk assessment, insight is provided into the PEU that is experienced by cybersecurity professionals in an IS risk assessment. In Subsection 3.2.4 below, the different types of PEU that can be experienced according to the theory are depicted.

3.2.4. Types of perceived environmental uncertainty

PEU manifests itself when the cybersecurity professional perceives its environment to be unpredictable [50]. Thereby experiencing uncertainty (the inability to predict or identify something accurately because it is perceived to be lacking knowledge/information or because the cybersecurity professional is unable to discriminate among information sources) [26, 50]. Three different types of PEU have been identified in the literature, see definitions listed below in italic [26, 50]:

- *State uncertainty* is experienced when the “state” of the PE, or a component, is perceived to be unpredictable. In such a case, the individual perceives uncertainty because it does not understand how the components of the PE might be changing or what the interrelations are between the components in the environment.

  The perception of state uncertainty demonstrates itself in the perceived inability to assign accurate probability estimates or the lack of understanding of the nature of possible future events/changes in the PE.

- *Effect uncertainty* is experienced when by the inability to predict what the impact of possible events/changes in the PE will have on the organisation. The impact of future events/changes may involve uncertainty about the nature, severity and timing of impact.

  Effect uncertainty is consequently argued to involve a lack of understanding of the cause – effect relationship between the organisational interface and the PE, i.e. the organisation’s IS environment. In sum, effect uncertainty is about the perceived inability to predict the implications of a given events/changes in the PE terms of its likely impact for the organisation’s future ability to function.

- *Response uncertainty* is associated with a lack of knowledge about response options and/or the inability to predict the likely consequences of a response choice.

  The response uncertainty is experienced when choosing strategies or the formulation of a response option to an immediate threat.

The above listed types of PEU can be consequently identified with the help of the research model, as depicted in Figure 3.2. By understanding the sources of variability together with the issues described in the experience of uncertainty allows the identification of a type of PEU and the factors related to it. The identification of the type of PEU will be in line with the theory as described above. The operationalisation and identification are further explained in Chapter 4.

3.2.5. Synthesis on PEU in relation to IS risk assessments

The IS risk assessment, as described by the ISO27005, is divided into three subprocesses: risk identification, risk analysis and risk evaluation. Each of these subprocesses has several steps that help to determine the risk for an organisation, as is depicted in Table 2.1. To determine the risk for an organisation the cybersecurity professional is required to make accurate predictions relating to estimates on likelihood, consequences, cause — effect relations as well as the identification of the value and workings of security mechanisms within the organisation’s IS environment.

In the risk assessment process, the cybersecurity professional can experience uncertainty about the IS environment, i.e. PEU. After conceptualising the IS environment for the different steps in the IS risk

assessment, adopted from the ISO27005 methodology and depicted in Table 2.2, the research model as depicted in Figure 3.2 can be used to research PEU with cybersecurity professionals. The perceived inability to make accurate predictions/identifications about the IS environment in a risk assessment can be caused by an experienced lack of knowledge/information or the feeling of being unable to discriminate among informational sources. It is argued that several sources of variability will moderate the cybersecurity professional's PEU. This includes the PE's dimensions of complexity and dynamism, as well as the perceptual processes of the individual. Three types of PEU exist: state, effect and response uncertainty. Each of the types of PEU has its unique characteristics.

This research consequently aims at understanding how cybersecurity professionals experience uncertainty about the IS environment in a risk assessment. This is done by identifying the PEU theory with cybersecurity professionals in the different steps of the IS risk assessment that serves as the PE — thereby delineating the sources of variability as well as the type of PEU, answering to sub–question 1. The theory as such serves as a tool to gain understanding into the research problem. Please refer to the first three columns of Table 3.1, which delineates the conceptual framework for this research.

To the best of the researcher's knowledge, it must be concluded that the theory of PEU is currently absent in the literature of cybersecurity. Therefore this theory is believed to provide new insights into the current research problem.

3.3. Judgment operations under uncertainty

The second pillar in the conceptual framework focuses on how cybersecurity professionals provide judgment under perceived uncertainty in the IS risk assessment, catering to sub–question 2. In an IS risk assessment, cybersecurity professionals are expected to provide judgment in the different subprocesses as prescribed by the ISO27005. Understanding how this judgment is provided under perceived uncertainty about the IS environment is at interest for this research. As identified from the knowledge gap in Subsection 1.1.1, theory on judgment heuristics is used to theorise how cybersecurity professionals provide their judgment when under perceived uncertainty.

3.3.1. Heuristics defined

Psychological and behavioural research has identified that when judgment and decisions need to be made that are under risk and under uncertainty, people employ heuristics [65, 69]. Heuristics are defined as operations to provide judgment and make a decision by only incorporating the aspects of a complex problem that are considered relevant. Thereby reducing the number of options that reduces complexity [42]. Kahneman [37] refers to it as a rule of thumb that allows complex scenarios to be simplified for judgment purposes. Thereby effectively replacing the complex question for one that is less complex to provide judgment subsequently.

Although heuristics provide quick answers in which judgment is needed, it can also cause predictable biases that can lead to suboptimal outcomes compared to rational choice behaviour [37, 69]. Additionally, it is essential to consider the situation in which judgment is provided, whether this is under risk or under uncertainty. Because as seen in Section 3.1, risk implies that all possible outcomes and acts are known in which only the probability values are to be assigned. Whereas uncertainty implies that not all possible outcomes are known, or make no sense to assign probability values to [45, 68].

This research focuses on the uncertainty in IS risk management which is caused by the fast evolution and changes in the IS environment. This evolution creates limited available statistical information and objective data that can be used during IS risk assessments. In other words, the incomplete knowledge of eventualities, dependencies and values of a system or phenomena within the organisation's IS environment desires that judgment is provided from the cybersecurity professional. Consequently, the heuristics in judgment is researched in situations that the cybersecurity professional experiences perceived uncertainty.

3.3.2. Models of heuristics

The field of research that focuses on heuristics knows two separate and distinct models of heuristics, which are known as informal and formal models of heuristics. Marewski et al. [46] defines informal models to not rely on the computational models, such as the work of Tversky and Kahneman [69] in which verbal descriptions of a judgment problem show deviating behaviour based on collected data.

Whereas Marewski et al. [46] argues that formal models take the perspective that predicts deviating behaviour, relying on mathematical and quantitative proof as devised by Gigerenzer et al. [31].

The informal models on heuristics in the classic study on heuristics and biases are mostly known from the work of Tversky and Kahneman [69] with their paper "Judgment under uncertainty: Heuristics and biases". Their work had a massive impact in the field of psychology for judgment and decision–making [24]. Tversky and Kahneman [69] describing a finite amount of heuristics that provide mental shortcuts in judgment situations that are under uncertain conditions.

Despite the massive impact on the field of behavioural psychology, the theory by Tversky and Kahneman [69] is also met with scepticism and critique. Fiedler and von Sydow [24] accurately describe that the most critique is coming from Gigerenzer [28, 29], who argues that the results are too vague to count as explanations for describing the cognitive processes. Furthermore, Gigerenzer [29] argues that in the experimental designs the context and tasks play a crucial role, as well as that "probability theory is imposed as a norm for a single event…; this would be misguided by those statisticians who hold that probability theory is about repeated events" [29, p. 592-593]. Kahneman and Tversky [40, p. 589] however believe that subjective judgments of probability are important because it is often based on beliefs regarding single events. "Such events cannot be generally treated as a random sample from some reference population, and their judged probability cannot be reduced to a frequency count. Studies of frequency estimates are unlikely to illuminate the processes that underlie such judgments." Thereby arguing that it is important to take unique events to the individual into account in relation to the task and context of the judgment problem as it is pivotal to the individual's operations. Consequently, they argue that inductive reasoning and judgment under uncertainty provides more insight into the judgment processes of the individual.

In addition to the critique from Gigerenzer [28, 29], Gigerenzer et al. [31] and Gigerenzer [30] developed their own theoretical conception that is called the 'heuristic toolbox', also known as the 'adaptive toolbox'. This conception is based on clearly defined algorithms and mathematics to render the heuristics people employ [24], falling into the category of formal heuristic models. Despite the transparent models and simulations for these heuristics, several studies show that experimental evidence on the cognitive processes humans follow remains scarce [24].

Pivotal to this study is gaining an insight into the way cybersecurity professionals provide judgment under uncertainty. Therefore the heuristic models from the above paragraphs are synthesised to conceptualise theory that aids in understanding judgment operations as stated in the research problem. This research further conceptualises the informal models of heuristics, because as stated by Kahneman and Tversky [40] it is believed that due to the continually changing IS environment the inductive reasoning from single events experienced by the cybersecurity professionals will play an important role. Additionally, the unique events and unique IS environments create difficulties to be brought back to a frequency count, due to the lack of useful statistical information that can be used as input in IS risk assessments. Therefore the heuristics used from the informal models are further synthesised in the next subsection.

3.3.3. The informal heuristics model – critiques and applicability to this research

This research dives deeper into the use of informal heuristic models, as delineated above. The most prominent theory in this field comes from Tversky and Kahneman [69] who identify three heuristics. Arguing that people use the *anchoring heuristic* in which they anchor around values that are provided to them when subsequent judgment is required, thereby insufficiently adjusting away from the anchor. Their *availability heuristic* suggests that judgment relies on the cognitive ease by which an event comes to mind that consequently influences their judgment. Finally, the *representativeness heuristic* is argued to be employed to provide judgment by analysing the similarities of the subject under judgment, thereby comparing stereotype situations/examples [69].

It is however important to note that the theory is over forty (40) years old and has been subject to constant scrutiny. Despite the relevancy of the theory within in the academic community as "it remains one of the most highly cited works in social science (more than three hundred scholarly articles referred to it in 2010)" [37, p. 8], the theory is dissected on the academic appropriateness to incorporate new insights into the conceptual framework.

The anchoring heuristic has been subjected to many critiques. Several studies showed that it does not fit the model of heuristics. Identifying it is caused by a special case of semantic priming, which makes information more accessible in judgments [67]. Additionally, results showed that even when

people were made explicitly aware of the effects from anchoring [75] they would still fall victim. Kahneman and Frederick [38] revisited the theory on intuitive judgment themselves and noted that the anchoring heuristic does not comply with the new model of attribute substitution for heuristics. Even after retracting the anchoring heuristic, research continued to rule out the anchoring heuristic as initially proposed. They are showing that anchoring effects also work subliminal, which is according to the anchoring theory of Tversky and Kahneman [69] not possible due to the deliberate adjustment away from the anchor [51]. This result was backed by the fact that even under monetary incentives people could not avoid the anchoring effects [64].

Alongside the critique, Mussweiler and Strack [52] also introduced a model of selective accessibility that explains possible anchoring effects. This model is based on hypothesis–testing in comparative tasks of judgment. Thereby the selective accessibility model suggests that the provided information is evaluated against the hypothesis that the information is a suitable answer to the judgment problem. If the hypothesis is not deemed to be a suitable answer, new solutions are searched. However, they can remain close to the anchor which account for the anchoring effects [52]. This claim is supported from the evidence of various studies by Chapman and Johnson [12]. Thus as the anchoring heuristic is defined by Tversky and Kahneman [69] is rejected, the judgment process as proposed by the selective accessibility model that is driven by hypothesis–testing from Mussweiler and Strack [52] provides keen insights into the judgment operations.

The availability heuristics is together with all the initial heuristics as proposed by Tversky and Kahneman [69], subject to criticism from mostly Gigerenzer [29]. This criticism is in line with the arguments made by Gigerenzer [28] and Gigerenzer [29] in Subsection 3.3.2, but had a more general focus on the availability concept being undefined that allow post hoc explanations to many things. This criticism is discussed by Kahneman and Tversky [40] who argue that the point is to assess the heuristic experimentally which therefore does need to be defined a priori. The general critique is then to be aligned with the criticism from Subsection 3.3.2 in which the research approach, formal models versus informal models, fuels the polemic. As indicated in Subsection 3.3.2, the informal models of heuristic allow the subjective judgment of probability to be investigated in which individual experiences and inductive judgment is taken into account. The availability heuristic is as such used to understand the judgment operations.

The representative heuristic has also been subject of criticism. Multiple issues were raised against the explanatory role and the falsifiability of the heuristic as was presented. In the thesis of Van Dijk [71] it however becomes clear that these issues are mostly unfounded, showing that the representativeness heuristic provides an explanatory role as well as it is falsifiable. Consequently, the representativeness heuristic can be used to understand judgment operations.

Although there are clear conceptual differences between the availability and representativeness heuristic, Gigerenzer [29] argued that the different heuristics could explain the same biases. Based on the description as provided in the first paragraph of this subsection, one can see the heuristics can be perceived similar. However, Braga et al. [9] showed not only that the concepts are conceptually different, but also found empirical support for the use of different cognitive processes as conceptualised by Tversky and Kahneman [69] for the availability and representativeness heuristic. Braga et al. [9, p. 2] suggest “that representativeness is akin to prototype matching, based on categorical and abstract information, and availability is akin to exemplar matching, based on specific instances”. This description brings about a clear distinction, showing that availability is about the cognitive ease by which examples come to mind, whereas representativeness revolves around stereotypes that form the basis of the example to compare similarities. Additionally, it is essential to note that this research is not focusing on the same biases that can be explained from different heuristics, but rather the focus is on understanding the judgment operations of cybersecurity professionals. Therefore the availability and representativeness heuristics are treated as conceptually different to aid in understanding the research problem.

This subsection dissected the critique and applicability to this research on the heuristics from the informal models. The heuristics are further conceptualised and synthesised for this research in Subsection 3.3.4, providing this research with the conceptual framework to understand judgment operations of cybersecurity professionals.

3.3.4. Conceptualiation and synthesis on the heuristics used

The theory on judgment heuristics form the second pillar to this conceptual framework. The heuristics used come from the informal models as initiated by Tversky and Kahneman [69]. The updates to the theory and critique are incorporated as is depicted in Subsection 3.3.3. This consequently allows to assess how eventualities or the values of an unknown quantity are judged by cybersecurity professionals, understanding the judgment operations. The remainder conceptualises the definitions and provides synthesis to the use of the heuristics in this research. The below summation provides an overview of the defined heuristics:

1. The *availability* heuristic is used to judge the frequency/plausibility of the subject under judgment. Thereby the judgment relies on the cognitive ease by which a similar event on the subject comes to mind. The availability is a useful clue because large classes are often better recalled, however, the availability is also affected by other factors than frequency/plausibility. Biases resulting from the availability heuristic are [69]:

   (i) The bias due to retrievability — causes estimates to be judged more frequent/plausible because they are more easily retrievable, and vice versa. This can be caused by the impact it has made on the individual, large impact facilitates the ease with retrieving similar instances.

   (ii) Biases of imaginability — can occur when instead of relying on stored memory, the individual has to construct or generate instances. Frequency/plausibility is consequently assessed based on the ease of the constructed instances.

2. The *representativeness* heuristic is employed to judge the probability of the subject under judgment by how representative or similar the subject is to a certain stereotype. This heuristic can lead to serious errors because the similarity is not influenced by factors that affect judgments of probabilities. Biases resulting from the representative heuristic are [69]:

   (i) The insensitivity to prior probability outcomes — this causes people to neglect the prior probability estimates. This bias can be successfully combated by delineating critical information to provide probability estimates.

   (ii) The illusion of validity — causes people to predict by selecting outcomes that are most representative to the input. This creates confidence in estimates because a fit is created between input and output.

3. The *selective accessibility* model is employed to actively assess provided information (the anchor) as a suitable answer to the judgment problem. Thereby the hypothesis of the provided information being suitable is evaluated. If this is not the case other information is searched for that fits the hypothesis of being a suitable answer. Biases that can result from the selective accessibility model are [52, 67, 69]:

   (i) Sticking to provided values during the evaluation of conjunctive and disjunctive events, in the search for information that is hypothesised to be a suitable answer. Thereby newly provided suitable information is compared with the initial information, remaining close to the initial values.

   (ii) Staying close to subjective judgment of experts. However, often the confidence of these judgments are not justified or an objective measure, with the potential to result in suboptimal outcomes.

As can be seen from the above conceptualised heuristics and associated definitions, the use of heuristics has the potential to create biases in judgment. These biases are identified to show potential consequences. It is however not the intent to identify these biases with this research. The judgment heuristics from the informal models as described above are used in this research to understand how cybersecurity professionals provide their judgment, estimate/predict, in the event of perceived uncertainty about the IS environment. By first identifying whether the cybersecurity professional perceives to be uncertain about the IS environment, as depicted in Section 3.2, allows the concept from judgment heuristics to be identified. Thereby this research can subsequently focus on how judgment is provided in the IS risk assessment, answering sub–question 2. Please refer to the fourth (and last) column of Table 3.1, presenting the judgment operations options for the judgment heuristics for this research.

3.4. Constructing the conceptual framework

This section provides a conclusion to this chapter and incorporates the research domain to construct the conceptual framework. The conceptualised IS environment from Chapter 2 as indicated in Table 2.2 provide seven (7) steps from the research domain in which the theoretical concepts as defined in this chapter are explored.

Firstly the theory on perceived environmental uncertainty (PEU) is used to identify if cybersecurity professionals experience uncertainty. Thereby aiming to identify the type of PEU in the different subprocesses and its steps of an IS risk assessment. If PEU is experienced, the sources of variability as defined by the theory are to be identified, looking for the unique factors in the IS environment that contribute to experiencing uncertainty by cybersecurity professionals in IS risk assessments. This allows the answering of sub–question 1. The chapter is concluded with an overview of the terminology in this research.

To understand the judgment operations of cybersecurity professionals who experience uncertainty during IS risk assessments, the informal models on judgment heuristics are used as the second concept. Three heuristics are identified that will aid this research in understanding the judgment operations by identifying the described characteristics, which allows answering sub–question 2.

The synthesis of the two theoretical concepts and the IS environment from the research domain culminates in a conceptual framework, which is depicted in a tabular form in Table 3.1 below. This allows the synthesis in which sub–questions 1 & 2 provide the answer to the main research question with the help of the conceptual framework and empirically gathered data.

Table 3.1: The conceptual framework for this research

IS risk assessment	**Perceived environmental uncertainty**		**Judgment heuristics**
Subprocesses & Steps	*Type of PEU*	*Variability sources*	*Heuristics*
Risk identification			
1. Identification assets			
2. Identification threats	State uncertainty		Representativeness heuristic
3. Identification existing controls			
4. Identification vulnerabilities			
5. Identification consequences on CIA		PE characteristics	
Risk analysis	Effect uncertainty		Availability heuristic
1. Assessing consequences			
2. Assessing likelihood		Perceptual processes	
3. ~~Determining risk level~~			
~~Risk evaluation~~	Response uncertainty		Selective accessibility

3.4.1. Terminology from conceptual framework

The chapter is concluded with a subsection that provides the reader with an overview of the different definitions used for this research. These definitions have been introduced in the first three chapters and are of interest to this research and key to understand for the reader. Please refer to Table 3.2 for the different terminology.

Table 3.2: Terminology for key concepts in this research

Term	Description
Availability heuristic	Judgment for plausibility/frequency that is based on the ease by which events/instances come to mind [69].
Complexity	Described by the large amount of components that are present in an IS environment and are non–similar by nature [21].
Dynamism	Described by the changing nature of the IS environment which is perceived by the degree in which environmental factors change as well as the emergence of new environmental factors [21].
Effect uncertainty	The perceived inability to predict the implications of a given state change in terms of its likely impact for the organisation's future ability to function, relating to the nature, severity and timing of impact [50].
Information security (IS)	The discipline that is involved with the development and implementation of security mechanisms of all available types (technical, organisational, human–oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and consequently, information systems, where information is created , processes, stored, transmitted and destructed free from threats [14].
Information security (IS) risk assessment	The identification and analysis of consequences and likelihoods that events materialise and affect the state of consequences. This subsequently allows the expected value outcomes from the risk calculation to be evaluated and prioritised [54].
Perceived uncertainty	The individual's experienced inability to predict or identify something accurately because it perceives to be lacking information/knowledge to make accurate predictions, or because the individual feels unable to discriminate among informational sources [26, 50].
Representativeness heuristic	Judgment on probabilities based on how representative/similar the subject is to the description of a certain stereotype [69].
Response uncertainty	The perceived inability to predict the likely consequences of response choices/the response options available [50].
Risk	The expected value that can occur if estimated consequences materialise from the estimated likelihood of an event occurring. The uncertainty domain allows estimates that are based on knowledge [4, 54].
Selective accessibility model	Judgment based on actively evaluating provided information (the anchor) as a suitable answer to the judgment problem. Thereby the hypothesis of the provided information being suitable is evaluated. If this is not the case other information is searched for, but could potentially be influenced by sticking close to values from the initial provided information [52, 67].
State uncertainty	The perceived inability to estimate probabilities or to estimate the nature of possible future state changes. State uncertainty is perceived because it is difficult to understand how components of the PE might be changing or what the interrelations are between the components in the environent [50].
Uncertainty in calculating risk in accordance with ISO27005	The incomplete knowledge of eventualities, dependencies and values of a system or phenomena.

4 Methodology

This chapter describes the research methodology for this study. First the research design is delineated in Section 4.1, this subsequently gives way to operationalise the theoretical concepts in Section 4.2. The qualitative nature of this research in combination with the conceptualised theoretical concepts consequently demands a rigorous approach to the data collection and data analysis phases as described in Sections 4.3 and 4.4. The chapter is finalised with a conclusion on the research methodology in Section 4.5.

4.1. Research design

To answer the research question, a qualitative research strategy is chosen. The qualitative approach is adopted because the research is exploratory in nature, requiring data that is suitable for in–depth analysis that allows the researcher to understand the context and situation. The project aims at describing how cybersecurity professionals experience uncertainty about the IS environment and how they subsequently provide judgment while under their perceived uncertainty. The theories on perceived environmental uncertainty (PEU) and judgment heuristics under uncertainty are used to identify the constructs in the information security (IS) risk assessment setting as prescribed by the ISO27005. According to the researcher's knowledge, the extrapolation of these theories into the IS field has not been done before, therefore the qualitative approach is appropriate for this research.

The research focuses on theory development at a descriptive level through inductive reasoning. The school of inductive reasoning is suitable for this research question because it aims at answering the *how*, which allows an understanding of the underlying perceptual and judgment operations of cybersecurity professionals in an IS risk assessment. The remainder of the section describes the research method and the considerations to this method in relation to the theory used.

4.1.1. Qualitative survey research

This study uses a qualitative data from interviews, i.e. a face-to-face survey that in this research will be referred to as qualitative survey research, to analyse and synthesise the theories as depicted in the conceptual framework of Chapter 3. A rigorous approach is pivotal when deploying a qualitative survey research method to ensure all relevant data is gathered, analysed and synthesised in the same way to provide an answer to the research questions. The rigorous approach is delineated by the reliability and validity, which is depicted per phase of this research study (see Sections 4.2 to 4.4).

The research question aims at describing how cybersecurity professionals *deal* with uncertainty about the information security environment in an IS risk assessment. The word "deal" creates a research question that is two–fold, which is captured by the different sub–questions. SQ1 aims at describing the *perceived environmental uncertainty (PEU)*, i.e. the experienced uncertainty of cybersecurity professionals about the organisation's information security (IS) during risk assessments. Whereas SQ2 aims at the *judgment operations* of the cybersecurity professional's when experiencing PEU during the risk assessment. Both the sub–questions are descriptive in nature and through the survey research design they allow theories to be explored in the IS risk assessment setting.

The research is cross–sectional in nature where data is gathered from multiple interviews in one specific data collection phase of the research project [10]. This is suited for this research project because the time constraint limits a longitudinal study, as well as the fact that the inductive approach allows theory development from one distinct that provide insights for future research.

4.1.2. Considerations to research design

The structure of the conceptual framework is formed by the ISO27005 prescribed risk assessment approach from the research domain. This forms the backdrop against which two theoretical concepts, perceived environmental uncertainty (PEU) and informal models of judgment heuristics, are explored in the field of IS risk assessments. It is important to consider the limitations to this research design and the associated theories, as will be described in the following subsections.

4.1.2.1. The theory on PEU in relation to the research design

The theory on PEU is filled with controversies regarding the appropriate research technique, whether this should be quantitative or qualitative. The literature shows different dilemmas, concerning the objectivity and subjectivity of the object that is being researched and how this consequently relates to the research outcomes Ashill and Jobber [2], Downey [18], Downey and Ireland [19]. It is important to underscore that the objective of this research is to identify subjective processes and that properly capturing this subjectivity is crucial to the research outcomes. The road taken in this research design, a qualitative approach, is therefore critical to reflect on for the validity of this research project.

Downey and Ireland [19] have proposed a framework to determine the appropriateness of the research design to the object that is being researched. They consequently argue that qualitative approaches are most useful for the assessment of environmental attributes, whereas quantitative approaches are more useful to assess the interpretations of participants. In response to the work of Downey and Ireland [19], it is important to consider that many attempts have been made to create scales that measure PEU. It is additionally important to mention that many have failed because issues existed with the reliability and validity of these scales [2].

Although Ashill and Jobber [2] argue to have created valid and reliable scales, their approach is aimed at marketing management decisions. The extrapolation of the theory on PEU into the field of IS creates a new dimension which has not been tested before with their scales. Therefore the validity and reliability of the scales produced by Ashill and Jobber [2] can not be guaranteed in the research domain. This essentially constrains the use of a quantitative research approach because there are no reliable and validated scales available to this research setting. Furthermore, the objective of this research is to identify relationships between theories in the IS risk assessment setting to form input for a conceptual model, which makes it difficult to use a quantitative approach in the first place.

The use of interviews in a survey research design consequently provide the opportunity of structuring specific topics as well as understanding the perceptional processes on a qualitative level. This constitutes the need for semi–structured interviews. The structured interview part allows the identification of the perceptual processes, i.e. the interpretation of PEU, as was suggested to be the most useful by Downey and Ireland [19]. Additionally it provides the means to stick to structured methodology as indicated by the ISO27005 approach. But it is important to consider that the semi–structured approach also allows for follow–up questions as to what constitutes the interpretation of PEU. Thereby capturing the sources of variability from PEU, such as the IS environment characteristics or perceptual processes of the cybersecurity professionals as was depicted in Section 3.2.

In sum, the use of semi–structured interviews provides the best opportunity to explore how the theory on PEU manifests itself in an IS risk assessment setting. This approach allows the identification of perceptual processes from structured interview questions, whereas the attributes to the IS environment can be assessed through more open–ended questions.

4.1.2.2. The theory on judgment under uncertainty in relation to the research design

The work by Mussweiler and Strack [52], Strack and Mussweiler [67], Tversky and Kahneman [69] on informal models of judgment heuristics under uncertainty has emerged from experimental research designs. Their method included different experiments to identify heuristics that people employ when they are asked to provide judgment under uncertainty. Although their research method is fundamentally different from the proposed research design in this study, it is crucial to understand that this research does not aim to identify new heuristics, or the identification of heuristics and biases in general. The

theory is rather used to see if heuristics are described by cybersecurity professionals in their judgment operations when experiencing uncertainty about the IS environment.

The use of semi–structured interviews allows the identification of descriptions of heuristics by cybersecurity professionals from qualitative data. Similar attempts have been undertaken, most recently by Hansen et al. [34] who researched the presence of cognitive biases with clinicians in the recommendation process of vaccines. By developing a clear coding scheme the researcher ensures the validity and reliability for the identification of heuristics in the data, the scheme is further elaborated in Table 4.1.

In sum, the fact that this research does not aim to discover new heuristics, but rather identify heuristics in the description of cybersecurity professionals their judgment operations allows the use of qualitative data to identify elements from the judgment heuristics theories using a specified coding scheme (see Section 4.4).

4.2. Operationalisation

To operationalise the theories from the conceptual framework in Chapter 3 in relation to the research question, it is important to define the variables of interest into identifiable factors. This process allows the empirical data to be analysed constructively to answer the research question.

4.2.1. Operationalising PEU

The theory on PEU is operationalised according to the research model as depicted in Figure 3.2. The model knows two sources of variability that can cause the cybersecurity professional to perceive uncertainty about the IS environment in a risk assessment:

1. *Perceptual processes*
    a The individual cognitive characteristics — the way in which an individual deals with ambiguity.
    b The availability of response options — referring to the variety of experiences that are available to the individual.
    c The social expectation — this denotes the socialisation process of an organisation's influence on an individual's response to uncertainty.
2. *The characteristics of the perceived environment*
    a The complexity dimension — this describes the similarities within the environment, i.e. the more component that are present the more complex the environment can be perceived.
    b The dynamism dimension — this refers to the changing nature of the environment, i.e. the perceived degree of change of environmental factors and the emergence of new environmental factors.

The sources of variability are individually operationalised for this research, marked by the category number of the sources of variability and the associated letter.

4.2.1.1. The perceptual processes

The perceptual processes are a source of variability that is unique to the cybersecurity professional. To understand these sources of variability, questions posed to the cybersecurity professional need to underpin these unique and personal factors. The perceptual processes are operationalised as follows:

1.a To operationalise an individual's cognitive characteristics, in this case for cybersecurity professionals, is extremely difficult. However, the only objective measure that could be derived from qualitative data on how one deals with ambiguity is directly linked to the training/education they have followed. In the case of cybersecurity professionals who execute IS risk assessments, it is important to consider their training/education because ambiguity is an inherent factor within risk management. Training/education in IS risk management will consequently provide the cybersecurity professional with methods or knowledge for how to deal with this ambiguity, which in turn should influence their perception of uncertainty.

    Consequently, the training/educational background of the cybersecurity professional is operationalised as a factor that is a source of variability and can consequently influence the perceived

uncertainty about the IS environment. Thereby it will be firstly important to identify the training/ education in an objective measure. Secondly, training/education can be identified from responses as a factor to why the cybersecurity professional feels to be uncertain or certain, for instance in the case where the respondent feels that lack of training/education is influencing their perception of uncertainty.

1.b The availability of response options is operationalised by the measure of working experience within the field IS risk management. An important factor is the years of working experience in which the cybersecurity professional is actively involved (or responsible) in the execution of IS risk assessments.

This factor in the source of variability is consequently operationalised by identifying the relevant working experience of cybersecurity professionals in the field of IS risk management practices as an objective measure. Secondly, the working experience can be identified from responses as a factor as to why the cybersecurity professional perceives to be uncertain or certain.

1.c The social expectations from the socialisation process of the organisation that influences an individual in their response to uncertainty is difficult, if not impossible, to operationalise with objective measures for this research.

The social expectations are as a consequence not directly operationalised with a dedicated question. However, it can be identified as factor from responses as to why the cybersecurity professional perceives to be uncertain or certain. Please refer to the coding scheme in Table 4.1 for how this item is identified.

Please refer to Subsection 4.2.3 for the questions that are associated to the above operationalised concepts.

4.2.1.2. The characteristics of the perceived environment

The characteristics of the perceived environment (PE) are a source of variability that is depending on the conceptualised part of the IS environment, for details on the conceptualised IS environment please refer to Section 2.3. It is important to note that the IS environment's characteristics are difficult to be objectively defined or measured. Because the theory on PEU states that the perception is determined by the individual who perceives its environment to have certain environmental characteristics. The characteristics of the perceived IS environment are operationalised as follows:

2.a The complexity dimension is operationalised by the responses given by the cybersecurity professional, who can indicate that the IS environment is perceived either complex or not. Therefore the degree of complexity cannot be measured, but the complexity dimension is indicated as a source of variability as to why the cybersecurity professional perceives to be uncertain about the IS environment. Attributing factors for the complexity dimension as to why the IS environment is perceived to be uncertain are identified from the responses.

2.b The dynamism dimension is operationalised by the responses given by the cybersecurity professional, who can indicate that the IS environent is perceived either dynamic or not. Therefore the extent of dynamism within the IS environment is not objectively measured, but it is indicated by the cybersecurity professional as a factor to its perceived uncertainty about the IS environment. Attributing factors for the dynamism dimension as to why the IS environment is perceived to be uncertain are identified from the responses.

Please refer to Subsection 4.2.3 for the questions that are associated to the above operationalised concepts.

4.2.1.3. The types of PEU

The theory on PEU elaborates on three types of uncertainty that can be perceived about the IS environment. The type of uncertainty that can be experienced is the result of the mapping process about the IS environment and the sources of variability, which consequently results in perceived uncertainty about the IS environment (see Figure 3.2).

The type of PEU is operationalised by questioning the respondents to identify the nature of their perceived uncertainty. The answers will describe defining features as to what creates the perception

of uncertainty. This does not directly relate to the sources of variability as discussed above, it rather focuses on the elements that define the type of uncertainty as is described by the theory. These identifiers allows the coding of the respondent answers by mathcing the description of perceived uncertainty with the theoretical identifiers as defined by Gerloff et al. [26] and Milliken [50]. The elements are associated with identifiers for each of the PEU types and are described in Section 3.2. The identification of the PEU type is further elaborated on in Table 4.1. Please refer to Subsection 4.2.3 for the questions that are associated to the operationalised concepts for the theory on PEU.

4.2.2. Operationalising judgment heuristics

The theory on judgment heuristics is conceptualised with three (3) heuristics for judgment operations. The theory is synthesised with this research as a concept to identify whether the cybersecurity professionals describes the use of heuristics when they need to provide judgment about the IS environment in an IS risk assessment.

As discussed in Subsection 4.1.2.2, the theory on judgment under uncertainty is used to explore a fit between the theory and the IS risk assessment setting in relation to the concept of PEU. Therefore the theory is operationalised by questioning the respondent to elaborate on their judgment operations when experiencing uncertainty during the IS risk assessment steps. Thereby explicitly asking how the cybersecurity professionals provide estimates despite the experienced uncertainty, as well as posting follow–up questions to find out what the steps are that allows them provide the estimate. The responses to this question are analysed for identifiable elements from the theory on judgment heuristics. Please refer to Subsection 4.2.3 for the questions that are associated to the above operationalised concepts. Please see that the identifiers for this theory are depicted in a coding scheme in Table 4.1.

4.2.3. Building the interview questions from the operationalised concepts

The interview is build up in two main parts and a third closing part. The first part is a context establishing part that collects data about the cybersecurity professional, catering to parts of the factors from perceptual processes as described in Subsection 4.2.1.1.

The second part of the interview uses the IS risk assessment methodology steps from the ISO27005 as its backdrop against which the different conceptualised IS environments are discussed in relation to the two theoretical concepts. This entails that the two concepts are discussed in a repetitive order for each of the steps of the risk assessment methodology as prescribed by the conceptual framework, thereby identifying the concepts within the different steps (see Table 3.1).

The third part reflects on the interview itself, requesting feedback to improve as well as providing the respondent the option to pose questions with regard to the research. Please refer to Figure 4.1 below for a schematic representation of the interview setup. For a complete overview of the interview script with the connection to the research questions and theory, please refer to Appendix A.

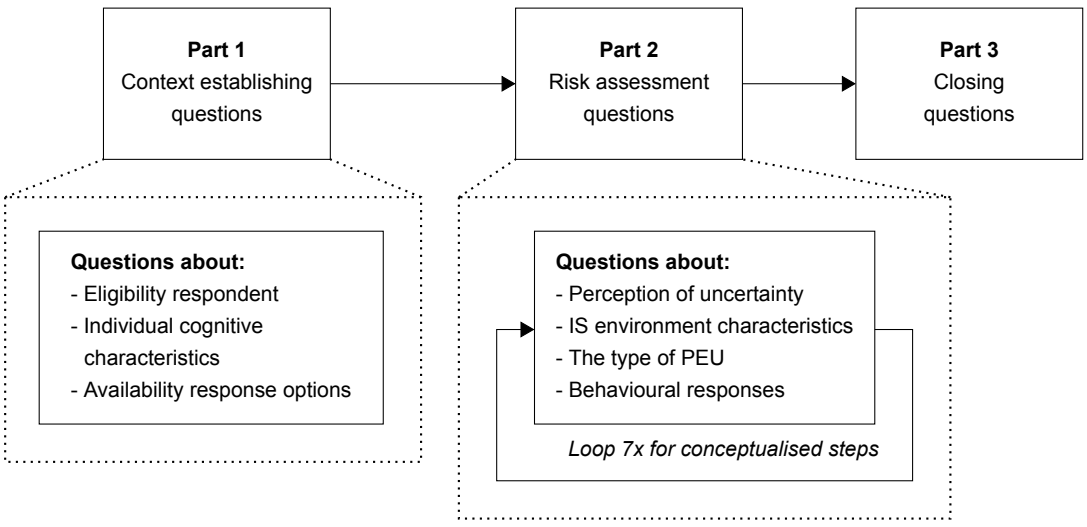


Figure 4.1: The interview setup

4.2.3.1. Part 1: The context establishing questions

The context establishing questions have a dual purpose. First it is important to determine if the respondent is suited and fits the criteria (as will be discussed Subsection 4.3.1). Therefore two questions have been designed which provide insight into the activities and involvement of the respondent with regard to the execution of IS risk assessments:

Q1 Could you briefly describe your role within your organisation?

Q2 Could you briefly describe how you are involved in organisational information security risk assessments?

The second goal is to measure a part of the perceptual processes as was operationalised in Subsection 4.2.1. Thereby focussing on (1.b) the availability of response options and (1.a) the individual cognitive characteristics.

Q3 Could you briefly describe how long you have been working in this role or similar?

Q4 Are you educated to execute information security risk assessments? Do you believe this helps/hinders you in the execution?

4.2.3.2. Part 2: The risk assessment questions

The risk assessment questions dive into the conceptualised steps from the ISO27005, as depicted in the conceptual framework (see Table 3.1). For each of these steps the two theories from Chapter 3 are assessed in the IS risk assessment setting. The below sequence of questions was followed for the next seven (7) times to discuss the theories in all conceptualised steps.

Q5 — Q11 Could you briefly describe how you identify/estimate <step of ISO27005> for your organisation?

The above depicted question is used for each of the steps to get the respondent in the mindset of how they execute that step of the IS risk assessment. Additionally this question provides the researcher with some additional context of how the cybersecurity professional executes the step within that particular organisation, allowing organisational factors to be taken into account as well. It is important to remember that this question doesn't relate to any of the research questions or theories, but is to guide the conversation that allows a constructive manner of data collection.

The next question aims at identifying if the cybersecurity professional experiences uncertainty in the execution of the particular step of the IS risk assessment.

Q5U — Q11U Do you ever experience uncertainty while doing so?

If the respondent indicates to experience uncertainty, then the follow–up question aims at identifying the theory on PEU, which is directly linked to sub–question 1 (SQ1). Thereby looking into the nature of the type of uncertainty (as depicted in Subsection 4.2.1.3), as well as the identification of sources of variability (1.c, 2.a and 2.b).

Q5Y-A — Q11Y-A Could you describe the nature of your perceived uncertainty? What are the factors that contribute to this?

Because the respondent has indicated to perceive uncertainty in Q5U — Q11U and has elaborated on the perception of uncertainty in Q5Y-A — Q11Y-A, the follow–up question aims to identify if the cybersecurity professional employs heuristics in providing judgment in the IS risk assessment step. This question directly relates to the theory on judgment under uncertainty, linking to sub–question 2 (SQ2).

Q5Y-B — Q11Y-B Could you describe how you provide an estimate despite the experienced uncertainty? What are the steps that your undertake to arrive at your judgment?

After capturing all information relevant to the step of the IS risk assessment, the process repeats itself for the rest of the steps as indicated in Figure 4.1.

However, if the respondent indicates not to perceive any uncertainty in the IS risk assessment step, then the follow–up question is aimed to identify why the respondent is not experiencing uncertainty. Thereby looking into factors that can relate to the sources of variability (as prescribed by the theory on PEU) as well as other factors.

Q5N — Q11N Could you briefly describe why you don't experience uncertainty?

After collecting the data on why the respondent does not perceive to be uncertain, the question for that particular step stops and the interview is continued with the next step of the IS risk assessment.

After looping the risk assessment questions seven (7) times, for each of the conceptualised steps, the interview is finalised with closing questions in *part 3*.

4.2.4. The identification of theoretical concepts

To answer the research questions, the theoretical concepts need to be identified from the empirically gathered data. To ensure that the research is executed *reliable* and *valid* in the way the concepts are identified, Table 4.1 provides a coding scheme that specifies identifiable elements for the theoretical concepts. This coding scheme is based on the theoretical foundation of Chapter 3 and the operationalisation of the theory as depicted above in this section. The first column provides the theoretical concepts and the elements that are contained by the theory. The second column provides the identifying factors that allow the data to be linked to the theoretical concepts.

Table 4.1: Coding scheme — Indicators for coding the theoretical concepts from qualitative data

Theoretical concept	**Identifying factors**
Perceived environmental uncertainty (PEU) — Sources of variability	
Perceptual processes	
Individual cognitive characteristics	The identification follows from identified training/education of the respondent. Thereby the training/education becomes an identifier of the sources of variability if the respondent provides argumentation for why uncertainty or certainty is perceived about the IS environment.
Availability of response options	The identification follows from the years of relevant working experience in IS risk assessments. It is identified as a source of variability if the respondent perceives to be uncertain or certain about the IS environment based on their experience.
The social expectations	The identification does not directly follow from a question in the interview script, but is solely identified from answers linking to: • The organisational viewpoint on risk • The management perspective on risk • The guidelines from internal audit in relation to risk appetite.
Characteristics of perceived environment	
Complexity	The indicators follow from the literal definition of complexity that is applied to the IS setting. This provides indicators such as: • Many different components within the IS environment • Many interrelations within the IS environment • Lack of transparency the IS environment.

Table 4.1: Coding scheme — Indicators for coding the theoretical concepts from qualitative data

Theoretical concept	**Identifying factors**
Dynamism	The indicators follow from the literal definition of dynamism that is applied to the IS setting. This provides indicators such as: • Changing IS environmental factors; • The emergence of new IS environmental factors and the disappearance of old IS environmental factors.
Perceived environmental uncertainty (PEU) — Types	
State uncertainty	The identification follows from answers indicating that respondents perceive to be unable to: • Assign accurate probability estimates; • Estimate how components of the IS environment seem to be changing; • Grasp all the exiting interrelations between the components in the IS environment.
Effect uncertainty	The identification follows from answers indicating that respondents perceive to be unable to: • Predict the impact from possible events/changes in the IS environment on the organisation (involving the nature, severity and timing of impact); • Grasp the cause – effect relationship between the organisational interface and the organisational IS environment.
Response uncertainty	The identification follows from answers indicating that respondents: • Perceive to lack knowledge about how to respond to changes in the IS environment; • Perceive to lack knowledge about the consequences for the chosen responses.
Judgment heuristics — Judgment operations	
Availability heuristic	The identification follows from answers indicating that the respondents: are led by events that quickly come to mind to address the frequency/plausibility of the subject under judgment. Generally such events have had a big impact and are therefore easily retrieved by the respondent.
Representative heuristic	The identification follows from answers indicating that the respondents: actively compare the subject under judgment to similar (i.e. representative) cases and base their judgment on the similarity of the stereotype.
Selective accessibility model	The identification follows from answers indicating that provided information is hypothesised as a suitable answer for the subject under judgment. The deliberate assessment of information provides subsequently input for accepting or a continued search for information that is considered a more suitable answer for the judgment problem.

Because this research takes an inductive approach, new findings can be gained that are not fitting the theoretical concepts but are to mentioned as part of the results. In the event that responses cannot be related to the identifiers of the theoretical concepts, the findings are assigned a definition and associated code which are based on the content of the findings and are elaborated upon in Chapter 5.

4.2.5. Reliability and validity for the operationalisation

The interview questions, as depicted above, allow the researcher to reliably execute the qualitative survey research design. As such the answers can be compared to one another, allowing generalisability of the findings with limited influence from the researcher's interpretation.

To ensure that the operationalisation of the theoretical concepts and their associated interview structure is valid, the interview script was assessed during the mid–term meeting with the graduation committee. To allow the interview script to be repeated successfully, a Deloitte cybersecurity professional with interview expertise was consulted to finalise the interview script. This resulted in an interview script that is reliable and valid for this qualitative survey research design.

4.3. Data collection

The research questions are answered by analysing and synthesising the theoretical concepts and empirical data. This section discusses the sampling method, the safeguarding of the reliability and validity of the data collection phase, as well as the ethics around human research.

4.3.1. Sampling

The population that is of interest to this research are cybersecurity professionals that execute qualitative and semi–quantitative IS risk assessments. This research consequently adopts a purposeful sampling method because special knowledge and skills are required to provide information-rich data [63, Ch.13 - Sampling]. The primary information that is gathered from the semi–structured interviews is consequently validated as being representative by setting selection criteria for the interviewees, which are validated during *part 1* of the interview (see Subsection 4.2.3). Eligible respondents for this study are selected based on the following criteria:

- *The respondent needs to be 18 years or older;*

  This is required by the Human Research Ethics Commission in case research is executed with human subjects.

- *The respondent has relevant working experience in ISRM processes, focussing on IS risk assessments, with a minimum of one (1) year;*

  This criteria is included to ensure the respondents has been actively involved in ISRM processes and is thereby familiar with the terminology associated to the IS risk assessments.

- *The respondent is used to working with a qualitative or semi–quantitative information security risk assessment approach and is familiar with the ISO27005 standard;*

  This criteria is included because this research focuses on the perception of uncertainty, therefore a qualitative and semi–qualitative angle allows the inclusion of discussion on this perception. This is also indicated in Chapter 3.

- *The respondent executes information security risk assessments at an organisational level, taking the organisational context into account (not focussing on hardware only).*

  This criteria is included for two reasons. Firstly, the theory on PEU is an organisational theory that looks at uncertainty about the environment in relation to a complete organisation. Within IS, risk assessments can also be executed on one single piece of hardware which consequently neglects the organisational perspective. Secondly, the broad scope generally forces risk assessments to take a qualitative or semi–qualitative approach due to the fuzzy relations within an organisation. This helps in the selection of eligible respondents.

The respondent inclusion criteria for this research are not based on the type of sector in which the cybersecurity professional is active. There are three main reasons for this approach. First, the unifying factor of this research is the backdrop of the ISO27005 IS risk assessment approach. This method provides the universally applicable steps for an IS risk assessment, which is indifferent of the sector and thereby leading for respondent inclusion. Second, this research aims at providing a conceptual model to identify if relationships between theory and the practical backdrop of IS risk assessments exist. Thereby using the ISO27005 IS ris assessment methodology which is universally applicable. Lastly, it is anticipated that the target sample size in itself will be difficult to meet because expected hesitance of

respondents to this research. Constraining factors such as sectors would thereby limit the population drastically and possibly jeopardise this research.

4.3.1.1. Sample size

The qualitative nature of the research approach and the time constraint set for this project forces a limited sample size. To get a representative number of respondents that allows the plausibility for the valid identification of the theoretical concepts within the IS risk assessment setting, a target sample size is set to twenty (20) respondents.

4.3.1.2. Three lines of defence model

An important aspect to consider for this research is the governance of risk structure, prescribed in the Three Lines of Defence model. Based on the eligibility description, it will be most likely that the cybersecurity professional is aligned with the second line of defence (see Figure 4.2). This role demands the professional to oversee and specialise in the risk management and compliance processes. Thereby facilitating and implementing effective risk management practices for the risk owners from the first line of defence [13]. This essentially means that the cybersecurity professional is not primarily responsible or to be held accountable for the risk itself. They are however expected to facilitate, oversee and provide input, having an active voice in the decision–making process.

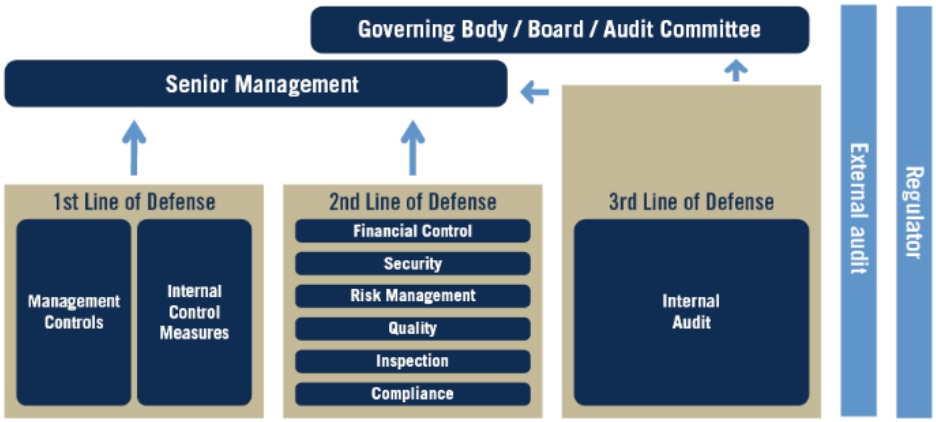


Figure 4.2: Three lines of defence model, adopted from Luburic et al. [44].

4.3.2. Human research ethics

This research involves human subjects that provide primary information through semi–structured interviews. Consequently, this research has gained approval from the Human Research Ethics Committee (HREC) of the Delft University of Technology.

4.3.3. Reliability and validity for the data collection

The reliability and validity of the data collection is safeguarded by following a strict data collection protocol. The below enumerated items provide a short summary of the data collection protocol, refer to Appendix C for the details:

- The respondent search and selection was based on the criteria set in Subsection 4.3.1, contributing to the validity of the research. The search was executed via the Deloitte network and the social media platform LinkedIn.
- When it was expected that the respondent would fit the research criteria, a research invitation letter was sent. This letter describes all information necessary to consider participation for this research (see Figures C.4 and C.5).
- Via telephone or e–mail a face-to-face meeting was scheduled. Additionally, the informed consent form (see Appendix B) was sent ahead of the scheduled interview for the respondent to read prior to the meeting and sign for during the interview. This allows the respondent any remaining questions to be answered.

- The interview followed a rigorous and structured approach. This was enabled by an interview protocol that ensured all respondents were provided the same information and were asked the same questions, safeguarding the reliability of the research (see Figure C.6).

4.4. Data analysis

The analysis of empirical data is at the centre of this thesis. This section discusses how the data is synthesised to provide answers to the research questions.

4.4.1. Language of interviews

This research is executed in an English format. It is however important to note that the interviews are conducted in Dutch with interviewees to whom this is their native language. This is done to allow the respondents to answer in the language that is most comfortable to them. The data transcripts are consequently all in the language in which the interview was recorded. During the analysis phase a translation step from Dutch to English is made, allowing the data to be linked to the theoretical concepts. By translating in this step the information–rich data is the least altered for the use of this research, maintaining its informational integrity. Non-Dutch speakers are interviewed in English.

4.4.2. Transcribing

The interviews in this research are recorded to ensure that all relevant spoken data is captured by the researcher. The spoken data is subsequently transformed to text data by means of transcription. The interviews are transcribed using an edited transcription technique. This entails that only the relevant parts of the interview are transcribed in a coherent manner, cleaning clutter from the transcript.

The edited transcription method is chosen due to repetitive character of part 2 in the interview. The interview circles around the same two concepts in different conceptualised IS environments, allowing any non–relevant information to be omitted without losing the meaning of the recorded answers. This provides the researcher with a readable and coherent text for further analysis.

The interviews are transcribed using the special tooling of NVivo12. This tooling provides the researcher with several benefits. Firstly, the recordings are automatically segmented which provides a transcript that is categorised per theme of the interview script. Secondly, it provides time–stamps to the audio file in the transcribed text, providing easy traceability.

Through the edited transcription technique the validity is safeguarded because the integrity and meaning of the responses are preserved. The use of the transcription tooling provides reliability due to the automated segmentation techniques that improve further analysis.

4.4.3. Coding approach

This research adopts two coding approaches. First an open coding approach is taken in which in vivo codes are used to identify findings that cannot be directly related to the theoretical concepts. This allows the inclusion of new findings in the process. Additionally targeted codes are used to directly identify and link the data to the theoretical concepts.

The second approach that is undertaken is axial coding process. Thereby the codes from the open coding approach are categorised to allow the identification of underlying axes and dimensions of the data. This is done using a hierarchical tree structure that is based on the interview questions. This tree structure approach is adopted to provide overview of the codes because all the IS risk assessment questions revolve around the same concepts with similar questions. By using the ISO27005 framework and the interview questions as the tree structure an overview is created that allows the research questions to be answered specific to the conceptualised IS risk assessment steps.

4.5. Conclusion for the methodology

The study adopts a qualitative survey research design which used the theories on (PEU) and judgment heuristics in an information security (IS) risk assessment setting. Although the theories from the conceptual framework have different research methods, the current combination of theories is best suited for a qualitative approach which provides the most insight into the research problem. The theories are operationalised into identifiable elements that can be synthesised from semi–structured interviews, which follow a rigorous method for the collection of data. The data is synthesised using specialised

tools for data analysis and is guided by a coding scheme that provides a coherent set of indicators to identify the theories within the IS risk assessment setting. Provided by the rigorous methodology, the reliability and validity of this research is ensured and consequently allows the research questions to be answered.

5 Results

In this chapter the results from fifteen (15) interviews are presented. The results are presented in the same order as the interview questions in accordance with Figure 4.1. Starting with Part 1, Section 5.1 provides the sample characteristics coming from the first two questions and Section 5.2 delineates the first elements of te perceptual processes for the perception of uncertainty of the respondents from question three and four. Part 2 is described in accordance with the ISO27005 framework, the results for the risk identification and risk analysis are described separately in Sections 5.3 and 5.4. The results from the sections associated to Part 2 of the interview revolve around the theoretical concepts from the conceptual framework. This allows a structured approach that provides a coherent and succinct depiction of the empirical data.

Prior to reading the results, a set of instructions are provided to allow easy reading and coherent interpretation to the reader. Whenever text is displayed in **boldface**, a theoretical concept is highlighted that directly reflects the theoretical terminology. If text is displayed in *italic*, a noteworthy finding is indicated that is considered of value to this research. Furthermore, the results are delineated with reference to the respondent that has provided the answers. Whenever a reference is made to a respondent an identifier is indicated which is marked by the letter 'D' and an associated #number for the interview count, e.g. D01 which is the first interviewee.

5.1. The sample — Part 1 of the interview

This study is focussing on how cybersecurity professionals deal with perceived uncertainty about the organisation's information security (IS) environment in an IS risk assessment. Therefore first hand data is gathered from cybersecurity professionals who are actively involved in executing IS risk assessments, that are as described in Chapter 4 the target population for this study. This section describes the respondent search and characteristics of the sample.

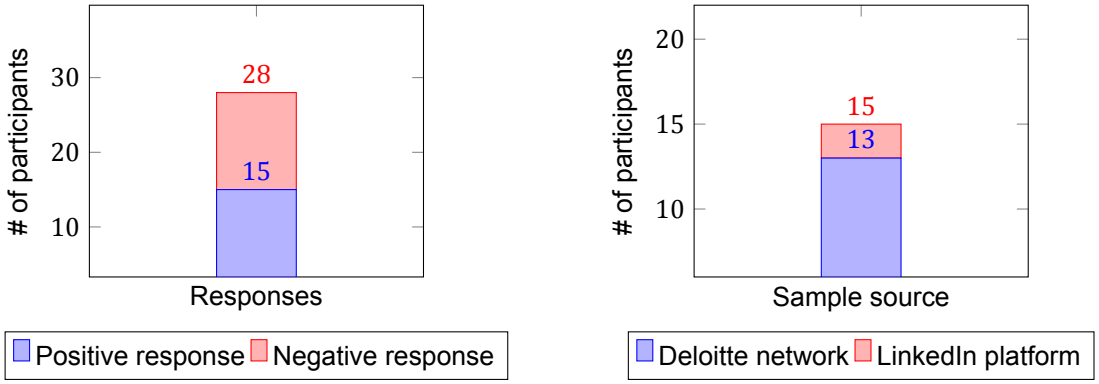
5.1.1. Responses & Participation

The respondents are approached via the Deloitte network and via the social media platform LinkedIn. A total of twenty-eight (28) research invitations have been sent via the Deloitte network and via LinkedIn. This yielded fifteen (15) positive responses that led to an interview (see Figure 5.1a). From the remaining thirteen (13) responses twelve (12) did not respond to the invite. Only one (1) respondent was considered not to fit this study after checking the eligibility criteria with the respondent as depicted in Subsection 4.3.1.

The Deloitte network has provided this research with an extensive reach into the target population. The number of respondents that are coming directly or indirectly from the Deloitte network accumulate for thirteen (13) out of the fifteen (15) respondents (see Figure 5.1b). The two (2) that did not come from the Deloitte network have positively responded to the LinkedIn–invite which resulted in an interview.

5.1.2. Characteristics of the respondents

The respondents that participated in this research study have several defining characteristics, relating to their job title as well as their sector. Although the sampling for this research is not focussed on



a) The respondent response rates

b) The respondent sample sources

Figure 5.1: Respondent search

either of the two, for validity purposes their characteristics are displayed. It is important to note that the job titles and sectors displayed are not one-to-one as indicated by the respondents, but merely show standardised and abstracted job titles and sectors to preserve the privacy of the respondents.

The interviewed respondents indicated four (4) times to be in a role of information security officer (ISO) or similar. In seven (7) instances the respondents indicated to be in the function of information/IT risk & security manager or similar. The remaining four (4) respondents indicated to carry the job title of chief information security officer (CISO) or equivalent.

The information/IT risk & security manager is associated with the execution of risk management practices. In general this is also applicable for the ISO/CISO roles, however, to be certain that all respondents are actively involved this is also checked with the eligibility criteria. It is important to note that the role of CISO is more devoted to managerial tasks in relation to the IS risk management practices. Figure 5.2 provides a concise overview of the job titles of the interviewees.

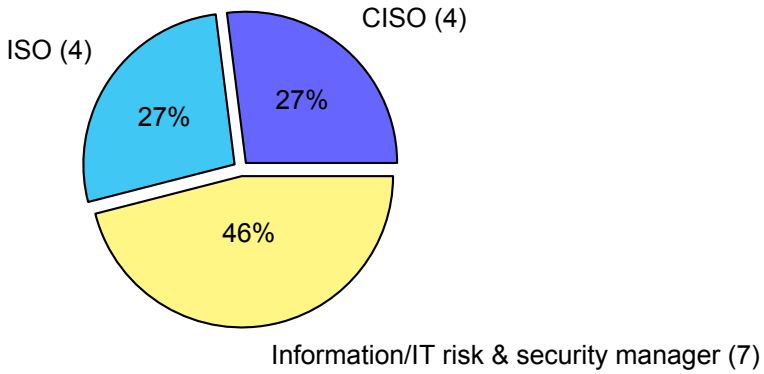


Figure 5.2: The job titles of the respondents (# of respondents)

The sector in which the respondents work are categorised based on their current employment company. Thus although this research draws upon the recollection of experiences from the cybersecurity professional, which can extent beyond the current company, they are categorised in accordance with their current employment situation. Additionally, it is not the intend of this research to generalise over a specific sector, which is therefore not included in the analysis. The synthesis thereby focuses on the experiences of cybersecurity professionals in the different IS risk assessment steps. This allows the findings to be attributed to the perception that cybersecurity professionals have about an organisation's IS environment in the specific steps of a risk assessment, indifferent of the sector.

From the interviews, three (3) respondents are categorised in the service providing sector. Two (2) of the interviewees are categorised in the sector for research & development. The largest sector, a total of four (4), are assigned to the banking & finance sector. In two (2) instances the retail sector is ascribed to the respondent. Only one (1) interviewee was active in the telecommunications sector and

the remaining three (3) were active in the industrial production sector. For an overview please refer to Figure 5.3.

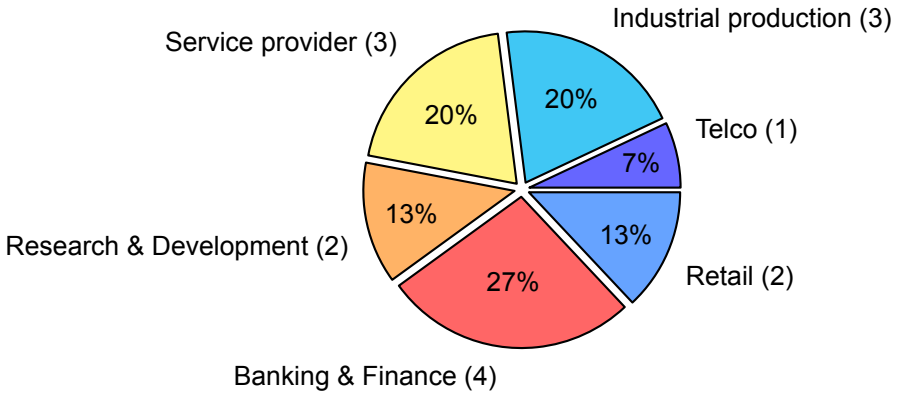


Figure 5.3: The sectors of the respondents (# of respondents)

The sample shows a wide variety of sectors which allows the perception of uncertainty to be attributed to the specific IS risk assessment steps as depicted by the ISO27005 methodology. This creates the opportunity to incorporate the sources of variability for the perceived uncertainty about the IS environment, indifferent of a specific sector, allowing generalisation of the findings to the population of cybersecurity professionals that are actively involved in the execution of IS risk assessments.

5.1.2.1. Language of the interviews

As indicated in Chapter 4, the interviews are conducted in Dutch if the interviewee is Dutch. In total fourteen (14) interviews were conducted in Dutch. One (1) interview was conducted in English with respondent D05.

5.1.3. Respondent involvement in ISRM processes

In Chapter 4 a reference was made to the three lines of defence model in Subsection 4.3.1.2, providing insight into the accountability structure concerning risk management within an organisation. In this research all of the fifteen (15) respondents indicated to be active in the second line of defence and only two (2) indicated to also have a first line of defence role, mostly indicated as duo–role. The second line of defence role prescribes that the respondents are not responsible for the risk itself, but have an active voice in the IS risk assessment and decision-making process due to their expertise with security. They facilitate and provide their professional judgment as input throughout the entire risk management processes together with the risk owners. It could be argued that the two (2) interviewees with a duo–role provide more valuable information. However when discussed with the respondents it was indicated that the backdrop of the ISO27005 methodology is more suited to reasoning from the second line of defence role.

There are two important reasons to take this factor into consideration during the analysis. First, this model caused for some of the respondents to not be involved or were not required to provide their professional judgment throughout all of the risk assessment steps as are interviewed. This created that not all the questions have fifteen (15) responses to them, which will be indicated accordingly per IS risk assessments step. In such a case the analysis is continued with the remaining responses. Second, because they are not the risk owners (business or asset owners), their ability to provide judgment about the organisation's IS environment is partly depending on the input and cooperation from the business side, the first line. The extent of inclusion of the cybersecurity professional in the risk assessment process thus might differ per respondent which is indicated accordingly.

5.2. The perceptual processes — Part 1 of the interview

This section depicts the results on the perceptual processes from the respondents that are directly operationalised with the interview questions of Part 1. Please note that reference made to the perceptual processes will also be depicted per IS risk assessment step if applicable.

The perceptual processes consist out of the individual cognitive characteristics (Subsection 5.2.1), the availability of response options (Subsection 5.2.2) and social expectations from the organisation. Please note (as described in Chapter 4 as well) that the social expectations are not explicitly operationalised with an interview question. Therefore the social expectations are displayed in the different IS risk assessment steps if applicable, identified in accordance with Table 4.1.

5.2.1. The individual cognitive characteristics

The individual cognitive characteristics are analysed from the educational background. From the fifteen (15) respondents, twelve (12) indicated to have been educated to execute information security risk assessments. The education programs mentioned are courses and training programs such as the CISA (Certified Information Security Auditor), CISSM (Certified Information Systems Security Manager), CISSP (Certified Information Systems Security Professional), ISO27001 Lead auditor/ implementer and the IT auditor postgraduate course. When asked whether their education helped them in their role of executing IS risk assessments, all twelve (12) answered that their educational background benefited them. Most notably, six (6) [D08, D09, D10, D11, D14 and D15] out of twelve (12) indicated that their education provided them with an understanding on different IS risk assessment methodologies as well as to think in terms of risks.

From the three (3) respondents that did not indicate to have been educated to execute IS risk assessments, two (2) indicated that this has hindered them in the beginning [D01, D05]. This required them to actively learn on the job after which they indicate to have sufficient knowledge about executing IS risk assessments. Whereas one (1) indicated that there was enough related material to learn from that provided the knowledge needed on how to deal with IS risk assessments [D02].

What is evident from the first analysis on the respondent's individual cognitive characteristics is the importance of education for the execution of IS risk assessments. It shows that 50% of the respondents indicate to benefit from a theoretical foundation because it allows them to think in terms of risks. This is in line with the individual cognitive characteristics item that is determined by how the individual deals with ambiguity, which is a fundamental concept of risk. The theoretical foundation should thereby support the individual in terms of dealing with ambiguity and thus uncertainty during the IS risk assessment. This aspect will be taken into account in the rest of the analysis.

Please note that the theory on perceived environmental uncertainty (PEU) does not describe what the direct relation is between the individual cognitive characteristics and the perception of uncertainty other than it being a source of variability. The individual cognitive characteristics are further synthesised during the rest of the analysis, indicating whether it serves as a reason to be perceive uncertainty about the IS environment.

5.2.2. The availability of response options

The availability of response options refer to the variety of experiences available to the individual. This item of the perceptual processes is operationalised by the experience that respondents have with executing IS risk assessments and ISRM processes. Figure 5.4 provides an overview of categorised years of experience available to the respondents. On the x-axis the different categories for years of experience in IS risk assessments are depicted, on the y-axis the number of participants are displayed per category.

What is evident from this measure of availability of response options is that the average experience (calculated from absolute values of years of experience in executing IS risk assessments) is seven (7) years. It is however important to note that the average is pushed up by D02 who has thirty-three (33) years of experience. This skews the average upwards by two (2) years.

It is critical to acknowledge that the respondents could have other experiences in relation to IS activities. This is however not identified as such and will only be depicted among the results if the respondent has explicitly indicated to rely on such experiences in their perception of uncertainty. Additionally the results show that the eligibility requirements are all met by the respondents, having minimum one (1) year of relevant working experience in executing IS risk assessments.

The analysis on the availability of response options of the respondents shows that the average working experience is seven (7) years. The theory on PEU does not describe what the direct relation is between the availability of response options and the perception of uncertainty other than it being a source of variability. The results for the availability of response options up to this point don't allow any further analysis because there is no question directly related to how the respondent perceives its own

Figure 5.4: The experience of respondents

experience, nor is there a measure defined by the theory. The synthesis is therefore executed in the IS risk assessment steps.

5.3. Risk identification — Part 2 of the interview

This section describes the different steps from the risk identification phase in chronological order as is described by the ISO27005 methodology, including the steps for the identification of assets, threats, existing controls, vulnerabilities and CIA values (Subsections 5.3.1 to 5.3.5).

The results for each step are systematically depicted. The first subsections in each of the risk identification steps is devoted to the empirical findings in relation to the perception of uncertainty, relating to the PEU theory and first sub–question of this research. The second subsection in each of the risk identification steps depicts how cybersecurity professionals provide judgment under the perception of uncertainty, relating to the theory on judgment heuristics and the second sub–question. Each risk assessment step is finalised with a subsection that depicts the concluding remarks and summarises the findings. This depiction of results will also be applicable in Section 5.4.

5.3.1. Asset identification

The process of asset identification is crucial to the information security risk assessment. It states that the process allows the organisation to map the informational assets that are of value to the organisation, i.e. the identification of assets that require protection from threats that could be harmful to the asset and thus the organisation.

5.3.1.1. PEU in asset identification

Not perceiving uncertainty

The respondents were asked if they experienced uncertainty in the asset identification process. From the fifteen (15) respondents, one (1) respondent was not involved in the asset identification process at all [D05]. From the remaining fourteen (14) respondents, six (6) indicated to not feel uncertain in the asset identification process [D01, D02, D04, D07, D08, D11]. The most striking observation is that four (4) out of these six (6) indicated to not feel uncertain based on their experience and knowledge about the business assets and how to deal with them in an IS risk assessment [D01, D04, D07, D08]. This directly relates to the sources of variability for the **individual cognitive characteristics state un-**

certainty — identified from the training/education from the respondents that allows them to deal with ambiguity and risk, see the coding scheme in Table 4.1 — and the **availability of response options** — identified from the years of relevant working experience in IS risk assessments, identified from the coding scheme in Table 4.1. These sources of variability are consequently of influence in the mapping process to not perceive uncertainty about the organisation's IS environment during the asset identification. The other two (2) respondents indicated to not perceive uncertainty because there are clear guidelines for the asset identification [D02] as well as having enough information to identify the assets [D07, D11].

Perceiving uncertainty

The remaining eight (8) respondents [D03, D06, D09, D10, D12, D13, D14, D15] indicated to perceive uncertain during the asset identification process. It is however important to note that their uncertainty was not with the identification of the crown jewels for the organisation, but related to the organisation's *general landscape of information and information systems*. The respondents thereby indicated that the crown jewels are well document and get much attention to ensure the informational security. This is however not the case for the general landscape of information and information systems. In five (5) of the eight (8) responses *shadow IT* was identified as a core theme which creates uncertainty in the asset identification [D03, D09, D12, D14,D15]. Shadow IT refers to information systems that is not registered with the IT or security departments but is in use within the organisation. Please refer to an example response below[1]:

> Nowadays it is of course easy to set up a server with Amazon which you stash with data. Per example, such an application can be purchased that pulls data from our crown jewels into a server but we don't know it is happening. Such an application infringes the crown jewels which in turn creates risk problems. This creates uncertainty for me, because outside of the IT department applications are put into our network that in return bring great risks to our crown jewels because it by-passes our controls. ***(D03)***

Evident from the response is that the current ease with which one can take an external application into use which might affect the crown jewels is a serious issue in accurately identifying one's organisational assets. Because these information systems are not known it is difficult to identify them by the IT and security departments, thereby contributing as a factor for perceiving uncertainty.

Another interesting finding to this step is that the concept of *organisational centralisation* plays a large role in the perception of uncertainty, indicated by six (6) respondents [D03, D09, D10, D12, D13, D15]. This refers to the extent at which an organisation has central procurement for IT applications, as well as the organisational structuring in which the IT department has a supporting role to the rest of the organisation. A lack of overview and involvement from decentralisation creates uncertainty because the departments that are responsible for IS are not always aware of changes made in the organisational information system's landscape. This can be directly related to the issue of shadow IT.

Furthermore two (2) respondents indicated factors for uncertainty to be the completeness of the asset identification, in which they are not sure whether they have identified all relevant assets to the organisation [D10, D14]. As well as one (1) instance of limited time to gather necessary information to determine the interrelations within the organsation's IS environment was indicated to cause state uncertainty [D06].

Understanding the nature of uncertainty and the factors

The respondents were consequently asked to describe the nature of their perceived uncertainty about the IS environment during the asset identification step. All of the eight (8) respondents indicated that it was difficult to determine the exact interrelations among the different components within the IS environment. Please see below an example response that embodies the state uncertainty of the respondents:

> It is not always clear which information systems are in use and what the information streams are, which connections exist and who is responsible. ***(D09)***

[1] Please note that references made to interviews are coming from edited transcripts. Additionally it needs to be taken into account that all interviews are conducted and transcribed in Dutch, except for interview with respondent D05. As such the researcher translated parts of the transcripts to English to provide example material to the reader. Please refer to additional information on data analysis to Section 4.4.

Contributing factors to this perception of uncertainty is by six (6) respondents argued due to the many connections and information streams within the organisation's information system landscape. This in turn makes it difficult to identify the interrelations among assets and if all assets are identified [D03, D09, D10, D13, D14, D15]. An interesting factor identified as a creator of complexity are the *mergers and acquisitions* of an organisation, stressing the asset identification [D13]. Furthermore the data shows that six (6) respondents experience a fast changing organisational landscape of information and information systems as a contributor to the perception of uncertainty. They identified that this is due to many different projects as well as innovation that is happening within the organisation and IT [D03, D09, D10, D13, D14, D15].

This descriptions from the above two paragraphs resemble the definition of **state uncertainty** — defined as the perceived inability to estimate the nature of possible future state changes which can be experienced because it is difficult to understand how components in the IS environment might be changing or what the interrelations are between the components (defined from the terminology in Table 3.2 and identified from the coding scheme in Table 4.1) — as derived from the PEU theory. Additionally the theorised IS environment's characteristics of **complexity** — defined by the large amount of components present in the IS environment which are perceived non–similar by nature (defined from the terminology in Table 3.2 and identified from the coding scheme in Table 4.1) — and **dynamism** — described by the changing nature of the IS environment which is perceived by the degree in which environmental factors change as well as the emergence of new environmental factors (defined from the terminology in Table 3.2 and identified from the coding scheme in Table 4.1) — could be identified from the results which are attributed as sources of variability.

Furthermore from the responses on the nature of perceived uncertainty, one (1) respondent indicates to perceive difficulty in identifying what the impact from the asset identification is on the organisation's future ability to function. Thereby taking into account what the controls were that are implemented and how this consequently affects the organisation's performance as well as ensuring that the identification is correctly executed based on the informational value of the assets [D06].

The respondent [D06] described that the processes and organisational landscape of information and information systems needs to be captured with limited information. This is argued to introduce a lack of transparency in the process, making it difficult to predict the implications from the asset identification. Additionally the respondent [D06] argued that the changing business contexts with the associated assets and its stakeholders create a fluid playing field during the IS risk assessment. The notion of governance is introduced by the respondent, arguing that the governance of stakeholders is a constant process in which the business contexts and associated objectives change that need to be governed properly.

The description from the above two paragraphs on the nature of uncertainty as described by the respondent aligns with the theorised definition and characteristics of **effect uncertainty** — defined as the perceived inability to predict the implications of a given state change in terms of its likely impact for the organisation's future ability to function, referring to the nature, severity and timing of impact (defined from the terminology in Table 3.2 and identified from the coding scheme in Table 4.1). The lack of transparency is argued to create **complexity** in keeping oversight in the organisational landscape of information and information sytems. Furthermore, the fluidity of changing business contexts and the associated stakeholders describe the **dynamism** during the asset identification (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

It is important to note that only one (1) respondent provided an answer that allowed the identification of effect uncertainty. Therefore it is important to consider that this respondent's method of asset identification is heavily relying on the CIA classification. This could be the reason for the identification of effect uncertainty in the answer. Furthermore it is seen in Subsection 5.3.5 that respondent D06 is again referring to effect uncertainty, which is supporting this analysis.

5.3.1.2. Providing judgment when under uncertainty for the asset identification

The eight (8) respondents [D03, D06, D09, D10, D12, D13, D14, D15] that indicated to perceive uncertainty about the organisation's general landscape of information and information systems are subsequently asked to indicate how they provide their judgment when under uncertainty. An interesting observation is the phenomenon of *accountability* for the asset identification. Inline with the three lines of defence model, discussed in Subsection 4.3.1.2, five (5) out of the eight (8) respondents indicated

that the accountability structure does not make them responsible for the assets and subsequent identification, thereby depending on the input from the business [D09, D10, D12, D13, D14].

Furthermore two (2) respondents indicated to take the asset owner's *security awareness and conformity* into account [D03, D06]. This was present in interviews that indicated that the asset identification was depending on the CIA classification (a step that is discussed in a later stage of this chapter). The CIA classification was argued to be partially based on the security awareness and conformity of the asset owner, but the results don't show the influence on the asset identification. Additionally one (1) respondent indicated that the context of the asset and the related *policy and philosophy* was taken into account to identify assets to the organisation [D06].

Finally, the results show that four (4) respondents heavily rely on information provided from databases and application discovery tooling [D12, D15], as well as on the documentation and archives from previous assessments [D13, D14]. Furthermore four (4) respondents indicate to simply *search for additional information* via weekly meetings, interviews with stakeholders or by getting involved in ongoing projects to track the developments in the IS environment [D03, D06, D12, D14]. The results from this paragraph closely resemble the **selective accessibility model**, in which the provided information is assessed to be a suitable answer and where additional information is searched for by the cybersecurity professional (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

5.3.1.3. Concluding remark for asset identification

The asset identification can be considered a step in which cybersecurity professionals perceive uncertainty about the IS environment. In total eight (8) out of the fourteen (14) respondents that were actively involved in the asset identification indicated to perceive uncertainty about the general information and information system landscape of the organisation. Please note none of the respondents experienced uncertainty about the identification of the organisation's crown jewels. The data supports the labelling of state uncertainty to all eight (8) respondents and effect uncertainty to one (1) respondent. This is indicated to be caused by the characteristics of the organisation's IS environment; complexity and dynamism. Important findings to the factors of perceived uncertainty relate to the issue of shadow IT within an organisation, creating a lack of transparency and difficult to determine interrelations. Additionally the amount of mergers and acquisitions executed by an organisation stresses the complexity of the organisation's IS environment. The six (6) respondents that did not perceive uncertainty in the asset identification step were mainly motivated by having enough knowledge and experience, relating to the individual cognitive characteristics and the availability of response options as a reason to not perceive uncertainty about the IS environment. What is apparent to the risk identification step is that there is a clear division between the sources of variability from the adapted model from Downey et al. [20] in Figure 3.2. The perceptual processes cause respondents to not perceive uncertainty, whereas the characteristics of the IS environment do create a perception of uncertainty about the organisation's IS environment. Please refer to Figure 5.5 for a generalised overview of the responses in relation to the concept of PEU.

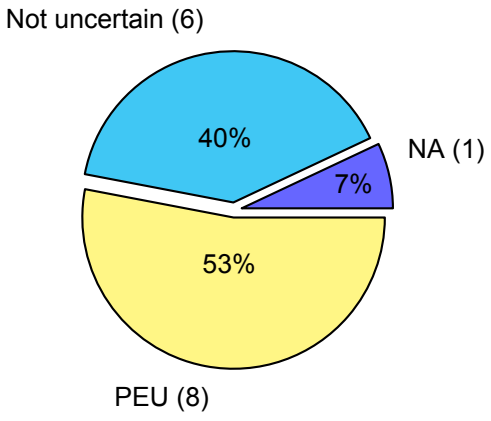


Figure 5.5: Uncertainty in asset identification

The results for judgment operations in the asset identification suggest that respondents closely align with the selective accessibility model in which the provided information forms the basis upon which they perform the asset identification. Thereby the information provided allows the respondents to deal with the complexity and dynamism in the organisational landscape of information and information systems to provide input on the judgment problem.

5.3.2. Threat identification

During the threat identification it is important that the relevant threats to the organisation's information and information systems are identified. Allowing the organisation to map the sources of harm to their IS environment.

5.3.2.1. PEU in threat identification

Not perceiving uncertainty

After the respondents briefly described how they identified the threats for the organisation, they were asked if they experienced uncertainty in the process. Out of the fifteen (15) respondents, one (1) respondent was not involved in the process of threat identification, as this was executed by a special cyber threat intelligence department [D11]. In total nine (9) out of the remaining fourteen (14) respondents did not perceive to be uncertain [D02, D03, D04, D08, D09, D10, D13, D14, D15]. The use of *security standards and frameworks* was indicated by three (3) respondents as a factor to not perceive uncertain about the threat identification [D08, D09, D15]. Additionally, input from a security operations centre (SOC) or industry threat intelligence caused three (3) respondents not to perceive uncertainty because this provided real–time and up-to-date threat information [D10, D13, D14]. Furthermore it was argued that common sense, experience as well as knowledge about the working of the controls causes them to not perceive uncertainty about the threat identification for their IS environment. Thereby it is again striking that four (4) out of nine (9) respondents indicated to not perceive uncertainty because of perceptual processes, the **individual cognitive characteristics** and the **availability of response options** [D02, D03, D04, D14] (please refer to Table 4.1 for the identifiers from the coding scheme).

Perceiving uncertainty and understanding the nature and factors

The remaining five (5) respondents [D01, D05, D06, D07, D12] indicated to perceive uncertainty during the threat identification process. They argued that there is the lack of *reference material* that allows comparison of threats typical to the type of organisation [D06]. This lack makes it difficult to predict the nature and severity of impact. Additionally the respondent indicated that it is difficult to predict if the organisation is an interesting target, creating overall uncertainty with the threat identification which can be directly related to the lack of reference material. Furthermore one (1) respondent indicated a factor of uncertainty to be the completeness of the threat identification. Thereby relating to the integrality of all the relevant threats to the organisation [D14].

Furthermore all of the five (5) respondents indicated that it was difficult to predict the impact from threat events in the organisation's IS environment. Thereby referencing to how a threat event causes damage to the organisation and what the magnitude will be. This entails difficulty in predicting the the type of threat, as well as the severity of impact. Please see below an example response indicating the effect uncertainty:

> But the uncertainty remains whether it is an actual threat to the asset. It can for instance be that threat is an issue for many organisations, but not necessarily to us, but just because of the volume of assets it can be still be a threat to our organisation. So we can not discount it, but we can also not prove it to be a threat. ***D05***

Three (3) respondents argue that the organisational landscape of information and information systems is complex, making it difficult to assess the relevance of threats to the assets [D05, D07]. This could well be enhanced by the argument that the organisational landscape of information and information system is perceived to be large and having many interrelations which hinders the analysis [D01, D05]. Additionally three (3) respondents describe the organisational IS environment knows many changes, which are attributed to the technological development as well as the threats adapting to technology and environmental changes [D01, D05, D12]. It is interesting to note that one (1) respondent indicated threats can also be hiding with the *innovation processes of the organisation* itself. Because this process has a high pace and is not always transparent, risks can go undetected within the organisation's innovation processes [D01].

Derived from the descriptions of the above two paragraphs, the theorised definition on **effect uncertainty** seems present as the type of PEU. Additionally the sources of variability on **complexity** and **dynamism** was attributed by the respondents as a factor of uncertainty (please refer to Table 3.2 for the definitions and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

5.3.2.2. Providing judgment under uncertainty for the threat identification

Subsequently to the identification of uncertainty about the IS environment, the five (5) respondents [D01, D05, D06, D07, D12] were asked to indicated how they provide judgment under uncertainty to identify possible heuristics. Furthermore four (4) respondents indicated that they stay close to the industry/market standards or heavily rely on the input from cyber threat intelligence that comes from the SOC of threat intelligence leaders. The respondents indicated to use the information that was provided to them and assessed the applicability of the input to the threat identification process. [D01, D06, D07, D12]. Additionally, the respondents indicated that the enterprise model is heavily relied upon that allows the cybersecurity professionals to stay close to the organisation's defined standards [D01].

The above paragraph describes judgment operations that show strongly conform to the **selective accessibility model**, because the respondents indicate to heavily rely on the information that is provided as input. The assessment of the provided information consequently shows, as defined by the respondents, that they stick around the values provided as they are considered suitable (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

5.3.2.3. Concluding remark for threat identification

Evident is that four (4) out of the nine (9) respondents do not perceive to be uncertain due to perceptual processes, because they perceive to have enough experience with the threat identification process and knowledge about the controls that should prevent the threats from becoming harmful. This is similar to Subsection 5.3.1, showing that conceptualised individual cognitive characteristics and the availability of response options is are factors that prevent the perception of uncertainty.

Five (5) out of the fourteen (14) respondents who indicate to experience uncertainty argue that the lack of transparency and the many interrelations within the organisation's information and information system landscape contribute to complexity. This makes it difficult to assess the possible impact of threats to the organisation. Additionally, the threats are considered to be adaptive, taking up new technologies and keeping up with the changes. Additionally the organisation's innovation processes progress quickly and are not always transparent which allows unintentional threats to go undiscovered. This processes create a dynamic factor to the perception of uncertainty that are in line with the theorised definition on effect uncertainty. Please refer to Figure 5.6 for a generalised overview of responses.

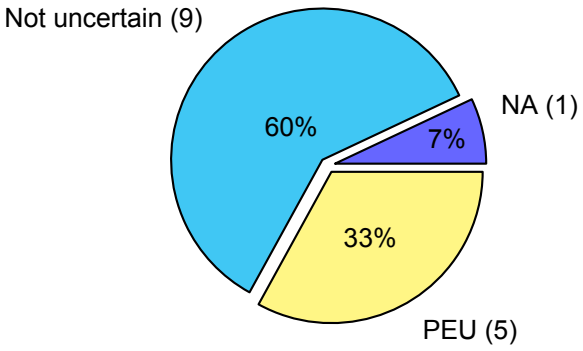


Figure 5.6: Uncertainty in threat identification

The remaining respondents indicated to actively assess and use the input that is provided to them from market/industry standards, the SOC and cyber threat intelligence. Thereby closely resembling the conceptualisation of the selective accessibility model. What is however striking, is that the use of provided input from market/industry standards and cyber threat intelligence is also ascribed by six (6) respondents who did not perceive uncertainty. Which could be an indication that the selective

accessibility model is also at work even though respondents indicate to not perceive uncertainty. There is however no data that further supports this analysis.

5.3.3. Identification of existing controls

The identification of existing controls is pivotal in IS risk management, allowing an organisation to map the current working state of the existing controls that protect the assets from harm.

5.3.3.1. PEU in identification of existing controls

Not perceiving uncertainty

Out of the fifteen (15) respondents, two (2) respondents indicated that their method of IS risk assessment did not explicitly incorporate the step of identifying existing controls as described by the ISO27005. An important observation to their responses is that both indicated that they are not working from a compliance domain, thereby taking a different approach to the IS risk assessment [D09, D10]. From the remaining thirteen (13) respondents, seven (7) indicated to not perceive to be uncertain in the identification of existing controls [D01, D02, D03, D04, D06, D11, D15]. What is seen as a recurring theme is that the three (3) out of these seven (7) respondents perceive not to be uncertain based on their experience as well as knowing on how to deal with the risks that are associated to the controls. This aligns with the **individual cognitive characteristics** and the **availability of response options** which causes them to not perceive uncertainty about the IS environment [D01, D02, D03] (please refer to Table 4.1 for the identifiers from the coding scheme).

What is prevalent in the answers given by the respondents is the reliance on the *three lines of defence model*. It is indicated by three (3) respondents that the tracking and mapping of existing controls is the responsibility of the risk owner and that their role is to advise, thereby not perceiving uncertainty [D04, D06, D13]. Another striking observation is that for seven (7) respondents the perception of uncertainty is limited/absent due to the *reliance on security standards and organisational frameworks* in which the controls are standardised [D01, D04, D06, D08, D11, D13, D15].

What is however apparent from the findings in the previous two paragraphs is that two (2) of the respondents [D08, D13] also indicated to perceive a form of uncertainty about the IS environment. These contradicting statements are therefore carefully interpreted and analysed over the following paragraphs.

Perceiving uncertainty and understanding the nature and factors

The remaining six (6) respondents indicated to perceive uncertainty during the identification of existing controls [D05, D07, D08, D12, D13, D14]. For the identification of existing controls the theme around *shadow IT* was highlighted by two (2) respondents, indicating that applications were designed with controls integrated without the IT department knowing about it [D12]. But also in relation to the asset identification, shadow IT that exploits previous control configuration management make it difficult to identify the existing controls [D14]. Furthermore two (2) respondents indicated that the vagueness of the control description makes it difficult to identify the existing controls, making it hard from a compliance perspective to accurately interpret the controls as specified [D05, D12].

The six (6) respondents indicated to experience difficulty in examining the existing interrelations between controls and the organisation's assets. Thereby focussing on how they work, if they work properly, if there are possible duplicates or if certain controls might annul one another. Please see below an example response indicating state uncertainty:

> To get an overview for all the layers of control is very difficult. You often know what controls are within a domain, but if you want to know it for one application and a specific stack then one push of the button will not provide you all information. If you want to know this you need to dive deeper into the control layers, but this cannot always be answered within a risk assessment. ***D07***

In total five (5) respondents argued that the organisation's general landscape of information and information systems has many different components with many interrelations. This prevents the cybersecurity professional from having a clear overview to identify the existence and applicability of the existing controls to the landscape [D05, D14]. Furthermore it was argued that the many interrelations create difficulty in identifying the functionality of the existing controls [D05, D07, D08]. Additionally it was argued that the *decentralised character* of the organisation creates difficulty in identifying the responsible stakeholders within the organisation or in relation to the external vendor [D13].

Additionally two (2) respondents argue that the organisation's general landscape of information and information systems is subject to many changes that are caused by the developments in IT, *organisational innovation* and the rise of *shadow IT* which make it difficult to identify the existing controls and their workings state [D07, D14].

The above three paragraphs are aligned with the theory on PEU and closely resemble **state uncertainty** being present with the cybersecurity professionals in identifying the organisation's existing controls. Furthermore it is seen that the IS environment's characteristics of **complexity** and **dynamism** can be attributed to cause the experienced uncertainty (please refer to Table 3.2 for the definitions and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

What is evident from the responses of D08 and D13, is that although their role and the use of standards enables them to accurately identify the existing controls, there remains a form of state uncertainty that revolves around the interrelations between the components within the IS environment. The key point to take away from this observation, is that the perception of uncertainty about the IS environment can be present in an advising role in an organisation that relies on standards. This can consequently influence the way in which cybersecurity professionals perceive to be able to accurately identify or estimate items of the organisation's IS environment.

5.3.3.2. Providing judgment under uncertainty for the identification of existing controls

The answers from respondents who identified to experience uncertainty are analysed for their judgment operations. What is evident is that an evidence–driven approach is adopted that eliminates the need for judgment from the cybersecurity professional. This evidence–driven approach is based on tooling and testing that identifies and assesses the working state fo the existing controls. Four (4) respondents indicate to adopt such an evidence–driven approach in which the control design, objective and effectiveness is tested [D05, D07, D08, D14]. Furthermore one (1) respondent indicates that the identification of existing controls is depending on the input the control owner provides during the process, effectively referring to the *accountability structure* within the organisation [D12].

Evident from the responses, it can be seen that the judgment operations from the cybersecurity professionals are limited to non–existing. This is caused by the evidence–driven approach which contradicts the premise of judgment heuristics, where theory states that judgment is provided based on data/information of limited validity (i.e. data/information that is not true by definition). Whereas above can be seen that the identification is largely relying on the evidence provided. Consequently the researcher argues that theory on judgment heuristics does not provide additional insights into the judgment operations during the identification of existing controls.

5.3.3.3. Concluding remark for the identification of existing controls

The step for the identification of existing controls identifies six (6) out of thirteen (13) respondents to experience uncertainty. The argue that the organisation's landscape of information and information systems knows many interrelations. Furthermore the organisation's decentralised character makes it difficult to grasp all interrelations, which together creates complexity. Additionally the organisation's landscape of information and information systems is perceived to be rapidly changing due to the developments in IT, innovation in the organisation and shadow IT. This creates a dynamic factor. Together these factors are describing state uncertainty. A recurring theme for not experiencing uncertainty comes from the reliance on experience and knowledge on how to deal with the identification of existing controls, attributing the individual cognitive characteristics and availability of response options.Please refer to Figure 5.7 for a generalised overview of the responses in relation to the concept of PEU.

The judgment operations could not be assessed in this step because an evidence–driven approach is taken, removing judgment from the cybersecurity professional.

5.3.4. Identification of vulnerabilities

The identification of vulnerabilities for an organisation's IS environment is critical to prevent exploitation by threats, thereby minimising the risk to the organisation.

5.3.4.1. PEU in vulnerability identification

Not perceiving uncertainty

The respondents have all been asked to describe how the vulnerabilities within the organisation's IS environment are identified. What is striking is that all fifteen (15) respondents show to take an *evidence*–

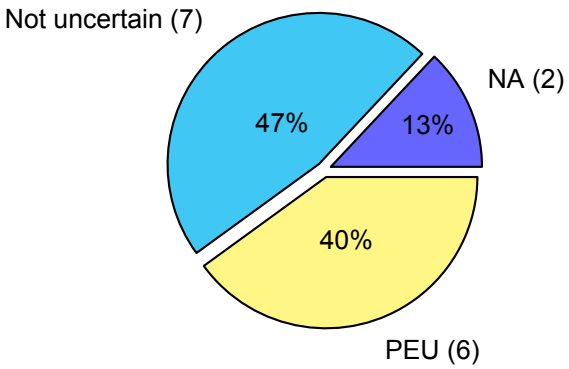


Figure 5.7: Uncertainty in the identification of existing controls

driven approach. Thereby relying on tooling, audit reports and other methods of testing that provide evidence for the existence of vulnerabilities within the organisation's IS environment. The use of scenario development methods to identify vulnerabilities is significantly less and is identified with only six (6) out of the fifteen (15) respondents [D03, D07, D08, D11, D14, D15]. What is key here is that the *reliance on evidence* plays a large role for the cybersecurity professional, which is arguably very logic in a world that is full of ambiguity.

After the respondents briefly described how they identify the vulnerabilities to the organisation's IS environment, they were asked whether they perceived uncertainty while doing so. From the fifteen (15) respondents six (6) respondents indicated to not perceive any uncertainty in the process [D02, D03, D04, D05, D07, D10]. Factors ascribed to this perception again heavily rely on the *evidence–driven approach*, being guided by facts from vulnerability tooling and tests. This reliance on evidence is interesting in relation to the theoretical concept of PEU in which the individual cognitive characteristic and the availability of response options previously played a significant role in most of the risk identification steps. The researcher therefore argues that the cybersecurity professional perceives to be certain from the evidence provided from unambiguous sources.

Perceiving uncertainty and understanding the nature and factors

From the remaining ten (9) respondents, one (1) respondent described to experience uncertainty because it was not sure what the severity of impact was from the vulnerability in the organisation's IS environment. The respondent indicated it was difficult to interpret the impact from the vulnerability scanning tools in relation to the organisation's IS environment [D09]. Please refer to a section of the response below:

> The uncertainty comes from the interpretation of the severity ranking of the vulnerabilities identified by the tooling. That is the reason why we currently follow the severity ranking of the tooling or party that delivers the information to us. ***D09***

The respondent argued that organisational IS environment has many different interrelations within the information and information systems landscape as well as with the threat landscape. The combined factors influence the severity if the vulnerability is exploited, which is hard to predict. This is considered difficult to identify and getting all information necessary would be almost impossible [D09].

Derived from the above two paragraphs, the theorised definition on **effect uncertainty** could be attributed to the respondent answers. Arguing it that it is difficult to predict the severity of impact. Factors ascribed by the respondent revolve around the **complexity** of the organisational IS environment, looking at the interrelations of information systems together with the threat landscape. Thereby the complexity characteristics from the IS environment is attributed (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

As indicated previously, all respondents take an evidence–driven approach to the vulnerability identification. This reliance on the vulnerability tooling and testing consequently creates a different dimension of uncertainty, one that is not in relation to the theory on PEU as is conceptualised for this research. For eight (8) respondents the issue of *integrality* for the identification of vulnerabilities was identified. It was indicated by the respondents that there was always the question if all essential vulnerabilities are

identified for the organisation's IS environment. Consequently it was indicated that the cybersecurity professional always assumed that there are vulnerabilities that are unknown to them. Additionally the severity and number of the vulnerabilities was indicated to be unknown as well. These unknowns were attributed to the possible lack of tooling/testing accuracy. Furthermore it was often referenced that there are previously undiscovered opportunities to attack that undermine the vulnerability identification (zero-day attacks). This consequently brings the identification of vulnerabilities on a path of unknown–unknowns. The researcher adopts the term of *unfathomable uncertainty* Kim [41], who first coined the term and has provided the characterisation. It is however important to note that this uncertainty is only applicable to the vulnerabilities that have not been identified by the vulnerability tooling and tests. This creates a dual–dimension for the vulnerability identification: (1) that is solely based on evidence (2) and another dimension that is categorised with *unfathomable factors of integrality*. The latter dimension is the cause for the perception of uncertainty in the vulnerability identification and is therefore described as *unfathomable uncertainty* from integrality [D01, D06, D08, D11, D12, D13, D14, D15].

5.3.4.2. Providing judgment under uncertainty for the vulnerability identification

Evident from the respondents who indicated to perceive uncertainty, is that the judgment operations are not present in this step. One (1) respondent [D09] indicated to incorporate the identified severity of the vulnerability tooling into the process as the truth of impact to their organisation.

Although the judgment is thus not provided in this step, as can be seen from the evidence–driven approach, it is interesting to highlight how the remaining eight (8) respondents subsequently deal with the uncertainty experienced. Interestingly, as indicated by the six (6) respondents who didn't perceive uncertainty, the remaining (8) also rely fully on the evidence provided from the tooling, tests and reports to identify the vulnerabilities in the organisation's IS environment. Furthermore it is emphasised by three (3) respondents that partial blindness with respect to unknown vulnerabilities has to be accepted because you can't know or detect all vulnerabilities [D01, D08, D15]. Furthermore it was indicated by three (3) respondents to rely on the *security strategy and associated philosophy* that is focused on detection and response, rather than prevention [D01, D06, D08].

5.3.4.3. Concluding remark for the vulnerability identification

The identification of vulnerabilities is marked by an evidence–driven approach. Effect uncertainty was identified for one (1) respondent who indicated to perceive uncertainty on how the vulnerability impacts the organisation's IS environment. The source for this uncertainty resides in the complexity of the organisation's IS environment. What is striking is that only one (1) respondent answer resembles a type of theorised uncertainty. This can arguably be caused from the evidence–driven approach which eliminates the *mapping process* about the IS environment, thereby eliminating judgement operations.

Eight (8) respondents also indicated to experience uncertainty due to unknown–unknowns that reside in the unknown if all vulnerabilities are identified as well as the unknown severity from the identified vulnerabilities. The term of unfathomable uncertainty from integrality was attributed to the experienced uncertainty. Please refer to Figure 5.8 for an overview on the uncertainty findings for the vulnerability identification.

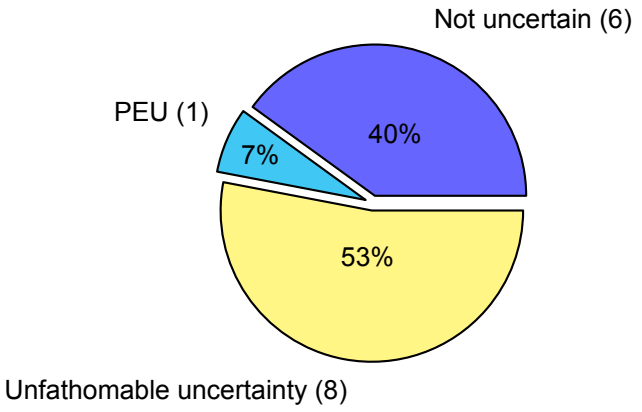


Figure 5.8: Uncertainty in the vulnerability identification

Additionally it is observed that the evidence–driven approach based on tooling and testing causes the judgment operations of the cybersecurity professional to be eroded from the process. Additionally it was mentioned that the partial blindness of not knowing all vulnerabilities has to be accepted. Furthermore a paradigm shift in the security strategy and philosophy that focuses on detection and response was pivotal to deal with the unknown–unknowns.

5.3.5. Identification of CIA values

The asset classification for confidentiality, integrity and availability (CIA) is an important component of an IS risk assessment, providing an information value classification.

5.3.5.1. PEU in CIA identification

Not perceiving uncertainty

The respondents were asked if they experience uncertainty during the CIA classification of the organisation's assets. A total of three (3) respondents indicated that this wasn't executed by them [D01, D04, D10]. From the twelve (12) respondents involved in the CIA identification, six (6) indicated not to perceive uncertainty in the process [D02, D03, D07, D08, D09, D14]. In total five (5) of these respondents indicated implicit and explicit that their experience causes them not to be uncertain. Indicating that the correct CIA classification in IS risk assessments is often obvious and pre–determined [D02, D08, D14]. Additionally a reference was made to the traction needed within the organisation, stipulating the importance of moving away from the theoretical approach and that practical relevance was key [D07]. Furthermore experience in risk management itself was indicated to not perceive uncertainty in the process [D03]. One (1) respondent indicated that their modular method for assigning the CIA values provides them with the desired overview necessary [D09]. These responses closely align with the theorised **availability of response options**, i.e. their experience, as a source to why respondents don't perceive uncertain (please refer to Table 4.1 for the identifiers from the coding scheme).

Perceiving uncertainty and understanding the nature and factors

The remaining six (6) respondents have indicated to perceive uncertainty during the CIA identification [D05, D06, D11, D12, D13, D15]. A core theme for the perception of uncertainty is indicated to be a *misfit between guidelines and the business*, making the grey areas a difficult topic. These grey areas can be defined as the misfit between the purpose of information and the information itself. If the purpose of the information is to identify people, and the information does so, there is a fit. However, if the purpose is to describe business processes, but it additionally identifies people, there is a misfit which makes it hard to classify the CIA values for the information asset because a point of discussion arises for the controls necessary for that asset. This was identified by four (4) out of the six (6) respondents [D05, D12, D13, D15]. Other reasons for the uncertainty was the general lack of information [D11] and the constantly changing business context of assets with limited information creating uncertainty [D06]. What is important to note for the perception of uncertainty here is that it is *only applicable to the grey areas*, where obvious choices are absent. This is similar to the asset identification in which it only concerns the general landscape information and information systems as opposed to the crown jewels.

The six (6) respondents argued that it was difficult to determine the importance of the general landscape of information and information systems. Identifying that it was difficult to determine the impact from a data breach and the organisation's future ability to function. This relates to the nature and severity of the impact. In total four (4) respondents argued that the general landscape of information and information systems is complex because there is a lot of data processed that passes many different applications that are all connected throughout the landscape [D05, D11]. Furthermore the organisational context and its politics create difficulty in classifying the CIA values for the organisation's assets. Arguing that the stakeholders are aware of the consequences inflicted on the business processes by additional controls that are depending on the CIA classification [D06, D13]. Additionally four (4) respondents argued that the constantly changing business context is perceived to influence their experience of uncertainty. Indicating the business context is highly variable on the asset owner they work with [D06, D11]. Furthermore it was argued that the asset itself is not set in stone, meaning that its content can be *highly dynamic* which can create issues with the CIA classification [D05, D12].

Based on the results described in the above paragraph, the PEU theory can be used for analysis. Identifying **effect uncertainty** from the difficulty in predicting the impact, relating to the nature and severity. The respondents also attribute **complexity** and **dynamism** in the organisation's IS environ-

ment as factors to the perception of uncertainty, i.e. the sources of variability as theorised (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

Evident from the interviews was that organisations have the asset and CIA identification interwoven, creating a strong link and pragmatic approach to the IS risk assessments. Reviewing the results from the asset identification and the CIA identification, it can be consequently argued that the *interwoven nature* creates one IS risk assessment step for many organisations. This argument is based on the defining indicators from the respondents who: (1) clearly state that it only relates to the grey areas for the CIA identification, which is similar to uncertainty perceived in the asset identification about the non–crown jewels (the organisation's general landscape of information and information systems) and (2) that the description of the IS environment characteristics, the complexity and dynamism, show similar factor descriptions. Furthermore an overlap of four (4) respondents is seen in both steps. This observation of an *interwoven identification process* consequently allows the argument that, if the CIA and asset identification can be seen as one step, these two steps combined are subject to two types of PEU: effect and state uncertainty. This is however not the premise of this research due to the methodology used which relies on the ISO27005 methodology. But it is an important observation and therefore highlighted as such, because this stresses the uncertainty that is perceived by the cybersecurity professionals in relation to the identification and classification of the organisation's IT and information assets.

5.3.5.2. Providing judgment under uncertainty for the CIA identification

The six (6) respondents who indicated to perceive uncertainty about the CIA identification, thereby noting that this reflects the grey areas of the organisation's general landscape of information and information systems, are asked how they provide judgment under uncertainty to identify the use of heuristics.

In total three (3) respondents indicate to actively compare classifications of assets that are seen as similar in providing judgment. Although argued this provides transparency and unambiguous classifications, they do note that situations can change and that the guided approach taken differs per case [D06, D13, D15]. Based on the theorised judgment heuristics, this judgment operation can be aligned with the **representativeness heuristic** due to the active comparison of the perceived similar subject (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

Furthermore it was observed that one (1) respondent indicated to incorporate large cyber incidents that have unfolded over in the past, highlighting the possibility of an event in the process. As an example a ransomware case was used in the respondent answer [D15]. This response seems to align with the **availability heuristic** in which large events now quickly come to mind in the judgment processes (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

Finally one (1) respondent indicated that judgment was based on the feeling with the asset and thus the CIA classification [D12]. The theorised judgment heuristics do not provide additional insight into the judgment operations. The revisited theory by Kahneman and Frederick [38] describe the affect heuristic that determines that people provide judgment based on the affective feelings towards the subject under judgment. However, the data doesn't provide insight into the affective feelings, but rather that it is matter of the feeling the respondent has with the asset.

What is again prevalent, as was in the asset identification, is the *accountability structure* within the organisation that is of importance within the CIA classification. Three (3) respondents referred to this accountability structure which is in line with the three lines of defence model. One respondent indicated that the person accountable provided insight into the importance of the asset and thus the CIA classification and was thereby provided insight into the business value [D11]. Furthermore it was indicated that the final responsibility for the CIA identification was not with them, where the responsible person makes final call. This resulted in data that did not provide further insight into the judgment operations [D12, D13].

Finally, one (1) respondent based their judgment on the *development of a worst case scenario* for the asset in question. Thereby the asset was assigned the worst case scenario CIA classification, allowing the respondent to be certain about the associated controls that would be assigned to the asset based on this classification [D05]. What is again striking from this particular answer is the *interwoven relationship* between the CIA and asset identification on which the organisations subsequently base their controls.

5.3.5.3. Concluding remark for CIA identification

During the CIA classification of the general landscape of information and information systems, six (6) out of thirteen (13) respondents indicated to experience uncertainty. It was indicated that there could be a misfit between guidelines and the business itself. Additionally the many applications and information within the landscape together with the interconnected nature is considered a factor. Additionally the changing content of assets and that are under control of asset owners with constantly changing business contexts are also attributing to the problem. The theorised effect uncertainty accurately describes the nature of uncertainty experienced, arguing it is difficult to identify the nature and severity of possible impact from a breach or to the organisation's business processes. What is again seen for the perception of uncertainty is that the availability of response options, i.e. the experience within risk assessments, are a primary reason for the cybersecurity professional to not perceive uncertainty. This was indicated five (5) times. Please refer to Figure 5.9 for a generalised overview on the findings in relation to the PEU concept.

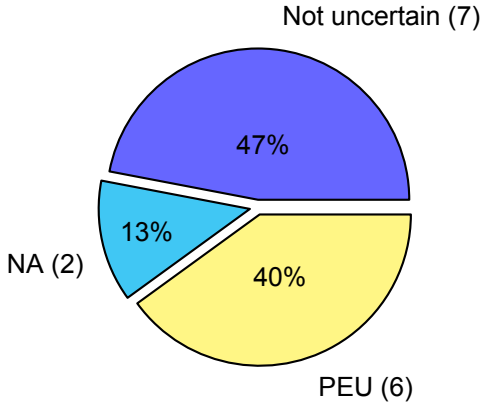


Figure 5.9: Uncertainty in the CIA identification

The judgment operations described by the cybersecurity professional revolve around the active comparison of assets that are perceived to be similar to the subject under judgment. Furthermore reference was made to large materialised incidents that were incorporated in the judgment process. Thereby referencing to the representativeness and availability heuristic in the CIA classification.

An important insight to this step is the interwoven relation between the asset and CIA identification steps, showing that the asset identification is heavily relying on the CIA classification. This could arguably create two types of uncertainty, state and effect uncertainty, for the cybersecurity professional in relation to the identification and classification of the organisation's assets. When the two steps are analysed combined, the findings with regard to the IS environment characteristics show a relation to the most important finding from the asset identification step. That step circled around the insight of the influence of shadow IT with the organisation's general landscape of information and information systems. What is pressing to that matter is that shadow IT entails that the cybersecurity professional is not aware of it, making the classification an issue. As such the shadow IT is frustrating multiple facets of the IS risk identification that are pivotal to the organisation's security. This consequently emphasises the influence of shadow IT throughout the risk identification and subsequent outcomes of the IS risk assessments.

5.4. Risk analysis — Part 2 of the interview

This section describes the different steps from the risk analysis process, consisting out of the first two steps as described by the ISO27005 methodology. This section includes the business impact value analysis and the likelihood analysis steps (Subsections 5.4.1 and 5.4.2).

5.4.1. Business impact value analysis

The analysis of the business impact value is a crucial step for an organisation to determine the financial risk to which it is exposed.

5.4.1.1. PEU in the business impact value analysis

Step not executed

From the fifteen (15) respondents, four (4) indicated that the analysis of the organisation's business impact value was not executed [D06, D08, D12, D15]. Although the respondents referenced the difficulty of estimating the damages resulting from impact, the actual costs are not expressed in monetary terms. What was striking from one (1) of the respondent's answer as to why the business impact value was not calculated, is the reference to the *organisation's strong entrepreneurial spirit* that stipulates that risk taking is part of the business. This directly links to the theorised **social expectations** from the organisation, denoting that the socialisation process of the organisation has influenced the execution of the IS risk assessment steps [D06]. Two (2) respondents indicated that this would just be a *crazy calculation without actual meaning* because the uncertainty was perceived too big, additionally this step *lacks priority* within the organisation [D08, D15]. Furthermore reference was made to the *maturity level* of the organisation for this step not to be executed by one (1) respondent [D12] (please refer to Table 4.1 for the identifiers from the coding scheme).

Another group of four (4) respondents indicated to not execute this particular step because it is the responsibility of the business, thereby referring to the organisation's *accountability structure* that prevents cybersecurity professionals to take ownership over the estimates on the business impact values [D02, D07, D10, D11].

Integrating CIA identification and business impact value analysis

What was additionally prevalent, is the *integration of the CIA classification step and the business impact value analysis*. Two (2) respondents indicated that this step was not executed explicitly in the scenario–approach as described by the ISO27005. But that the impact was integrated in the CIA classification to provide guidelines to determine the controls necessary for the assets [D03, D09].

Perceiving uncertainty and understanding the nature and factors

What is an important observation to this IS risk assessment step, is that the ten (10) respondents that either don't follow this step, are not responsible or have integrated it with the CIA classification, all referenced to a form of uncertainty that aligns with the theorised form of **effect uncertainty**. They all indicated that it would not be possible for them to assign accurate estimates to the business impact value from a cyber incident. Thereby stipulating the effect uncertainty present about the organisation's IS environment for this step even though it was not executed as such [D02, D03, D06, D07, D08, D09, D10, D11, D12, D15] (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

The remaining five (5) respondents indicated to perceive uncertainty during the analysis of the business impact value [D01, D04, D05, D13, D14]. Two themes have been identified, which are superfluously described within the literature of IS. Two (2) respondents indicated that a *lack of unambiguous data* on the financial costs from an incident make it difficult to estimate what the business impact value is [D01, D13]. The second theme, which is closely related to the first theme, circles around the *generalisation of scenario's*. This stipulates the uniqueness factor of incidents, effectively creating a lack of unambiguous data that prevents the respondent to estimate the impact accurately. As a consequence there is no unambiguous data available that allows the cybersecurity professional to create accurate estimates [D04, D05, D14]. These remaining five (5) respondents described that they consequently weren't able to accurately estimate the nature and severity of impact to the organisation resulting from a cyber incident. Please see an example below:

> It is not possible to accurately estimate the business impact value because every situation is very unique. Not a single scenario is the same, so you can't say what will happen. Therefore you also can't generalise the risk, but this is still often done because otherwise the risk can't be overseen any more. To reduce the complexity, risks are combined, but that provides huge amounts of uncertainty because it is simply not clear. In one situation the impact is much bigger than in others. ***(D04)***

Three (3) respondents described that many different factors in the IS environment, relating to the asset value, the controls in place and the way in which threats utilise and disclose data, dtermine the impact from an incident. This causes the inability to accurately estimate the impact to the organisation [D01, D14]. Furthermore it was argued that the landscape of information and information systems has many different components and interrelations, which is consequently of influence in accurately

estimating the impact [D05, D14]. Additionally one (1) respondent argued that the changing contexts and continually differing scenarios makes it difficult to generalise the impact from certain risks. Thereby arguing every scenario is unique and difficult to provide accurate predictions to [D04].

The above two paragraphs closely resemble the theorised concepts of **effect uncertainty**, relating to the difficulty in predicting the nature and severity from impact to the organisation. The organisation's IS environment's characteristics of **complexity** and **dynamism** are both attributed the experienced uncertainty, aligning with the concept to explain the uncertainty experienced (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

A striking observation in this step is that none of the respondents indicated to not perceive uncertain based on their individual cognitive characteristics or their availability of response options. This could be explained by the highly subjective process associated to this step, stemming from the lack of unambiguous data.

5.4.1.2. Providing judgment under uncertainty for the business impact value analysis

Although all interviewees referenced to effect uncertainty in their responses, only the answers from the five (5) respondents who indicated to actively be involved in the process and experience uncertainty were analysed for how they subsequently provided judgment. The results show that one (1) respondent uses provided information on materialised incidents as a starting point in the analysis. Thereby actively assessing the correctness of the input provided in relation to the specific scenario. However, the respondent noted that this is very difficult to do from a risk perspective, stipulating the difference between an incident (a materialised event) and a risk (the possibility of an event materialising) [D04]. Furthermore four (4) respondents indicated that the provided information from experts and business stakeholders was used on the accuracy in relation to the scenario and as such incorporated. It must however be noted that the *accountability structure* of the organisation was again argued to leave the final call with the business owners [D04, D05, D13, D14].

The judgment heuristics that align with the described judgment operations of the respondents is the **selective accessibility model**. It shows the respondent actively uses the information provided to them, indifferent from the providing source, and assesses the values to be an accurate answer to the analysis of the business impact value (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

5.4.1.3. Concluding remark for the business impact value analysis

The business impact value analysis is a step in the IS risk assessment which is marked as the step in which uncertainty is unambiguously present for the cybersecurity professional. Although only five (5) respondents are actively involved in the process of estimating the business impact value, the theorised form of effect uncertainty could be attributed to all fifteen (15) respondent answers. They all indicated that it was very difficult to determine what the severity from incidents would be on the organisation.

The most important insight gained from this particular step is that six (6) respondents indicated that within the organisation business impact value analyses are not explicitly executed. Reasons for this are ascribed to a lack of priority, the organisational maturity level and, linking to the theory on PEU, the social expectations in the organisation that is inspired by entrepreneurial spirit. Additionally the step is seen to be integrated with the CIA classification to serve more as a guideline, rather than to calculate the risk to the organisation. Again the accountability structure within the organisation has four (4) respondents not actively involved in the process of estimating the business impact value.

The remaining five (5) respondents argued that many different factors within the IS environment determine the impact of an incident adds to the perception of uncertainty. Additionally one (1) respondent highlighted the importance of the dynamic context, creating issues with the generalisability of scenarios due to the uniqueness involved with each risk scenario, creating difficulties to assess the business impact value. Furthermore respondents argued that there is a lack of unambiguous data, adding to the issues with generalisability of scenarios. This descriptions aligns with the theorised description of effect uncertainty, causing the nature and severity difficult to predict. The organisation's IS environment characteristics of complexity and dynamism are attributed to the experience of uncertainty in this step. Please refer to Figure 5.10 for a generalised overview of the findings in relation to theory on PEU.

The judgment operations from the respondents revolve around the continuous assessment of provided information. Thereby assessing the applicability of the information in relation to the scenario.

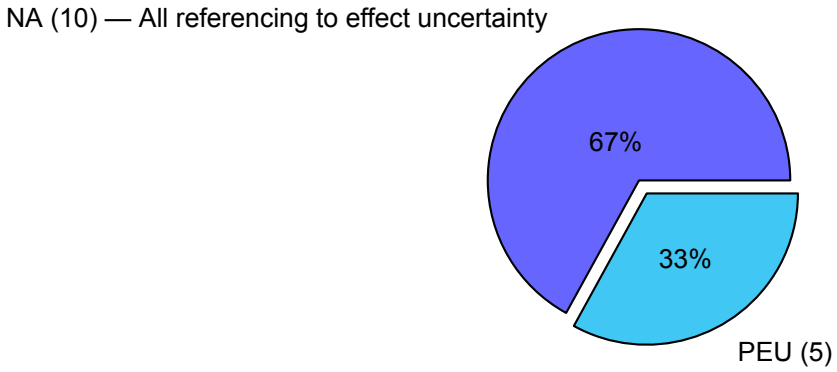


Figure 5.10: Uncertainty in the business impact value analysis

It must however be noted that the accountability structure prevents them from final decision–making, which prevented insight into further judgment operations. The described operations are closest to the theorised selective accessibility model, arguing that the provided information correctness is assessed and incorporated in the respondent's judgment.

5.4.2. Likelihood analysis

The likelihood analysis is the final step in this results chapter. It determines the probability value for the occurrence of a scenario materialising as delineated by from the risk identification.

5.4.2.1. PEU in likelihood analysis

Not perceiving uncertainty

The fifteen (15) respondents have all been asked if they perceive uncertainty during the analysis of the likelihood values for the identified scenario, i.e. the assigning of probability value for the occurrence of a scenario materialising. Two (2) respondents indicated that they were not involved in this step and that their job is to challenge the likelihood values if necessary [D02, D10].

Four (4) respondents indicated that the assigning of likelihood values for the scenarios materialising was not executed as such. Indicating that assigning accurate likelihood values would be extremely difficult and that there is not any added value from it. Consequently they adopt a *control–based approach* in which the *likelihood values are implicitly incorporated*, allowing them to stay away from discussion that might create confusion within the organisation. They thereby argue for a more pragmatic approach to their uncertainty [D03, D06, D08, D09]. Two (2) respondents indicated that their experience and knowledge about the controls used and whether a scenario would materialise helps them in this way to deal with the uncertainty associated to this step. This aligns with the theorised **individual cognitive characteristics** as well as the **availability of response options** in the respondent answers as to how they perceive uncertainty about the IS environment [D03, D09]. One (1) respondent also indicated that the *strong entrepreneurial spirit* from the organisation influenced the way in which the likelihood analysis is approached, linking to the theorised **social expectations** to the respondent answers [D06]. The respondent thereby indicated to the *possibility–probability dilemma*, only focussing on realistic scenarios where the necessary controls are employed. This was backed by another respondent [D06, D08] (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

Only one (1) respondent indicated to not perceive any uncertainty during the likelihood analysis [D11]. The respondent indicated that there is lots of information available that allows an accurate likelihood analysis. Thereby the respondent relied on the data from historical incidents and data from the security operations centre (SOC) of the organisation that allows statistical analysis necessary to provide accurate estimates. What is striking is that this answer is contradicting the answers of all other respondents, who indicated that even if the likelihood analysis was not executed explicitly or were not involved in the processes, that ascribe the difficulty in accurately estimating the likelihood values.

Perceiving uncertainty

The remaining eight (8) respondents indicated to perceive uncertainty during the likelihood analysis [D01, D04, D05, D07, D12, D13, D14, D15]. A recurring theme, as was in the business impact value analysis, is the *lack of unambiguous data* that allows the likelihood values to be accurately analysed and estimated for a scenario. A total of six (6) respondents [D01, D04, D07, D13, D14, D15] ascribed the lack of data as a major factor to the inability to accurately analyse the likelihood. As can be seen from the previous paragraph, this is contradicting the argument of respondent D11 in the above paragraph.

One (1) respondent indicated that the use of third party applications and services makes it difficult to assign accurate likelihood values. Because even though a type of *risk transfer* takes place by the use of a service provider, one also gets risk in return because there is less information and you have to trust the service provider to be up to the indicated standards. This makes the situation less transparent and creates a dependency on the service provider [D12].

One (1) respondent described the number of different controllable and uncontrollable factors that are associated to a scenario materialising. Thereby the respondent refers to the limited controllability of behaviour of information systems in the organisation's IS environment [D05].

Finally one (1) respondent also indicated to perceive uncertainty due to the inclusion of stakeholders in the process, thereby questioning the validity of the stakeholders. Factors of validity circle around the knowledge, interest and the informedness of the stakeholders included [D14].

The remaining eight (8) respondents who indicated to perceive uncertainty argued they were unable to accurately assign probability values to the identified scenarios materialising. The IS environment is argued to have many different domains about which one needs to have thorough knowledge, creating a lack of transparency to the respondent [D07]. Additionally it is argued that there are many different factors, controllable and uncontrollable, which are not all known and thereby create tremendous difficulty in analysing the likelihood of a scenarion [D04, D05, D14]. Furthermore one (1) respondent argues that the threat landscape changes rapidly with new technologies available t threats which make it easier to be targeted, creating uncertainty in assigning the likelihood values to scenarios materialising [D15].

The results from the above paragraph accurately depict the theorised form of **state uncertainty**. Whereby the organisation's IS environment, encompassing all facets as theorised environment as depitced in Table 2.2, is described as both **complex** and **dynamic** (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

However, the most pressing factor that is stipulated most often by all the respondents is the *lack of unambiguous data* which makes the likelihood analysis an absolute issue.

5.4.2.2. Providing judgment under uncertainty for the likelihood analysis

The eight (8) respondents [D01, D04, D05, D07, D12, D13, D14, D15] that indicated to perceive uncertainty during the likelihood analysis are subsequently asked to indicate how they provide judgment under their perceived uncertainty.

The results showed that five (5) respondents used provided information from third parties such as the National Cyber Security Center (NCSC), general market/industry reports as well as websites/ security blogs. This was actively searched for and incorporated in the judgment operations. The respondents argue to assess and mainly stay close to these provided values. This description shows close resemblance with the **selective accessibility model** in which the provided values are assessed to be a suitable answer and subsequently used in such cases, as described by the respondents [D01, D04, D07, D14, D15] (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

Furthermore three (3) respondents indicated that their judgment incorporated large incidents that have materialised in the past, or have been extensively covered by the media which contributed to having a large impact on the retrievability of their memories. Thereby allowing easy retrievability of instances to be incorporated in the judgment operations [D01, D14, D15]. Furthermore two (2) respondents indicated to actively rely on the experiences from the past. Thereby taking into account that large incidents with an arguably low likelihood can be considered to have a high likelihood instead due to the ease of retrievability by the respondent [D04, D07]. These description fits the theorised description of the **availability heuristic** in which the cognitive ease by which something comes to mind is incorporated in their judgment. It is however important to note that all respondents were aware of the workings

of such heuristics (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts). Please refer to an example description below:

> We will incorporate large incidents from the news, especially in the free format discussion. But you have to be wary, for what social psychologist have a nice term, that if something is extensively in the news now that the chance is higher. For instance, I believe that ransomware is here to stay, but if it is covered by the news it doesn't mean the likelihood for it happing is higher. But then there are so many threats, we can not determine an accurate chance for all of them. ***D14***

Four (4) respondents described in their judgment operations that they actively compare scenarios with similar cases to provide a likelihood analysis, based on the similarity of the scenario that is judged. Thereby indicating that the values from these similar cases are not necessarily true, but it provides a basis for discussion to analyse the likelihood of a scenario with a group of people [D01, D04, D14, D15]. This description aligns with the **representativeness heuristic** from the conceptual framework, relying judgment operations based on similarities from the subject that is under judgment (please refer to Table 3.2 for the definition and to Table 4.1 for the identifiers in the coding scheme for the in boldface depicted concepts).

A striking observation on how to provide judgment is coming from one (1) respondent who indicated to use risk matrix in an alternative order. First the colour of the risk is estimated with the help of the risk matrix, then based on the calculated impact the likelihood can be derived from the risk matrix. This provides a pragmatic approach in which the worst case scenario of the likelihood is taken [D12]. Thereby *reverse engineering* the likelihood estimate from the risk matrix. One (1) respondent indicated that the likelihood was determined based on the beliefs of how important the risk was to the organisation. If previous steps show that the impact is high with a number of vulnerabilities, that the likelihood was estimated to be high so that security was forced to treat the risk accordingly [D05]. Finally the Delphi method was indicated to be used to derive a likelihood estimate by one (1) respondent. Using the knowledge of many experts remove the uncertainty as much as possible [D13].

5.4.2.3. Concluding remark for the likelihood analysis

The likelihood analysis is a step that is generally perceived to be uncertain by the respondents. It was indicated by only one (1) respondent that there was no uncertainty experienced in the process due to the availability of information that allowed statistical analysis to provide accurate likelihood estimates. Two (2) respondents indicated that they weren't involved in the process as such but only challenged the input of others. Four (4) respondents indicated that the step was not explicitly executed, but rather a *control–based approach* was adopted. This allowed them to stay away from the uncertainty and additionally prevented confusion within the organisation with discussions about likelihood estimates which do not add value for the organisation's security. Although the approach does not perceive them to be certain about the likelihood analysis, it does take away uncertainty which is based on the knowledge and experience they have with executing risk assessments. Another striking issue highlighted by two (2) respondents was the *possibility–probability dilemma* of scenarios which makes estimating the likelihood difficult, thereby favouring the control–based approach.

The remaining eight (8) respondents identified with state uncertainty, ascribing difficulties in accurately assigning likelihood values to scenarios. The complexity of the environment was indicated as factor of their perceived uncertainty, indicating that many different controllable and uncontrollable factors influence the likelihood of a scenario. Additionally it was highlighted that the dynamic nature of the threat landscape makes it easier to be targeted by threats, creating the perceived inability to assign an accurate likelihood estimate for a scenario. However, the most prevalent issues with this step is the *lack of unambiguous data* that prevents accurate likelihood estimates to be made. This is in line with the business impact value analysis which together makes a risk calculation very difficult for the cybersecurity professional. Please refer to Figure 5.11 for a generalised overview on the results for the theory on PEU.

Remarkable to this last step was that the description on judgment operations aligned with the three theorised judgment heuristics. This finding is interesting because a good part of the judgment heuristics is theorised around probability estimates.

The most striking observation to deal with uncertainty was the *reverse engineering* approach of one (1) respondent who indicated to use a risk matrix in an alternative order. This allowed a pragmatic approach to the likelihood analysis.

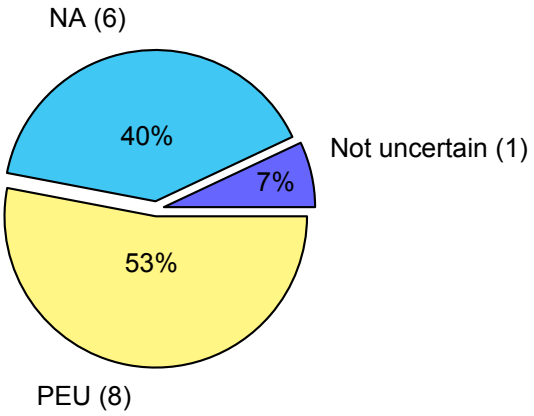


Figure 5.11: Uncertainty in the likelihood analysis

What was striking to the analysis of the data for this particular step is that the respondents were less focused on the organisation's accountability structure. Although everybody indicated that the likelihood analysis was mainly executed within a group, including stakeholders, experts and risk managers, the accountability structure was not invoked in the judgment process for this step by any of the respondents. The researcher believes that this is due to the highly subjective premise of this step, allowing respondents to more easily explain their own thought processes. Which subsequently allowed the identification of heuristics in judgment under uncertainty from the respondents.

5.5. Conclusion for the results

The results from all IS risk assessment steps are displayed and analysed. The theorised concepts from Chapter 3 provide guidance in the interpretation of the results concerning the perception of uncertainty as well as the judgment operations the respondents have. The chapter is finalised with a depiction of the uncertainty profiles of the respondents.

5.5.1. Overview of perceptual aspects explained with PEU

The analysis for the perception of uncertainty about the organisation's IS environment is supported with the PEU theory. For each of the IS risk assessment steps it was indicated what caused the respondents to experience uncertainty or what did not. Factors are attributed to the perception of uncertainty and analysed with the help of the PEU concept which allowed to gain an understanding in the respondent's perceptual processes. Please refer to Table 5.1 for an overview of respondent results that were explained with the PEU concept. The top row of the table provides the items relevant to the PEU theory. The second to fourth columns depict the uncertainty identified from the respondent answers. Please note that the fourth column includes the unfathomable uncertainty, which is not directly related to the PEU theorised concepts but is provided for completeness purposes. The remaining five (5) columns depict the sources of variability from the PEU theory. The rows are filled with the instances counted for each of the items from the theory in relation to the IS risk assessment steps, providing a quick overview to the reader. The instances are counted to identify the relevance of the items of the PEU theory, the more instances counted the higher the relevance. It is important to note that the values do not fulfil a statistical role, it merely provides an overview of the empirical results explained with theory.

5.5.2. Overview of judgment operations explained with judgment heuristics

To understand how cybersecurity professionals subsequently provide judgment when experiencing uncertainty in the different steps of the IS risk assessments, the judgment operations are analysed. The methods employed in providing judgment are depicted and consequently analysed with the help of the theorised judgment heuristics. Please refer to Table 5.2 for an overview of the instances in which judgment heuristics guided the analysis of the respondent judgment operations. The first column indicates the IS risk assessment steps. The remaining three columns indicate the theorised judgment heuristics and the rows are filled with the instances counted in each of the IS risk assessment steps. Please note that the table is again for illustrative purposes to see the relevance of items from the theoretical

Table 5.1: Overview of results relating to the theoretical concepts for each of the IS risk assessment steps

	Risk assessment	Effect uncertainty	State uncertainty	Unfathomable uncertainty[a]	Complexity[b]	Dynamism[c]	Availability of response options	Individual cognitive characteristics	Social expectations
	Risk identification								
1.1	Asset identification	1	8		1 / 6	1 / 6	4	4	
1.2	Threat identification	5			3	3	4	4	
1.3	Identification of existing controls		6		5	2	3	3	
1.4	Vulnerability identification	1		8	1 / -	1 / -			
1.5	CIA identification	6			4	4	5	1	
	Risk analysis								
2.1	Business impact value analysis	5			3	1			1
2.2	Likelihood analysis		8		4	1	2	2	1

[a] This form of uncertainty is not related to the PEU theory, but is depicted as findings from the perception of uncertainty
[b] The instances of complexity indicated per type of uncertainty if applicable. Separated by a forward slash for each of the uncertainty types, to be read in the uncertainty column order.
[c] The instances of dynamism indicated per type of uncertainty if applicable. Separated by a forward slash for each of the uncertainty types, to be read in the uncertainty column order.

concepts in relation to the specified steps. Thereby indicating how much the theory was able assist in understanding the judgment operations in the different steps.

Table 5.2: Overview of results relating to the theoretical concepts for each of the IS risk assessment steps

	Risk assessment	**Availability heuristic**	**Representative heuristic**	**Selective accessibility model**
	Risk identification			
1.1	Asset identification			6
1.2	Threat identification			4
1.3	Identification of existing controls			
1.4	Vulnerability identification			
1.5	CIA identification	1	3	
	Risk analysis			
2.1	Business impact value analysis			4
2.2	Likelihood analysis	5	4	5

5.5.3. The relevant findings

The results provide many relevant findings which are not explained by theoretical concepts, each of them are depicted among the different steps of the IS risk assessment in this chapter. The highlighted findings that relate to the perception of uncertainty reflect on shadow IT and innovation processes within an organisation. These findings are part of SQ1 which aims to identify how cybersecurity professionals perceive uncertainty in an IS risk assessment. These findings are marked as relevant to this research and are further synthesised in the next chapter.

The relevant findings to how cybersecurity professionals provide judgment when under uncertainty relate to the accountability structure of an organisation, the security policy and philosophy that focuses on detection and response, and the security awareness of people within the organisation. These findings relate to SQ2 of this research. The next chapter provides further synthesis on these findings.

5.5.4. Uncertainty profiles of respondents

This subsection focuses on the uncertainty profiles of the respondents. The aim of this subsection is to show a quick overview of the general perception of uncertainty during the IS risk assessment. Thereby depicting the instances in which each of the respondents indicate to not perceive uncertainty, to perceive uncertainty, to not be involved in the IS risk assessment step or to define if certain steps are not executed with the employed IS risk assessment methodology. Please refer to Table 5.3 for an overview of the uncertainty profiles. *Please note* that these profiles don't describe the respondent to be extremely uncertain, or not at all uncertain. It merely describes that the respondents indicate that in the identified steps they experienced difficulty in accurately identifying or estimating the certain values associated to the steps. For the details, please refer to the detailed result descriptions in this chapter for each individual chapter.

What can be observed from Table 5.3 is that a many of the respondents show to experience uncertainty in different stages of the IS risk assessment. Consequently it is evident that the results are not determined by a small group of respondents.

Table 5.3: Overview of uncertainty profiles respondents

	Respondents	D01	D02	D03	D04	D05	D06	D07	D08	D09	D10	D11	D12	D13	D14	D15
	Risk assessment															
1.1	Asset identification	⊖	⊖	⊕	⊖	⊙	⊕	⊖	⊖	⊕	⊕	⊖	⊕	⊕	⊕	⊕
1.2	Threat identification	⊕	⊖	⊖	⊖	⊕	⊕	⊕	⊖	⊖	⊖	⊙	⊕	⊖	⊖	⊖
1.3	Identification of existing controls	⊖	⊖	⊖	⊖	⊕	⊖	⊕	⊕	∅	∅	⊖	⊕	⊕	⊕	⊖
1.4	Vulnerability identification	⊕	⊖	⊖	⊖	⊖	⊕	⊖	⊕	⊕	⊖	⊕	⊕	⊕	⊕	⊕
1.5	CIA identification	⊙	⊖	⊖	⊙	⊕	⊕	⊖	⊖	⊖	⊙	⊕	⊕	⊕	⊖	⊕
2.1	Business impact value analysis	⊕	⊙	∅	⊕	⊕	∅	⊙	∅	∅	⊙	⊙	∅	⊕	⊕	∅
2.2	Likelihood analysis	⊕	⊙	∅	⊕	⊕	∅	⊕	∅	∅	⊙	⊖	⊕	⊕	⊕	⊕

⊕ The respondent indicated to experience uncertainty
⊖ The respondent indicated to not experience uncertainty
⊙ The respondent indicated to not be involved in that particular step of the IS risk assessment.
∅ The respondent indicated that this step wasn't executed within their IS risk assessment methodology

6

Synthesis of results

This chapter aims to provide synthesis on the research results from Chapter 5 about the theorised concepts. The different steps of the IS risk assessment are integrated to accommodate the analysis and gain an understanding of the research problem. The chapter explores if and how the findings can be explained with the theorised concepts on perceived environmental uncertainty (PEU) and judgment heuristics. This provides a general overview of the relevant findings.

First the theory on PEU is synthesised, analysing each of the different components in the concept (Section 6.1). This is followed by a synthesis on the judgment heuristics (Section 6.2). The chapter is finalised with a concluding remark in which the results are generalised in relation to the theory (Section 6.3). This consequently allows the research questions to be answered in Chapter 7.

6.1. Synthesis on PEU

6.1.1. Perceptual processes — Source of variability to PEU

The perceptual processes from the theory on PEU are indicated to be a source of variability and are described by three items that in theory influence the cybersecurity professionals' perception of uncertainty about the IS environment.

The individual cognitive characteristics

The results show that the individual cognitive characteristics — operationalised by the training/education in executing IS risk assessments of the individual that determines the ability to deal with ambiguity and uncertainty — are incorporated in the respondent's perception of uncertainty about the IS environment. Evident from Subsection 5.2.1, twelve (12) respondents were adequately trained/educated to execute IS risk assessments. Three (3) remaining respondents eventually learned enough on the job to say they are well equipped with the right knowledge to execute IS risk assessments. The results show that the individual cognitive characteristics are identified in four (4) risk assessment steps by multiple respondents as a reason not to perceive uncertainty. The results also show that none of the respondents has indicated to perceive uncertainty based on a lack of training/education on how to execute IS risk assessments.

Based on the characteristics from this respondent sample, the individual cognitive characteristics show a negative influence on the experience of PEU. I.e. the respondents do not perceive uncertainty about the IS environment due to a lack of knowledge from trainging/education on how to deal with the ambiguity and uncertainty in the execution of an IS risk assessment.

The availability of response options

The results show that the availability of response options — operationalised by the years of experience in the execution of IS risk assessments — is incorporated in the respondent's perception of uncertainty about the IS environment. Subsection 5.2.2 provides insight into the experience of cybersecurity professionals, indicating that the sample on average has seven (7) years of relevant working experience. Derived from the results, it is evident that the availability of response options is identified in five (5) risk assessment steps by multiple respondents as a reason not to perceive uncertainty. Additionally, the

results depict that none of the respondents indicated to perceive uncertain due to a lack of experience in the execution of IS risk assessments.

The results from this sample show that the availability of response options has a negative influence on the experience of PEU. I.e., the respondents attribute not to perceive uncertainty about the IS environment because they perceive to have relevant working experience in the execution of an IS risk assessment.

The social expectations from the organisation

The results for the respondent's social expectations from the organisation do not provide much insight into whether it is incorporated into the perception of uncertainty about the IS environment. There has not been posed any specific questions in relation to this item and identification is therefore depending on the input of the respondent. The results show only one (1) respondent referenced to the social expectations from the organisation in relation to two IS risk assessment steps. However, the responses did provide insight into how this was incorporated in the perception of uncertainty about the IS environment. Although none of the respondents indicated to perceive uncertainty based on the organisation's social expectations, indications for the incorporation of this perceptual process is considered thin based on this respondent sample.

The results do not allow the social expectations from the organisation to be attributed to influencing the perception of uncertainty about the IS environment in this sample. However, the concept itself is considered to be relevant because understanding how the socialisation process of an organisation influences the level of security to deviate from standards provides insights into the organisation's attitude towards security.

6.1.2. IS environment characteristics — Source of variability to PEU

The IS environment characteristics from the theory on PEU are also indicated as a source of variability. They are described by two features that in theory influence the cybersecurity professionals' perception of uncertainty about the IS environment.

The complexity dimension

The results for the complexity characteristic of the IS environment show it to be attributed in each of the seven (7) steps as described by the ISO27005. In each of the steps, the complexity of the IS environment is on average attributed by four (4) respondents as to why they do perceive to be uncertain during the IS risk assessment. The respondents ascribe the IS environment to be complex due it being filled with many different information systems over multiple layers that process information. This creates many interrelations within the IS environment which cannot be fully grasped by the cybersecurity professional and consequently contributes to the perceived uncertainty about the IS environment. Contributing factors of complexity are indicated to be shadow IT and the organisational structuring. These findings and factors are further synthesised in Subsection 6.1.6.

It is consequently argued that the perceived complexity of the organisation's IS environment has a positive influence on the respondent perception of uncertainty about the IS environment, i.e. the perceived complexity is creating uncertainty.

The dynamism dimension

The results for the dynamism characteristic of the IS environment also show to be attributed in each of the seven (7) steps as described by the ISO27005. On average the respondents attributed dynamism from the IS environment two-and-a-half (2.5) times per step when uncertainty is experienced. The respondents ascribe the IS environment to be dynamic due to rapid changes within the organisation's landscape of information and information systems. Furthermore, the fast–changing threat landscape is considered dynamic, due to the ability of the threats to quickly adopt new technologies and adapt to security measures. Contributing factors are described to be the innovation processes within the organisation, changing business contexts with the associated stakeholders and continuous changes in the threat landscape. These factors are further synthesised in Subsection 6.1.6.

The results show that the dynamism within the organisation's IS environment, consisting of the general landscape of information and information as well as the threat landscape, has a positive influence

on the respondent perception of uncertainty about the IS environment, i.e. the perceived dynamism is creating uncertainty.

6.1.3. PEU in the IS risk assessment

The theory on perceived environmental uncertainty (PEU) is researched against the backdrop of the ISO27005 methodology for IS risk assessments in accordance with the research model as depicted in Figure 3.2. The results from Chapter 5 show that the theory on PEU theory helps explain the findings from the empirical real world data on IS risk assessments, identifying a type of PEU from multiple respondents in seven (7) IS risk assessment steps. Refer to Chapter 5 for the identification in each of the steps. The uncertainty experienced during the identification of vulnerabilities could not be fully explained with the PEU theory. These findings in the vulnerability identification step are further synthesised in Subsection 6.1.5. Two types of PEU with the associated sources of variability are identified within these six (6) different steps of the IS risk assessment methodology.

State uncertainty

The type of state uncertainty is identified in the following IS risk assessment steps: (1.1) asset identification, (1.3) identification of existing controls, and (2.2) likelihood analysis. In each of these steps, the PEU theory explains how the respondents experience the inability to make accurate probability estimates as well as the difficulties perceived with grasping the interrelations between components and how they are changing within the IS environment. State uncertainty was identified with all respondents who indicated to perceive uncertainty during these identified steps.

Derived from the results, the sources of variability that have a positive influence on the perception of state uncertainty in the identified steps are complexity and dynamism. The complexity dimension refers to the many components and number of interrelations between the organisation's general landscape of information and information systems. This creates difficulties in assessing the interrelations within the organisation's IS environment. The dynamism dimension reflects on the changing nature of interrelations within the organisation's general landscape of information and information systems. This creates difficulties estimating and identifying the changes/events in the organisation's IS landscape.

Effect uncertainty

The type of effect uncertainty is identified with the following IS risk assessment steps: (1.2) threat identification, (1.4) vulnerability identification, (1.5) CIA identification, and (2.1) business impact value analysis. The PEU theory explains for each of these steps how the respondents perceive the inability to predict the impact from possible events/changes in the IS environment of the organisation. Effect uncertainty was identified with all the respondents who indicated to perceive uncertainty during these identified steps.

The results show that the sources of variability that have positive influence on the perception of effect uncertainty are complexity and dynamism, each explained below for the identified steps. The complexity reflects on the many interrelations and layers of the information and information systems in the organisation's IS environment. This makes it difficult to assess how threats are relevant to the organisation, how information is processed by the information systems, and how the context needs to be incorporated to examine the impact. The dynamism dimension reflects on the changing and ever–evolving nature within the IS environment. Dynamism addresses the threat landscape that continuously evolves and incorporates new technologies, as well as the changing business contexts within the organisation. This creates difficulties in keeping track of all changes that can have an impact on the organisation.

The sources of variability

Based on the synthesised results from Subsection 6.1.1, the individual cognitive characteristics and the availability of response options are identified to have a negative influence on the perception of uncertainty about the IS environment. The social expectations were referenced by one respondent, however, this research argues the influence to be unconvincingly identified.

The complexity and dynamism dimensions, i.e. the characteristics of the IS environment, as described above have a positive on the perception of uncertainty.

The synthesis of Subsections 6.1.1 to 6.1.3 allows the conceptual model for the PEU theory to be constructed in the IS risk assessment setting, which is based on results from this respondent sample.

6.1.4. The conceptual model for PEU in IS risk assessments

Based on the synthesis, a conceptual model in which the results are incorporated is presented in Figure 6.1. It presents the influence for the different items from the PEU theory, describing how the respondents perceive uncertainty about the IS environment in the context of an IS risk assessments. Please note that this conceptual model is based on qualitative data from one sample of fifteen (15) respondents as part of the exploratory approach of the PEU concept in the IS risk assessment setting. Consequently, the model is a representation of inductively derived findings and is not stating quantitative results.

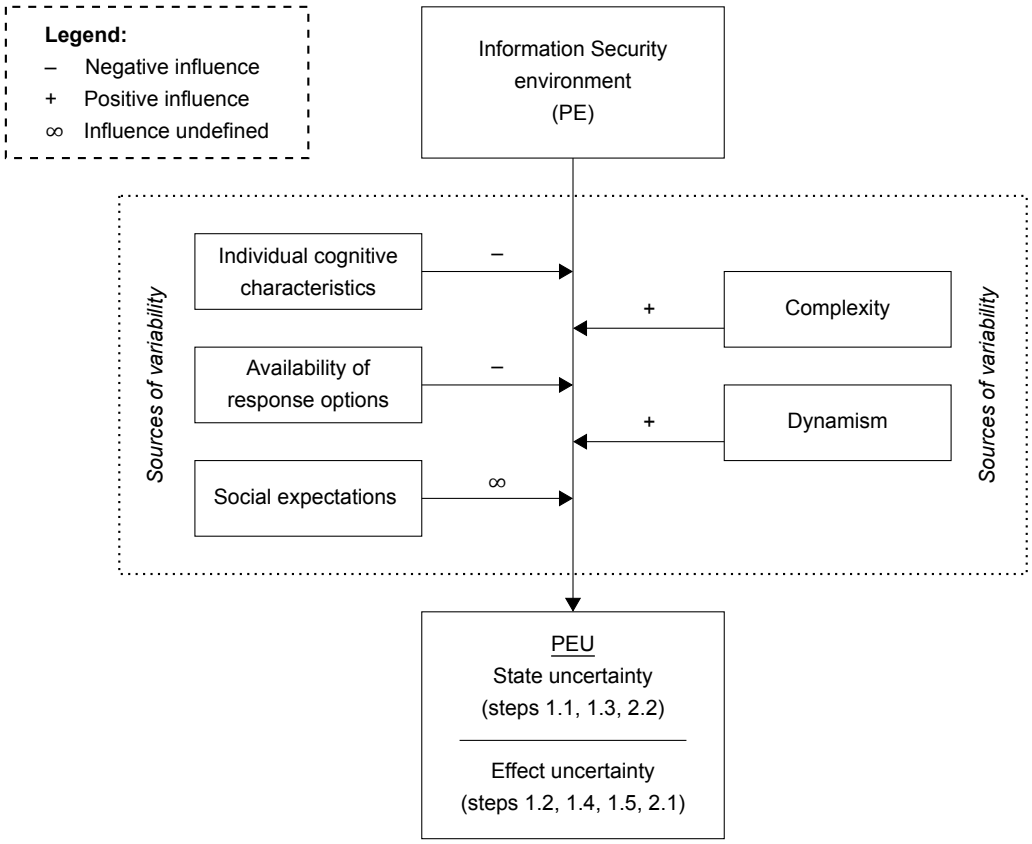


Figure 6.1: The conceptual model for the cybersecurity professional's perception of uncertainty about the IS environment in an IS risk assessment. Adapted from Downey et al. [20]

Please take note of the legend depicted in the top left corner, describing how the attributed signs for this model should be read. The negative sign indicates that the concept has a negative influence on the model. The positive sign indicates that the concept has a positive influence on the model. The infinity sign shows that the influence could not be defined based on the results of this study.

The model depicts how the respondents perceive uncertainty about the IS environment, supported by the PEU theory. The box labelled "Information Security environment (PE)" is the independent variable in this model. This independent variable has a direct link to the box labelled "PEU", which is the dependent variable that describes the type of perceived uncertainty about the IS environment. The five sources of variability, indicated in the dotted box are moderating variables on the respondent's PEU. Derived from the synthesised Subsections 6.1.1 to 6.1.3, the results show that both the individual cognitive characteristics and the availability of response options are identified to have a negative moderating influence on the respondent's PEU. The social expectations from the organisation are identified to be incorporated in the perception of uncertainty about the organisation's IS environment, but its influence is unidentified. The complexity and dynamism characteristics are identified to have a positive moderating influence on the respondent's PEU.

Synthesising the results with the model allows the identification of PEU and the associated sources of variability in the IS risk assessment steps as described by the ISO27005 methodology for this sample.

The “PEU” labelled box indicates the type of uncertainty perceived about the IS environment by the respondents for the different IS risk assessment steps.

6.1.5. Unfathomable uncertainty during the IS risk assessment

The results of Chapter 5 show that the PEU theory could not explain a large part of the experienced uncertainty during the vulnerability identification. The theory only explained one (1) respondent’s perceived uncertainty, whereas the remaining eight (8) respondent experiences could not be explained. Thereby the PEU theory was not able to accurately describe how the respondents perceive uncertainty about the IS environment. However, another form of uncertainty perceived by the cybersecurity professionals was unambiguously present. Eight (8) respondents indicated that they perceived to be uncertain about the integrality of all vulnerabilities for their organisation’s IS environment. Indicating that it was difficult to determine if all relevant vulnerabilities for the organisation have been identified and are included in the IS risk assessment. The respondents argued they assumed vulnerabilities are unknown to them, as well as the impact from these vulnerabilities. This creates a set of unknown–unknowns, which is identified as unfathomable uncertainty about the vulnerability identification for the organisation’s IS environment. This term is adopted from Kim [41]. This uncertainty was ascribed to all eight (8) respondents that indicated to perceive uncertain during the vulnerability identification step.

The factors for this perceived uncertainty could based on the results not be ascribed to either of the five sources of variability that the theory on PEU prescribes. The factor attributed by the respondents is solely based on the integrality of unknown–unknowns, creating unfathomable uncertainty for the cybersecurity professional in the identification of vulnerabilities.

Furthermore, it is worth mentioning that the remaining six (6) respondents also referenced to this type of unfathomable uncertainty but indicated not to perceive uncertain based on their reliance on tooling and their security strategy that shifted from prevention to detection–response. However, their reference is important to take into consideration because it best describes how the respondents perceive uncertainty during the vulnerability identification.

Additionally, the results show that the issue of integrality is also spotted with one (1) respondent during the threat identification. Indicating that the respondent perceives to be uncertain due to the possible not-integrated threats that are unknown. It must be noted that this respondent was also labelled to perceive unfathomable uncertainty in the vulnerability identification.

6.1.6. Relevant findings for uncertainty perception

This subsection describes the relevant findings that relate to the uncertainty perception of the cybersecurity professional. These findings have been indicated to relate to the sources of variability that reside in the characteristics of organisation’s IS environment, as indicated in Subsection 6.1.2. The concepts are further synthesised to start a discussion.

Shadow IT, Organisational structuring & Innovation processes

The concept of shadow IT is highlighted in numerous steps of the IS risk assessment as a factor that creates both complexity and dynamism. Shadow IT is defined by this research as information and information systems within an organisation about which the department responsible for IS is unaware/uninformed. Shadow IT can range from complete applications that are in use within the organisation but are hosted elsewhere to little things such Excel sheets with important data on which an organisation is depending. The concept was identified in three steps of the risk identification process, most prominently in the asset identification where it stresses the complexity dimension of the IS environment (step 1.1.) and the identification of existing controls where the dynamism dimension is indicated to be affected (step 1.3).

The exploratory angle of this research has discovered that the concept of shadow IT is seen as a fundamental issue for the respondents when executing IS risk assessments. It hinders them in the mapping of all valuable assets of an organisation. Additionally, from a security perspective it also has the potential to infringe crown jewels or misuse an enterprise’s IT configuration management, thereby by-passing the controls with consequences that cannot be overseen by the IS department. The respondents indicated that shadow IT is currently developing quickly with many cloud applications that by-pass the need of an IT department. Additionally, the organisation’s structuring, with decentralised procurement and IT departments that are supporting within an organisation, are seen as reasons why

shadow IT develops quickly. The decentralisation allows procurement in which the IS department is not always involved and are therefore depending on the input provided to them.

The innovation processes within an organisation are highlighted in the first three steps of the risk identification subprocess as a source of a dynamic IS environment. The respondents referred to the innovation processes of the organisation as a factor that is contributing to the perception of uncertainty — thereby indicating that innovation processes create changes in the information and information systems landscape. The changes relate differently to each of the three steps.

The asset identification (step 1.1) refers to the innovation processes in relation to the factor of shadow IT, as discussed above. Thereby indicating that due to the many innovation processes in the organisation, shadow IT is creating difficulty in accurately identifying the assets of an organisation.

During the threat identification (step 1.2) the organisational innovation processes are identified as a source of threats. The lack of transparency within these processes allow threats that are unintentionally developed during innovation activities to remain undetected for the IS department. The innovation activities can often not be notified with the IS department in which case it becomes shadow IT, thereby creating difficulties in identifying the threats to the organisation.

Finally, in the control identification (step 1.3), the development of information and information systems in the organisation's innovation processes again relate to shadow IT. As a consequence, controls can be designed that take effect on an organisation without an IS department knowing about it. Thereby creating difficulties with the identification of controls, relating to identifying controls, check the working status and if there are duplicate controls.

In sum, the concept of shadow IT, also in relation to the innovation processes of an organisation, is much discussed in this thesis and the impact on an IS risk assessment is perceived to be present by cybersecurity professionals. However, considering the focus of this study was not on the shadow IT and innovation processes within organisations any additional insights cannot be provided.

6.2. Synthesis on judgment operations

6.2.1. Judgment heuristics

The theory on judgment heuristics is used in this research to understand how cybersecurity professionals provide judgment in IS risk assessments when under uncertainty about the IS environment. Thereby gaining insight in the judgment operations from the respondents. The conceptual framework has adopted and conceptualised three heuristics that are employed when people are required to provide estimates for or identify elements about the organisation's IS environment that are not true by definition. The respondents who indicated to perceive uncertainty during the IS risk assessment steps were consequently asked how they provide their judgment. First, each individual heuristic is synthesised that provides insight into the meaning of the results. After describing the findings on the heuristics, Subsection 6.2.3 depicts te relevant findings that can not be linked to the theory on judgment heuristics.

Availability heuristic

The theory on judgment heuristics describes that people employ the availability heuristic — reliance on the cognitive ease by which instances of an event comes to mind — to judge the frequency/plausibility of the subject under judgment. This can be caused by large incidents that are well imprinted in the minds of the cybersecurity professional, or items that are of big impact which are extensively covered in the media that allows easy retrievability. From the results it can be derived that this heuristic is identified in two (2) steps of the IS risk assessment: the CIA identification (step 1.5) and the likelihood analysis (step 2.2).

The CIA identification (step 1.5) aims at providing an information classification to the identified asset, determining the importance of the confidentiality, integrity and availability of the assets to the organisation. Thereby it is important to understand what the implications from the assets and the possible threats that they can attract are, delineating the effects possible to the organisation. This directly links to effect uncertainty, however only for the grey areas in which an obvious identification is absent. One (1) respondent answered to heavily rely on the media, indicating that large events in the cybersecurity world were highlighted quickly in the process of assigning an information classification. Thereby allowing the availability to aid in the estimating the CIA values. It is however important to note, than only

one (1) respondent was labelled with the availability heuristic, showing limited support for the use of the availability heuristic in this step.

For te likelihood analysis (step 2.2) probability estimates for scenarios are identified. State uncertainty was identified based on the perceived inability to accurately assign probability estimates. The respondents indicated to incorporate cybersecurity incidents that were extensively covered in the media. Furthermore respondents relied on instances from their experience which they included in their judgment of the likelihood analysis.

In conclusion for the availability heuristics in relation to step 1.5 and 2.2, the results show the respondents refer to elements of the availability heuristics, implying its use. Thereby the theory partially explained how judgment is provided in these different steps of the IS risk assessment.

Representativeness heuristic

According to theory, the representative heuristics — judgment that is based on how representative/ similar the subject under judgment is — is employed to assess probabilities and to predict values with limited information. From the results it can be derived that the representative heuristics is identified in two (2) steps of the IS risk assessment: the CIA identification (step 1.5) and the likelihood analysis (step 2.2).

As discussed in the availability heuristic, the CIA identification provides an information classification to the organisation's asset. Effect uncertainty is identified in step 1.5, in which the effect of the assets to the organisation is perceived difficult to estimate for the assets within a certain grey area. The respondents indicated to actively compare assets that are seen as similar to provide their judgment, relying on the similarity of the subjects that are classified.

During the likelihood analysis, as previously indicated, scenarios are assigned an estimate of materialising which is perceived difficult for which state uncertainty is identified. The respondents indicate to actively compare scenarios for similarities to provide likelihood estimates for them to materialise.

In sum, the representative heuristic is identified for step 1.5 and 2.2. The results show the respondents elements of the representative heuristic in their answers as a way to provide judgment when under uncertainty. Actively searching for representative cases thereby supports the respondents. Furthermore, the likelihood analysis of a scenario materialising, or in other words, determining where the scenario belongs on a range of "not at all possible" to "certainly possible" forces the respondent to assign a class to which the respondent believes the scenario is representative. Thereby a fit between the theory and data is identified that supports understanding the judgment operations.

Selective accessibility model

The use of the selective accessibility model — judgment on actively evaluating information provided as a suitable answer, and if this is not considered suitable, searching for other information in which further information is assessed against the initial information which causes the individual to stick close to the initial information — is according to the theory a method that allows the individual to hypothesise the suitability and accuracy of the information for a judgment problem. From the results it can be derived that the selective accessibility model is identified in four (4) steps of the IS risk assessment: the asset identification (step 1.1), the threat identification (1.2), the business impact value analysis (2.1), and the likelihood analysis (2.2).

During the asset identification (step 1.1) all information and information systems of value to the organisation are mapped, which is impossible without information to build up on. As indicated by the respondents, the general landscape of information and information systems is complex and dynamic which makes the identification of interrelations between all assets difficult. This directly refers to state uncertainty. The respondents consequently indicated to stick close to the information from databases and application discovery tooling as well as the documentation and archives from previous assessments to identify the assets.

The threat identification (step 1.2) identifies all possibilities of harm, i.e. effect from impact, to the organisation. This step refers to effect uncertainty in which it is difficult to determine what the consequences are from changes/events in the threat landscape of the organisation's IS environment. With the large and fast changing threat landscape and new technologies that are developed it is difficult to determine an organisation's relevant adversaries. The respondents indicated to heavily rely on industry/market standards which allows simplification of the process. Thereby the respondents indicated to

stick close to the values provided from the industry/market standards to identify the relevant threats for the organisation.

When analysing the business impact value (step 2.1), it is difficult to determine the consequences of an event that has not happened. This makes it difficult to determine the effect from changes/events in the organisation's IS environment, referring the effect uncertainty. Sticking close provided values from research or partial computed values on the topic, thereby allows the individual to provide a business impact value estimate. The respondents indicated that values from known incidents are used as an initial starting point of discussion for providing an estimate. Furthermore the respondents indicated to stick close to the information provided from the business stakeholders and experts, assessing their accuracy and correctness of their input.

Finally, the likelihood analysis (step 2.2) demands a probability estimate on a scenario from the cybersecurity professional. The many interrelations within the IS environment make it complex to estimate what the probability is for an event to occur, referring to state uncertainty. The respondents indicate to heavily rely on the information from third parties that is provided. Thereby assessing the applicability to the organisation and sticking close to the values provided.

In sum, the results show that the respondents identify elements of the selective accessibility model in the identified steps. Thereby the theory partially explains the judgment operations followed by the respondents in the identified step of the IS risk assessment.

6.2.2. Concluding remarks judgment heuristics

This subsection reflects on how the theory on judgment heuristics have helped in explaining the empirical findings. Firstly, the results show that the use of heuristics could only be identified with respondent answers in five (5) out of the seven (7) IS risk assessment steps. The results for the identification of existing controls (step 1.3) and the vulnerability identification (step 1.4) did not have reference to any of the judgment heuristics when input was required from the respondents in either processes. Synthesised from Subsections 5.3.3 and 5.3.4, these steps take an evidence–driven approach in which the respondents solely rely on tooling and evidence from it to determine the working state of existing controls and the vulnerabilities to the organisation. Consequently, there could not be identified any judgment operations from the respondent answers. This creates a mismatch between the premises of the theory and the IS risk assessment steps. Consequently, it shows that the evidence–driven approach erodes the judgment operations from these steps.

Furthermore, it is observed that the use of heuristics is most prominently identified with the likelihood analysis (step 2.2). From analysing the theory on judgment heuristics in relation to the premise of the likelihood analysis, it must be concluded that step 2.2 is theoretically closest to the premise of the theory. Thereby it can be concluded that for estimating the likelihood of scenarios, the judgment heuristics best aid in explaining how cybersecurity professionals provide judgment in that particular step.

Finally, it must be noted that this research does not identify heuristics to be actively used, it merely identifies from the respondent answers that reference is made to these heuristics. These references help in answering the question of how respondents provide their judgment when under uncertain conditions during the IS risk assessment steps. Consequently there is no research result that elaborates on the extent/impact of using heuristics in IS risk assessments. This research merely provides qualitative insights and the opportunity for follow-up research to statistically identify the use of heuristics by cybersecurity professionals in IS risk assessments.

6.2.3. Relevant findings for providing judgment

The synthesis in Subsection 6.2.1 showed that the use of heuristics is supported by the data. However, when comparing the instances count (allowing to identify relevance of the concepts), it is also noted that on average only half of the respondents described judgment operations in line with the heuristics as theorised. Consequently it describes for half of the respondents how they provide judgment when under uncertain conditions during an IS risk assessment. This section therefore depicts the relevant findings on how judgment is provided by the respondents when under uncertainty in the IS risk assessment steps.

Accountability structure

The findings in relation to providing judgment that is most referenced to by the respondents is the accountability structure of the organisation. Described in Subsection 4.3.1.2, the three lines of de-

fence model puts the cybersecurity professional generally in the second line of defence. This could also be observed from the data in Subsection 5.1.3. Consequently, the model adopted within the organisation is by many respondents used in their answers. Thereby describing that the respondent is not responsible for the final judgment call and that they leave the final decision with the business/risk owner. The accountability structure was mentioned in five (5) out of the total seven (7) steps, where the threat identification (step 1.2) and vulnerability identification (step 1.4) was not referenced. This caused many respondents to stay away from describing judgment operations and consequently prevented any heuristics to be identified. The accountability structure consequently prevented the respondents from providing more information on their judgment operations.

Although this reference hindered the observation of judgment operations with cybersecurity professionals, it was indicated by the respondents that this is not a source that reduces uncertainty. Whenever the accountability structure was referenced, it was often mentioned that even though it is not the responsibility of the cybersecurity professional, they often had doubts with the stakeholders (business/ risk owners) involved. These doubts reference to whether the right stakeholders are selected, as well as the interest, the informedness and knowledge of the stakeholder to make these decisions. Consequently, the outcomes of the IS risk assessments are highly depending on the stakeholders' judgment operations. This is however not researched in this study, therefore no further results can be depicted in that regard.

Security policy and philosophy

A finding that is considered interesting is the paradigm shift in the security policy and philosophy and the influence of it on the IS risk assessment. This was mentioned three (3) times in the vulnerability identification (step 1.4). The respondents indicated to accept the partial blindness from unfathomable uncertainty, coming from the unknown–unknowns, and relied on the security policy and philosophy that has shifted from prevention to the detection and response. Thereby indicating that the cybersecurity professional knows it cannot keep up with all changes and complexity within the IS environment of its organisation to prevent all IS incidents. Without neglecting preventive security, the focus shifts on how to detect and respond to an IS to minimise the impact to the organisation. The change in policy and philosophy thereby allows them to accept the partial blindness and work with the evidence with which an IS risk assessment is executed.

Security awareness of people involved

Another finding that is unique to this research on how cybersecurity professionals provide their judgment when under uncertainty, is the judgment of security awareness with the people involved. It was indicated by two respondents during the asset identification that the security awareness of the people involved was taken into account. Thereby indicating that depending on the awareness within the organisation the cybersecurity professional trusted certain people more than others when it comes to the organisation's IS, thereby judging the risk on the security awareness of the individual. From the responses, it could not be identified what the relationship is between judging the security awareness of the individual and the effect on the asset identification step. Therefore not further analysis is concluded, however, it is worth noting.

6.3. Conclusion for synthesis

This chapter has provided the reader with synthesis on the results. The different steps of the IS risk assessment are integrated with each other to accommodate the analysis using the theoretical concepts. The relevant findings are delineated and show how the results are interpreted. What is important to note from this study is that the findings can not be considered conclusive due to the qualitative and exploratory nature. However, the richness of the qualitative data provides insight into the fundamental questions on how the respondents experience uncertainty and how subsequently estimates are provided in an IS risk assessment. The theoretical concepts provide guidance in the interpretation process, exploring if there is a fit between the theory and the empirical data.

The research identifies that the theory on PEU in the IS risk assessment setting is suitable to understand uncertainty perceptions, which consequently aided in interpreting the results. Thereby state uncertainty and effect uncertainty were identified to be perceived by the cybersecurity professionals

in different steps. Sources of variability that had a negative influence on the perception of uncertainty are the individual cognitive characteristics and the availability of response options of the cybersecurity professional. The results show that the complexity and dynamism in the IS environment are having a positive influence on the perception of uncertainty. The many interrelations between information and information systems make it difficult grasp all elements in the IS environment. The added dynamics in the IS environment contribute to the perception of uncertainty for the cybersecurity professional. The highlighted findings that attributed to the complexity and dynamism are shadow IT and the innovation processes within the organisation. They are attributed in most of the IS risk assessment steps. However the research does not focus on these specific elements and can therefore not provide additional insights other than identifying their relevance to the respondents.

Whenever uncertainty about the IS environment is experienced, judgment operations are required to provide estimates. This study focussed on the judgment heuristics theory, aiming to identify if judgment operations from cybersecurity professionals are guided by heuristics. It is however to be noted that the identification of the heuristics was not present with all the respondents who were labelled to perceive uncertainty. The relevant findings delineate responses that could not be explained with judgment heuristics theory, showing that the accountability structure of an organisation is at influence in the final call of risk assessments. This hindered further analysis of the judgment operations from cybersecurity professionals. Furthermore, the judgment operations of the respondents relied on the security policy and philosophy within an organisation, as well assessing the security awareness of the people involved. The relevant findings in regard to providing judgment can however are not further analysed because it is out of scope of this research.

According to the researcher's knowledge, there is a knowledge gap in the current body of literature about the cybersecurity professionals' perception of uncertainty in an IS risk assessment. The synthesis of the IS risk assessment steps in relation to the PEU theory and judgment heuristics theory in this chapter has shed a first light on the issue that is to improve the understanding on the perception and judgment operations of cybersecurity professionals in IS risk assessments.

7

Conclusion & Discussion

This research aimed to create an understanding of the way cybersecurity professionals deal with uncertainty about the IS environment in an IS risk assessment. Thereby this research diverted from the identification of quantifying uncertainty, but instead aimed to understand the perceptual aspects and judgment operations of cybersecurity professionals during an IS risk assessment. Through theoretical exploration, a conceptual framework was constructed that allowed the research objective to be studied. Fifteen (15) cybersecurity professionals who are actively involved in the execution of IS risk assessments were interviewed to create an understanding of the research problem.

This chapter provides a conclusion to this research project. The synthesised results are interpreted to answer the research questions in Section 7.1. The research is consequently discussed, delineating the limitations in Section 7.2 and the implications in Section 7.3. The possibilities for future research are discussed in Section 7.4. Finally, the thesis is concluded with a link to the curriculum in Section 7.5.

7.1. Answering the research questions

This section will answer the research questions. First, the two (2) sub–questions are answered, and the section is finalised with the answering of the main research question.

SQ1: How do cybersecurity professionals perceive uncertainty about the organisation's information security environment in a risk assessment?

To answer this question, it is essential to underscore that uncertainty about the IS environment has to be experienced by the cybersecurity professional. This experienced uncertainty was not the case for all respondents of this research. The findings to this research question therefore show how the respondents perceive uncertainty about the IS environment if they, in fact, experience to be uncertain during judgment operations in the IS risk assessment. The results relate to the theory on perceived environmental uncertainty (PEU) from Gerloff et al. [26] and Milliken [50], identifying two types of uncertainty perceived about the IS environment in a risk assessment. Contributing factors for the perception of uncertainty are identified as well as new insights:

State uncertainty

The results show that cybersecurity professionals perceive state uncertainty during the asset identification (step 1.1), the identification of existing controls (step 1.3) and the likelihood analysis (step 2.2). State uncertainty is experienced by the cybersecurity professional when the state of the IS environment is perceived to be unpredictable. Thereby difficulties are experienced in understanding how the IS environment is changing, or in grasping the interrelations between components within the IS environment. This form of uncertainty demonstrates itself when difficulties are experienced in assigning accurate probability estimates about the IS environment or in estimating the current state/nature of changes and interrelations in the IS environment.

The findings suggest that complexity and dynamism cause state uncertainty in the IS environment. Complexity references to the many components and number of interrelations between the organisation's general landscape information and information systems. This makes it difficult to assess the interrelations in the organisation's IS environment. Dynamism refers to the changing nature of interrelations within the organisation's general landscape of information and information systems. This creates difficulties in estimating the likelihood of changes/events in the organisation's IS environment.

Effect uncertainty

The results show that respondents perceive effect uncertainty during the threat identification (step 1.2), the vulnerability identification (step 1.4), the CIA identification (step 1.5) and the business impact value analysis (step 2.1). This is experienced when the respondent experiences to be unable to accurately predict what the impact is from changes/events in the organisation's IS environment. This form of uncertainty demonstrates itself when cause – effect relationships are difficult to identify, experiencing to be unable to accurately predict the nature, severity and timing of impact.

The findings suggest that both complexity and dynamism create effect uncertainty in the IS environment. The complexity references to the many interrelations and layers of the information and information systems in the organisation's IS environment, which make it difficult to assess how threats are relevant, how information is processed by the information systems and how the context needs to be incorporated to examine the impact. Dynamism is referring to the changing and ever–evolving nature within the IS environment, relating to the threat landscape that evolves and incorporates new technologies, as well as the dynamics of different business contexts. Creating difficulty in tracking all changes that can impact the organisation.

Factors for uncertainty

Contributing factors of complexity and dynamism for both state and effect uncertainty are identified to be shadow IT, organisational structuring and the innovation processes that are active within an organisation IS environment.

The theory delineates the sources of variability as complexity, dynamism, individual cognitive characteristics, the availability of response options and the social expectation from the organisation. Indicated above, the complexity and dynamism attribute to causing uncertainty, i.e. have a positive influence on the perception of uncertainty. The findings suggest that the individual cognitive characteristics and the availability of response options have a negative influence on the respondents' perception of uncertainty, i.e. do not create uncertainty.

Unfathomable uncertainty

The study also discovered a form of uncertainty that was not directly related to the PEU theory. This form of uncertainty was identified with the vulnerability identification (step 1.4) and revolved around unknown–unknowns. Thereby the respondents experienced unknowns from whether all vulnerabilities have been identified, as well as what the impact of vulnerabilities would be on the organisation's IS environment. The factor attributed to the perception of uncertainty centres around the partial blindness in which the respondents indicate to assume not being able to identify all vulnerabilities of the organisation.

SQ2: How do cybersecurity professionals provide judgment under the perception of uncertainty about the organisation's information security environment?

This sub–question is answered based on the results from the respondents who indicated to experience uncertainty during the IS risk assessment steps. The theory on judgment heuristics from Tversky and Kahneman [69], Mussweiler and Strack [52] and Strack and Mussweiler [67] is partially used to understand how judgment is provided under uncertainty. The theorised concepts allow analysing the judgment operations from the cybersecurity professional. Thereby the theory aids in explaining and interpreting the responses about the judgment operations when uncertainty is experienced during the IS risk assessment. Also, findings that are not related to the theorised concept on judgment heuristics are extracted from the data, which will be explained after the parts explained by the theorised concepts. The conceptual framework delineates three (3) judgment heuristics from which the findings are

depicted below, as well as the relevant findings on how judgment is provided under uncertainty when theory could not be used to explain the judgment operations:

Availability heuristic
The findings identify the use of the availability heuristic during the CIA identification (step 1.5) and the likelihood analysis (step 2.2). The respondents indicated that easy retrievability of large events was taken into account during the likelihood analysis. They referred to incidents experienced or cases that were extensively covered that created a thorough imprint in the respondent's recollection that allowed it to be easily retrievable to provide judgment in the identified steps.

Representative heuristic
The representative heuristic is identified within the CIA identification (step 1.5) and the business impact value analysis (step 2.1). Thereby respondents indicated to actively compare cases to find similarities that allow judgment. For the CIA identification, a representative asset was analysed for similarities to allow the CIA classification. Furthermore, the respondents indicate to analyse scenarios that were deemed similar to the scenario of the risk assessment, thereby looking for a business impact value based on the representativeness of the scenario.

Selective accessibility model
The results show that the respondents use the selective accessibility model for the asset identification (step 1.1), the threat identification (step 1.2), the business impact value analysis (step 2.1) and the likelihood analysis (2.2). Thereby judgment operations are provided by actively evaluating the information provided as a suitable answer to the judgment problem. The results show that respondents often stay close to the values provided, such as reports from previous assessments, input from stakeholders, industry/market standards and the data available from materialised incidents. Thereby the hypothesised correctness and accuracy of answers in judgment operations often resulted in the respondent staying close to the initial information/values provided.

Remarks and relevant findings
The results show that heuristics are not identified with all the IS risk assessment steps when the respondents experience uncertainty. Additionally, it is to be noted that not all respondents reference to judgment heuristics. Respondents also highlighted other methods/processes on how they provide judgment when under uncertainty, depicted in this subsection.

The results show that the respondents do not always actively provide judgment whenever they perceive to be uncertain during the IS risk assessment steps. Often reference was made to the accountability structure of the organisation, indicating that final judgment was not part of the respondent's responsibilities because they are in the second line of defence. Thereby the business/risk owner was responsible for providing a final judgment call, which prevented the respondents from providing more information on their judgment operations. What is important to note is that the accountability structure does not reduce the uncertainty, because the respondents indicated that often they were uncertain if the people involved in the final decision–making are interested, well-informed or possess the right knowledge to provide judgment during the IS risk assessment.

Additionally, the respondents indicated to rely on the security policy and philosophy within the organisation that was focused on detection and response, not providing further judgment. The respondents indicated that a paradigm shift in the security policy and philosophy. They are thereby indicating that the focus has shifted from prevention to the detection and response on IS incidents. This focus shift does not entail that the prevention is neglected, but it is somewhat accepted that not all incidents can be prevented and that the subsequent detection and response will go a long way to reduce the impact from an incident to the organisation. Consequently, the respondents did not provide further judgment whenever they perceived to be unable to provide accurate estimates. It could not be identified what the influence on the uncertainty was with the respondents.

Finally, the respondents indicated to judge the security awareness of the people involved to determine the risk. These processes allowed respondents to assign values for the elements within the organisation's IS environment. The results do not provide insight into the influence on the uncertainty of the respondents.

Research question:
How do cybersecurity professionals deal with perceived uncertainty about their organisation's information security environment in a risk assessment?

The research question is answered by combining the knowledge from the above depicted sub–questions. It is essential to acknowledge that the research question has a double–barrelled character due to the word *'deal'* which implies that the respondent first has to perceive uncertainty about the IS environment before providing judgment about the IS environment. This combines both sub–questions and is supported by the conceptual framework of this research. Consequently, the research question is answered in the order of the posed sub–questions. Please note that the respondents are referred to as cybersecurity professionals. However, this does not imply the results can be generalised over the population but is merely for illustrative purposes to identify the sample.

The results show that cybersecurity professionals perceive uncertainty about the IS environment in which it is difficult to: grasp the different interrelations in the organisation's landscape of information and information systems, assign accurate values to the occurrence of changes/events in the IS environment and to determine the impact from changes/events to the organisation. This uncertainty is caused by the complexity and dynamism dimension within the organisation's IS environment. Indicated factors attributed to these dimensions are shadow IT, the innovation processes within an organisation and the organisational structuring.

The judgment operations of the cybersecurity professionals are partly explained with the help from judgment heuristics. The data shows that the selective accessibility model is predominantly used to provide judgment about the IS environment during risk assessments. Thereby heavily relying on the information provided to them from different sources, consequently staying close to the initial values. The availability and representative heuristic are also identified but are referenced in fewer instances. This would suggest that the cybersecurity professional assess the information more on a case–by–case basis, rather than providing judgment based on similarity or the ease with which a scenario is retrieved from memory. Aside from the identified heuristics, the cybersecurity professional is observed not to be included in the final judgment. In such cases the uncertainty is then accepted because it is not part of their responsibility. Additionally, the security policy and philosophy paradigm shift from prevention to detection and response allow the cybersecurity professional to accept that not all IS incidents can be prevented. But that detection and response of IS incidents allow the impact to the organisation to be minimised. Finally the cybersecurity professional also judges the security awareness of the people involved when providing judgment operations during an IS risk assessment.

7.2. Limitations

This section describes the limitations of the varying aspects of this research study. The defined aspects are shown in italic.

The access to *literature* that examines the perception of uncertainty in IS risk assessments is considered limited. Although much literature is available on the concepts of risk and uncertainty, much is devoted to the quantification of the phenomena in relation to decision theory in the field of IS. This makes it hard to situate this research within the current body of knowledge, which is also identified by the knowledge gap in Subsection 1.1.1. Additionally, it is acknowledged that the literature available on the concepts is considered relatively old. The concept of PEU is mostly researched from the 1960s – 1990s and from that point on little attention is given to the theory. This is considered to be a limitation because the researcher argues that the organisational structuring has changed much since which is arguable of influence on an organisational/management theory.

It is essential to acknowledge that the *data collected* is coming from the respondent's memory on how one perceives to be experiencing the situation and subsequently acts. Additionally, the topic of uncertainty can be interpreted ambiguously, despite the researcher having provided a clear definition in the context of this research (see introduction text in Figure C.6). As such the from memory generated data can be distorted by the human cognition which needs to be acknowledged.

Furthermore, it needs to be stipulated that the *language* of the interviews are not all in English. Fourteen (14) of the fifteen (15) interviews are conducted in Dutch to accommodate the native language of the respondent. This forced a translation step from the researcher in both the designing of interview

questions as well as during the coding process. The researcher points out that the interview questions are kept as close to the theoretical concepts as possible, to minimise the introduction biases.

The *semi–structured interview approach* in combination with the ISO27005 methodology add rigour to this methodology. Although the ISO27005 methodology is widely known, including its terminology, the interpretation and execution vary significantly among organisations. This depends on whether the organisation is in a compliance domain and what the general attitude towards pragmatism in the execution of an IS risk assessment is. Consequently, it was found that not all questions had fifteen responses due to the structure of involvement as well as the methodology adopted. Although the amount of missing data from the sample was limited, it is important to note as a limitation.

During the *analysis phase in which the theory and data are synthesised*, it proofed that the PEU theory could not explain a large part of the uncertainty experienced in the vulnerability identification (step 1.4). The researcher had to adopt terminology on unfathomable uncertainty from Kim [41] in this step. As such, it must be concluded that the PEU theory was unable to provide guidance in the interpretation of data for all IS risk assessment steps as prescribed by the ISO27005.

Finally, it needs to be acknowledged that the *interpretation of the data* (i.e., the coding process) is executed by one (1) researcher. The coding scheme (depicted in Table 4.1) intends to provide rigour, but it must be acknowledged that the identification and interpretation of key themes depend on one pair of eyes.

7.3. Implications

7.3.1. Scientific implications

This study contributes knowledge in various ways to the current body of literature. This study is the first to break ground on researching the perceptual aspects of uncertainty and the judgment operations in dealing with uncertainty from cybersecurity professionals in IS risk assessments. Contributing novel research to the current body of knowledge.

Secondly, based on the definition of IS by Cherdantseva and Hilton [14] this research created a novel way of conceptualising the IS environment of an organisation and thereby allowing the PEU theory to be used for research. This conceptualisation opens the door for new methods of research based on the conceptualised IS environment. Furthermore, previously unknown phenomena to the cybersecurity professionals perception of uncertainty in IS risk assessment setting are discovered.

Thirdly, new insights are created of the perception of unfathomable uncertainty that circles the integrality of unknown–unknowns about the vulnerability identification of the IS risk assessment. Although the concept of unknown–unknowns is central to literature on risk assessments (in which unfathomable uncertainty is coined by Kim [41]), the conceptualisation based on the integrality for the vulnerability identification is according to the researcher's knowledge novel to the current body of literature.

Finally, to the best of the researcher's knowledge, this study is novel in unifying the theorised concepts in relation to the IS risk assessment setting. Previous research has focused on identifying heuristics and biases in the IS context [7, 47], but this focused on Prospect Theory from Kahneman and Tversky [39]. Furthermore, no other instance of the PEU theory in relation to the IS context could be discovered.

7.3.2. Managerial and societal implications

This research identifies concrete factors that contribute to the cybersecurity professionals' perception of uncertainty about the organisation's IS environment. The results can be used by organisations to identify and treat potential factors that create difficulties for their cybersecurity professionals to accurately provide judgment during IS risk assessments.

The most crucial managerial aspect that needs to be taken into consideration are the stakeholders in the IS risk assessment. This refers not only to the cybersecurity professionals but also to the business/risk owners. It is evident that the accountability structure within an organisation plays a decisive role in the IS risk assessment. The results show that even though the cybersecurity professionals are not accountable for the risks, which prevents them from final judgment operations to provide value estimates, their doubts with the informedness, interest and knowledge of the business/risk owners is not reduced with this accountability structure. Thereby it is argued that the cybersecurity professionals are not always confident with the judgment from the business/risk owners when it comes to security. Considering the ownership of security is with the cybersecurity professional, it is essential to understand

from a managerial perspective how these different stakeholder influence one another in order for an organisation to have the most useful information security. Consequently, the discussion about ownership of risk and security for the organisation's informational assets is argued a priority for managers.

Furthermore, by understanding the factors that inflict difficulties in the IS risk assessment process organisations can spend their financial resources most effectively to achieve the operational goals with minimum risk, as is stressed by Beautement et al. [6]. This consequently benefits both the organisation and society at large that benefit from the possibility of lower costs for a more accurately assessed level of organisational IS.

This research has shed light on how cybersecurity professionals deal with perceived uncertainty about the IS environment in a risk assessment. Thereby the goal of creating a safer digital environment for society is supported through increased understanding of the perceptual aspects and judgment operations of cybersecurity professionals in an IS risk assessment.

In sum, the managerial and societal relevance can be found in the understanding of sources for perceived uncertainty and the subsequent actions from cybersecurity professionals in IS risk assessments. This allows the organisations to fulfil the societal needs that demand a safer digital environment in the most cost–efficient way.

7.4. Future research

This study has provided insights into the perceptional aspect and judgment operations of cybersecurity professionals during an IS risk assessment. However, future research opportunities are also identified in this study. These are partly based on the limitations, but also new themes are identified that are considered relevant for further exploration.

This research has adopted a qualitative approach to identify if the theoretical concepts can be used in the IS risk assessment setting. Future research could focus on developing quantitative methods to explore the perception of uncertainty from cybersecurity professionals. The current results on PEU (as depicted in Figure 6.1) can be tested with a larger sample of respondents that would allow the findings to be generalised.

To validate the results, a replication study would be appropriate because this is the first study of its kind that uses these theoretical concepts in this IS context. This replication study is consequently advised to be executed in native English speaking countries to remove any possible biases introduced by translating efforts from the researcher.

The issue of integrality, i.e. the completeness of the identification processes, during the IS risk assessment was identified in three (3) steps as a factor for the perception of uncertainty. Future research could focus on items that contribute to the integrality issue during an IS risk assessment to better understand how they contribute to the perception of uncertainty and to compare the factors with relevant findings from this research. This could create a complete picture on the factors and perceptions of uncertainty during an IS risk assessment.

Relevant to the research findings is the identification of shadow IT that influences the perception of uncertainty of cybersecurity professionals. The researcher however did not identify the relationship with the IS policies of an organisation in relation to shadow IT, as this was not the scope of the study. However, currently lots of research is executed on the security awareness of employees within an organisation. Amongst others, Bulgurcu et al. [11] focuses on the employee's compliance with IS policy from a rationality–based perspective. Consequently, future researchers could focus on the interpretation of the IS policy of an organisation in relation to shadow IT. Understanding and aiming the reduction of uncertainty from shadow IT by effectively incorporating it with the organisation's policies and subsequent IS risk assessments.

This research has adopted a rigorous approach based on the ISO27005 methodology. As explained in Section 7.2, this had some limitations. Future research could adopt a methodology in which the ISO27005 framework does not form the backdrop of the interviews. Instead, a topic list can be used that focuses on issues experienced during IS risk assessments, rather than focusing solely on the concept of perceived uncertainty. This topic list allows the identification of possibly undiscovered fundamental issues experienced by cybersecurity professionals in an IS risk assessment.

Finally, the researcher observed the influence of the organisation's accountability structure, based on the three lines of defence model, on the cybersecurity professional's judgment operations during an IS risk assessment. Reference was made to the correctness, informedness and interest of the stake-

holders involved in the IS risk assessment. From this study it could be identified that ownership over security against the business/risk ownership do not always align, thereby stressing the IS risk assessment. Work regarding the effectiveness and influence on the correctness of the IS risk assessments could be executed in relation to the accountability structure within an organisation. Additionally, this research could be extended by incorporating the perceptual aspects and judgment operations of the business/risk owners.

7.5. Link with the Management of Technology curriculum

The master's program in Management of Technology requires analysing the impact from technology and the associated processes on the organisation's ability function. Thereby taking the technological, economical and societal perspectives into account.

This research project has provided me with the opportunity to analyse these different perspectives within the field of IS risk assessments. It is thereby focusing on the inception of the decision–making process on the integration and use of technologies. Insights are gained into how IS technologies with the associated processes are used within an organisation, examining the technological and economical perspective in relation to the risks of an organisation bears. However, crucial to an organisation's IS activities, is the societal perspective. This essentially provides security to society at large, that demands a safe digital environment. The combination of the three perspectives in an IS risk assessment determine the organisation's future profitability because appropriate strategies can be devised that allow solutions to be incorporated to mitigate the risks from the IS environment — thereby adhering to all three perspectives.

Bibliography

[1] Luca Allodi and Fabio Massacci. Security events and vulnerability data for cybersecurity risk estimation. *Risk Analysis*, 37(8):1606–1627, 2017. doi: 10.1111/risa.12864.

[2] Nicholas J. Ashill and David Jobber. Measuring state, effect, and response uncertainty: Theoretical construct development and empirical validation. *Journal of Management*, 36(5):1278–1308, sep 2010. ISSN 0149-2063. doi: 10.1177/0149206308329968. URL http://journals.sagepub.com/doi/10.1177/0149206308329968.

[3] Terje Aven. Foundational issues in risk assessment and risk management. *Risk Analysis*, 32(10): 1647–1656, 2012. doi: 10.1111/j.1539-6924.2012.01798.x.

[4] Terje Aven. The risk concept—historical and recent development trends. *Reliability Engineering & System Safety*, 99:33–44, 2012. doi: 10.1016/J.RESS.2011.11.006.

[5] Terje Aven and Ortwin Renn. The role of quantitative risk assessments for characterizing risk and uncertainty and delineating appropriate risk management options, with special emphasis on terrorism risk. *Risk Analysis*, 29(4):587–600, 2009. doi: 10.1111/j.1539-6924.2008.01175.x.

[6] Adam Beautement, M. Angela Sasse, and Mike Wonham. The compliance budget. In *Proceedings of the 2008 workshop on New security paradigms - NSPW '08*, page 47. ACM Press, 2008. ISBN 9781605583419. doi: 10.1145/1595676.1595684.

[7] Nicole L Beebe, Diana K Young, and Frederick R Chang. Framing information security budget requests to influence investment decisions. *Communications of the Association for Information Systems*, 35(7):133–143, 2014. doi: 10.17705/1CAIS.03507.

[8] Bob Blakley, Ellen McDermott, and Dan Geer. Information security is information risk management. In *Proceedings of the 2001 workshop on New security paradigms - NSPW '01*, page 97, New York, New York, USA, 2001. ACM Press. ISBN 1581134576. doi: 10.1145/508171.508187.

[9] João Pedro Niza Braga, Mário Boto Ferreira, and Steven J. Sherman. Disentangling availability from representativeness: Gambler's fallacy under pressure. In C. Andrade, D. Garcia, S. Fernandes, T. Palma, V. Silva, M. B. Monteiro, and P. Castro, editors, *Research Directions in Organizational and Social Psychology*. Edições Sílabo, 2013. URL https://www.researchgate.net/profile/Joao_Braga/publication/271133677.

[10] Alan Bryman. *Social Research Methods*. Oxford University Press, 4th edition, 2012. ISBN 9780199588053.

[11] Burcu Bulgurcu, Hasan Cavusoglu, and Izak Benbasat. Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3):523, 2010. doi: 10.2307/25750690.

[12] Gretchen B. Chapman and Eric J. Johnson. Anchoring, activation, and the construction of values. *Organizational Behavior and Human Decision Processes*, 79(2):115–153, 1999. doi: 10.1006/OBHD.1999.2841.

[13] Charted Institute of Internal Auditors. Governance of risk: Three lines of defence | Audit committees | Resources | IIA, 2019. URL https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/.

[14] Yulia Cherdantseva and Jeremy Hilton. Information security and information assurance: The discussion about the meaning, scope and goals. In *F. Almeida, and I. Portela (eds.), Organizational, Legal, and Technological Dimensions of IS Administrator*, pages 167–198. IGI Global Publishing, 2013. doi: 10.4018/978-1-4666-4526-4.ch010.

[15] Darthmouth Engineering. The future of cyber security risk [Video File], 2012. URL https://www.youtube.com/watch?v=zBx0hcj9_AU{&}t=461s.

[16] Jennie De Vries. What drives cybersecurity investment?, 2017. URL https://repository.tudelft.nl/islandora/object/uuid%3A119719ff-cb69-44c5-a566-3ee8373509f7?collection=education.

[17] Laura DeNardis. A history of internet security. In *The History of Information Security*, pages 681–704. Elsevier Science B.V., 2007. ISBN 9780444516084. doi: 10.1016/B978-044451608-4/50025-0. URL https://www.sciencedirect.com/science/article/pii/B9780444516084500250.

[18] H. Kirk Downey. Perceived uncertainty: Conceptual frameworks and research instruments. *Academy of Management Proceedings*, 1974(1):54–54, 1974. ISSN 0065-0668. doi: 10.5465/ambpp.1974.17531402.

[19] H. Kirk Downey and R. Duane Ireland. Quantitative Versus Qualitative: Environmental Assessment in Organizational Studies. *Administrative Science Quarterly*, 24(4):630, 1979. ISSN 00018392. doi: 10.2307/2392368.

[20] H. Kirk Downey, Don Hellriegel, and John W. Slocum. Individual characteristics as sources of perceived uncertainty variability. *Human Relations*, 30(2):161–174, 1977. doi: 10.1177/001872677703000205.

[21] Robert B. Duncan. Characteristics of organizational environments and perceived environmental uncertainty. *Administrative Science Quarterly*, 17(3):313–327, 1972. URL https://www.jstor.org/stable/pdf/2392145.pdf?acceptTC=true.

[22] European Commission. EU data protection rules | European Commission, 2019. URL https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

[23] Nan Feng and Minqiang Li. An information systems security risk assessment model under uncertain environment. *Applied Soft Computing*, 11(7):4332–4340, 2011. doi: 10.1016/J.ASOC.2010.06.005.

[24] Klaus Fiedler and Momme von Sydow. Heuristics and biases: Beyond Tversky and Kahneman's (1974) judgment under uncertainty. In *Cognitive psychology: Revisiting the classical studies*, chapter 12, pages 146–161. Sage, London, 2015. ISBN 9781446294475.

[25] Vaibhav Garg and Jean Camp. Heuristics and biases: Implications for security design. *IEEE Technology and Society Magazine*, 32(1):73–79, 2013. ISSN 02780097. doi: 10.1109/MTS.2013.2241294.

[26] Edwin A. Gerloff, Nan Kanoff Muir, and Wayne D. Bodensteiner. Three components of perceived environmental uncertainty: An exploratory analysis of the effects of aggregation. *Journal of Management*, 17(4):749–768, 1991. doi: 10.1177/014920639101700408.

[27] William E. Gifford, H. Randolph Bobbitt, and John W. Slocum. Message characteristics and perceptions of uncertainty by organizational decision makers. *Academy of Management Journal*, 22 (3):458–481, 1979. ISSN 0001-4273. doi: 10.5465/255738.

[28] Gerd Gigerenzer. How to make cognitive illusions disappear: Beyond "heuristics and biases". *European Review of Social Psychology*, 2(1):83–115, 1991. doi: 10.1080/14792779143000033.

[29] Gerd Gigerenzer. On narrow norms and vague heuristics: A reply to Kahneman and Tversky. *Psychological Review*, 103(3):592–596, 1996. doi: 10.1037/0033-295X.103.3.592.

[30] Gerd Gigerenzer. Why heuristics work. *Perspectives on Psychological Science*, 3(1):20–29, 2008. doi: 10.1111/j.1745-6916.2008.00058.x.

[31] Gerd. Gigerenzer, Peter M. Todd, and ABC Research Group. *Simple heuristics that make us smart*. Oxford University Press, 1999. ISBN 9780195143812.

[32] Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, and Lei Zhou. Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security*, 06(01):24–30, 2015. doi: 10.4236/jis.2015.61003.

[33] Rajesh Kumar Goutam. Importance of cyber security. *International Journal of Computer Applications*, 111(7), 2015. URL https://pdfs.semanticscholar.org/5cfb/7a5bd2e6c181e8a69ebd49b1dadb795f493b.pdf.

[34] Caitlin E. Hansen, Anna North, and Linda M. Niccolai. Cognitive bias in clinicians' communication about human papillomavirus vaccination. *Health Communication*, pages 1–8, 2019. doi: 10.1080/10410236.2019.1567439.

[35] Paul Hunton. Data attack of the cybercriminal: Investigating the digital currency of cybercrime. *Computer Law & Security Review*, 28(2):201–207, 2012. doi: 10.1016/J.CLSR.2012.01.007.

[36] ISACA. *CISA Review Manual 2006*. Information Systems Audit and Control Association, 2006. ISBN 978-1-933284.

[37] Daniel Kahneman. *Thinking fast and slow*. Penguin Books, 2011. ISBN 978-0-141-03357-0.

[38] Daniel Kahneman and Shane Frederick. Representativeness revisited: Attribute substitution in intuitive judgment. *Heuristics and biases: The psychology of intuitive judgment*, 49(81), 2002. doi: 10.1017/CBO9780511808098.004.

[39] Daniel Kahneman and Amos Tversky. Prospect theory: An analysis of decision making under risk. *Econometrica: Journal of the Econometric Society*, 47(2):263–291, 1979. URL https://www.uzh.ch/cmsssl/suz/dam/jcr:00000000-64a0-5b1c-0000-00003b7ec704/10.05-kahneman-tversky-79.pdf.

[40] Daniel Kahneman and Amos Tversky. On the reality of cognitive illusions. *Psychological Review*, 103(3):582–591, 1996. doi: 10.1037/0033-295X.103.3.582.

[41] Seong Dae Kim. Characterizing unknown unknowns. In *Papter presented at PMI Global Congress 2012 - NOrth America Vancouver, British Columbia, Canada. Newton Square, Pa: Project Management Institttue*, 2012.

[42] Alan Lewis. *The Cambridge handbook of psychology and economic behaviour*. Cambridge University Press, 2008. ISBN 9780521856652.

[43] William M. Lindsay and Leslie W. Rue. Impact of the organization environment on the long-range planning process: A contingency view. *Academy of Management Journal*, 23(3):385–404, 1980. doi: 10.5465/255507.

[44] Radoica Luburic, Milan Perovic, and Rajko Sekulovic. Quality management in terms of strengthening the "three lines of defence" in risk management - process management. Technical report, 2015. URL https://www.researchgate.net/publication/279180559.

[45] R.D. Luce and H. Raiffa. *Games and decisions: introduction and critical survey*. John Wiley & Sons, Inc., 1957. ISBN 9780471553410.

[46] Julian N. Marewski, Wolfgang Gaissmaier, and Gerd Gigerenzer. We favor formal models of heuristics rather than lists of loose dichotomies: A reply to Evans and Over. *Cognitive Processing*, 11(2):177–179, 2010. ISSN 1612-4782. doi: 10.1007/s10339-009-0340-5.

[47] Konstantinos Mersinas, Bjoern Hartig, Keith M. Martin, and Andrew Seltzer. Are information security professionals expected value maximizers?: An experiment and survey-based test. *Journal of Cybersecurity*, 2(1):57–70, 2016. ISSN 2057-2085. doi: 10.1093/cybsec/tyw009.

[48] Raymond E. Miles, Charles C. Snow, Alan D. Meyer, and Henry J. Coleman. Organizational strategy, structure, and process. *The Academy of Management Review*, 3(3):546, 1978. doi: 10.2307/257544.

[49] David Miller. How has cyber security changed?, 2017. URL https://www.uzado.com/blog/how-has-cyber-security-changed.

[50] Frances J Milliken. Three types of perceived uncertainty about the environment: State, effect, and response. Technical Report 1, 1987. URL https://www.jstor.org/stable/257999?seq=1{&}cid=pdf-reference{#}references_tab_contents.

[51] Thomas Mussweiler and Birte Englich. Subliminal anchoring: Judgmental consequences and underlying mechanisms. *Organizational Behavior and Human Decision Processes*, 98(2):133–143, 2005. doi: 10.1016/j.obhdp.2004.12.002.

[52] Thomas Mussweiler and Fritz Strack. Hypothesis-consistent testing and semantic priming in the anchoring paradigm: A selective accessibility model. *Journal of Experimental Social Psychology*, 35(2):136–164, 1999. doi: 10.1006/JESP.1998.1364.

[53] NEN. NEN-EN-ISO/IEC 27050 Information technology - Security techniques - Storage security. Technical report, Nederlandse Norm, 2015.

[54] NEN. NEN-ISO/IEC 27005 Information technology - Security techniques - Information security risk management. Technical report, Nederlandse Norm, 2018.

[55] NEN. NEN-EN-ISO/IEC 31000 Risk Management - Guidelines. Technical report, Nederlandse Norm, 2018.

[56] NIST. Guide for conducting risk assessments. Technical report, National Institute of Standards and Technology, 2012.

[57] Shari Lawrence Pfleeger and Deanna D. Caputo. Leveraging behavioral science to mitigate cyber security risk. *Computers & Security*, 31(4):597–611, 2012. ISSN 0167-4048. doi: 10.1016/J.COSE.2011.12.010.

[58] Heather Rosoff, Jinshu Cui, and Richard S. John. Heuristics and biases in cyber security dilemmas. *Environment Systems and Decisions*, 33(4):517–529, 2013. ISSN 21945403. doi: 10.1007/s10669-013-9473-2.

[59] Brent R Rowe and Michael P Gallaher. Private sector cyber security investment strategies: An empirical analysis. In *The Fifth Workshop on the Economics of Information Security (WEIS 2006)*, 2006. URL https://pdfs.semanticscholar.org/a188/0f3fc72ab11f5eca24fa6970eb2a8ab69c4f.pdf.

[60] Julie J.C.H. Ryan, Thomas A. Mazzuchi, Daniel J. Ryan, Juliana Lopez de la Cruz, and Roger Cooke. Quantifying information security risks using expert judgment elicitation. *Computers & Operations Research*, 39(4):774–784, 2012. doi: 10.1016/J.COR.2010.11.013.

[61] Daniel Schatz and Rabih Bashroush. Economic valuation for information security investment: A systematic literature review. *Information Systems Frontiers*, 19(5):1205–1228, 2017. ISSN 15729419. doi: 10.1007/s10796-016-9648-8.

[62] Neil J. Schroeder. Using prospect theory to investigate decision-making bias within an information security context, 2005. URL https://apps.dtic.mil/dtic/tr/fulltext/u2/a445399.pdf.

[63] Uma Sekaran and Roger Bougie. *Research methods for business*. John Wiley & Sons, Ltd, 6 edition, 2013. ISBN 9781119942252.

[64] Joseph P. Simmons and Robyn A. LeBoeuf. The effect of accuracy motivation on anchoring and adjustment: Do people adjust from provided anchors? *Journal of Personality and Social Psychology*, 99(6):917–932, 2010. doi: 10.1037/a0021540.

[65] Herbert A. Simon. The scientist as problem solver. Technical report, Carnegie Mellon University - Department of Psychology, Pittsburg, Pennsylvania, 1989.

[66] Statista. Annual number of data breaches and exposed records in the United states from 2005 to 2018 (in millions), 2019. URL https://www.statista.com/statistics/273550/.

[67] F Strack and T Mussweiler. Explaining the enigmatic anchoring effect: Mechanisms of selective accessibility. *Journal of personality and social psychology*, 73(3):437–446, 1997. doi: 10.1037/0022-3514.73.3.437.

[68] D. P. Thunnissen. Uncertainty classification for the design and development of complex systems. In *3rd annual predictive methods conference*, pages 1–16, CA: Newport Beach, 2003.

[69] A Tversky and D Kahneman. Judgment under uncertainty: Heuristics and biases. *Science (New York, N.Y.)*, 185(4157):1124–31, 1974. ISSN 0036-8075. doi: 10.1126/science.185.4157.1124.

[70] Nicole Van der Meulen. Investing in cybersecurity. Technical report, RAND Europe, 2015. URL https://www.wodc.nl/binaries/2551-full-text_tcm28-73946.pdf.

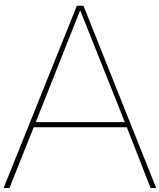
[71] Willem Van Dijk. An evaluation of Gigerenzer's criticism on the heuristics and biases program's base-rate neglect studies, 2016. URL https://pdfs.semanticscholar.org/1286/f0e4cd2c933dd62af2691f222e05eb2a9ccd.pdf.

[72] Paul Van Schaik, Debora Jeske, Joseph Onibokun, Lynne Coventry, Jurjen Jansen, and Petko Kusev. Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, 75:547–559, oct 2017. ISSN 0747-5632. doi: 10.1016/J.CHB.2017.05.038. URL https://www.sciencedirect.com/science/article/pii/S074756321730359X.

[73] Ping Wang and Melva Ratchford. Integrated Methodology for Information Security Risk Assessment. In *Information Technology - New Generations*, pages 147–150. Springer International Publishing, 2018. ISBN 9783319549781. doi: 10.1007/978-3-319-54978-1_20.

[74] Eva Weishäupl, Emrah Yasasin, and Guido Schryen. Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. *Computers and Security*, 77:807–823, 2018. ISSN 01674048. doi: 10.1016/j.cose.2018.02.001.

[75] Timothy D. Wilson, Christopher E. Houston, Kathryn M. Etling, and Nancy Brekke. A new look at anchoring effects: Basic anchoring and its antecedents. *Journal of Experimental Psychology: General*, 125(4):387–402, 1996. URL https://pdfs.semanticscholar.org/9c84/a4a66e23dc43143a6b8e706ae550d39a31f8.pdf.



Interview script and associated concepts

This appendix contains the interview script in which it is elaborated per question how the theoretical concepts from Chapter 3 are associated.

Context establishing questions							Comments
Q1	Could you briefly describe your role within your organisation?						The role provides insight in the activities and involvement in ISRA.
(NL)	Zou u kort uw rol binnen uw organisatie kunnen beschrijven?						
Q2	Could you briefly describe how you are involved in organisational information security risk assessments?						The role provides insight in the activities and involvement in ISRA.
(NL)	Zou u kort kunnen beschrijven hoe u betrokken bent bij de organisatorische informatiebeveiligings risico assessments?						
Q3	Could you describe how long you have been working in this role or similar (also in other companies/positions)?						This question relates to the concept of PEU, where experience (identified by 'response options') counts.
(NL)	Zou u kunnen beschrijven hoe lang u al in deze rol of vergelijkbaar werkzaam bent?						
Q4	Are you educated to execute information security risk assessments? Do you believe this helps/hinders you in the execution?						This aims to identify some of the individual's cognitive characteristics for the PEU concept.
(NL)	Bent u opgeleid in het uitvoeren van informatiebeveiligings risico assessments? Heeft u het idee dat dit u helpt/hindert?						
PEU & Judgment under uncertainty questions							
Research question		**Risk assessment step**	**Sub-questions**	***Theory concepts***	**Q#**	**Questions (EN)**	**Questions (NL)**
How do security professionals deal with perceived uncertainty about their organization's information security environment in a risk assessment?		**1.1** - Asset identification	What type of uncertainty do security professionals perceive about the organization's information security environment in a risk assessment?		**Q5**	Could you briefly describe how you identify **assets (crown jewels, assets of value)** of your organisation?	Zou u kort kunnen beschrijven hoe u de **assets (kroonjuwelen, assets van waarde)** van uw organisatie identificeert?	This question allows the respondent to retrieve instances and examples of how they execute the task in the risk assessment process. It additionally provides insight into the processes and allows the researcher to build upon the given information.
					Q5 - U	Do you ever experience uncertainty while doing so?	Ervaart u hierbij wel eens onzekerheid?	This question is to identify if the respondent experiences uncertainty.
				Perceived environmental uncertainty	**Q5Y - A**	Could you describe the nature of your perceived uncertainty? What are the factors that contribute to this?	Zou u de aard van uw ervaren onzekerheid kunnen beschrijven? Wat zijn de factoren hiervoor?	This questions looks into the PEU concept, looking for the nature of the experienced uncertainty and for the contributing factors/causes of this. These can range from environmental items, but also items such as experience (identified by 'response options') and social expectations from the organisation's environment.
			How do security professionals provide judgment under the perception of uncertainty about the organization's information security environment?	*Judgment under uncertainty*	**Q5Y - B**	Could you describe how you provide an estimate despite the experienced uncertainty? What are the steps that you undertake to arrive at your judgment?	Kunt u aangeven hoe u met de ervaren onzekerheid toch tot een inschatting komt? Wat zijn de stappen die u hierin doorloopt?	This questions is to find out how people deal with the experienced uncertainty of that particular step in the risk assessment process. The aim is to identify heuristics in the process.
					Q5N	Could you briefly describe why you don't experience uncertainty?	Kunt u kort kunnen beschrijven waarom u geen onzekerheid ervaart?	This question is to understand why the respondent doesn't experience uncertainty in that particular step of the risk assessment process.

1.2 - Threat identification	What type of uncertainty do security professionals perceive about the organization's information security environment in a risk assessment?		**Q6**	Could you briefly describe how you identify **threats** to your organisation? As an example, think of Russian hackers infiltrating your organisation.	Zou u kort kunnen beschrijven hoe u de **threats** voor uw organisatie identificeert? Hierbij kunt u denken aan bijvoorbeeld een Russische hacker die uw organisatie infiltreert.	This question allows the respondent to retrieve instances and examples of how they execute the task in the risk assessment process. It additionally provides insight into the processes and allows the researcher to build upon the given information.
			Q6 - U	Do you ever experience uncertainty while doing so?	Ervaart u hierbij wel eens onzekerheid?	This question is to identify if the respondent experiences uncertainty.
		Perceived environmental uncertainty	**Q6Y - A**	Could you describe the nature of your perceived uncertainty? What are the factors that contribute to this?	Zou u de aard van uw ervaren onzekerheid kunnen beschrijven? Wat zijn de factoren hiervoor?	This questions looks into the PEU concept, looking for the nature of the experienced uncertainty and for the contributing factors/causes of this. These can range from environmental items, but also items such as experience (identified by 'response options') and social expectations from the organisation's environment.
	How do security professionals provide judgment under the perception of uncertainty about the organization's information security environment?	*Judgment under uncertainty*	**Q6Y - B**	Could you describe how you provide an estimate despite the experienced uncertainty? What are the steps that you undertake to arrive at your judgment?	Kunt u aangeven hoe u met de ervaren onzekerheid toch tot een inschatting komt? Wat zijn de stappen die u hierin doorloopt?	This questions is to find out how people deal with the experienced uncertainty of that particular step in the risk assessment process. The aim is to identify heuristics in the process.
			Q6N	Could you briefly describe why you don't experience uncertainty?	Kunt u kort kunnen beschrijven waarom u geen onzekerheid ervaart?	This question is to understand why the respondent doesn't experience uncertainty in that particular step of the risk assessment process.
1.3 - Identification of existing controls	What type of uncertainty do security professionals perceive about the organization's information security environment in a risk assessment?		**Q7**	Could you briefly describe how you identify **existing controls** organisation wide?	Zou u kort kunnen beschrijven hoe u organisatiebreed **bestaande controls** identificeert?	This question allows the respondent to retrieve instances and examples of how they execute the task in the risk assessment process. It additionally provides insight into the processes and allows the researcher to build upon the given information.
			Q7 - U	Do you ever experience uncertainty while doing so?	Ervaart u hierbij wel eens onzekerheid?	This question is to identify if the respondent experiences uncertainty.
		Perceived environmental uncertainty	**Q7Y - A**	Could you describe the nature of your perceived uncertainty? What are the factors that contribute to this?	Zou u de aard van uw ervaren onzekerheid kunnen beschrijven? Wat zijn de factoren hiervoor?	This questions looks into the PEU concept, looking for the nature of the experienced uncertainty and for the contributing factors/causes of this. These can range from environmental items, but also items such as experience (identified by 'response options') and social expectations from the organisation's environment.

	How do security professionals provide judgment under the perception of uncertainty about the organization's information security environment?	*Judgment under uncertainty*	**Q7Y - B**	Could you describe how you provide an estimate despite the experienced uncertainty? What are the steps that you undertake to arrive at your judgment?	Kunt u aangeven hoe u met de ervaren onzekerheid toch tot een inschatting komt? Wat zijn de stappen die u hierin doorloopt?	This questions is to find out how people deal with the experienced uncertainty of that particular step in the risk assessment process. The aim is to identify heuristics in the process.
			Q7N	Could you briefly describe why you don't experience uncertainty?	Kunt u kort kunnen beschrijven waarom u geen onzekerheid ervaart?	This question is to understand why the respondent doesn't experience uncertainty in that particular step of the risk assessment process.
1.4 - Identification of <u>vulnerabilities</u>	What type of uncertainty do security professionals perceive about the organization's information security environment in a risk assessment?		**Q8**	Could you briefly describe how you identify **vulnerabilities** of your organisation?	Zou u kort kunnen beschrijven hoe u de **vulnerabilities** van uw organisatie identificeert?	This question allows the respondent to retrieve instances and examples of how they execute the task in the risk assessment process. It additionally provides insight into the processes and allows the researcher to build upon the given information.
			Q8 - U	Do you ever experience uncertainty while doing so?	Ervaart u hierbij wel eens onzekerheid?	This question is to identify if the respondent experiences uncertainty.
		Perceived environmental uncertainty	**Q8Y - A**	Could you describe the nature of your perceived uncertainty? What are the factors that contribute to this?	Zou u de aard van uw ervaren onzekerheid kunnen beschrijven? Wat zijn de factoren hiervoor?	This questions looks into the PEU concept, looking for the nature of the experienced uncertainty and for the contributing factors/causes of this. These can range from environmental items, but also items such as experience (identified by 'response options') and social expectations from the organisation's environment.
	How do security professionals provide judgment under the perception of uncertainty about the organization's information security environment?	*Judgment under uncertainty*	**Q8Y - B**	Could you describe how you provide an estimate despite the experienced uncertainty? What are the steps that you undertake to arrive at your judgment?	Kunt u aangeven hoe u met de ervaren onzekerheid toch tot een inschatting komt? Wat zijn de stappen die u hierin doorloopt?	This questions is to find out how people deal with the experienced uncertainty of that particular step in the risk assessment process. The aim is to identify heuristics in the process.
			Q8N	Could you briefly describe why you don't experience uncertainty?	Kunt u kort kunnen beschrijven waarom u geen onzekerheid ervaart?	This question is to understand why the respondent doesn't experience uncertainty in that particular step of the risk assessment process.
1.5 - Identification of <u>consequences on CIA</u>	What type of uncertainty do security professionals perceive about the organization's		**Q9**	Could you briefly describe how you determine the **the CIA classification** for the identified assets in your organisation?	Zou u kort kunnen beschrijven hoe u beoordeelt de **BIV classificatie is** voorde geïdentificeerde assets in de organisatie?	This question allows the respondent to retrieve instances and examples of how they execute the task in the risk assessment process. It additionally provides insight into the processes and allows the researcher to build upon the given information.

		Organization's information security environment in a risk assessment?		**Q9 - U**	Do you ever experience uncertainty while doing so?	Ervaart u hierbij wel eens onzekerheid?	This question is to identify if the respondent experiences uncertainty.
			Perceived environmental uncertainty	**Q9Y - A**	Could you describe the nature of your perceived uncertainty? What are the factors that contribute to this?	Zou u de aard van uw ervaren onzekerheid kunnen beschrijven? Wat zijn de factoren hiervoor?	This questions looks into the PEU concept, looking for the nature of the experienced uncertainty and for the contributing factors/causes of this. These can range from environmental items, but also items such as experience (identified by 'response options') and social expectations from the organisation's environment.
		How do security professionals provide judgment under the perception of uncertainty about the organization's information security environment?	*Judgment under uncertainty*	**Q9Y - B**	Could you describe how you provide an estimate despite the experienced uncertainty? What are the steps that you undertake to arrive at your judgment?	Kunt u aangeven hoe u met de ervaren onzekerheid toch tot een inschatting komt? Wat zijn de stappen die u hierin doorloopt?	This questions is to find out how people deal with the experienced uncertainty of that particular step in the risk assessment process. The aim is to identify heuristics in the process.
				Q9N	Could you briefly describe why you don't experience uncertainty?	Kunt u kort kunnen beschrijven waarom u geen onzekerheid ervaart?	This question is to understand why the respondent doesn't experience uncertainty in that particular step of the risk assessment process.
2.1 - Assessing the <u>business impact value</u>		What type of uncertainty do security professionals perceive about the organization's information security environment in a risk assessment?		**Q10**	Could you briefly describe how you estimate the **business impact value** from an individual scenario on an identified asset?	Zou u kort kunnen beschrijven hoe u de **business impact value inschat** van een individueel scenario op een geïdentificeerd asset?	This question allows the respondent to retrieve instances and examples of how they execute the task in the risk assessment process. It additionally provides insight into the processes and allows the researcher to build upon the given information.
				Q10 - U	Do you ever experience uncertainty while doing so?	Ervaart u hierbij wel eens onzekerheid?	This question is to identify if the respondent experiences uncertainty.
			Perceived environmental uncertainty	**Q10Y - A**	Could you describe the nature of your perceived uncertainty? What are the factors that contribute to this?	Zou u de aard van uw ervaren onzekerheid kunnen beschrijven? Wat zijn de factoren hiervoor?	This questions looks into the PEU concept, looking for the nature of the experienced uncertainty and for the contributing factors/causes of this. These can range from environmental items, but also items such as experience (identified by 'response options') and social expectations from the organisation's environment.
		How do security professionals provide judgment under the perception of uncertainty about the organization's information security environment?	*Judgment under uncertainty*	**Q10Y - B**	Could you describe how you provide an estimate despite the experienced uncertainty? What are the steps that you undertake to arrive at your judgment?	Kunt u aangeven hoe u met de ervaren onzekerheid toch tot een inschatting komt? Wat zijn de stappen die u hierin doorloopt?	This questions is to find out how people deal with the experienced uncertainty of that particular step in the risk assessment process. The aim is to identify heuristics in the process.

				Q10N	Could you briefly describe why you don't experience uncertainty?	Kunt u kort kunnen beschrijven waarom u geen onzekerheid ervaart?	This question is to understand why the respondent doesn't experience uncertainty in that particular step of the risk assessment process.
	2.2 - Assessing the <u>likelihood of scenarios materializing impacting</u> business value	What type of uncertainty do security professionals perceive about the organization's information security environment in a risk assessment?		**Q11**	Could you briefly describe how you estimate the **likelihood/probability that identified scenarios materialize** for your organisation?	Zou u kort kunnen beschrijven hoe u de **kans op het uitkomen van de geïdentificeerde scenarios** voor uw organisatie inschat?	This question allows the respondent to retrieve instances and examples of how they execute the task in the risk assessment process. It additionally provides insight into the processes and allows the researcher to build upon the given information.
				Q11 - U	Do you ever experience uncertainty while doing so?	Ervaart u hierbij wel eens onzekerheid?	This question is to identify if the respondent experiences uncertainty.
			Perceived environmental uncertainty	**Q11Y - A**	Could you describe the nature of your perceived uncertainty? What are the factors that contribute to this?	Zou u de aard van uw ervaren onzekerheid kunnen beschrijven? Wat zijn de factoren hiervoor?	This questions looks into the PEU concept, looking for the nature of the experienced uncertainty and for the contributing factors/causes of this. These can range from environmental items, but also items such as experience (identified by 'response options') and social expectations from the organisation's environment.
		How do security professionals provide judgment under the perception of uncertainty about the organization's information security environment?	*Judgment under uncertainty*	**Q11Y - B**	Could you describe how you provide an estimate despite the experienced uncertainty? What are the steps that you undertake to arrive at your judgment?	Kunt u aangeven hoe u met de ervaren onzekerheid toch tot een inschatting komt? Wat zijn de stappen die u hierin doorloopt?	This questions is to find out how people deal with the experienced uncertainty of that particular step in the risk assessment process. The aim is to identify heuristics in the process.
				Q11N	Could you briefly describe why you don't experience uncertainty?	Kunt u kort kunnen beschrijven waarom u geen onzekerheid ervaart?	This question is to understand why the respondent doesn't experience uncertainty in that particular step of the risk assessment process.
	2.3 - Assessing risk values				NOT RELEVANT		This step is the outcome of the risk value, which is not an prediction/estimation, therefore not relevant.
	3.1 - Risk evaluation				NOT RELEVANT		This step looks at evaluating the outcomes of step 2.3 with the acceptable risk levels of the context establishing phase of the ISO27005 process, therefore this is not relevant.

Closing questions	
I	Do you have any feedback about or for the interview?
I	Heeft u nog feedback voor/over het interview?
II	Do you have any other remaining questions about the research?
II	Heeft u nog andere vragen over het onderzoek?

III	Could you possibly help me with finding respondents?
III	Zou u mij mogelijk verder kunnen helpen met respondenten?

B

Informed Consent Form

This appendix contains the informed consent form that is used to gain affirmative and granular consent for collecting and using data of respondents in this research study.

Informed Consent Form

Part I
Information Sheet

1 Research group

1.1 Researchers in charge of the project

Kay J.C. Hagenaars[1,2]	MSc. Student/Graduate Intern	Delft University of Technology/ Deloitte Risk Advisory B.V.
Kirsten V.M. Meeuwisse[2]	Senior Consultant	Deloitte Risk Advisory B.V.
Prof. dr. Michel J.G. van Eeten[3]	Professor	Delft University of Technology
Dr. ir. Wolter Pieters[3]	Associate Professor	Delft University of Technology
Dr. Maarten P.M. Franssen[4]	Associate Professor	Delft University of Technology

1.2 Organisations

1. MSc. Program in Management of Technology, Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands
2. Cyber Risk Services, Deloitte Risk Advisory B.V., Amsterdam, The Netherlands
3. Section of Organisation & Governance, Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands
4. Section of Ethics/Philosophy of Technology, Faculty of Technology, Policy and Management, Delft University of Technology, Delft, The Netherlands

2 This document

This informed consent form has two parts, consisting of:

- Information Sheet, pages 1 – 4
- Certificate of Consent, page 5

Prior to agreement of participation in this research study, you are required to read this document carefully. The Information Sheet (Part I) describes the purpose, benefits and risks of participation, procedures, information on the collection of and use of personal data in relation to the privacy of participants. If there is anything unclear after reading the information sheet, we will be happy to elaborate on the requested items. You should feel comfortable to speak to any of the researchers involved to answer any questions you may have at any time. After you have read the information sheet and after all outstanding questions have been answered by the researcher, you can decide if you would like to participate in the study. At the end you are asked to sign a Certificate of Consent (Part II) to confirm that you are voluntarily willing to participate in this research study. You will receive a copy of the full Informed Consent Form.

3 Purpose of the research

For organisations to protect their valuable information assets from cybercriminals, accurate information security risk assessments are necessary. However, the cybersecurity field lacks hard objective data that can provide objective and unambiguous input to risk assessments. This consequently creates reliance on the judgment of the risk assessors who complement the available knowledge with their estimates. This research is conducted to assess how cybersecurity professionals perceive uncertainty about the information security environment and how they subsequently provide estimates from judgment in information security risk assessments. The knowledge obtained from this research creates a better understanding into how cybersecurity professionals deal with uncertainty in information security risk assessments.

4 Benefits and risks of participation

It is not expected that this project will directly benefit you personally. However, by participating in this study you will add to the current understanding of how estimates in risk assessments are provided when cybersecurity professionals experience uncertainty about the information security environment. Your participation in turn assists with assessing the current approaches of information security risk assessments which will benefit the future safety of the digital society.

The research group does not expect that participation poses any psychological or physical risks to the participant.

5 Participation

5.1 Location of the interview

Participating in this research study will involve one in–person interview at a location and time that is indicated to suit the participant.

5.2 Eligibility criteria

The participants need to meet the following criteria to participate in this research study:

- You are 18 years or older;
- You have relevant working experience in information security risk management processes, focussing on focussing on information security risk assessments, with a minimum of one (1) year;
- You are used to working with a qualitative or semi-quantitative information security risk assessment approach as prescribed by the ISO 27005 standard.
- You are used to executing information security risk assessments at an organizational level.

The researchers reserve the right to refuse the participant at any time if the study requirements are not met.

5.3 Voluntary participation and right to refuse or complete withdrawal

Your participation in this research study is completely voluntarily. The choice of participation to this research study is consequently yours and yours only. If you agree to participate it is important to understand that as a respondent you have the right to withdraw while already in the process of the research study. Complete withdrawal is always available to the respondent at any time of the project without comment or penalty. The results from interviews can be discarded as long as this is technically feasible, i.e. as long as the study is ongoing. The results from the study once published can not be changed.

6 Procedure

6.1 Your task

You are asked to respond to a series of interview questions. The interview questions concern an evaluation of your own experiences while executing information security risk assessments with regard to providing estimates about the information security environment in an organisational context. The focus is on perceptual processes and how judgment is provided by you as a risk assessor.

You are ***not*** asked to discuss any details concerning organisational IT architectures, assets, threats or any other specific details that relate to the organisational context in which you are employed. This study is about your experiences from a perceptual point of view and is not interested in organisational details.

6.2 Duration and time commitment

The interview is expected to take 60–90 minutes maximum, involving signing the Certificate of Consent and answering your questions related to the interview and research itself.

6.3 Data collection

Your responses from the interview will be audio–recorded to ensure that all necessary data is properly captured. This data will be transcribed into to text where it is also anonymized to provide privacy to you as a respondent. The recordings are saved in a secure location during the research period. After completion of the research project, the recordings are destroyed. The remainder of information rests in the form of transcribed and *anonymized* text that is only accessible to the research group for the duration of this project.

The research limits the collection of personally identifiable information from the respondent (you). The data that is collected is necessary to identify context establishing factors.

7 Privacy & Confidentiality

The privacy and confidentiality of the respondents is a top priority of this research study and are guided by the GDPR regulations. Consequently, all comments and responses given during the interview are treated confidentially unless required otherwise by law. The personally identifiable information is anonymized to protect the identity of respondents. This is necessary because the anonymized and non–personally identifiable information are subject to pub-

lication within the TU Delft research repository and possible future journal publications and presentations.

Any data that is collected as part of this research study will be stored in a secure fashion as prescribed by the GDPR and academic research guidelines.

8 Sharing of results

The results of this study will be published within the TU Delft Repository as part of the partial fulfilment to obtain the degree of Master of Science in Management of Technology. Furthermore, the results of the study might be presented on conferences within the field of cybersecurity, published as part of a PhD thesis or be published in scientific journals related to the fields on cybersecurity, decision–making and risk assessment methodologies.

Please note that the results are anonymized and that personally identifiable information is removed prior to any of the above mentioned sharing options to protect your privacy.

9 Responsibility

The researchers, funding bodies or institutions/organizations that are involved in this research project do not bear any responsibility for possible damages or inconveniences during travel to or from the agreed upon interview location.

10 Questions/Information details about the research project

If you have any questions about the research project or require further information, please contact one of the researchers via the below methods. This allows us to answer your question in the most proper fashion.

Researchers	E–mail	Phone
Kay J.C. Hagenaars	k.j.c.hagenaars@student.tudelft.nl	<Telephone number>
Wolter Pieters	w.pieters@tudelft.nl	

11 Ethical approval

This study is approved by the Delft University of Technology's Human Research Ethics Committee (HREC) under the research title *"Dealing with uncertainty in an information security risk assessment"*. If needer or desired, verification of approval can be provided by sending an e–mail to HREC@tudelft.nl.

Please note that the HREC is an independent body from this research project. If you have any concerns or complaints, then they can provide impartial facilitation if necessary.

Part II
Certificate of Consent

Title of research project:
Dealing with uncertainty in an information security risk assessment

Please check and sign the desired fields — Participant

Taking part in the study	**Yes**	**No**
I have read and understood the study information sheet, or it has been read to me. I have been able to ask questions about the study and my questions have been answered to my satisfaction.	○	○
I consent voluntarily to be a participant in this study and understand that I can refuse to answer questions and I can withdraw from the study at any time, without having to give a reason.	○	○
I understand the study involves a recorded interview in which the researcher is looking into the perceptual processes that cybersecurity professionals experience during information security risk assessments. The recordings are transcribed, anonymized and used in this research project as part of the results.	○	○
I understand that personally identifiable information collected about me , e.g. my name, years of experience or role within my organisation when executing an information security risk assessment, will not be shared beyond the study team.	○	○
I give permission for the interview data (that is transcribed and anonymized in the form of results without a direct link to me the respondent) that I provide to be archived in TUDelft Repositories (`https://repository.tudelft.nl`) so it can be used for future research and learning	○	○

Name participant	Date	Signature

Please sign the desired fields — Researcher

Participant ID: . . . . . .

I have provided to the best of my abilities and after a satisfactory response of the respondent a sufficient oral and written explanation of this research project. Remaining questions of this research study I will also answer to the best of my abilities. The participant will not suffer any adverse consequences by premature termination or withdrawal from the study.

Kay J.C. Hagenaars		
	Date	Signature

C

Research protocol

This appendix provides the details of the research protocol that safeguards the reliability and validity of the research project for the data collection phase.

C.1. Searching and selecting respondents

The respondent search knows two different methods for the purposeful sampling, based on the criteria of subsection 4.3.1:

1. Deloitte allowed its network to be searched for respondents that fit the requirements. The Deloitte network was searched by actively engaging with team members of the Deloitte Cyber Risk Services department for referrals to people who would fit the described respondent profile. In case of a fit between the respondent criteria and the referred person (first analysed from the LinkedIn–page), an introduction was made accompanied with a standardized invitation letter for the research. Depending on whether the respondent was Dutch speaking or not, an invitation letter was sent in either Dutch or English (see Figures C.4 and C.5).

2. The second method employed to search for respondents was via the social media platform LinkedIn. Queries on several 'typical' job titles were run, providing a series of potential respondents. The queries included: "information security officer", "chief information security officer", "information security risk manager", "IT risk manager" and "information risk manager". Based on their experience and job description they were approached via a LinkedIn–invite to connect. If the LinkedIn–invite was accepted, the research invitation letter was sent (see Figures C.4 and C.5).

3. If the respondent agreed to participate in the research, a face-to-face meeting was set up at a time and location of the respondent's choosing. Additionally the informed consent form was sent ahead for the respondent to read. Allowing them to prepare questions for the researcher during during the interview.

C.2. The interview

The interview was performed in a rigorous and structured manner, during an on–site face-to-face meeting. The physical proximity between the researcher and the respondents was considered critical for multiple reasons. First and foremost, the interview takes a rigorous approach in which the sharing of information to the respondent is an important aspect. This research used an interview setup document that provided the respondent with the information applicable to this research and the structure of the interview. Consequently, the on–site interview allows control over the shared information. Secondly, this research uses empirical data from human subjects and is consequently subject to the guidelines of the Human Research Ethics Commission (HREC). These guidelines require the respondents to sign an informed consent form (see Appendix B). To ensure the research validity, this is overseen during the interview by the researcher.

The interview was guided by the interview checklist (see Figure C.6), providing a step-by-step checklist of what needs to be done during the interview to ensure high reliability.

1. The respondents were asked if they had any remaining questions about the research or the informed consent form prior to signing it.
2. Each respondent was read an introduction text that again briefly explained the approach of the interview, the goal of the research and the notion of limited time (see introduction text in Figure C.6).
3. The respondent was provided with an interview setup document, which allows the respondent to see the type of questions that are posed with some additional context explaining factors (see Figures C.7 and C.8).
4. All the interview questions were posed to the respondent according to the interview script as can be seen in Appendix A. For the interviews themself a simplified version of the script was used which also indicates the approximate time line for the interview (see Figures C.9 and C.10).
5. All the interviews were recorded and stored on a local PC.

C.3. Data collection

This research is cross–sectional in nature and inline with this premise the respondent data was collected within a fixed time frame. Please refer to Table C.1 for the dates and time for each of the conducted interviews, all fitting within the outlined time frame as indicated in the invitation letter (see Figures C.4 and C.5).

Table C.1: Data collection phase timeline — execution of interviews

ID	Date	Time
D01	14-06-2019	12:00-13:30
D02	18-06-2019	12:30-14:00
D03	19-06-2019	10:00-11:30
D04	26-06-2019	10:00-11:30
D05	26-06-2019	18:00-19:30
D06	01-07-2019	15:00-16:30
D07	04-07-2019	14:00-15:30
D08	08-07-2019	10:00-11:30
D09	10-07-2019	10:00-11:30
D10	12-07-2019	09:00-10:00
D11	12-07-2019	13:00-14:30
D12	19-07-2019	10:30-12:00
D13	22-07-2019	11:00-12:00
D14	22-07-2019	13:30-15:00
D15	25-07-2019	10:30-12:00

C.4. Data analysis

The recorded interviews are transcribed using NVivo12, providing specialized transcription tooling. The interviews are segmented based on the topic. Additionally they are timestamped to review the data from the specified segments. Please refer to Figure C.1 below for an overview of the transcription environment of NVivo12.

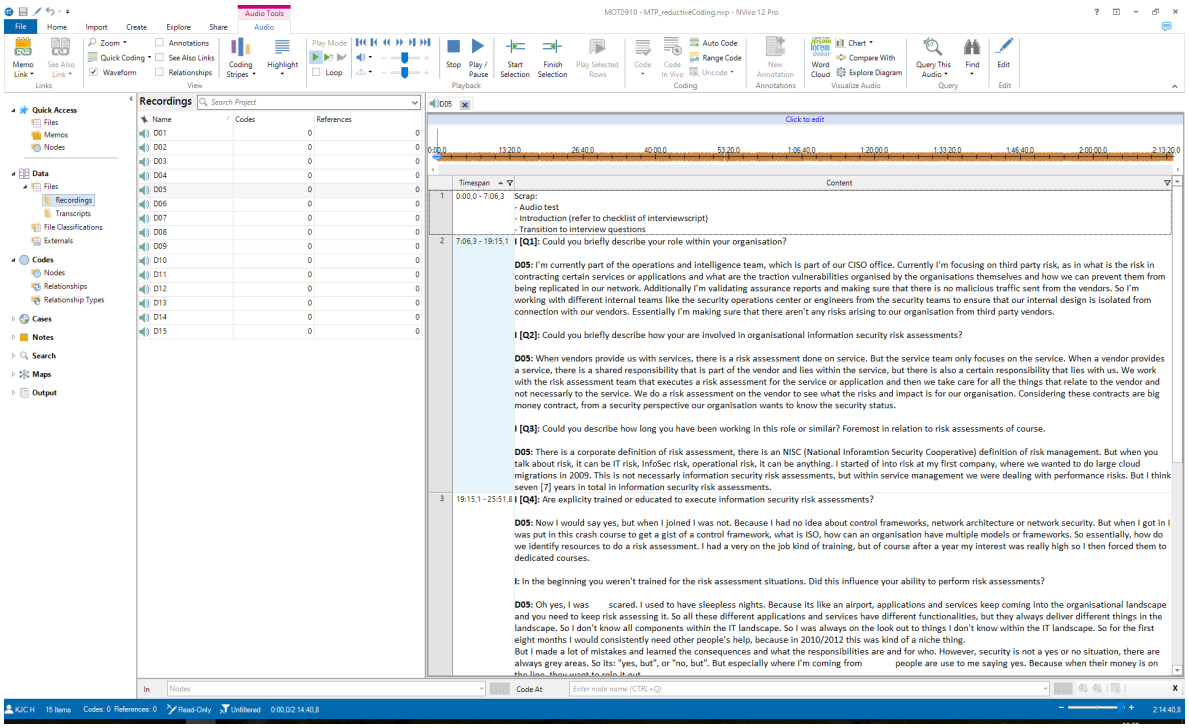


Figure C.1: Transcription in NVivo12

The first step after transcribing the interviews is the coding of the data. Again, NVivo12 is used to support the researcher in this task. The program allows the data to be coded easily, grouping the codes and help in the identification of underlying axes between the different data documents. Although NVivo12 is crucial to this process, it must be noted that the program does not provide the coding process to the researcher. The program is merely a representation tool that relies on input from the researcher.

Although this research aims at identifying two theoretical concepts in an IS risk assessment setting, an open coding process provides the researcher with insights that might not be directly related to the concepts but are of interest. Therefore a first open coding procedure was executed, providing the researcher initial codes. These codes are pre-grouped per interview segment because the interview takes an iterative process and removing any grouping makes a quick an thorough analysis per segment of the IS risk assessment step very difficult.

The next step is a reductive coding process, also known as axial coding, in which underlying structures are identified. This is again done per step of the IS risk assessment, holding on to the tree structure as coming from the segmentation of the interview data. The reduction in codes is possible because the analysis is focused on the themes as identified in Chapter 3.

As an indication, Figure C.2 provides an overview of the coding environment in NVivo12. The tree structure that is based on the segmentation of topics in relation to the interview is shown next to the red letter “A”. The topic from the segment is the top node. This is followed by child nodes that indicate the themes discussed in this segment. These themes have second degree child nodes that provide specific information which will be consequently grouped into underlying axes applicable to the theme. The red rectangle consequently provides a quick overview of the number of responses that link to the axis and its theme, creating a quick overview of the data. The section in which the green letter “B” is visible shows the data in transcribed text format, this is the data to which the codes are applied. On the right side of the figure it is shown what codes are ascribed to the different text segments, indicated by the blue letter “C”. The blue rectangle consequently shows the coded text that corresponds to the code in C, which relates to the codes from A.

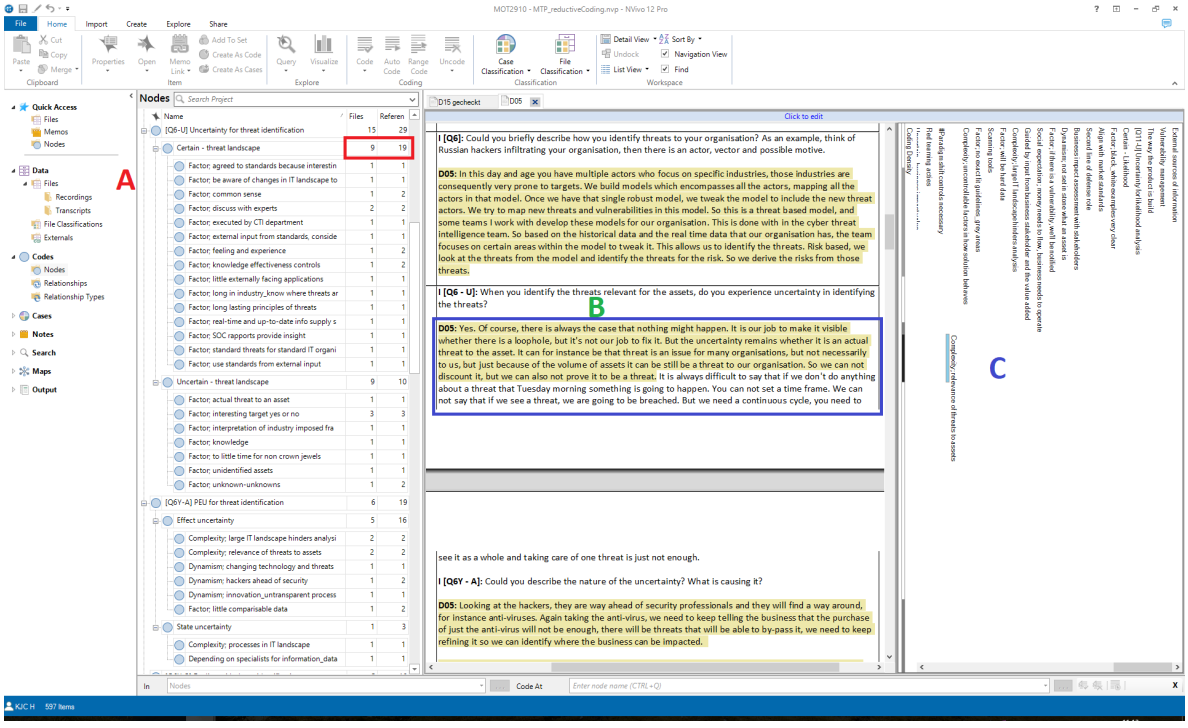


Figure C.2: Coding in NVivo12

After coding the data is synthesized that allows the results to be written up coherently, concise and correct. Therefore a map is created that shows the relationships between the codes and the data, enabling a succinct depiction of the results. As an example, Figure C.3 shows such a relationship map.

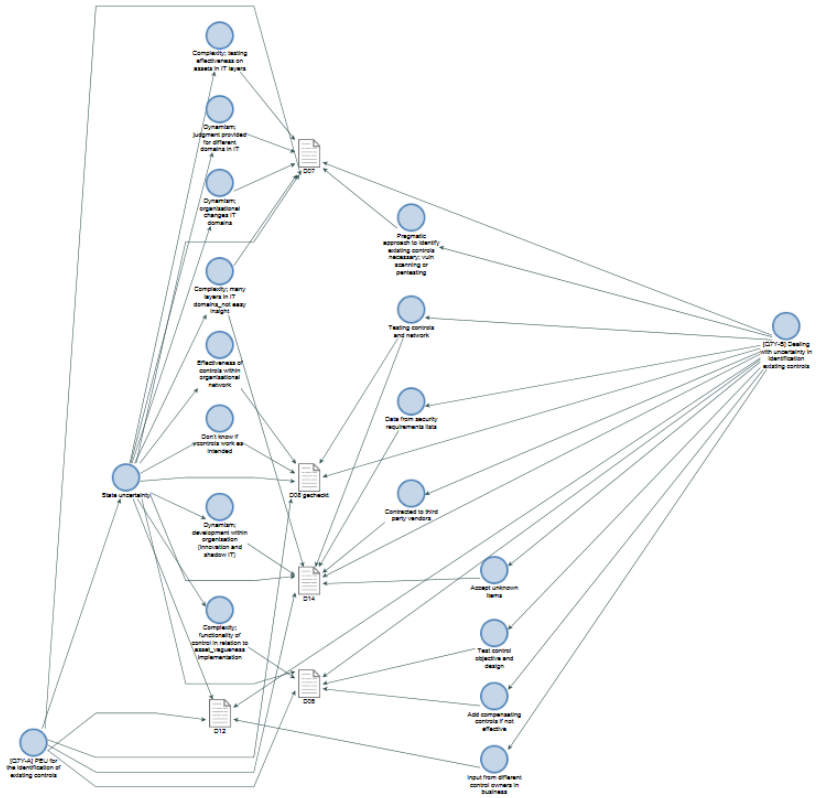


Figure C.3: Creating a map for synthesis in NVivo12

Dear Sir/Madam,

My name is Kay Hagenaars, a MSc. student Management of Technology at Delft University of Technology. For my master thesis I'm doing research into how cybersecurity professionals experience uncertainty in risk assessments and how estimates are subsequently provided. Therefore I'm looking for cybersecurity professionals that execute risk assessments and who are willing to participate in an interview at a time and location of your choosing.

The goal of the research
In risk assessments it is common that uncertainty about an organisation's cybersecurity environment are supplemented with estimates from professionals to obtain risk values. The goal of this research is to identify how cybersecurity professionals perceive uncertainty about the organisation's cybersecurity environment in the different phases of the risk assessment and how they subsequently arrive at their given estimates. With this research we try to better understand how cybersecurity professionals deal with uncertainty in risk assessments.

The purpose of this research ***is not*** to discuss organisation specific details. The research focuses on the identification of experiences from cybersecurity professionals in risk assessments.

Benefits of participation in the research and the use of data
By participating in this research you have the possibility to review the research results and use outcomes within your organisation which creates reflection opportunities. At the same time you will contribute to the current body of scientific knowledge that aims at creating a safer digital environment for organisations.

All obtained data will be anonymized to protect the identity of the respondent. The data will be treated confidentially and in accordance with the GDPR-regulations made available to the respondent. The results derived from the data will be used for the publication of a master thesis as the outcome of this research project.

The research procedure
The research procedure for the collection of data consists out of one face-to-face interview (60 – 90 minutes) at a time and location of your choosing. The data collection is preferably planned in the period from the middle of June to the end of July 2019.

The interview consists out of two parts:

1. Context establishing data collection: this part looks at your position and activities in relation to risk assessments to establish the correct context of your experiences.
2. Risk assessment steps in accordance with ISO 27005: this part looks at how you experience uncertainty about the organisation's cybersecurity environment per individual step of the risk assessment and how you subsequently deal with it when providing estimates. To exemplify, this research is not interested in organisation specific details, but solely in how cybersecurity professionals execute and experience the steps of a risk assessment in an organisational context.

Involved research group
This research is executed by Kay Hagenaars and supervised by Dr. ir. Wolter Pieters.

Referrals
If you know other cybersecurity professionals, who like yourself have fundamental knowledge and experience with risk assessments in an organisational context, then I hope you could refer them to me. This will contribute to the validity and reliability of this research and is greatly appreciated.

I'm looking forward to your response.

Kind regards,

Kay Hagenaars | MSc. student Management of Technology
E: k.j.c.hagenaars@student.tudelft.nl
T: <Telephone number>

Figure C.4: Research invitation letter (EN)

Beste heer, mevrouw,

Mijn naam is Kay Hagenaars, ik ben een MSc. student Management of Technology aan de Technische Universiteit Delft. Voor mijn masterthesis onderzoek ik hoe cybersecurity professionals onzekerheid ervaren in risico assessments en daarbij inschattingen geven. Hiervoor ben ik op zoek naar cybersecurity professionals die risico assessments uitvoeren en bereid zijn om mij te ontmoeten voor een interview op een tijd en locatie naar uw keuze.

Het doel van het onderzoek
In risico assessments is het gebruikelijk dat onzekerheid over de cybersecurity omgeving van een organisatie wordt aangevuld met inschattingen van professionals om tot een risico-inschatting te komen. Het doel van het onderzoek is om te identificeren hoe cybersecurity professionals de onzekerheid over een organisatie haar informatiebeveiligingsomgeving ervaart in de verschillende fases van het risico assessment en hoe zij vervolgens tot hun inschattingen komen. Met de uitkomsten van dit onderzoek willen we beter begrijpen hoe cybersecurity professionals handelen in risico assessments.

Dit onderzoek heeft ***niet*** als doel om organisatie specifieke details te behandelen. Het gaat om het identificeren van ervaringen van cybersecurity professionals tijdens een risico assessment.

Voordelen van participatie in het onderzoek en gebruik van data
Door deelname aan het onderzoek krijgt u de mogelijkheid om de resultaten van het onderzoek in te zien en te gebruiken binnen uw organisatie wat reflectiemogelijkheden biedt. Tevens zult u bijdragen aan de huidige wetenschappelijke kennis om de digitale omgeving van organisaties veiliger te maken.

Alle verkregen data zal worden geanonimiseerd om de identiteit van de respondent te beschermen. De data wordt vertrouwelijk en volgens de AVG-richtlijnen behandeld en beschikbaar gemaakt aan de respondent. De resultaten afkomstig van de data zullen worden gebruikt voor de publicatie van een master thesis als gevolg van dit onderzoek.

De onderzoeksprocedure
De onderzoeksprocedure voor het verzamelen van data zal bestaan uit één interview (60 – 90 minuten) op een tijd en locatie van uw keuze. De dataverzameling wordt bij voorkeur gepland in de periode van half juni tot eind juli 2019.

Het interview zal bestaan uit twee delen:

1. Context bepalende data collectie: hierbij zal er worden gekeken naar uw positie en werkzaamheden in het kader van risico assessments om de juiste context te bepalen van uw ervaringen.
2. Risico assessment stappen volgens ISO 27005: hierbij zal er per individuele stap gekeken worden naar hoe u onzekerheid over de organisatorische informatiebeveiligingsomgeving ervaart in het geven van inschattingen en hoe u daarmee omgaat. Nogmaals, in dit onderzoek gaat het niet om organisatiespecifieke details, maar om hoe cybersecurity professionals risico assessment stappen doorlopen en ervaren.

De betrokkenen in dit onderzoek
Dit onderzoek wordt uitgevoerd door Kay Hagenaars en begeleid door Dr. ir. Wolter Pieters.

Referenties
Mocht u andere cybersecurity professionals kennen, die net als u fundamentele kennis en ervaring hebben met risico assessments in een organisatorische context, dan hoop ik dat u mij kunt refereren. Dit zal namelijk bijdragen aan de validiteit en betrouwbaarheid van het onderzoek.

Graag zie ik uw antwoord tegemoet.

Met vriendelijke groet,

Kay Hagenaars | MSc. student Management of Technology
E: k.j.c.hagenaars@student.tudelft.nl
T: <Telephone number>

Figure C.5: Research invitation letter (NL)

Checklist

- ☐ Prepare: hardcopy questions; ICF; interview setup document; gift
- ☐ Answer questions regarding informed consent form or research related
- ☐ Sign informed consent form
- ☐ Provide introduction text:

EN During the interview we want to discuss your personal and cognitive experiences in risk assessment. Therefore try to think in for you in distinct examples. The interview consists out of two parts; (1) context establishing part to situate your experiences within the risk assessment context, (2) the questions from the risk assessment steps as depicted by ISO27005. The interview questions in part two (2) have a repetitive character, in which the steps from the ISO27005 form the backdrop of the interview structure to find out what your experiences are. In these steps of the risk assessment we want to identify if you experience uncertainty (the perceived inability to make accurate estimates) about the information security environment. Subsequently we want to identify how you, despite the experienced uncertainty, arrive at an estimate. Due to the limited available time I might have to interupt some answers to finish the interviewscript, my apologies in advance.

NL Tijdens het interview wil ik ingaan op uw persoonlijke en cognitieve ervaringen in risico assessments. Probeer daarom te denken in voor u exemplarische voorbeelden. Het interview bestaat uit twee delen; (1) context bepalend deel om je ervaringen omtrent risk assessments te situeren, (2) de vragen van de risk assessment stappen uit ISO27005. De interviewvragen in deel twee (2) hebben een repetitief karakter qua vraagstelling, waarin de stappen van de ISO27005 de leidraad vormen om achter uw ervaringen te komen. Het doel van het onderzoek is om te identificeren of u onzekerheid ervaart (het gevoel van onvermogen om een nauwkeurige inschatting te geven) in de verschillende stappen van het risico assessment over de informatiebeveiligingsomgeving. Vervolgens willlen we identificeren hoe u ondanks de ervaren onzekerheid toch tot een inschatting komt. Vanwege de beperkt beschikbare tijd zal ik af en toe moeten inbreken op de antwoorden om het interviewscript af te kunnen lopen, alvast mijn excuses.

- ☐ Run interview questions
- ☐ Closing interview questions
- ☐ Gift

Figure C.6: The interview checklist

Interview setup

The interview consists out of two parts, a series of context establishing questions and risk assessment questions.

Part I: Context establishing questions

This part consists out of questions that define the context of your experiences, which is necessary to correctly interpret your answers. There are four (4) context establishing questions [Q1 – Q4].

Part II: Risk assessment questions

This part is focused on the information security risk assessments process as described by the ISO 27005 standard, that forms the backdrop against which the questions are formulated (see figure). See below interview question steps:

Q#	**Risk identification**	**Description**
Q5	1.1 – Asset identification	The mapping of organisational assets that require protection.
Q6	1.2 – Threat identification	The mapping of malicious threats to the organisation and its assets.
Q7	1.3 – Identification of existing controls	The mapping of the current working state of controls in relation to the assets they need to protect against harm from threats.
Q8	1.4 – Identification of vulnerabilities	The mapping of vulnerabilities in the organisation's information security environment which provides opportunity to be exploited by threats.
Q9	1.5 – Identification of consequences on CIA	Determining the impact on the confidentiality, integrity and availability of assets that are exploited through a vulnerability by an identified threat.
Q#	**Risk analysis**	**Description**
Q10	2.1 – Assessing business impact value	Estimating the consequences for the business impact value (BIM), expressed in financial losses.
Q11	2.2 – Assessing likelihood	Estimating the probability of the scenarios materializing for the BIM.
N.A.	2.3 – Assessing risk values	Combined value from 2.1 and 2.2, not relevant to this research.
Q#	**Risk evaluation**	**Description**
N.A.	3.1 – Evaluate risk values	Evaluation of 2.3 against context establishment phase, see figure.

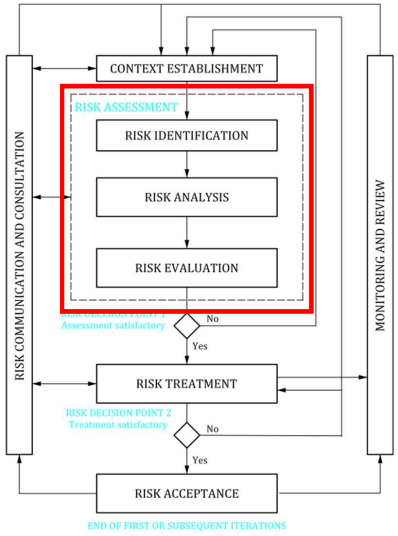


Figure C.7: The interview setup document (EN)

Interview setup

Het interview bestaat uit twee delen. Het eerste deel bestaat uit context bepalende vragen en het tweede deel uit risico assessment vragen.

Deel I: Context bepalende vragen

Dit deel bestaat uit vragen die de context van uw ervaringen in risico assessments bepalen, dit is noodzakelijk om uw antwoorden goed te interpreteren. Er zijn vier (4) context bepalende vragen [Q1 – Q4].

Deel II: Risico assessment vragen

Dit deel is gefocust op het informatiebeveiligingsrisico assessment proces zoals beschreven in de ISO27005 norm, welke als leidraad wordt gebruikt voor de formulering van de interviewvragen (zie het figuur). Zie hieronder de opzet voor de interviewvragen:

Q#	**Risk identification**	**Beschrijving**
Q5	1.1 – Asset identificatie	Het identificeren van assets die moeten worden beschermd.
Q6	1.2 – Threat identificatie	Het identificeren van gevaren voor de organisatie en haar assets.
Q7	1.3 – Identificatie van bestaande controls	Het identificeren van huidige controls en hun werking in relatie tot de assets die moeten worden beschermd van geïdentificeerde gevaren.
Q8	1.4 – Identificatie van vulnerabilities	Het identificeren van vulnerabilities in de organisatie haar informatiebeveiligingsomgeving die kunnen worden gebruikt door gevaren.
Q9	1.5 – Identificatie van consequenties voor BIV	Het bepalen van de impact op de beschikbaarheid, integriteit en vertrouwelijkheid van assets.
Q#	**Risk analysis**	**Beschrijving**
Q10	2.1 – Inschatten van business impact value	Het inschatten van de consequenties op de business impact value (BIM), uitgedrukt in financiële verliezen.
Q11	2.2 – Inschatten van kans	Het inschatten van de kans dat scenarios voor het BIM voltrekken.
N.A.	2.3 – Berekenen van risico	De gecombineerde waarde van 2.1 and 2.2, niet relevant in dit onderzoek.
Q#	**Risk evaluation**	**Beschrijving**
N.A.	3.1 – Risico evaluatie	Evaluateer waardes 2.3 ten opzichte van de context bepalende fase.

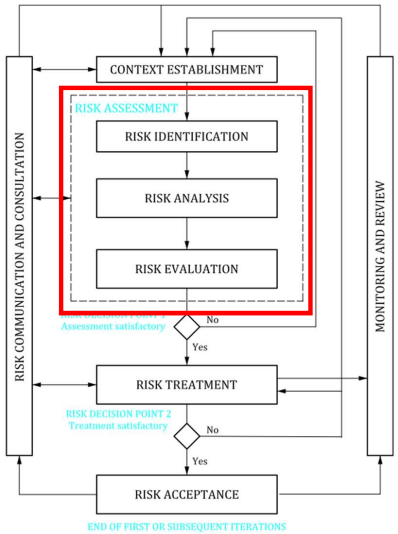


Figure C.8: The interview setup document (NL)

Interviewscript (EN)

		Time (min)
Q1	Could you briefly describe your role within your organisation?	10
Q2	Could you briefly describe how you are involved in organisational information security risk assessments?	13
Q3	Could you describe how long you have been working in this role or similar (also in other companies/positions)?	15
Q4	Are you educated to execute information security risk assessments? Do you believe this helps/hinders you in the execution?	17
Q5	Could you briefly describe how you identify assets (crown jewels, assets of value) of your organisation?	20
Q# - U	Do you ever experience uncertainty while doing so?	
Q#Y - A	Could you describe the nature of your perceived uncertainty? What are the factors that contribute to this?	
Q#Y - B	Could you describe how you provide an estimate despite the experienced uncertainty? What are the steps that you undertake to arrive at your judgment?	
Q#N	Could you briefly describe why you don't experience uncertainty?	
Q6	Could you briefly describe how you identify threats to your organisation? As an example, think of Russian hackers infiltrating your organisation.	28
Q7	Could you briefly describe how you identify existing controls organisation wide?	36
Q8	Could you briefly describe how you identify vulnerabilities of your organisation?	44
Q9	Could you briefly describe how you determine the the CIA classification for the identified assets in your organisation?	52
Q10	Could you briefly describe how you estimate the business impact value from an individual scenario on an identified asset?	60
Q11	Could you briefly describe how you estimate the likelihood/probability that identified scenarios materialize for your organisation?	68
	Closing questions Do you have any feedback about or for the interview? Do you have any other remaining questions about the research? Could you possibly help me with finding respondents?	80

Figure C.9: The simplified interview script with time line (EN)

Interviewscript (NL)

		Tijd (min)
Q1	Zou u kort uw rol binnen uw organisatie kunnen beschrijven?	10
Q2	Zou u kort kunnen beschrijven hoe u betrokken bent bij de organisatorische informatiebeveiligings risico assessments?	13
Q3	Zou u kunnen beschrijven hoe lang u al in deze rol of vergelijkbaar werkzaam bent?	15
Q4	Bent u opgeleid in het uitvoeren van informatiebeveiligings risico assessments? Heeft u het idee dat dit u helpt/hindert?	17
Q5	Zou u kort kunnen beschrijven hoe u de assets (kroonjuwelen, assets van waarde) van uw organisatie identificeert?	20
	Q# - U Ervaart u hierbij wel eens onzekerheid?	
	Q#Y - A Zou u de aard van uw ervaren onzekerheid kunnen beschrijven? Wat zijn de factoren hiervoor?	
	Q#Y - B Kunt u aangeven hoe u met de ervaren onzekerheid toch tot een inschatting komt? Wat zijn de stappen die u hierin doorloopt?	
	Q#N Kunt u kort kunnen beschrijven waarom u geen onzekerheid ervaart?	
Q6	Zou u kort kunnen beschrijven hoe u de threats voor uw organisatie identificeert? Hierbij kunt u denken aan bijvoorbeeld een Russische hacker die uw organisatie infiltreert.	28
Q7	Zou u kort kunnen beschrijven hoe u organisatiebreed bestaande controls identificeert?	36
Q8	Zou u kort kunnen beschrijven hoe u de vulnerabilities van uw organisatie identificeert?	44
Q9	Zou u kort kunnen beschrijven hoe u beoordeelt de BIV classificatie is voorde geïdentificeerde assets in de organisatie?	52
Q10	Zou u kort kunnen beschrijven hoe u de business impact value inschat van een individueel scenario op een geïdentificeerd asset?	60
Q11	Zou u kort kunnen beschrijven hoe u de kans op het uitkomen van de geïdentificeerde scenarios voor uw organisatie inschat?	68
	Closing questions Heeft u nog feedback voor/over het interview? Heeft u nog andere vragen over het onderzoek? Zou u mij mogelijk verder kunnen helpen met respondenten?	80

Figure C.10: The simplified interview script with time line (NL)