

Beyond Levels: Supporting  
Information Classification

Simon Andersson

Information Systems



---

# Beyond Levels: Supporting Information Classification

**Simon Andersson**

Department of Computer Science, Electrical and Space Engineering  
Luleå University of Technology  
Luleå, Sweden

---

## **Supervisors:**

Christine Große - Luleå University of Technology &  
Erik Bergström - Jönköping University



---

## ACKNOWLEDGEMENTS

---

This thesis marks the culmination of my doctoral studies. I have achieved a lot during these years, both in and outside academia. I, of course, wrote the doctoral thesis that is in your hands (or on your screen), completed a full-distance triathlon, became a father, got married, and so much more. I am proud of all of these accomplishments, and they have required persistence, discipline, support from others, and, perhaps most importantly, a great deal of stubbornness. Naturally, I could not have done any of those things by myself, and as such, there are plenty of people to thank for their help and support.

First and foremost, I would like to express my gratitude to both of my supervisors. To my main supervisor, Christine Große, thank you for your support, guidance and seemingly endless ideas for how to approach and develop my work. To my co-supervisor, Erik Bergström, thank you for the close collaboration throughout these years. I am grateful for our many discussions, and I have greatly enjoyed working with someone so proficient in information classification. I look forward to continuing to work with both of you.

I would also like to express my thanks to Ella Kolkowska, who served as opponent for my mid-seminar, and to Shang Gao, who served as opponent for my final seminar. Both of you provided feedback that significantly improved my work, and I am thankful for your time.

Next, I would like to thank my colleagues at the Information Systems department at LTU. From the very start, you have been a welcoming, kind, and enjoyable group of people to work with, and you continue to teach me a great deal. A very special thank you goes to my favourite colleague of all time, Anton Holmström, who has been, and continues to be, my constant academic companion. You have inspired me to go outside my comfort zone and do things I did not think I could do, the main example being running, swimming, and cycling very, very far.

To my parents, Hans and Cecilia, and to my brother Martin, thank you for your support and for the always-welcome distractions during both winter and summer vacations. Your encouragement means a lot.

Last, but certainly not least, I want to thank my amazing wife Elin, our newborn son Alfons and our dog Råkan. Thank you for always being there for me and for being a constant source of support in everything I do. You all mean the world to me.

*Simon Andersson*  
Luleå, June 2026



---

## ABSTRACT

---

Information is a critical asset for organisations, enabling business processes and planning at strategic, tactical, and operational levels. Given its importance, information must be protected against risk, typically through information security risk management. Effective protection, however, requires an understanding of what information is valuable and why. Information classification provides this foundation by assessing the value of information assets and determining their organisational importance. Although classification is addressed in standards and academic literature, it has received limited empirical attention. Existing guidance explains what classification aims to achieve but offers little insight into how it is conducted in practice or how organisational conditions influence the process across strategic, tactical, and operational levels. As a result, key aspects of classification work remain underexplored.

Against this background, the purpose of this thesis is *to create knowledge about the relevance of information classification within the strategic, tactical, and operational levels of an organisational context*. To fulfil this purpose, the thesis identifies organisational prerequisites that enable meaningful classification, challenges that hinder it, and ways to support the practice and documentation of classification. These prerequisites, challenges, and support categories are analysed using a multi-level planning framework.

The research is based on five peer-reviewed studies, four of which were conducted in Swedish public sector organisations and one of which was conducted in the air traffic management domain. The empirical material includes semi-structured interviews, document analysis, tool demonstrations, and expert validation.

The findings demonstrate that information classification should not be understood merely as an isolated operational workshop activity. Instead, it is a multi-level organisational process shaped by strategic direction, tactical preparation, and operational execution. By adapting and applying a multi-level planning framework to information classification, the thesis shows that challenges and prerequisites identified during classification often originate from insufficient strategic framing and limited tactical support. Furthermore, classification is shown to be inherently interpretive. Subjective judgment plays a central role in assessing the value of information assets. In contrast to prior research, which often frames subjectivity as a weakness to be minimised, this thesis reconceptualises subjectivity as a necessary and unavoidable component of meaningful classification decisions. Finally, two main avenues for supporting classification are identified: automation and assistance. Automation refers to automating mainly administrative parts of classification, while assistance refers to providing support to carry out the process. Building on the assistance perspective, the thesis addresses an underdeveloped aspect of existing methods by developing structured documentation support that enables workshop participants to capture contextual knowledge and decision rationale.



---

## SAMMANFATTNING

---

Information är en kritisk tillgång för organisationer som möjliggör verksamhetsprocesser samt planering på strategisk, taktisk och operativ nivå. Med hänsyn till dess betydelse måste information skyddas mot risk, vanligtvis genom informationssäkerhetsriskhantering. Ett effektivt skydd förutsätter dock en förståelse för vilken information som är värdefull och varför. Informationsklassning utgör denna grund genom att bedöma värdet av informationstillgångar och fastställa deras organisatoriska betydelse. Även om informationsklassning behandlas i såväl standarder som akademisk litteratur har området fått begränsad empirisk uppmärksamhet. Nuvarande vägledning beskriver vad informationsklassning syftar till att uppnå men ger begränsad insikt i hur det genomförs i praktiken eller hur organisatoriska förutsättningar påverkar processen på strategisk, taktisk och operativ nivå. Detta har lett till att viktiga aspekter av klassningsarbetet är otillräckligt utforskade.

Mot denna bakgrund är syftet med avhandlingen *att skapa kunskap om informationsklassningens relevans inom strategiska, taktiska och operativa nivåer i en organisatorisk kontext*. För att uppfylla detta syfte identifierar avhandlingen organisatoriska förutsättningar som möjliggör meningsfull informationsklassning, utmaningar som försvårar den samt stöd för genomförandet och dokumentationen av klassning. Dessa förutsättningar, utmaningar och stödformer analyseras med hjälp av ett flernivåbaserat planeringsramverk.

Avhandlingen baseras på fem sakkunniggranskade och publicerade studier, varav fyra har genomförts i svensk offentlig sektor och en i flygtrafikledningsområdet. Det empiriska materialet består av semistrukturerade intervjuer, dokumentanalys, verktygsdemonstrationer och expertvalidering.

Resultaten visar att informationsklassning inte bör ses som en enbart operativ workshopaktivitet. I stället framställs den som en organisatorisk process som påverkas av flera organisatoriska nivåer, formad av strategisk inriktning, taktiska förberedelser och operativt genomförande. Genom att anpassa och tillämpa ett flernivåbaserat planeringsramverk på informationsklassning visar avhandlingen att de utmaningar och förutsättningar som identifieras under klassningsprocessen ofta har sitt ursprung i bristande strategisk inramning och otillräckligt taktiskt stöd. Vidare visas att klassning är en i grunden tolkande process, där subjektiva bedömningar har en viktig roll i värderingen av informationstillgångar. I kontrast till tidigare forskning, som ofta framställer subjektivitet som en svaghet som bör minimeras, omkonceptualiserar avhandlingen subjektivitet som en nödvändig komponent i meningsfulla klassningsbeslut.

Avslutningsvis identifieras två huvudsakliga vägar för att stödja klassning: automatisering och assistans. Med automatisering menas automatiseringen av främst administrativa delar av klassningen. Assistans hänvisar istället till att stödja utförandet av processens olika delar. Med utgångspunkt i ett assistansperspektiv bidrar

---

avhandlingen till en underutvecklad del av befintliga klassningsmetoder genom att utveckla ett strukturerat dokumentationsstöd som möjliggör för deltagare i klassningsworkshops att fånga upp och dokumentera både kontextuell kunskap och beslutsmotivering.

---

## LIST OF PUBLICATIONS

---

This thesis is based on five publications which are referred to in the text as Paper **A** through **E**. The original publications are available as appendices at the end of the thesis.

### Paper A

**Andersson, S.** (2023). *Problems in information classification: insights from practice*. *Information & Computer Security*, 31(4), 449-462. <https://doi.org/10.1108/ICS-10-2022-0163>

**Personal Contribution:** As the sole author of the paper, I did all of the work.

### Paper B

Bergström, E., **Andersson, S.**, & Lundgren, M. (2024, July). In: Furnell, S., & Clarke, N. (eds) *To risk analyse, or not to risk analyse: That's the question*. In International symposium on human aspects of information security and assurance (pp. 107-119). Springer Nature Switzerland.

**Personal Contribution:** I contributed to the study design, conducted part of the interviews, co-led the analysis, and co-authored the manuscript.

### Paper C

**Andersson, S.**, Ericson, Å., Lugnet, J., & Große, C. (2025). *What Makes Information Critical? Information Classification in Organizational Practice*. In: Bergström, E., Hämmerli, B., Kitkowska, A & Kävrestad, J. (eds) *Critical Information Infrastructures Security* (pp. 3-19). Springer Cham.

**Personal Contribution:** I contributed to the study design, conducted all of the interviews, led the data analysis, and co-authored the manuscript.

### Paper D

**Andersson, S.**, Bergström, E., Lundgren, M., Bernsmed, K., & Bour, G. (2025). *Information security risk management tools in the air traffic management domain: what are practitioners' needs?* *Information Security Journal: A Global Perspective*, 1-18. <https://doi.org/10.1080/19393555.2025.2498472>

**Personal Contribution:** I was the driving force of the paper, co-led the analysis, and co-authored the manuscript.

## Paper E

**Andersson, S.**, Bergström, E. (2026) *The importance of records in information classification - "If you have not documented it, you have not done it"*. Information & Computer Security, 1-23. <https://doi.org/10.1108/ICS-04-2025-0124>

**Personal Contribution:** I was the driving force of the paper, conducted part of the interviews, led the data analysis and authored the full manuscript.

**The following publications have a lower relevance to the thesis:**

Holmström, A., Ahlmark, D, I., Lugnet, J., **Andersson, S.**, Ericson, Å. (2024) *Cybersecurity and the AI Silver Bullet*. In T. Sipola et al., *Artificial Intelligence For Security*. Springer Nature Switzerland AG 2024. [https://doi.org/10.1007/978-3-031-57452-8\\_2](https://doi.org/10.1007/978-3-031-57452-8_2)

Holmström, A., **Andersson, S.**, & Wenngren, J. (2025). *Towards Operationalizing Cyber Resilience - A Socio-Technical Analytical Framework*. In 11th International Workshop on Socio-Technical Perspectives in Information Systems (STPIS 2025), September 17-18, 2025, Hybrid/Skopje, North Macedonia (Vol. 4134). CEUR.

---

# TABLE OF CONTENTS

---

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Problem Background . . . . .	1
1.2	Research Problems . . . . .	3
1.3	Purpose and Research Questions . . . . .	4
1.4	Delimitations . . . . .	5
1.5	Thesis Structure . . . . .	5
<b>2</b>	<b>Background</b>	<b>7</b>
2.1	Organisational Context . . . . .	7
2.2	Information Security and Risk Management . . . . .	10
2.3	Information Classification . . . . .	12
2.3.1	Previous Work . . . . .	12
2.3.2	Information Assets . . . . .	13
2.3.3	Granularity . . . . .	14
2.3.4	Conducting Information Classification . . . . .	15
2.3.5	Classification Matrix & Consequence Categories . . . . .	18
2.3.6	Records . . . . .	20
2.3.7	Classification Terminology . . . . .	21
<b>3</b>	<b>Research Approach</b>	<b>23</b>
3.1	Positionality . . . . .	23
3.2	Research Process . . . . .	24
3.3	Data Collection . . . . .	28
3.3.1	Semi-Structured Interviews . . . . .	28
3.3.2	Collected Documents . . . . .	31
3.3.3	Observations . . . . .	31
3.3.4	Expert Panels . . . . .	32
3.4	Data Analysis . . . . .	33
3.4.1	Thematic Analysis . . . . .	33
3.4.2	Document Analysis . . . . .	34
3.4.3	Expert Panel Validations . . . . .	34
3.5	Thesis Analysis . . . . .	34
3.6	Research Reflections . . . . .	36
3.6.1	Ethical Reflections . . . . .	39
<b>4</b>	<b>Thesis Results</b>	<b>41</b>
4.1	Summary of Appended Papers . . . . .	41
4.2	Thesis Results . . . . .	46
4.2.1	Prerequisites in Information Classification . . . . .	46
4.2.2	Challenges in Information Classification . . . . .	49

4.2.3	Supporting Information Security Risk Management and Information Classification . . . . .	53
4.2.4	Records in Information Classification . . . . .	55
<b>5</b>	<b>Analysis and Discussion</b>	<b>61</b>
5.1	Levels of Planning . . . . .	61
5.2	Coordination and Collaboration Between Planning Levels . . . . .	69
5.3	Research Contributions . . . . .	71
5.4	Practical Contributions . . . . .	73
5.5	Limitations . . . . .	76
5.6	Future Research . . . . .	77
<b>6</b>	<b>Conclusion</b>	<b>79</b>
	<b>References</b>	<b>83</b>

---

## ABBREVIATIONS

---

**ATM** – Air Traffic Management

**CIA** – Confidentiality, Integrity, and Availability

**GDPR** – General Data Protection Regulation

**ISO** – International Organization for Standardization

**IEC** – International Electrotechnical Commission

**ISMS** – Information Security Management System

**ISRM** – Information Security Risk Management

**IT** – Information Technology

**MSB** – Swedish Civil Contingencies Agency

**NIS-2** – Network and Information Systems Directive 2

**NIST** – National Institute of Standards and Technology

**NIST RMF** – National Institute of Standards and Technology Risk Management Framework

---

## KEYWORDS

---

Information Security, Information Security Risk Management, Information Classification, Organisational Practice, Multi-level planning



---

## LIST OF FIGURES

---

1	Concepts of Multi-Level Planning - Adapted to Information Classification . . .	9
2	An Overview of the Low Granularity Approach . . . . .	16
3	A Standard Classification Matrix . . . . .	19
4	The Relationship Between the Thesis Purpose, Research Questions and In- cluded Papers . . . . .	25

---

## LIST OF TABLES

---

1	Overview of Materials and Approaches Used in Appended Papers . . . . .	29
2	Prerequisites Identified in Papers A - E . . . . .	48
3	Challenges Identified Papers A - E . . . . .	52
4	Contextual Knowledge in Business Process/System Analysis. . . . .	57
5	Contextual Knowledge in Requirements . . . . .	58
6	Contextual Knowledge in Classification Results. . . . .	60
7	Prerequisites, Challenges and Support, Positioned in Relation to Organisa- tional Planning Levels . . . . .	69



## 1.1 Problem Background

Organisations in today's day and age greatly rely on information assets, such as information and where it resides, mainly in information systems and information technology. Most business activities depend on such assets, as they support and inform decision-making and enable business operations at the strategic, tactical and operational levels of an organisation. As such, how organisations understand and work to protect information assets is shaped by organisational planning, which includes strategic intent, tactical preparation, and operational execution. These levels represent different forms of planning and decision-making and are interdependent. The strategic level defines long-term directives and priorities, the tactical level translates these directives into methods, processes and support, while the operational level concerns the carrying out of activities in practice (Schmidt & Wilhelm, 2000; Whitman & Mattord, 2022). Alignment across these levels influences how organisational practices are structured, supported and in turn, how effectively they can be carried out.

Further, information assets play a key part in understanding and managing businesses (Leming, 2015). If not understood, there is little chance of successfully implementing strategies, improving and maintaining business processes or understanding demands of compliance regulations (Evans & Price, 2020; Swartz, 2007; von Solms & von Solms, 2006). In short, information assets are very important to organisations, and they are a primary target for organised cybercrime. According to IBM (2023), the average total cost of a data breach in 2023 was \$4.45 Million, which is an increase of 15.3% from 2020. The consequences of information compromise extend beyond financial losses and can lead to a loss of operational ability and the unavailability of critical systems and information (Whitman & Mattord, 2022). A recent example of such consequences was the cyberattack against the system provider "Miljödata" in 2025, which affected a large share of Swedish municipalities, as the company delivers human resources and personnel administration systems to local authorities across the country (SVT, 2025). The incident resulted in prolonged system unavailability and the leak of personal information for 1 million Swedish citizens to the dark web. As such, organisations must protect their information assets and manage potential risk (Shameli-Sendi et al., 2016). To do so, organisations need information security.

The purpose of information security is to prevent information from being compromised in terms of confidentiality, integrity, and availability (Wangen et al., 2018). Confidentiality refers to information being accessible only to authorised individuals, integrity refers to information remaining accurate and unaltered except by authorised users, and availability concerns information being accessible to those who need it when required (Whitman & Mattord, 2022; von Solms & Van Niekerk, 2013;

Åhlfeldt et al., 2007). Together, these three concepts are known as the CIA triad, and compromising any of them can cause serious setbacks for an organisation (Gerber & von Solms, 2005).

To handle and manage information security, an Information Security Management System (ISMS) can be used (Bergquist et al., 2021). Management systems, in general, attempt to provide a holistic perspective and cover what is needed to manage, in this case, information security (Heras-Saizarbitoria & Boiral, 2013). It is important to note that management systems are tools used for managing, and not a complete solution or a replacement for all management activities (Whitman & Mattord, 2022). To implement such a system, standards based on best practices are typically used, one example being the ISO 27000 series (ISO/IEC 27000, 2018), which focuses on the design, implementation, and management of an ISMS (Disterer, 2013). A key part of an ISMS is that of Information Security Risk Management (ISRM).

If risk is not managed, it can cause operational failures and even organisational collapse (Whitman & Mattord, 2022). However, it is well known that managing risks is not an easy task, and different ISRM activities provide different challenges (Fenz et al., 2014). A foundational process for managing risk is information classification, which involves classifying information assets according to their value to the organisation (Bergström et al., 2021; ISO/IEC 27002, 2022). Classification is done by estimating the level of consequence an organisation would suffer if an information asset were to lose its confidentiality, integrity or availability (Bergström et al., 2021; ISO/IEC 27002, 2022). The outcome of the classification process is an information asset labelled with a classification level that indicates its need for protection. Based on the classification, an organisation can define requirements for how the information asset can be handled, in which systems it can exist, and how it can be transferred or shared (Fibikova & Müller, 2011). Importantly, it also serves as a crucial input to the risk assessment (Bergström et al., 2021; Gerber & von Solms, 2005; ISO/IEC 27002, 2022). If the classification is not done properly, it will, as a result, provide lacklustre input to the risk assessment, leading to unreliable results in the risk management process, following the "garbage in garbage out" phenomenon as explained in Shamala et al. (2017).

However, large amounts of information remain unclassified. According to Veritas (2020), 53% of information in businesses remains 'dark', meaning it is neither identified nor classified. This is problematic, as there is no knowledge of the potential value of the information assets, nor of what they might contain. Following this, no risk assessment will be conducted on the information assets, meaning they will remain vulnerable to potential threats, putting the organisation at unnecessary risk. Given that there is no knowledge of what the 'dark' information assets contain, there is also the risk for compliance breaches. One such example is the General Data Protection Regulation (GDPR) and the stipulated "right to be forgotten", which allows customers to request to be completely removed from an organisation's systems. If information assets are 'dark', i.e., not identified, organisations will struggle to comply with regulations, as they cannot guarantee that all customer data will be deleted. There has been an increase in the amount of data being classified, however, it is small. Over 5 years Veritas (2020) mentions that there has been a 6% decrease in

dark data (from 59% to 53%), indicating that while improvement is being made, organisations still struggle with both identifying and classifying information, and that further improvement is needed.

## 1.2 Research Problems

As explained, information classification is an important process. However, there are plenty of challenges connected to it. Some of the more prevalent issues that have been identified is the difficulty of translating standards into organisational practice (Niemimaa & Niemimaa, 2017), holistic descriptions of security activities that do not detail how to conduct the different activities (Tehler, 2023), difficulties in creating organisational classification schemes (Bergquist et al., 2021; Bergström et al., 2021; Fibikova & Müller, 2011; Ghernaouti-Helie et al., 2011), and choosing a granularity level of information assets to classify (Bergström & Åhlfeldt, 2014). Further, it is recommended that the classification process is conducted in a workshop format with actors of different backgrounds and organisational roles taking part. Involving a variety of actors is positive, as it will allow for a broader knowledge base to serve as a foundation for the classification. However, actors will be subjective in their assessment of information asset value and may reach different conclusions, highlighting the problem of subjective judgment (Bergquist et al., 2021; Kaarst-Brown & Thompson, 2009; Ku et al., 2009; Metin et al., 2024).

Some of the above issues have been addressed in previous research. For example, Bergquist et al. (2021) tailored a classification scheme for Swedish public sector organisations, Bradford et al. (2022) investigated drivers and challenges in classification work, and Bergström et al. (2021) developed a structured method based on ISO 27002. Despite these efforts, there remains limited empirical knowledge of how information classification is actually carried out in organisational practice. In particular, there is a lack of understanding of how organisational prerequisites and challenges influence the classification process. Without knowledge of how classification is influenced by such conditions, efforts to support and improve information classification risk being detached from practice. There is therefore a need to identify the prerequisites that enable meaningful classification, the challenges that hinder it, and to investigate how classification practices can be supported.

Another underexplored aspect concerns the role of records in the information classification process. In ISRM, maintaining up-to-date documentation is considered a cornerstone of effective information security management (Mattord & Wiant, 2016), as documenting, sharing, and verifying the outcomes of security processes enables well-informed and auditable decisions (Barraza de la Paz et al., 2023). In the context of information classification, prior research such as Bergström et al. (2021) emphasises the importance of producing records that document classification results. However, existing methods provide little guidance on what such records should contain beyond the final classification level. As a result, the reasoning and other knowledge, acting as the basis for classification decisions, often remain undocumented. This lack of structured documentation limits transparency and makes it difficult to revisit or justify earlier decisions. In the case of classification, this issue is particularly signif-

icant given that decisions are typically made in workshop settings, where discussion and subjective judgment are central elements of the decision-making process. Without documented rationale, there is limited basis for understanding why an asset has been assigned a particular classification level. This complicates re-classification and, later on, risk analysis. As such, there is a need to examine what types of knowledge should be documented during classification, and how documentation practices can be supported as part of the classification process.

Taken together, the above problems indicate that information classification remains insufficiently understood as an organisational activity. Existing research has primarily focused on methods and isolated challenges, while paying less attention to how classification is shaped by organisational contexts. In particular, limited attention has been given to how strategic direction, tactical preparation, and operational execution influence the classification process. This points to a need of understanding the prerequisites that enable meaningful classification, the challenges that hinder it, and how to support classification practices from a strategic, tactical and operational perspective.

### 1.3 Purpose and Research Questions

The purpose of this thesis is to *create knowledge about the relevance of information classification within the strategic, tactical and operational levels of an organisational context*. To fulfil this purpose, the following research questions have been formulated:

1. What are the prerequisites and challenges with information classification in organisational practice?
2. How can the practice and documentation of organisational information classification be supported?

To address RQ1, the research examines the organisational context in which information classification takes place, identifying the prerequisites that enable meaningful classification and the challenges that hinder it in practice. In doing so, the thesis contributes a foundation for further understanding and supporting information classification.

Building on this understanding, RQ2 investigates how information classification can be supported, identifying two main avenues of support, those of assistance and automation. Particular attention is paid to documentation practices and the types of knowledge that should be captured in classification records. A structured approach to supporting classification and documentation is developed, contributing practical support for classification workshop participants. It also contributes to an existing classification method by extending the missing guidance regarding documentation practices.

The insights generated through RQ1 and RQ2 are analysed through the lens of strategic, tactical, and operational planning levels. This multi-level analysis contributes a perspective on how classification is enabled, hindered, and supported across organisational levels, thereby addressing the overall purpose of the thesis.

By positioning information classification as part of all levels of planning, the thesis advances the understanding of classification as more than an operational task, highlighting that to support classification, all levels of planning must be included and collaborate.

## 1.4 Delimitations

This thesis focuses on information classification as it is understood and carried out in organisational practice. The empirical material is primarily drawn from Swedish public sector organisations, complemented by a study conducted within the Air Traffic Management (ATM) domain. As such, it is limited to those perspectives. Both of these perspectives were deemed to be interesting for the thesis work. It should be noted that the thesis does not aim to provide comparisons across sectors or national contexts, nor does it seek to generalise its findings statistically. Instead, the focus is on developing an in-depth understanding of information classification within organisational settings.

Furthermore, the thesis limits its scope to a low-granularity approach to information classification (as described in 2.3.4), in which information assets are classified at a system or business-process level. This is the most common approach in practice, and the recommended approach in prior literature. As such, it does not address a high-level granularity approach. In addition, the thesis focuses on the classification process itself and on how workshop participants can be supported in carrying it out. It does not evaluate the classification outcome or its later use in ISRM.

Finally, the thesis focuses on information classification from an organisational and practice-oriented perspective. The emphasis is placed on how classification is understood and carried out by practitioners, as well as on the organisational conditions that shape these activities. As such, the thesis does not address the technical aspects, such as the technical implementation of support. While technical solutions and tools are discussed where relevant, they are considered from the perspective of how they support classification work in practice rather than how they are designed or implemented at a technical level.

## 1.5 Thesis Structure

This thesis consists of a cover manuscript and five peer-reviewed research papers. It is organised into six chapters. Chapter 1 introduces the research topic, outlines the problem, and presents the purpose and research questions. A visualisation of the relationship between the purpose, research questions, and included papers is shown in Figure 4 in Section 3.2. Chapter 2 provides background on the organisational context, information security and risk management, and information classification. Chapter 3 describes the scientific positioning of me as an author and the research methods used. Chapter 4 summarises the included papers and the thesis results. Chapter 5 analyses and discusses the results using a multi-level planning perspective, and addresses limitations and directions for future research. Finally, Chapter 6 revisits the purpose and research questions and concludes the thesis work.



This chapter presents the theoretical domain of the thesis, including the organisational context, information security risk management and information classification.

## 2.1 Organisational Context

As the purpose of this thesis is to *create knowledge about the relevance of information classification within the strategic, tactical and operational levels of an organisational context*, it is important to situate the classification process within the organisational context. As such, this section describes the organisational context in which classification is situated and explains the organisational levels of planning.

In this thesis, an organisation is understood as a structured environment of people, roles, and processes working toward shared goals (Scott & Davis, 2016). These shared goals are formulated by the organisation's management through strategic planning (Whitman & Mattord, 2022). To achieve such goals, the organisation will develop and implement policies, directives and strategies that outline how to carry out organisational activities and processes. These directives are typically expressed through three levels of organisational planning: strategic, tactical, and operational (von Solms & von Solms, 2006). Strategic goals define the organisation's long-term direction, tactical plans translate those goals into actionable steps, and operational plans guide the day-to-day execution of those steps. This creates a flow of guidance from high-level goals down to operational practice (Whitman & Mattord, 2022). In this manner, organisational planning levels shape how high-level directives are translated into actions that are to be realised in practice. The planning levels can therefore be summarised as strategic addressing the why, tactical addressing the how, and operational addressing the what (White, 2024). In general, the level of detail increases, and the time horizon decreases as directives move from strategic to operational (Schmidt & Wilhelm, 2000).

Planning can also be understood in two senses: narrow and broad (Schmidt & Wilhelm, 2000). In the narrow sense (A), planning refers to preparation, defining goals, designing processes, and preparing the means to carry out processes and activities before execution. In the broad sense (B), planning also includes the implementation and decision-making included in said processes and activities. In other words, narrow planning focuses on how to prepare, while broad planning includes the decision-making and extends to how those plans are made in practice (Große, 2019).

From the above explanations, it can be said that information classification will be affected by the people and processes that make up the organisation. It is also evident that organisational processes and activities depend on how directives at the different levels of organisational planning are developed and implemented. For example, if

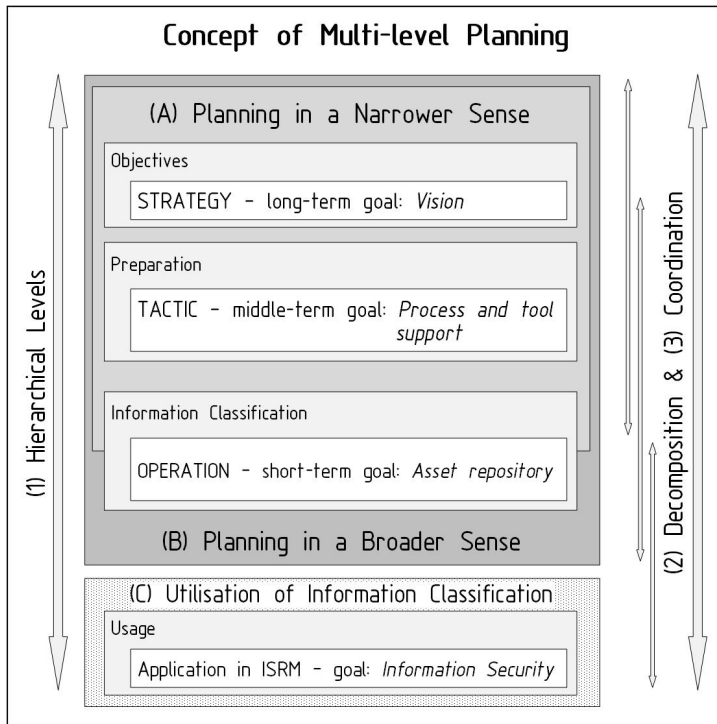
no strategic direction or long-term goal is established for risk management within a specific organisation, the organisation will struggle to provide adequate tactical support to risk analysts and managers, and as a result, they face difficulties in carrying out activities effectively at the operational level.

The concept of organisational planning levels is well-established and has been applied in other areas of research, such as in plan monitoring, where Allouche and Berger (2011) propose a multi-level framework for monitoring plan decision-making. In Große (2019), a multi-level planning approach was used to investigate interrelationships between uncertainty and planning activities in a Swedish response planning setting. Further, in relation to information security, the organisational planning levels have been used, for example, in (White, 2009), to investigate the types of work done at each of the strategic, tactical, and operational levels. Another example is Liu et al. (2025), which uses the planning levels to investigate and develop a cybersecurity management and performance assessment model.

In addition to multi-level planning, other models can be used to analyse organisational activities, such as information classification. One example is the direct-control cycle proposed by von Solms and von Solms (2006), which views information security activities from the perspective of a governance loop. In this model, senior management provides direction at the strategic level, the tactical layer translates these directives into policies and procedures, and the operational level executes the operational tasks according to those policies and procedures. Once implemented, control mechanisms are used at the operational level by collecting performance data intended to demonstrate how effectively the directives are functioning. This information is later analysed at the tactical level and aggregated for senior management, thereby completing the governance loop.

While the two models consist of the same organisational levels, they differ in focus. The multi-level planning perspective provides a way of distinguishing between strategic, tactical, and operational activities, and highlights how these levels relate to one another through decomposition and coordination. This perspective makes it possible to examine how organisational activities are prepared at one level and realised at another, and how alignment between levels is established. In contrast, the direct-control cycle primarily emphasises governance and control, describing organisational activities as the result of directives made at a strategic level and checking how effectively the activity is carried out. In other words, there is little focus on the planning or preparation of activities.

As information classification is affected by the preparation of directives, the development of process and tool support, and the execution in practice, it can be understood as part of an organisational planning process. The multi-level planning approach is therefore adopted as an analytical model, as it offers a structured way of analysing how classification is positioned and related across the three organisational levels. The model presented in Figure 1 is adapted from Große (2019). In its original form, the model was used to analyse planning activities in a response planning context. In this thesis, the hierarchical structure of strategic, tactical, and operational levels is retained, as are the concepts of decomposition and coordination between levels.



**Figure 1:** Concepts of Multi-level Planning (Große, 2019) - Adapted to Information Classification

The adaptation consists primarily of repositioning information classification as the organisational activity analysed within this structure. Rather than focusing on response planning, the model is used here to examine how information classification is prepared, structured, and carried out across organisational levels. No logical modifications have been made to the model itself; instead, its conceptual components are applied to the domain of information classification.

As explained, planning can be divided into a *narrower* (A) and *broader* sense (B). In the case of an information classification, it is difficult to distinguish between the two, as it is difficult to clearly state what is part of the decision-making and what is part of the preparation / carrying out of the process. For example, is the collection of information during the classification workshop (further explained in 2.3.4) part of the decision-making or planning? Given this difficulty, Figure 1 represents the operational layer as part of both wide- and narrow-planning. For planning to be effective, there must also be cooperation and collaboration between the levels in the form of, for example, feedback on the usability of support from the operational to the strategic level, represented as *decomposition*(2) and *coordination*(3).

The *hierarchical levels*(1) can be represented by strategic, tactical and operational perspectives. As mentioned, the *strategic* level represents the long-term goals and

directions of an organisation. It involves establishing objectives, allocating resources, and defining the principles that guide, for example, information security and risk management efforts (AlGhamdi et al., 2020; Whitman & Mattord, 2022; von Solms & von Solms, 2006). Decisions at a strategic level are typically made by senior management or executive leadership and are aimed at aligning information security with organisational goals and external requirements (Veiga & Eloff, 2007). In other words, it provides the tactical level with directives that are to be translated into policies and standards for the organisation to use (von Solms & von Solms, 2006).

Relating to information classification, the strategic level defines the purpose and use of the classification activities. It should establish why classification is necessary, what organisational goals it serves, how it helps with achieving the long-term goals, and how it fits within, for example, broader information security policies and risk management frameworks. It does not, however, decide on specific frameworks or models to use for conducting the classification activity.

The *tactical* level represents the translation of strategic high-level goals into actionable steps or processes. The intent is to develop or state procedures that are to be used, and to coordinate activities across departments in an organisation. Actors at this level, such as information security managers or coordinators, ensure that strategic intentions are implemented consistently and supported with the necessary resources (Whitman & Mattord, 2022; von Solms & von Solms, 2006). Connecting to information classification, the strategic directives are translated into guidance on how information classification should be conducted in practice. This involves developing or stating the methods and tools to be used that support the activity, such as the classification matrix illustrated in Figure 3. Typical outputs from this level would include the classification method itself, roles who should participate, statements defining which consequence levels to apply, and other forms of procedural support required to carry out the activity effectively.

The *operational* level represents the day-to-day activities through which the organisation's plans and policies are executed to achieve the goals set in both the strategic and tactical levels (Whitman & Mattord, 2022; von Solms & von Solms, 2006). The focus of the operational level is on execution and ensuring that tasks are performed in accordance with procedures set in the tactical stage. In terms of information classification, the operational level would translate to the practice of classifying information. This includes conducting the information classification process as it is stated in the tactical level (in the case of this work, see Figure 2) using tools and instructions as provided. The result of the operational layer will lead to the *utilisation of information classification*, meaning the classification results are used in information security risk management.

## 2.2 Information Security and Risk Management

In general, the purpose of information security is, as is indicated by the name, to keep information, such as knowledge in the minds of people, written physical documents, or digital entries in a database, from compromise of *confidentiality*, *integrity* or *availability* (Gritzalis et al., 2018; ISO/IEC 27002, 2022; Whitman & Mattord,

2019). As mentioned in Section 1.1, confidentiality, integrity and availability are commonly known as the CIA-triad. These three are principles that, when connected to information, should be kept intact for information to be deemed protected (von Solms & Van Niekerk, 2013). Confidentiality refers to information only being available and readable to those with the correct privilege, integrity refers to information staying unchanged, and availability refers to information being available to those with the correct access privilege when they need to use it (Wheeler, 2011; Whitman & Mattord, 2019). Maintaining the CIA-triad of information assets within an organisation requires coordinated efforts. Within organisations, this is achieved through information security management, understood as the structured coordination of policies, processes, and controls intended to define, implement, maintain, and continually improve the protection of information assets (ISO/IEC 27000, 2018; Whitman & Mattord, 2019). Effective information security management supports the organisation in achieving its objectives by ensuring that information remains protected in alignment with organisational goals and risk tolerance. A central part of information security management is information security risk management, which focuses specifically on identifying and addressing risk.

Risk management is a cornerstone of the information security field, with the purpose of identifying, analysing and mitigating information security risk towards organisational information assets (Gritzalis et al., 2018; Whitman & Mattord, 2019). Conducting risk management is usually done in a process-like manner and is explained differently in standards such as the ISO 27000 family (ISO/IEC 27000, 2018), the NIST Risk Management Framework (NIST RMF) (National Institute of Standards and Technology [NIST], 2018) and Octave Allegro (Caralli et al., 2007). Each standard proposes a slightly different process, with different names and explanations for the steps described. A key part of risk management revolves around three common activities, often referred to as risk assessment. While there are minor differences, the general outline of risk assessment is explained in, for example, ISO 27005 (ISO/IEC 27005, 2022), NIST RMF (NIST, 2018) and Octave Allegro (Caralli et al., 2007), and can be summarised as follows:

1. **Asset Identification and Classification** - Information assets, both tangible and intangible, that are necessary for the business to operate, are identified. Once this is done, the identified assets are classified, meaning the value of each asset to the organisation is investigated and assessed. This results in a list of assets labelled with a classification level.
2. **Risk Analysis** - Threats against the confidentiality, integrity and availability of the identified assets are identified, paired with how those threats could exploit potential vulnerabilities present in the assets. An analysis is then conducted, where the likelihood level of a threat exploiting a vulnerability is estimated. Following, the potential impact on the business in the case of threat realisation is determined. The impact level is based on the classification level that resulted from the classification. This results in a level of risk tied to each asset.

- 3. Risk Treatment** - Based on the two previous activities, a decision can be made for how to best treat the risk if deemed necessary. Such treatment is usually done by either addressing the vulnerability of the asset, mitigating the consequences of a risk manifesting, or reducing the likelihood of the threat occurring.

The above-described activities follow a step-by-step approach (1 through 3), i.e., they build upon each other and together form risk assessment. It is important to note that risk assessment must be iterative and not conducted only once, rather, it must be continuously monitored and managed (Lundgren, 2020; Nieves et al., 2017; Wheeler, 2011). The landscape in which organisations and their information assets reside is constantly evolving, and threats follow the same pace. As such, if the risk assessment is conducted only once, the results will soon become outdated, and new threats will arise that remain untreated. As explained in the above process, the first step and main input into the risk analysis is that of information classification.

While risk management and its included concepts are not the main focus of this work, a high-level explanation is included to contextualise information classification. A more in-depth explanation of the above-mentioned concepts can be read in the works of, for example, (Nieves et al., 2017; Wangen et al., 2018; Wheeler, 2011; Whitman & Mattord, 2022).

## 2.3 Information Classification

This section reviews previous work on information classification and introduces the concepts of information assets and granularity. It then describes the classification process and its key components, and concludes with a discussion of classification terminology.

### 2.3.1 Previous Work

Information classification is commonly described as a foundational activity within information security risk management. Despite this, it remains a relatively understudied area of research (Bergquist et al., 2021; Bergström & Åhlfeldt, 2014). As a result, the literature on classification is limited. However, there are contributions that address the classification process and parts of it in different ways. As of late, the most expansive contribution is that of Bergström et al. (2021), whose work developed a method covering an information classification process from start to end based on how it is described in the ISO/IEC 27002 (2022) standard. Other scholars have investigated specific aspects of the process and its tools, such as Bergquist et al. (2021), who examined the use of classification matrices in Swedish public-sector organisations and how they can be tailored to specific needs. Other studies, such as (Bradford et al., 2022), examined the classification process and provided general insights from security managers regarding its use and necessity. Earlier research, such as that of (Fibikova & Müller, 2011) explained a simplified classification process and pointed out that classification should always happen within the context of a business process, where they then further explained how to classify applications as information assets through a self-developed tool based on Microsoft Excel. Ghernaouti-Helie

et al. (2011), while not focusing on classification in their work, point out that there is an understanding of the need of effective information classification, but also state that doing so is difficult. In another recent study, Ignaczak et al. (2026) presented a value-based approach to information classification that applies natural language processing techniques to estimate information value from document content. Their work focuses on automating classification by combining indicators of personal data and contextual features, with the aim of supporting flexible multi-level classification schemes.

It should also be noted that there are other sources of information classification approaches that are not based on research. One such example is the "Information Classification Method Support" created by the Swedish Civil Contingencies (MSB) (MSB, 2023). Their support covers most of the classification activities and tools, including creating an organisational classification scheme and how to conduct a classification workshop. This support, as in the work by Bergström et al. (2021), is based on the ISO 27002 standard.

While the above-mentioned contributions provide valuable insights into different aspects of information classification, much of the existing literature either focuses on the design and development of classification methods or on isolated components and tools of the classification process. Little attention has been paid to the organisational conditions under which classification is carried out, or to how different organisational levels influence the classification process. In addition, very few empirical studies have examined how classification unfolds in organisational practice.

In this thesis, the method developed by Bergström et al. (2021) serves as the primary framework for describing how the information classification process is carried out. The process is explained in Section 2.3.4, and an overview can be seen in Figure 2. Earlier studies also contribute valuable insights to specific parts of the process, for example, Bergquist et al. (2021) discuss the use of classification matrices, which are further explained in Section 2.3.5. The model proposed by Bergström et al. (2021) was chosen because of its comprehensive scope and detailed description of the full process and its activities. However, parts of the method are underdeveloped, mainly concerning the creation and contents of records, which is further problematised and discussed in Section 2.3.6.

### **2.3.2 Information Assets**

Information can be understood as a representation of some part of the world, carrying semantic or representational content (Fallis, 2015; Scarantino & Piccinini, 2010). Building on this understanding, an information asset can be described as information held and managed within an organisation's information systems (Flowerday & Von Solms, 2005). According to Evans and Price (2020), information assets are essential for business processes, stakeholder interactions, decision-making, and the planning of an organisation in the strategic, tactical and operational levels of planning (as explained in 2.1).

However, determining what qualifies as an information asset is not entirely straightforward. It is generally understood to encompass any information that holds value to

an organisation, as well as the locations or systems where such information resides. Consequently, an information asset may refer both to the informational content itself and, depending on the level of granularity applied, to the systems or environments that store or process it. In the information security management literature, the term is often used broadly to include hardware, software, data, and information, as well as the people who support and use IT systems (ISO/IEC 27001, 2022; Shamala & Ahmad, 2014; Shedden et al., 2016; Whitman & Mattord, 2022).

Within an organisation, information assets can typically be recognised through some key characteristics. They possess some form of value, often ranging from critical to negligible (Spinellis et al., 1999); they are identifiable, meaning they can be located, described, and assigned ownership or responsibility; and they exist in relation to organisational processes, supporting operations and decision-making (Leming, 2015).

The identification of information assets is an important prerequisite for the information classification process. Classification presupposes an understanding of what information assets exist, where they reside, and how they are used. Without this understanding and context, it becomes difficult to assess protection needs and assign classification levels.

Identifying information assets and keeping an up-to-date asset inventory are two well-known challenges in information classification (Bergström & Åhlfeldt, 2014; Fenz et al., 2014; Rees & Allen, 2008). There are several reasons as to why this is the case, such as there being an over-reliance on methods to identify only technological assets (Dhillon & Backhouse, 2001), defaulting to only identify high-level assets, such as systems and databases (Shedden et al., 2010), and the rapid creation, modification and removal of information assets in organisations (Rees & Allen, 2008).

### 2.3.3 Granularity

Before conducting the information classification process, the organisation should take a stance on whether to use a high- or low-level granularity approach. A high level of granularity involves, for example, classifying individual files, providing a detailed view of assets, but requiring a high amount of resources. In contrast, a low level of granularity classifies assets at a broader scope, such as entire systems or organisational processes, thereby reducing the level of detail but also the resources required (Shedden et al., 2016). The latter approach is common in practice, as it is perceived to be more efficient, however, it can lead to overlooked components of a system or process, as it tends to treat systems and processes as black holes of information, focusing only on the value of the process or system itself (Shedden et al., 2016).

Although deciding on the level of granularity may appear straightforward, it represents a choice that will influence the classification. A low level of granularity will reduce the effort and resources required for classification, but simultaneously means accepting that some information assets are likely to be missed or ignored. On the other hand, a high level of granularity will improve the precision of the classification, but demand a greater investment of resources. As is observed in Fibikova and Müller (2011), there is no universal recommendation for determining the appropri-

ate level of granularity, as the decision depends on each organisation's context and priorities. Furthermore, asset value and associated risks evolve over time, further complicating decisions (Fibikova & Müller, 2011). It should also be noted that the low granularity approach is the most commonly used in practice (Bergström et al., 2021). As this thesis examines information classification as it is carried out in organisational settings, focusing on the approach most frequently used in practice was deemed beneficial. For this reason, the low granularity approach is adopted.

### 2.3.4 Conducting Information Classification

Classifying information assets is an essential part of both asset and risk management. It involves investigating and determining the value of information assets and serves as an indicator of the need for protection. It is a key input to risk analysis, as its results are used to determine the impact or consequence levels when assessing risk. The process is recommended in several widely used (ISMS) standards, including ISO/IEC 27002 (ISO/IEC 27002, 2022) and the NIST Risk Management Framework (NIST, 2018). Additionally, in some countries, public sector organisations are legally required to work systematically with information security and classification. For example, in Sweden, regulations stipulate that public sector organisations must adopt a risk-based approach in their information security work, by classifying their information assets, identifying risks, and implementing as well as monitoring appropriate security measures (MSB, 2020a). Similarly, in Japan, subcontractors are required to establish and apply information classification practices in order to be eligible for government contracts (METI, 2025). Further, the purpose of classification is described as "To ensure identification and understanding of protection needs of information in accordance with its importance to the organization" (ISO/IEC 27002, 2022, p. 22). As such, information classification is an important and foundational activity within information security management.

Information classification can also be viewed as a process. Davenport (1993, p.5) defines a process as "*...a specific ordering of work activities across time and place, with a beginning, an end, and clearly identified outputs and inputs.*" Viewing information classification as a process, therefore, means considering it as a series of activities undertaken to achieve the end goal of a labelled information asset. The classification process starts with a need for information classification. Such a need could be triggered by, for example, the procurement of a new system, movement or merging of information, or as the result of a scheduled re-classification (ISO/IEC 27002, 2022). As explained in section 1.1, the classification process is recommended to be done in a workshop format where participants of different backgrounds and roles within the particular organisational setting are included, allowing for more information to be identified and for more nuanced decisions to be taken. In Figure 2, Bergström et al. (2021) suggests the following activities to build the information classification process, which is based on the process outline found in ISO/IEC 27002 (2022). The activities are visualised and marked with their corresponding activity number in the Figure 2, matching the numerical list below the figure.

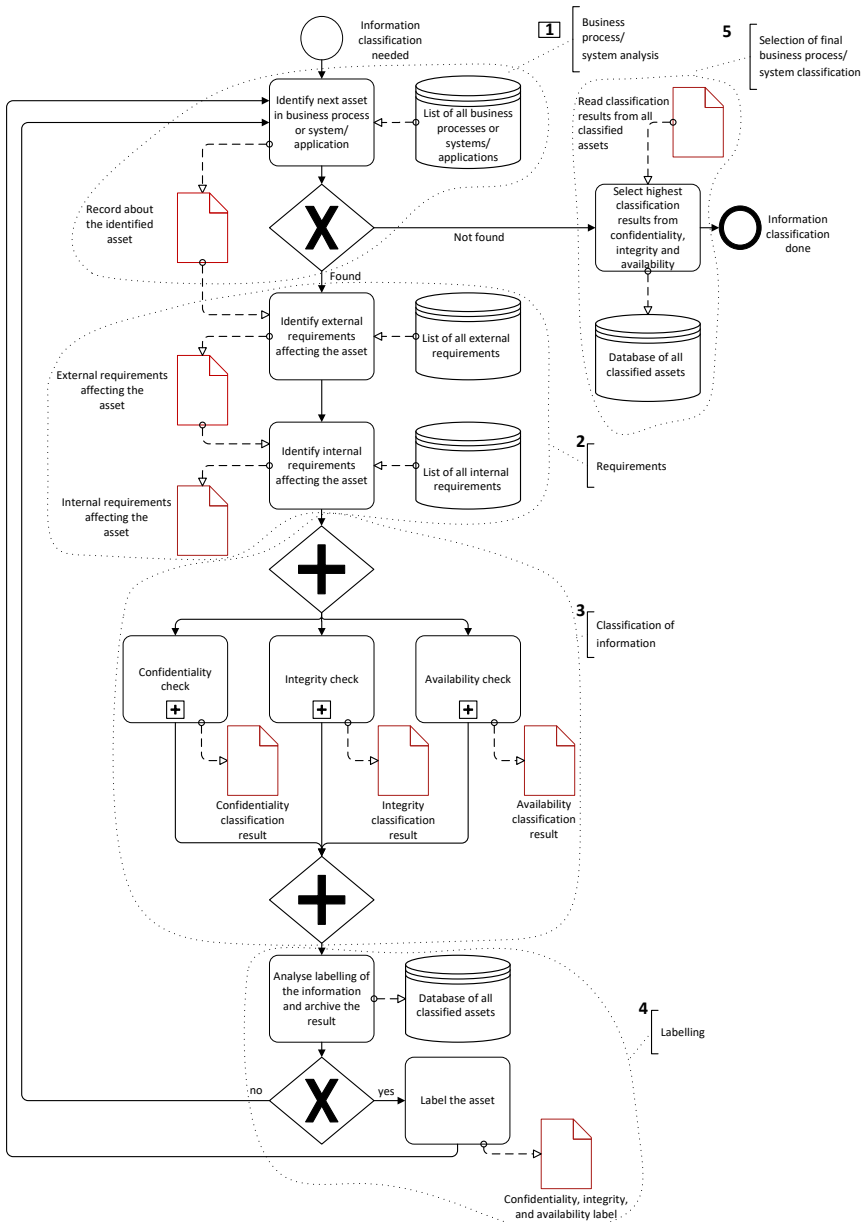


Figure 2: An Overview of the Low Granularity Approach - Adapted from (Bergström et al., 2021)

1. **Business Process / System Analysis** - The classification process begins with the business process/system analysis step, with the aim of identifying information assets present in a system, application or business process. This includes both tangible information assets, such as information systems and physical technical equipment, and intangible assets, including reputation and employee knowledge. This requires a list, or registry, of all business processes, systems, and applications. In this thesis, it is assumed that the creation of such an asset list has been created by the organisation, as it is not part of the classification process, but rather an assumed prerequisite. The workshop participants will continue to identify additional assets found in the business process, system, or application that is to be classified. Once all assets have been identified by the workshop participants, a record should be kept, tracking each asset identified, containing a short description, usage, and the roles that use the asset.
2. **Requirement identification** - The "Requirement Identification" step includes two main activities: "identify external requirements affecting the asset" and "identify internal requirements affecting the asset." In the first activity, "Identify external requirements affecting the asset," previously identified assets serve as the input. The goal is to determine the external requirements that apply to each asset. This begins with a list of national and international laws relevant to the specific context of the organisation. Examples of these laws include data protection regulations (such as the GDPR), laws about public access to information, and sector-specific laws, such as patient data regulations in healthcare.

The second activity, "Identify internal requirements affecting the asset," focuses on uncovering the internal rules related to the identified assets. This may involve examining agreements with external service providers and internal policies. The results of both these activities should be added to the previously created record of assets.

3. **Classification of Information** - The third activity is the Classification of Information. To conduct this activity, a classification matrix must be created and then used (see Section 2.3.5). Such a matrix will consist of a number of consequence levels, indicating the value of the asset to the organisation and the different aspects of consequence that the organisation will use to classify information. An example of a classification matrix can be found in Figure 3, where the concept is further discussed. Do note that Figure 3 use the CIA triad as security aspects. In Figure 2, the organisation instead use one classification matrix for each aspect of the CIA-triad, thus, there will be three valuations, one connected to each part. There is, however, no stated right or wrong way of doing it. In addition, there is the possibility of using different consequence categories; these are different ways of looking at potential consequences, such as reputational, financial and operational consequences. Such categories are further discussed in 2.3.5

- 4. Labelling of information** - The next step is Labelling of Information, which includes the activity “analyse labelling of the information and archive the result”. This is done after all activities for an asset are completed. The input for this activity is the previously collected data (i.e., the record) and the classification result. In this step, the information is archived, ensuring that the record is saved for future reference.

After this activity, a decision must be made on whether to label the asset or not. Labelling, sometimes called marking, means adding a label that shows the classification result to the information. This label can be applied to both physical and electronic formats. The way labelling is done can vary depending on factors like the granularity of the information being classified, storage methods, and file formats.

If the decision is made not to label the information, the process moves on to the task of “identify next asset in the business process or system/application” (i.e., Activity 1). If the decision is to label it, the next task is to “label the asset,” where the classification result is added to the information asset.

- 5. Selection of final business process/system classification** - The final activity, “Selection of final business process/system classification,” is carried out once all assets have been classified and no more can be identified. This step includes the activity “select highest classification results from confidentiality, integrity, and availability” to determine the overall classification of the business process or system.

The input for this task are all the classification values previously assigned to the identified assets. The final classification is determined by selecting the highest classification values found for each security aspect: confidentiality, integrity, and availability. These final numbers, indicating the classification level, are then recorded in the central repository to represent the classification for the entire business process or system.

Once the final step has been reached for the last asset contained in the business process and a classification decision has been made, the information classification process is at an end.

### 2.3.5 Classification Matrix & Consequence Categories

To conduct the information classification process, a classification matrix is commonly used, which is constructed and adapted according to organisational needs. It consists of some key elements, namely consequence levels, e.g., none, limited, serious and severe, and security aspects, often times the CIA-triad (Bergström et al., 2021). The security aspects can be adapted to specific organisational needs, however, (ISO/IEC 27002, 2022) recommends starting with the CIA-triad. The consequence level refers to the level of consequence the organisation deem that the loss of the asset being classified would cause. The security aspects refer to the aspect of security, in the case of Figure 3, the aspects are the CIA-triad. The loss of confidentiality could, for example, have a higher consequence level than that of loss of integrity, as such, it

is important to take several perspectives into account. Additionally, an explanation of each level can be included, as can be seen in Figure 3.

Security Aspect (→) Consequence Level (↓)	Confidentiality	Integrity	Availability
None	Information where the loss of <b>confidentiality</b> has a <b>no</b> negative impact on one's own or another organization and its assets, or on an individual	Information where the loss of <b>integrity</b> has <b>no</b> negative impact on one's own or another organization and its assets, or on an individual.	Information where the loss of <b>availability</b> has <b>no</b> negative impact on one's own or another organization and its assets, or on an individual.
Limited	Information where the loss of <b>confidentiality</b> has a <b>limited</b> negative impact on one's own or another organization and its assets, or on an individual	Information where the loss of <b>integrity</b> has a <b>limited</b> negative impact on one's own or another organization and its assets, or on an individual.	Information where the loss of <b>availability</b> has <b>limited</b> negative impact on one's own or another organization and its assets, or on an individual.
Serious	Information where the loss of <b>confidentiality</b> has a <b>serious</b> negative impact on one's own or another organization and its assets, or on an individual	Information where the loss of <b>integrity</b> has a <b>serious</b> negative impact on one's own or another organization and its assets, or on an individual.	Information where the loss of <b>availability</b> has <b>serious</b> negative impact on one's own or another organization and its assets, or on an individual.
Severe	Information where the loss of <b>confidentiality</b> has a <b>severe</b> negative impact on one's own or another organization and its assets, or on an individual	Information where the loss of <b>integrity</b> has a <b>severe</b> negative impact on one's own or another organization and its assets, or on an individual.	Information where the loss of <b>availability</b> has <b>severe</b> negative impact on one's own or another organization and its assets, or on an individual.

**Figure 3:** A Standard Classification Matrix - Based on MSB (2023)

The purpose of including the explanation is to provide more insight into what each consequence level, in each security aspect entails. Formulating the explanations of the consequence levels can be difficult, as there is a paradoxical dilemma that must be handled: that of simplifying the descriptions enough to make them easy to understand while at the same time keeping them detailed enough to allow for precise and consistent classifications (Fibikova & Müller, 2011). There is also the possibility of participants having a bias to the middle when presented with the different options, in a similar manner to the centre-stage effect (Rodway et al., 2012).

In a similar manner, other categories can be used in information classification to view and analyse the consequence of information asset compromise. Such categories have been named differently in both research and practice, such as "Perspective of potential impact" by Bergström et al. (2021) who suggests the use of "own organisation", "other organisation", and "individuals" as examples of perspectives, "Consequence Categories" (Bergquist et al., 2021; MSB, 2023), who instead suggest financial loss, damaged brand / decreased confidence, personal injury and environment damage as perspectives. Other examples are classification categories (Whitman & Mattord, 2022) and impact categories (Wheeler, 2011).

For each consequence category, the scale of consequences must be explained, this means that one classification matrix has to be used for each consequence category. Another option is to use one classification table, focusing on, e.g., the CIA aspects and then having definitions for other consequence categories, i.e., what would a severe confidentiality loss entail when using the consequence category of financial

impact? A third option is to use one classification scheme for different consequence categories; however, doing it this way, the matrix will not be able to fit the security aspects.

### 2.3.6 Records

Documenting processes or activities is essential to know what has been done, how it has been done, and what the outcome is. In ISMS, documentation has been explained to be the process of identifying, creating, updating and controlling information determined to be necessary for the effectiveness of a system (Haufe et al., 2022; ISO/IEC 27001, 2022). Having comprehensive and up-to-date documentation is also recommended practice, and deemed to be a keystone of good information security management (Johnson & Schulte, 2004; Mattord & Wiant, 2016; Tatar & Karabacak, 2012). ISO/IEC 27001 (2022) mention that the amount of documentation necessary will differ between organisations and that documented information should be available to the extent necessary to have confidence that the different processes have been carried out as planned. What this entails, however, is not specified, leaving room for interpretation regarding what constitutes as sufficient documentation.

A related concept to records is that of documents, which can be viewed as carriers of knowledge (Alavi & Leidner, 2001), or as records that have been further contextualised and formalised. While the terms "record" and "document" are often used interchangeably, in this thesis a record specifically refers to the information captured through the execution of a process. The act of creating a record is referred to as documenting.

In descriptions of information classification and ISMS, e.g. Beckers et al. (2014), Bergström et al. (2021), ISO/IEC 27002 (2022), and NIST (2018), records are emphasised as essential, reflecting the principle that "if it has not been documented, it has not been done." However, these sources provide little guidance on what to document beyond the final classification level. While the classification level is an important output, the reasoning and discussions underlying the decision are equally critical. Without documentation of this reasoning, transparency is lost, making it difficult to understand or revisit previous decisions. This lack of traceability has also been noted in ISRM, where Tehler (2023) observe that earlier decisions are often accepted as truths despite limited justification or reasoning. Similarly, Beckers et al. (2014) emphasise that documentation is vital both for enabling other security experts to follow the reasoning behind decisions and for facilitating ISMS audits.

Accordingly, documentation should not only state the classification result but also make explicit how and on what basis the decision was made. This idea is reflected in the model proposed by Bergström et al. (2021), where each process activity produces a record of its output, highlighted in red in Figure 2. These records are intended to inform subsequent classification decisions. Yet, even in this model, there are no descriptions or explanations of what such records should contain.

This lack of guidance has practical implications. Participants in the classification workshops lack clarity on what it is that should be documented and how. The record

then risks becoming lacklustre, providing little to no transparency on how and why decisions were made. Supporting participants in classification workshops on what to document could increase the transparency of made decisions, the quality of the documentation, and the confidence of the classification results as input to the risk analysis.

### 2.3.7 Classification Terminology

Different explanations and guidelines use different terminology for information classification, and it is interchangeably referred to as information categorisation (see e.g., (Collard et al., 2017)), data classification (see e.g., (Everett, 2011)) and information (or asset) valuation (see e.g., (Fenz & Ekelhart, 2011) and (Tatar & Karabacak, 2012)). Although these terms often describe the same activity, the terminology used reflects slightly different emphases on the purpose and scope of the classification activity, which is discussed below.

For example, ISO/IEC 27002 (2022) uses the terminology of information classification, where its purpose is described as *ensuring the identification and understanding of the protection needs of information in accordance with its importance to the organisation*. In this definition, the focus is put on identifying and understanding protection needs based on how important the asset is to the organisation. This is commonly done, and recommended, to be from a consequence perspective using consequence categories, which are exemplified in ISO/IEC 27002 (2022).

Data classification is used in the works of e.g., Bradford et al. (2022), Everett (2011), Shivayogi (2025), Singh et al. (2018), and Tankard (2015). It is apparent, however, that those works describe what this thesis refers to as information classification. There is, however, a conceptual distinction to be made regarding the difference between data and information. Information has been referred to as organised data, or data with a provided context (see, for example, (Zins, 2007)). In other words, data can be viewed as the building blocks of information. Classifying data in a literal sense would imply classification at a lower level of granularity, without necessarily recognising the value that may emerge when data is aggregated and contextualised as information. In this thesis, the focus is therefore placed on information classification, as it captures the organisational and contextual aspects of how information is understood and valued.

The term categorisation is mainly used in the American public administration context (Collard et al., 2017), e.g., in FIPS (Federal Information Processing Standard) 199 (NIST, 2004) and the NIST RMF (NIST, 2018). The categorisation process is described and explained in a manner similar to information classification, and can, as such, be seen as another synonym.

Information valuation is sometimes presented as a synonym for information classification. Valuation can be understood as the importance, worth, or usefulness of something (Collard et al., 2017). While information classification does involve identifying value, it approaches information assets primarily from a consequence perspective, essentially asking: “What would the consequence be if this information were lost, compromised, or made unavailable?” If the classification were instead

approached from the perspective of identifying the value or value creation of the asset, the question would instead be: "How valuable is this information asset to the organisation, and what value creation does it provide?"

Another related concept is security classification (Eloff et al., 1996). While information classification refers to the process of assessing value and consequences to determine protection needs, security classification usually refers to the outcome of that process: the label or category assigned to the information. In governmental and military contexts, this typically takes the form of predefined levels such as confidential, secret, or top secret (Quist, 1993). The purpose of such labels is to regulate handling and access according to established rules. While security classification and information classification are closely connected, this thesis investigates information classification as a process and its activities, rather than focusing on its potential results.

As showcased in the section above, there is no single term that is consistently used for what this thesis refers to as information classification. However, this thesis draws from a theoretical base of information classification, data classification, information (asset) valuation, and information categorisation literature, but it uses the term "information classification" inclusively.

This chapter explains how the purpose of this thesis was achieved by presenting the positionality of the researcher behind the thesis, including the ontological and epistemological stances taken. Following, the research approach and methods used are explained. The chapter closes with the researcher's reflections on the choices made.

### 3.1 Positionality

Positionality describes an individual's world-view and the position adopted about a research task and its context, i.e., 'where the researcher is coming from' based on ontological (the beliefs about the nature of social reality) and epistemological (the beliefs about knowledge creation) assumptions (Furlong & Marsh, 2010; Orlikowski & Baroudi, 1991; Thapa & Haj-Bolouri, 2023). For the sake of transparency, some assumptions and underlying stances taken in this work are explained in the sections below.

In the context of information systems, where this thesis is written, two general epistemological categories are often discussed: positivism and interpretivism (Silverman, 1998). A positivist view assumes that knowledge is objective and can be verified and observed scientifically through logical or mathematical proof, often using quantitative research methods (Crotty, 1998; Thapa & Haj-Bolouri, 2023). Interpretivism, on the other hand, assumes that knowledge is socially constructed, meaning that the interpretation of knowledge depends on the context through which the knowledge was constructed, often using qualitative research methods (Walsham, 1995). In relation to this work, the user perspective, being the perspective of classification workshop participants, was considered important to investigate. Both to understand the needs and challenges of the information classification process and its activities, but also to understand how the classification workshop participants, who conduct the process of classification, can be supported. Focusing on those participants and the process of information classification can be seen in previous work, such as in Everett (2011, p. 22), where information classification is described as: "*...very much a people and process problem*". As such, given the classification workshop participant focus and need to understand their perspectives in-depth, this research is interpretative.

Interpretative research focuses on understanding a phenomenon by including the perspectives of individuals and their contexts (Maxwell, 2013). A phenomenon can be defined as "*... any problem, issue, or topic that is chosen as the subject of an investigation*." (Van de Ven, 2016, p. 150). A phenomenon can be very significant to some, and ignored by others, meaning it is important to choose and understand whose perspective is of importance for an investigation. In the case of this thesis,

the phenomenon being researched is the information classification process, as it is explained in section 2.3.4. The perspectives viewed as important are those of users conducting information classification, both from a participant's and a manager's point of view.

Concerning ontology, there are two main branches of belief: relativism and realism (Guba, Lincoln, et al., 1994). In realism, it is believed that the world exists independently of humans and is out there to be discovered. Relativism, in contrast, holds that reality is socially constructed and depends on the perspectives and experiences of individuals and groups (Baghranian & Coliva, 2019). Among qualitative researchers, the more common belief is relativism (Stake, 1995). In the context of this work, information classification is not viewed as an objective process but as one that takes shape through the interactions, interpretations, and practices of those involved. What information is considered critical or valuable, therefore, varies depending on organisational context, roles participating in the workshop, and their individual experiences. The research has, as such, investigated individuals and their views on what information classification is and how it is conducted. It does not attempt to find a one true value of specific information assets, as the belief is that there is no such thing, it is instead viewed to be relative.

There is also something to be said about the approach to reasoning used. In information systems, there are three general approaches to reasoning: inductive, deductive and abductive. Inductive reasoning involves deriving patterns and insights from empirical material, whereas deductive reasoning begins with predefined theoretical assumptions that are then tested against data (Azungah, 2018; Braun & Clarke, 2006). Abductive reasoning combines these approaches through iterative movement between empirical observations and theoretical interpretation (Dubois & Gadde, 2002). In the case of this thesis, the research has primarily followed an inductive reasoning approach. The empirical material was analysed without predefined hypotheses, and patterns related to prerequisites, challenges, and support for information classification were identified from the data. The focus has been on understanding how information classification is carried out and experienced in organisational contexts. At later stages of the research process, theoretical perspectives, such as multi-level planning, were used to structure and interpret the findings. However, in Paper E, the data analysis and thematisation were guided by an existing model, and were therefore deductive in nature. This is further elaborated in Section 3.4.

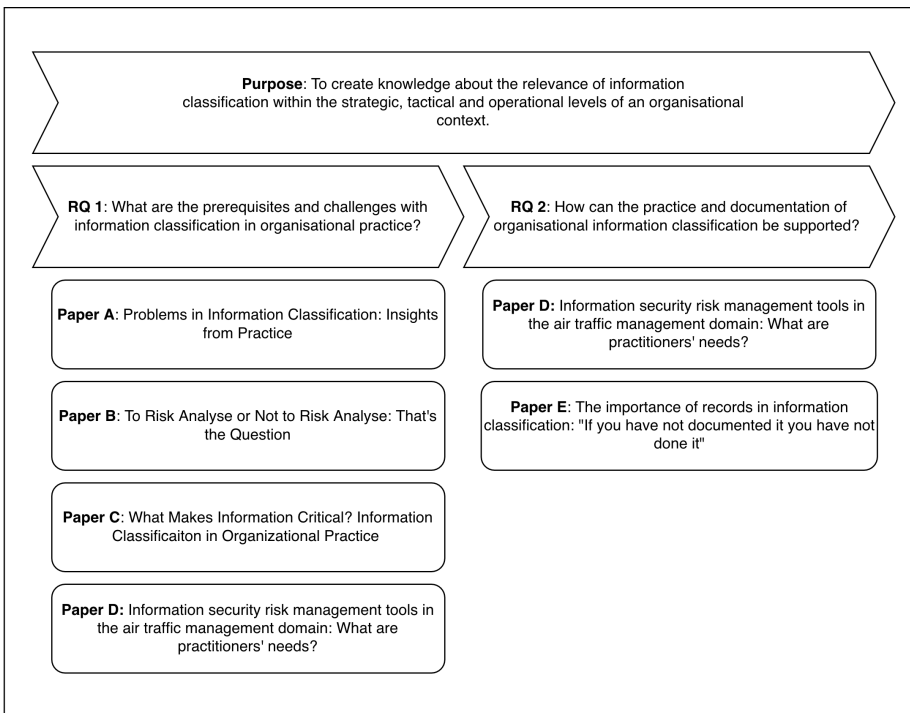
Lastly, this thesis used a qualitative research approach. This was deemed fitting, given that qualitative methods are more appropriate when it is important to understand phenomena from a participant's view and to gain a deeper understanding of a phenomenon (Goundar, 2012; Maxwell, 2013).

## 3.2 Research Process

The thesis consists of five appended papers, each investigating aspects of information classification and information security risk management within organisational contexts. While the individual studies differ in scope and setting, they are connected

through the overall thesis purpose and the two research questions. Together, they represent an iterative research process that developed from exploratory investigations towards more focused analyses of support and documentation practices.

Papers A–C primarily address RQ1 by identifying and analysing prerequisites and challenges associated with information classification in organisational practice. Papers D and E primarily contribute to RQ2 by examining how information classification can be supported, both through tool assistance and improved documentation practices. Figure 4 illustrates the relationship between the thesis purpose, the research questions, and the appended papers, and how the research progressed over time. Note that Paper D is included twice, one time below each research question, as it played a part in both.



**Figure 4:** The Relationship Between the Thesis Purpose, Research Questions and Included Papers

The following sections describe the focus of each paper and outline why the study was conducted as well as its place in the research process. Further explanations on how certain methods were used can be found later in this chapter. A more thorough summary of the appended papers and their main contributions can be found in Section 4.1.

**Paper A** served as the foundation for the thesis and the overall research process by identifying problems in the information classification process reported in previous

literature. These problems were first identified through a review of the literature, and through semi-structured interviews, the identified problems were confirmed to remain in organisational practice, and the study provided additional empirical evidence on those problems and the information classification process as a whole. As the starting point of the research, the study was exploratory in nature, allowing me as a researcher to develop an initial understanding of both the foundational literature in the field of classification and the practical challenges that respondents perceive as significant. The paper uses empirical material gathered with semi-structured interviews in both a private and public sector setting, which allowed for a wider perspective than would have been possible by using only one of the two. Verifying that the identified problems still exist in practice was considered essential for the thesis work, as it provided a basis for continuing the research. It also furthered my personal understanding of how the classification process is conducted in practice.

**Paper B** investigated how risk analysis is carried out in practice compared to standardisation frameworks. In this study the information security method support created by MSB (2021) was used as the framework for analysis. The method support is based on the ISO 27000-series. The study used semi-structured interviews with respondents that had managerial positions tied to information security work in Swedish public sector organisations. While the focus was on risk analysis, a lot of the discussions in the interviews revolved around information classification, which in this thesis is seen as a prerequisite for risk analysis. A discussion on this is expanded upon in section 4.2. For the research process, this paper was an important piece in understanding that information classification has a tendency to turn into a risk analysis, and that the two concepts are easily mixed up.

**Paper C** investigated the practice of information classification in practice and aimed to further understand how the process is carried out. The reason for this is that there is limited empirical research on information classification (Bergquist et al., 2021; Bergström et al., 2021). The study targeted considerations classification workshop participants take into account when making classification decisions, as well as the prerequisites for the classification activity. The empirical base was solely a private sector consultancy firm that mainly consults IT and security services to public sector organisations. This was considered an interesting perspective, given that the consultants mostly assist classification workshop participants with little experience in classification, who in turn require more support. In this paper, it became apparent that just as in Paper B, the classification activity becomes part of the risk analysis. It also provided empirical evidence of prerequisites with classification.

Together **Papers A–C** represent a more exploratory phase of the research. These studies were designed to build a broad understanding of the information classification process and its challenges from different organisational settings and perspectives. The diversity of contexts, spanning both public and private sectors, was considered an advantage in developing an understanding of how the process is carried out in practice, although it also meant that less emphasis was placed on the specific organisational context in any single case. As the research progressed, my focus gradually shifted from understanding classification and confirming challenges to examining specific aspects of the classification process and how it can be supported.

This transition marked a move from an exploratory to a more analytical phase of the research, where the aim was to deepen the understanding and address the need for support identified in earlier literature. This was the main purpose of papers D and E.

**Paper D** investigated practitioner needs for information security risk management tools, with a particular focus on how such tools can assist and support users in conducting activities such as information classification and risk analysis. The study was conducted within the air traffic management domain, where respondents described both functional and practical needs for tool support in highly regulated environments. The research identified two overarching categories of needs: assistance, referring to functions that guide users in following procedures, and automation, referring to functions that simplify or perform repetitive tasks. Notably, in this paper, it was identified that automation is not something that users necessarily expect. They do, however, wish for guidance throughout the process and clear instructions on what to do in each step. This was particularly prevalent when discussing documentation, and acted as basis for further investigation.

**Paper E** built on the needs of documentation assistance identified in Paper D, and focused on what information should be documented during the information classification process. This was considered important to address, as there are no current guidelines for documentation in current information classification literature. The study examined what types of knowledge and decisions are created in classification activities, but which are often lost due to limited or inconsistent documentation. Empirical data were collected through semi-structured interviews with information security professionals across multiple Swedish public sector organisations, and later on complemented by an analysis of existing classification tools and templates. The study proposed a structured view of what should be recorded in the various steps of classification, such as rationale, roles, and relationships between assets, to preserve the contextual understanding that emerges during classification. Within the context of this thesis, this paper is of extra importance, as it extends the discussion from how classification is conducted to how it can be supported through documentation practices.

The above research process was developed iteratively, where insights from each study informed the next. This approach fits well within interpretive qualitative research (Klein & Myers, 1999; Walsham, 1995), where understanding grows gradually through the interaction between theoretical background and empirical findings. Rather than following a strict, predefined plan, the studies evolved over time as new perspectives and questions emerged. Further, the thesis work has investigated multiple different settings, such as Swedish public and private sector, and the air traffic management domain. In the context of this research, the inclusion of several empirical settings has been considered a strength. It provided an opportunity to view the research questions from different perspectives and organisational settings, which helped broaden the overall understanding of the prerequisites, challenges and support needs tied to information classification in practice. It could also be argued that this strengthens the transferability of the results, as recurring challenges across settings point to issues that go beyond a single organisational context. On the other

hand, the approach has meant that I have not been able to do a deep dive into one specific setting or perspective. The nature of the problems addressed in this thesis, however, benefits from including several viewpoints rather than focusing on one context alone. As such, the approach taken is viewed as a generally positive aspect of the research, contributing to a more comprehensive understanding of the information classification process.

### 3.3 Data Collection

The empirical data collected for this thesis has been gathered from both public- and private-sector organisations and has been of a qualitative nature, mainly through the use of semi-structured interviews. To validate the results of the research, sessions with expert panels, both in groups and individually, were held. Additionally, preliminary results of Paper B were presented at a risk-focused conference and the peer comments informed the developments of the published paper. Table 1 presents an overview of the empirical material collected as well as the analytical approach used in each paper and for the thesis. Papers A, B, C, and E draw on a shared empirical foundation based on data collected from Swedish public sector organisations, with each paper including additional data. Paper D is instead situated in the domain of Air Traffic Management (ATM) and is based on empirical data collected specifically within that context, thereby providing a complementary perspective to the other papers. In total, the thesis work draws on data gathered from 34 respondents, 14 tool demonstrations, and 6 qualitative validation sessions.

#### 3.3.1 Semi-Structured Interviews

In qualitative research, interviews are a recognised research method for gathering qualitative data that can be explored and interpreted in various ways (Denzin & Lincoln, 2011; Oates, 2006). The interviews conducted to gather data for this thesis were of a semi-structured nature, characterised by open-ended questions that allowed respondents to formulate answers freely (Kallio et al., 2016; Longhurst, 2003). This approach was deemed as fitting given the exploratory nature of the thesis work.

As preparation for the interviews, an interview guide was prepared that consisted of themes and questions related to the topic of each appended paper. Different interview guides were used for the different papers included in the thesis, however, they were all constructed in a similar manner. In general, however, there was no use of previous theoretical frameworks for the creation of the interview guides. Instead, the interview guides were informed by relevant literature and the identified purpose of each study, while remaining open-ended to allow respondents to describe their experiences in their own terms. The reason for this was that no study aimed to test predefined theoretical assumptions, but instead to explore, for example, how information classification is understood and conducted in organisational practice, or what type of tool support is needed from a practitioner perspective. Using an existing theory as the primary structure for the interview guides could have constrained the discussion and limited the emergence of different valuable perspectives. For example, in Paper A, a typical question asked was *How do you go about con-*

**Table 1:** Overview of Materials and Approaches Used in Appended Papers

<b>Part of Thesis</b>	<b>Empirical Material</b>	<b>Analytical approach</b>
Paper A	Review of literature mentioning information classification problems, and eight semi-structured interviews conducted in both the public and private sector.	Based on the review of literature, a categorisation was conducted, resulting in five identified problems that guided the empirical data collection and thematic analysis.
Paper B	Sixteen interviews (seventeen participants) with information security professionals in Swedish public sector organisations.	Thematic analysis using a two-cycle coding process to analyse how risk assessments are conducted in practice in relation to established frameworks.
Paper C	Four semi-structured interviews with information security consultants in a private sector organisation.	Thematic analysis to examine how classification is conducted, and how information is valued in practice.
Paper D	Seventeen interviews with information security professionals in the Air Traffic Management domain and five validation sessions (4 expert panels and a conference presentation).	Thematic analysis using a two-cycle coding process to identify practitioner needs. Validations were done by using expert review sessions.
Paper E	Seventeen interviews with information security professionals in Swedish public sector organisations; participation in tool demonstrations; validation session with 14 experts.	Thematic analysis using a two-cycle coding process guided by an existing model to identify documentation needs within classification, validation through an expert panel.
Thesis	Synthesised empirical material from Papers A–E.	Overarching thematic analysis to identify prerequisites, challenges and support for the classification process, and documentation of it. Later, a secondary analysis using the multi-level planning framework as an analytical lens to fulfil the thesis purpose.

*ducting the classification process?* and *Do you see any challenges with information classification?*. In Paper E, a typical question used was *In the classification process, what do you see as important to document, and why?*. Asking questions in this manner allowed respondents to freely explain their ideas and thoughts surrounding the topic, and if they were deemed interesting by the researcher, follow-up questions were asked in a similar manner to further investigate the topic. An example of an interview guide used was added as an appendix in Paper C, where it can be seen in full.

Regarding the recruitment of respondents, most were selected based on their professional involvement in information security and information classification. The focus was primarily on individuals working in senior information security roles within Swedish public sector organisations, such as "Chief Information Security Officer" and similar, as these roles are typically responsible for managing or overseeing classification and risk management activities. This was considered important in order to gain insights from respondents with both practical experience and organisational responsibility. In some cases, initial respondents facilitated contact with additional individuals who had more operational roles in classification workshops, who were also included. The potential respondents were identified through publicly available information, such as organisational websites and professional networks. In some cases, initial contacts led to further introductions with other potential respondents. Further, the number of interviews conducted in each study was not predetermined in advance. However, as interviews progressed, recurring patterns and themes began to emerge across respondents. When additional interviews no longer contributed new perspectives related to the research focus, the data collection was concluded, and saturation was deemed to have been reached. Given the professional population involved in information classification and risk management, the number of respondents was considered sufficient to capture the variation relevant to the research questions.

All interviews, except one, were recorded and later transcribed verbatim, i.e., word for word (Halcomb & Davidson, 2006). The interview that was not transcribed was the result of a corrupted file that could not be recovered; however, notes were taken during the interview and acted as empirical material in that case. Most interviews were conducted with only one researcher present. However, in several cases two researchers were present and asked questions and follow-up questions interchangeably.

Lastly, some actions were taken to adhere to the ethical guidelines associated with in-depth and semi-structured interviews, as explained by Allmark et al. (2009). Namely, starting the interviews with an introduction and explanation of the agenda for the day, how the collected data would be used, and that the respondents were free to leave or withdraw their participation at any time. Additionally, a question was asked to confirm whether the respondent had consented to the interview being recorded, both before and after the recording started, to ensure informed consent. Names and other identifying information, such as the name of the organisation where the respondent worked and the respondent's name, were removed from the interview transcripts and replaced with pseudonyms to ensure compliance with privacy and confidentiality. This was done according to the recommendations suggested by (Allmark et al., 2009).

### 3.3.2 Collected Documents

In the field of information security, and especially risk management, a substantial amount of conceptual knowledge can be found in established standards, such as ISO/IEC 27002 (2022), or NIST 800-37 (NIST, 2018). These frameworks often form the basis of organisations' strategic, tactical and operational security work, and are therefore important to consider when examining how classification and risk assessment are conducted in practice.

In Paper B, a document collection was carried out focusing on the method support provided through the website *Informationssakerhet.se*, created by the Swedish Civil Contingencies Agency (MSB) and several other Swedish government agencies (MSB, 2020b). The website aims to bridge the gap between ISO/IEC 27001 and organisations seeking to implement systematic information security practices. The method support is structured into four main phases, 1. Identify and analyse, 2. Design, 3. Use, and 4. follow up and improve, and includes extensive descriptive material as well as a toolbox containing templates for, for example, risk matrices and valuation matrices.

In the case of Paper B, the sections of the method support relevant to information classification and risk assessment were treated as empirical material. The contents of these phases and templates were reviewed and extracted in order to allow comparison between the prescribed method and how classification and risk assessment were described by interview respondents. The collected documents thus functioned as a reference framework against which organisational practice could be examined.

### 3.3.3 Observations

In Paper E, one of the main objectives was to understand how current tools enable documentation in information classification. To understand the current state of support connected to both ISRM and information classification, participating as an observer in tool demonstrations were used as a data collection method. This allowed for a general understanding of how tools can support ISRM and information classification in practice, but also how they support documentation in particular. The tools that were showcased were created with the intent of supporting organisations with a variety of tasks, mostly targeting governance, risk and compliance management. All sessions included a live walk-through of the tool being demonstrated by a presenter who showcased its use and features in real time. The demonstrations were not used to evaluate the tools in any way, and my role as a researcher was observational only, meaning I did not use the tools in any way. The selection of tools to observe was done in collaboration with a Swedish national interest group which focuses on risk analysis and closely related areas, the group consists of 22 members from academia and industry. To come up with a list of tools to select, the ENISA list of Risk Management tools (European Union Agency for Cybersecurity (ENISA), 2023) was used, supplemented with personal suggestions from members of the interest group.

The demonstrations were arranged by the interest group, which invited developers to showcase their tools and respond to questions. Each session followed a similar

format: first, a presentation and walk-through of the tool’s interface and functions, followed by an open question and answer session. The demonstrations provided an opportunity to examine the tools in greater detail and to ask questions such as “Practically, how does the tool support information classification?” and “How do you capture external requirements in practice?”. The latter aimed to explore what kinds of information existing tools targeted in terms of documentation. The demonstrations also offered rare access to proprietary tools that would otherwise have been difficult to review. Screenshots and descriptive notes were used to record which fields in each tool were used to represent information to be documented. The results of the tool demonstrations were used as input for the thematic analysis of Paper E.

### 3.3.4 Expert Panels

Research in the sphere of ISRM often lacks validation, however, it is recommended that it is done where possible (Fenz & Ekelhart, 2011; Silverman, 2015). Examples of methods on how to conduct validation are exemplified by returning your results to the initial respondents or using expert panels (Fenz & Ekelhart, 2011). In this thesis, the appended Papers D and E have had the results validated by the use of several expert panel sessions and at a professional risk-focused conference involving participants from both practice and academia.

It should be noted that expert panels are opinion-based; however, as one of the few ways to validate data in the ISRM sphere (Fenz & Ekelhart, 2011), they were deemed valuable for the research conducted. For Paper D, an initial validation was conducted with an expert panel consisting of 10 senior experts from the Swedish Civil Contingencies Agency (MSB), all of whom work with systematic information security. The panel session was divided into two parts. First, a presentation of the preliminary results was held, followed by a discussion of said results. The results of this initial validation were a re-categorisation of the preliminary results presented, which included changes in both categories and the developed themes. Following this, three expert panels were held, where the end results were presented and discussed. Two of the panels included participants from the larger initial panel, and the third panel included two participants from another government agency not involved in either data collection or validation. A final validation was then conducted by presenting the preliminary results at a risk-focused conference, which involved 20 people from different backgrounds. The latter validation sessions resulted in minor adjustments, primarily in the categorisation naming. The validation sessions included professionals from various organisations, both in the private and public sectors.

When validating the results of Paper E, an expert panel session was conducted, involving 14 information security experts in roles such as Chief Information Security Officer and Senior Information Security Consultant. The participants represented organisations from both the private and public sectors. This allowed for a broad variety of experiences and knowledge to provide feedback. The session began with a presentation of the purpose and the presentation of the results, followed by a Q&A. A typical question that was asked and discussed were: *"Do you think our results*

*could improve the classification work?"*. The session was then transcribed verbatim, and the audio recordings were deleted. More information on the validation sessions can how they were used can be found in Section 4.1.

### 3.4 Data Analysis

The empirical material was mainly gathered through semi-structured interviews, but was complemented by the collection of documents, observations from tool demonstrations, and validation sessions using expert panels. While the material varied across the appended papers, the overall analytical approach has been that of thematic analysis. The method of thematic analysis developed iteratively over the course of the research process, beginning with a more exploratory open coding approach and later adopting a more structured two-cycle coding procedure. In addition to the thematic coding of interview data, collected documents were analysed and integrated into the coding process, and validation sessions were treated as further data collection, based on the initial results of the studies where validation took place. The following sections describe how the analytical approaches were conducted.

#### 3.4.1 Thematic Analysis

For the initial work (Paper A), an open coding approach, as described in (Burnard, 1991), was used on both the identified literature and empirical material. This was deemed a fitting approach, given the exploratory nature of the study and early stages of the research, and the exploratory focus of the open-coding approach (Burnard, 1991). Initially, problems related to information classification were identified and a quote from the relevant article was extracted and connected to a problem category. This was done for all of the collected articles resulting in five problems. These problems later on guided the semi-structured interviews. The same open coding approach was used on the empirical material.

Following the initial study, the remaining work (Papers B to E) were analysed and coded using the recommendations from (Saldaña, 2021) where the use of a two-cycle coding process is emphasised. This change in method allowed for the remaining work to conduct more in-depth analyses. The transition from open coding to a two-cycle coding approach also reflects the overall development of the research project. In the early phase, the purpose was primarily exploratory, to identify problems and to build an understanding of avenues of research. As the work progressed and the understanding matured, the need for a more structured and iterative approach emerged. In Papers B, C and D an inductive approach to creating themes and categories from the data was used, meaning the themes were created based on relationships and patterns found in the empirical material. In Paper E, a deductive approach was used, where themes were based on the information classification method, as described in 2.3.4. More details on the analyses and thematisation can be found in either the paper summaries in 4.1, or read in full in the appendices section.

In general, the first coding cycle involved reading interview transcripts, identifying similarities and patterns, extracting relevant quotations, and developing initial codes

that were then grouped into categories. The second cycle consisted of iterative re-coding and re-categorisation, allowing for a deeper examination of the previously identified text segments and the development of higher-level themes composed of categories (Saldaña, 2021). This structural coding and categorisation approach is well suited for analysing data from semi-structured interviews (MacQueen et al., 2008; Saldaña, 2021). The coding work throughout all the studies was conducted using the word-processing functions of Microsoft Word.

### 3.4.2 Document Analysis

The documents collected from "Informationssäkerhet.se" were analysed as part of the thematic analysis conducted in Paper B. In line with the approach to document analysis described by Bowen (2009), the material was treated as empirical data and reviewed systematically rather than used only as background information. The relevant sections were coded using the same thematic structure applied to the interview material, following the themes of "how", "when", and "why".

The purpose of this analysis was to identify how information classification and risk assessment were described in the formal method support, and to compare these descriptions with how respondents explained their practical work. This allowed for a comparison between prescribed processes and organisational practice. In this way, the document analysis complemented the interview data and contributed to a broader understanding of how classification and risk assessment are framed and how it is actually carried out in practice.

### 3.4.3 Expert Panel Validations

As presented above, the work in Papers D and E was validated primarily through expert panels. The insights obtained from these sessions were incorporated directly into the thematic analysis. For Paper D, the initial panel discussion led to a re-categorisation of several preliminary results and the refinement of existing themes. Feedback from the subsequent panels was treated as additional empirical input, where the comments were transcribed, coded, and compared with the original data to confirm, adjust, or nuance the emerging categories.

In Paper E the panels reflections and suggestions were coded in the same way as the interview data, serving both as a means of confirming the relevance of the identified documentation items and as a way to highlight aspects that had been overlooked. In this way, the validation sessions were not only used to verify findings but also functioned as an analytical extension of the data, helping to strengthen the internal consistency and practical relevance of the results.

## 3.5 Thesis Analysis

As explained in section 3.4, each appended paper includes its own analyses, in addition to this, two overarching analyses aimed at fulfilling the research questions, as well as the overall purpose of the work been done. These analyses draw on the

empirical base across all included studies and re-analyses the findings to answer the research questions and purpose of this thesis.

The first thesis-level analysis began with a review of the results sections across all papers, as well as the underlying empirical material. Based on this material, a thematic analysis was conducted focusing on challenges and prerequisites related to information classification in organisational practice. To structure the analysis in relation to the first research question, two overarching themes were used: *Prerequisites for Information Classification* and *Challenges in Information Classification*. Within these overarching themes, subcategories were identified through open coding, as explained by (Burnard, 1991). These codes were later grouped and made into categories that were positioned in one of the overarching themes, in a similar approach that was used in Paper A, as explained in section 3.4. The results of this initial analysis are presented in Sections 4.2.1 and 4.2.2. Regarding the second research question, the results from Papers D and E, which focused on support, were directly used and are presented in Sections 4.3 and 4.4.

The second analysis aimed at interpreting the thesis results in relation to the overall purpose of the work. This thesis-level analysis is presented in Section 5 and aims *to create knowledge about the relevance of information classification within the strategic, tactical and operational levels of an organisational context*. The analysis draws on the synthesised results presented in chapter 4, including the identified prerequisites, challenges, and support related to information classification and documentation. To structure the analysis, the strategic, tactical, and operational planning levels presented in Figure 1, as well as the concepts of narrow and wide planning were used as an analytical framework.

Each identified prerequisite, challenge and support was investigated in relation to the strategic, tactical, and operational planning levels, as well as the concepts of narrow and wide planning, as they are explained in section 2.1. This examination was guided by a set of questions rather than by a fixed categorisation scheme. For each prerequisite, challenge and support, the analysis considered (1) at which planning level it would originate, and (2) at what or which level(s) it becomes visible in practice. This approach made it possible to reason about the role of each planning level in relation to information classification.

The analysis also considered the distinction between narrow and wide planning. Each prerequisite, challenge and support was therefore also analysed with regard to whether it could be addressed through preparatory planning, or whether it primarily emerged during execution. Throughout the analysis, several prerequisites and challenges were found to span multiple planning levels. Rather than treating this as an error, such overlap was interpreted as indicative of necessary collaboration and dependency between planning levels. The results of the analysis are presented in Section 5 of the thesis.

### 3.6 Research Reflections

From the beginning of my research process, the intent has been to advance the understanding of, and provide support for, the information classification process. To achieve this, the research was conducted using a qualitative and interpretive approach. One of the most well known frameworks for reflecting on interpretive research is that proposed by Klein and Myers (1999), who present seven key principles intended to support reflection on the conduct and interpretation of such studies.

Other approaches to reflection were also considered, such as the guidelines for qualitative research proposed by Lim (2025) and the quality assessment criteria presented by Mays and Pope (2000). While both provide useful guidance, Lim (2025) places greater emphasis on describing qualitative methods and their application, and Mays and Pope (2000) focuses primarily on evaluating the quality of qualitative research. In contrast, the seven principles proposed by Klein and Myers (1999) more explicitly address the reflective process itself, including contextualisation, interaction between researcher and participants, and the iterative development of understanding. The principles have also been used in other interpretive studies in the information security domain, such as (Paananen & Siponen, 2023) and (Hsu et al., 2014), which further support their suitability for this work. For these reasons, the framework proposed by Klein and Myers (1999) is used as a reflective lens in the following section to discuss how the principles are manifested in this thesis and how encountered challenges were handled.

*The fundamental principle of the hermeneutic circle* is described as a meta-principle, emphasising that human understanding develops through an iterative process in which the meaning of individual parts and the whole to which they belong are continuously interpreted in relation to one another. In this process, individual parts are first considered on their own, and are later reinterpreted in the light of a broader understanding formed by relating them to other parts and to the emerging whole. In this sense, the hermeneutic circle acts as the basis for rest of the principles.

As has been previously discussed and explained, this thesis consists of several individual parts in the form of its included studies. The data collected in these studies were individually interpreted at the time the studies were carried out, and as explained in section 3.5, have later been reinterpreted and analysed together in the writing of this thesis. There has also been an inherent reiteration in the papers when following the two-cycle coding process, as explained in section 3.4. Additionally, my understanding of the topics at hand had grown when re-visiting the individual studies in the analysis stages of this thesis, which allowed me to see new patterns and gain new insights.

*The principle of contextualisation* requires reflection on the social, organisational, and institutional context in which a phenomenon is studied, so that the reader can understand how the situation under investigation has emerged. Rather than treating practices as isolated or universal, this principle emphasises that meaning is shaped by the conditions in which it is produced, in other words, the research setting for the work.

In this thesis, information classification was examined from an organisational context point of view, meaning how information classification is conducted in an organisational context. The studies were conducted in different organisational contexts, as explained and discussed in 3.2, where it is mentioned that including several viewpoints is considered a strength in this study. However, focusing on only one context and going further in depth in that specific domain would have been interesting. In general, however, including different contexts has been considered as a strength of the work, and it could also be argued that it has increased the transferability of its contributions slightly.

*The principle of interaction between the researcher and the subjects* requires reflection on how the empirical material was socially constructed through interaction between the researcher(s) and the participants.

Throughout the thesis work, most of the empirical material was collected through semi-structured interviews, where interaction between the researcher and participants played a central role. The interviews were conducted as open dialogues, allowing participants to reflect on their experiences of information classification and to elaborate on issues they considered important. In my role as a researcher, I guided the dialogue to ensure that the topics relevant to the study were covered, asked follow-up questions when necessary, and encouraged participants to explain and clarify their reasoning.

In some interviews, one of my co-authors led parts of, or the entire interview, which allowed me to take on more of an observer role. Additionally, the empirical material was analysed not only by me, but also in collaboration with co-authors across the different studies (in Papers B, C, D, and E). This collaborative analysis provided additional perspectives and interpretations that would have been difficult to achieve individually. Furthermore, interviewing participants in a variety of organisational roles contributed to capturing various perspectives of the information classification process, which supports a more nuanced understanding.

*The principle of abstraction and generalisation* concerns how detailed, context-specific empirical findings are related to more abstract concepts that describe how people understand and act in organisational settings. In other words, rather than treating empirical observations as isolated or unique to a specific case, this principle emphasises the importance of interpreting such observations in relation to broader patterns, such as theories.

In this thesis, individual interview statements and observations were first analysed within their specific organisational contexts, as described in section 3.4, and later on related to more general concepts, as described in section 3.5. In the final analysis, the work moved beyond single cases and instead contributes to a more abstract understanding of how information classification is understood, enacted, and supported in organisational practice. In my work, I have tried to be transparent in my interpretations, both in the appended papers, but also in section 4 of this thesis, by including respondent quotes and explaining my interpretations of them. The aim of the interpretations is not to claim universal validity, but to provide conceptual insights that can inform the understanding of information classification in organi-

sational contexts, and to provide knowledge of how information classification can be understood from the perspectives of strategic, tactical and operational planning levels, as presented in chapter 6.

*The principle of dialogical reasoning* requires the researcher to confront his or her preconceptions that guide the original research design with the data that emerge through the research process, and make clear the philosophical underpinnings of the work.

In this work, the philosophical underpinnings and my personal positionality have been explained and discussed in section 3.1. There are, however, additional preconceptions that I, as a researcher, brought into the research process that had to be challenged and, in some cases, changed. One such preconception concerned my personal initial assumptions about what challenges would be most prominent in relation to information classification. At an early stage, I expected the primary challenges to relate to a lack of tool support and a corresponding need for artefacts to assist classification workshop participants in carrying out the classification process. While this expectation was partly confirmed, the empirical findings revealed challenges and prerequisites that were more closely tied to how information classification is understood as a concept and how its purpose is interpreted in organisational practice. In particular, I did not anticipate that issues related to the purpose of classification and its distinction from risk analysis would be as central as they turned out to be. And in many ways, I did not expect information classification to be a "people problem" in the manner that it is. This led to a reassessment of the initial focus and contributed to a broader understanding of information classification from several perspectives. Another example concerns documentation practices. At the outset of the research, missing or insufficient documentation was not identified as a central issue in information classification. However, findings from Paper D highlighted documentation as a recurring challenge and a key area where practitioners expressed a need for support. This empirical insight showcased a path I did not expect, which led to a more detailed investigation of documentation practices in Paper E.

*The principle of multiple interpretations* is explained to require sensitivity to possible differences in interpretations among the participants of the studies. In a sense this can be likened to witness accounts, in that multiple people might have seen the same thing, but their stories and experiences might be different.

In this thesis, multiple interpretations are reflected in the empirical material through the inclusion of participants from different organisational roles, such as information security specialists, system owners, chief information security officers and, and consultants. These actors sometimes described information classification in different ways, emphasising different aspects of the process depending on their responsibilities and experiences. The main difference was in the role they took in the classification workshops, for example, the more senior information security roles that had experience leading classification workshops often talked about difficulties in managing the workshops, and, for example, how important it is that everyone understands that purpose of classification, uses the same terminology and so on. Study respondents who instead had the role of a workshop participant instead spoke about issues such

as subjective judgments, and difficulties in deciding what granularity to classify information assets as, in other words, more practical and operational issues. However, rather than treating these differing views as inconsistencies or as a negative, the analysis considers them as complementary perspectives that together contribute to a richer understanding of information classification in practice. By including and analysing these multiple interpretations, the research highlights how classification is understood differently across organisational contexts and roles, and includes them to provide a more thorough understanding of the process as such.

Lastly, *The principle of suspicion* requires sensitivity to possible biases and is closely related to the previous *principle of multiple interpretations*.

Related to this principle, no apparent contradictions could be identified during the analysis of the studies. In a sense, it could be argued that some contradiction were encountered when respondents spoke of challenges, while others spoke of prerequisites, even if they talked about the same topic. However, this was not viewed as a contradiction as such, but instead looked at as a matter of perspective of the topic at hand.

### 3.6.1 Ethical Reflections

In a similar manner to how Klein and Myers (1999) propose seven principles for reflection on interpretive qualitative research, Orb et al. (2001) highlight a set of ethical principles intended to guide qualitative research practice. Although the examples discussed by Orb et al. (2001) are drawn from nursing research, the principles are applicable to qualitative research more broadly, and are a good fit for studies relying on interviews and interaction with participants. In particular, they emphasise the ethical principles of *autonomy*, *beneficence*, and *justice* as central to addressing ethical challenges in qualitative research.

*Autonomy* emphasises the importance of respecting participants' right to make informed and voluntary decisions about their participation in research, which was addressed by ensuring that participation in the study was voluntary and based on informed consent. All participants were informed about the purpose of the research, how the empirical material would be used, and their right to withdraw at any point without consequence: this is further explained in section 3.3.1, based on further ethical considerations explained by Allmark et al. (2009).

*Beneficence* concerns the researcher's responsibility to minimise potential harm for respondents. This principle was taken into consideration by replacing the names and any other identifying information that could reveal the identity of the participants in the transcripts with pseudonyms. In addition, the studies included in this thesis, and the thesis itself, include quotes from respondents whose names have been anonymised. This was deemed important both from a perspective of protecting respondents, but also to make assumptions and interpretations as transparent as possible.

*Justice* relates to fairness in the selection of participants and in how different perspectives are represented and interpreted in the research. Participants were included

based on their involvement in information classification and related practices, and efforts were made to include individuals from different organisational roles and contexts. By representing multiple perspectives and avoiding using a single viewpoint, the analysis aimed to provide a fair account of information classification practices in organisational settings from more than only, for example, a managerial perspective.

This chapter introduces and summarises the publications included in the thesis, outlining their original contributions. A total of five peer-reviewed articles, published in international conferences and journals, are presented. Following the summary of the papers, the thesis results are presented.

### 4.1 Summary of Appended Papers

#### **Paper A - Problems in information classification: insights from practice**

The aim of this paper was to identify and analyse recurring problems in information classification, both from a theoretical perspective and in light of empirical experiences from practice. The study identifies that although classification is a cornerstone of information security risk management, its human and organisational challenges have been relatively unexplored.

Building on previous literature and qualitative data from two organisations, one public sector organisation, and one public IT-consultancy firm, the paper categorises five central problems in information classification: (1) deciding on a level of granularity, (2) non-complete registry of assets, (3) actor subjectiveness, (4) discourse interpretation, and (5) difficult to adapt guidelines. These categories were first derived through open coding of previous literature, and then explored through semi-structured interviews with practitioners.

The findings show that deciding on the level of granularity is not only a technical matter but also tied to resource constraints and conflicting perspectives among actors, such as developers and information security specialists who often hold different perspectives of what level of granularity is needed. The challenge of non-complete asset registries was explained as especially important, since a requirement prior to classification is knowing what assets exist. However, keeping an up to date registry is considered to be very resource intensive. Actor subjectiveness was shown to cause lengthy discussions and sometimes “over-protection” of assets, but the study also suggests that when structured, subjectiveness can improve classification by broadening perspectives and promoting learning. The problem of discourse interpretation reflected barriers to communication across departments, often linked to jargon, vague terms, and inconsistent language use. Finally, adapting guidelines emerged as a difficult task, as standards such as ISO/IEC 27002 are intentionally generic, forcing organisations to balance between overly abstract and overly specific guidance.

The paper concludes that these problems highlight the importance of moving beyond technical considerations to also study the social and organisational dynamics of classification. Directions for further research are outlined, including investigating communicative practices around granularity decisions, exploring how different

roles maintain asset registries and its role in increasing interaction between actors, structuring subjectiveness as a positive resource, developing operative language for discourse across departments, and studying how guidelines can be better adapted to organisational contexts.

### **Paper B - To Risk Analyse, or Not to Risk Analyse: That's the Question**

The purpose of this paper was to explore how risk analysis is conducted in practice within Swedish public sector organisations, against the backdrop of existing standards and method support. While risk analysis is described in theory as a cornerstone of information security risk management (ISRM), the study responds to observations that it is not always performed systematically, raising the question of whether organisations rely more on compliance checklists and valuations rather than “classic” risk analysis.

The study combined semi-structured interviews with 17 senior security experts, document studies of ISO/IEC 27001, and an analysis of a swedish method support for information security (Informationssäkerhet.se) created with swedish public sector in mind. Using thematic analysis, the results are structured around three guiding questions: how, when, and why risk analysis is done.

The findings show that organisations often establish an organisational-wide risk profile but then omit, or reduce, risk analyses on individual systems or assets. Risk analysis is frequently conducted in a sporadic, trigger-based fashion (e.g., during system changes or migrations) rather than continuously, and is often performed at the system rather than the asset level. A recurring pattern is that classification results become a deciding factor on if to conduct the risk analysis at all, effectively reducing the latter to an implicit activity. I.e., the risk analysis is sometimes skipped because most of the work is done implicitly in the classification stage. The “how” theme also highlights the difficulty of translating generic standards into concrete practices, and the method support is sometimes ambiguous, resulting in confusion rather than clarity and assistance.

The “when” theme identified that there is no clear consensus on when risk analysis is done, it may be performed during major organisational reviews, at points of change, or only when deemed necessary by information security professionals. Different interpretations of the method support leave practitioners to rely heavily on experience, and some respondents expressed that since everything in ISO 27000 is risk-based, risk analysis itself could appear redundant if security controls are already mandated through classification or external requirements such as laws and regulations.

The “why” theme revealed differing rationales. Some respondents see risk analysis as very important for specifying security controls, while others claim that classification alone can justify selection of controls. Several informants admitted to bypassing formal risk analysis, relying instead on experience or regulatory compliance and making sure to follow laws (e.g., GDPR, NIS-2). This raises concerns that risk analysis is shifting away from its role as the central justification for security controls, towards becoming a complementary or even redundant activity in environments increasingly driven by compliance obligations.

The paper concludes that while risk analysis is widely recognised as necessary, it is not always conducted in the classical sense and practitioners do not always follow standards they claim to adhere to. Instead, organisations navigate between information classification, compliance requirements, and practical constraints dynamically. This raises questions about the future of risk analysis and whether it will remain a central activity for risk-based security or evolve into a supportive activity that fine-tunes security control selection already prescribed by regulations.

### **Paper C - What Makes Information Critical? Information Classification in organisational Practice.**

The purpose of this paper was to investigate how information classification is carried out in practice, given its foundational role in information security risk management, but with a limited amount of previous empirical studies. The paper explores how professionals identify, value, and classify information assets, and the role of trust, terminology, and organisational context in the classification process.

The study used semi-structured interviews with four professionals from a national consultancy firm active in the Swedish public sector, complemented by a small-scale experiment in which respondents classified information using two schemes while “thinking aloud.” The data was analysed thematically, resulting in three themes: identification and classification of assets, common criteria in practice, and security communication and trust.

The findings show that classification is not a purely formalised procedure but a collaborative and interpretive activity. The identification and classification of assets are made difficult by inconsistent terminology, varying levels of information granularity, and non-complete asset inventories. Respondents noted that classification schemes (e.g., high/medium/low or 1–5) often fail to capture organisational nuances, with terms such as confidentiality, integrity, and availability often rephrased or replaced with other words to make them understandable by client organisations. Instead of scales and matrices, practitioners preferred discussing scenarios, often worst-case, to make classification decisions. The study also highlights that successful classification requires heterogeneous teams representing different roles and perspectives, as individual experiences strongly influence how value and criticality are perceived.

A central theme emerging from the study is the importance of trust, both within teams and between organisations. Trust in colleagues and clients was described as essential for effective classification and decision-making, particularly in consultancy contexts where subcontractors handle sensitive client data. Trust was linked not only to people but also to the perceived accuracy and integrity of information itself. Building a common language and terminology was found to be an important means of fostering such trust.

The paper contributes empirical insights into the challenges of information classification in organisational practice and proposes a three-step approach: (1) Asset Identification, what information is used in the organisation and where is it located, (2) Asset Valuation, what information supports value creation in the organisation?, and (3) Asset Classification, What level of protection is demanded to ensure contin-

ued value creation? This perspective emphasises valuing information as an enabler of organisational processes and value-creation, rather than only considering its potential loss or compromise.

### **Paper D - Information security risk management tools in the air traffic management domain: what are practitioners' needs?**

The purpose of this paper was to investigate what practitioners in the Air Traffic Management (ATM) domain need from supporting tools for information security risk management (ISRM). While risk management is often described as the cornerstone of information security, implementing ISRM in practice remains difficult. Tool support, in the form of spreadsheets, templates, or dedicated software, has been developed to support ISRM, yet little research has examined what users actually require from such tools.

The study focused on the ATM domain because practitioners there use SecRAM, a method based on ISO/IEC 27005 that, unlike some other frameworks, does not provide dedicated tool support. Seventeen semi-structured interviews with ATM security practitioners were conducted, complemented by analysis of SecRAM documentation, and validated through five sessions involving 34 experts from multiple sectors. The data was analysed using a two-cycle coding approach, resulting in 18 categories, grouped under two overarching themes: automation and assistance.

The findings show that practitioners do not expect ISRM to be fully automated. Instead, they emphasise a need for tools that reduce repetitive work and support consistency. Under the automation theme, respondents highlighted efficiency (avoiding double-work such as copy-pasting, automating calculations, generating reports, and issuing reminders), accuracy (reducing human errors in input and risk scoring), and consistency (ensuring coherence across activities and automatically updating linked assessments). In particular, they ask for assistance with documentation practices tied to risk analysis and classification activities.

Under the assistance theme, practitioners requested more guidance and support to make ISRM manageable. Needs included learning resources (explanations for difficult steps in the method, examples, explanations for concepts), enhanced communication (standardised language within organisations and secure external sharing of results), access to external intelligence, and process guidance (clear workflows, overviews and explanations for each step of the process, documentation assistance). Importantly, respondents valued assistance in understanding concepts and the broader purpose of ISRM tasks, noting that current tools leave too much room for guesswork.

The study concludes that future ISRM tools must balance automation and assistance: automating repetitive, error-prone tasks while providing practitioners with guidance and explanations throughout the ISRM process to support decision-making. It challenges the idea that risk management should or could be fully automated, showing instead that practitioners value support that helps them understand and navigate the process.

**Paper E - The importance of records in information classification - "If you have not documented it, you have not done it"**

The purpose of this paper was to investigate what should be documented during the information classification process and how such documentation (records) can support information security risk management. While classification schemes and tools often capture classification levels, they rarely include the rationale behind decisions or contextual knowledge, leaving gaps that makes for more challenging reclassification, audits, and subsequent risk analysis.

The study applied a qualitative research design, combining 16 semi-structured interviews with information security professionals in managerial roles and observations of 14 tool demonstrations. The interviews provided insights into current documentation practices and practitioner expectations, while the tool observations revealed how documentation assistance is implemented in practice. A thematic analysis was conducted, guided by an existing ISO/IEC 27002-based information classification method.

The findings are structured into three phases: business process/system analysis, requirements, and classification results, following the 3 first parts of the information classification method (as explained in 2.3.6). In the first phase, respondents highlighted the importance of recording asset descriptions, usage, location, flows of information, responsible roles, and connections to business processes. Tools added further items such as stakeholders, external recipients, and purposes. In the requirements phase, both internal (e.g., policies, disaster recovery plans) and external requirements (e.g., GDPR, NIS-2, sector-specific laws) were identified as important documentation elements. In the classification results phase, practitioners emphasised not only recording the assigned classification level but also the decision rationale. Such records create what respondents called a "collective memory," supporting transparency, enabling further understanding once information assets are to be reclassified.

The study concludes that documenting only classification results, i.e., a number or a level, is insufficient. Instead, contextual knowledge and decision rationale and more should be considered to capture. The paper contributes by outlining a structured overview of what to consider recording across classification activities, and in doing so, provides procedural guidance currently missing. Beyond supporting reclassification and risk analysis, the findings suggest that classification workshops themselves are valuable for raising awareness and producing organisational knowledge. Thus, the act of documenting could be as important as the records produced.

## 4.2 Thesis Results

The appended papers address different aspects of information classification. Together, they provide a coherent picture of different prerequisites and challenges connected to organisational practice as a result of the initial analysis, as explained in section 3.5, and how classification workshop participants can be supported in the process. This section synthesises the results across the five studies in relation to the research questions of the thesis. A summarising table of the prerequisites and challenges can be found at the end of their corresponding subsection in Table 2 and 3.

### 4.2.1 Prerequisites in Information Classification

For the information classification process to be effective, certain prerequisites need to be in place. Some are technical in nature, such as having a complete asset registry and an overview of the organisation's processes or systems, more examples of such prerequisites are mentioned in chapter 2.3. While these types of prerequisites are essential for the work to take place at all, others are more closely tied to the organisation itself and to the participants involved in a classification workshop.

The results show that one of the main prerequisites for meaningful information classification is a comprehensive *understanding of organisational value-creation*. Such understanding includes the organisations' processes and how identified information assets create value within their specific context. Without understanding how and why the organisation creates value, assessing the values of an asset becomes difficult at best. However, no single individual possesses sufficient insight into all parts of an organisation to perform classification independently, it is therefore regularly recommended as a collaborative workshop activity, both in existing literature and based on the evidence obtained in the research for this thesis. Consequently, another prerequisite is to include *heterogeneous teams* in the classification process.

Including a *heterogeneous team* with representatives from different departments and roles allows for a broader and deeper understanding of the value of an asset. The formal responsibilities and personal experiences of the workshop participants shape how the value of information assets is perceived. Such experiences include how participants reason about and interpret the organisation's core values, as well as how they perceive the role of information assets in creating value across organisational processes. In other words, the participants will have subjective opinions on asset values based on their experiences. It should be stated, however, that while subjective judgments are often viewed as a challenge and an issue, different subjective viewpoints are necessary to get an accurate classification, as is shown in the empirical evidence from the studies in this thesis.

Furthermore, for participants to contribute meaningful input to the classification process, they must *understand the purpose of classification*. This was exemplified by one respondent when discussing how workshop participants understand the classification process:

*"If you are a system administrator and enter a classification workshop... This [the classification] is nothing that people I meet think about all the time. So, a lot of what I do also involves explaining why I do things and why I use the terms that I am using" - Senior Information Security Consultant (Paper C)*

*Understanding the purpose of classification* is viewed as a challenging but important prerequisite. Workshop participants usually do not reflect on information asset value in day-to-day activities, and it is, as such, considered important for them to understand why and how to do so. Further reasons for why understanding the purpose of classification matters is mentioned and exemplified by another respondent, who discussed the choice of granularity in classification workshops:

*"Developers for example, they bring a database model and start to classify each row with an extreme amount of detail with timestamps etc. It is not necessary to be at that level; you have to think about it logically - Information Security Specialist (Paper A)"*

Another prerequisite that emerged from the studies is the need for a *shared terminology*. Information classification relies on language and interpretations, and participants must agree on the meaning of key terms such as "information asset," "value," and "consequence." Without such shared understanding, discussions in classification workshops risk becoming confusing, as participants interpret the same words differently depending on their backgrounds or professional roles. One respondent provided the following example of how this might affect a classification:

*When I arrive at a new customer and mention the term document, it can mean a Word document for one person, a collection of 40 appendices and one missive for another, and for a third person, it could simply be a paper. It is very important that you agree on the meaning of certain terms - Business Developer (Paper C)*

Establishing a common vocabulary ensures that participants are aligned in their understanding and can focus on the classification task rather than negotiating definitions. This was also suggested as a way to build trust between participants when starting a classification workshop.

Closely related to shared terminology is the need to understand classification levels used in the classification process. The process requires participants to estimate the potential impacts should an information asset be compromised or made unavailable. When consequence levels are interpreted differently by participants, the resulting classifications become inconsistent and difficult to compare across the organisation. Clarifying and discussing these levels before or during workshops helps create a shared frame of reference, allowing for more coherent outcomes.

A further organisational prerequisite is *trust between colleagues*. Classification workshops depend on open dialogue and the exchange of perspectives between participants with different expertise. For the classification work to be productive, participants must trust that their contributions will be valued and that other participants do what they are expected to do. Without trust, discussions risk becoming superfi-

cial or dominated by a few confident voices. A builder of trust is suggested to be a discussion around shared terminology, this is further discussed in Paper C

Finally, the results show the importance of having *adequate tools and process support*. Tools such as classification matrices, templates and physical or digital tools can guide participants through the process and help, for example, with what to document. The use of tools could not only make the process more consistent but also, guide and provide information to participants in an attempt to ensure that the knowledge created during workshops is preserved for future use. Such support could provide a link between strategic goals and operational execution.

**Table 2:** Prerequisites Identified in Papers A - E

Prerequisite	Description	Source paper
Understanding of organisational value-creation	Understanding the organisation, its context and how it creates value is important to understand how information assets provide value	B, C
Heterogeneous teams	Include workshop participants from different areas of the organisation to get several perspectives and an in depth understanding of information assets	A, B, C
Understand the purpose of classification	Workshop participants must understand the purpose of the information classification, and its unique way of thinking.	A, C
Shared Terminology	A shared understanding of key terms (e.g., <i>asset</i> , <i>value</i> , <i>confidentiality</i> ) is needed to avoid confusion and misinterpretation during classification activities	A, C, D
Understand classification levels	Being able to differentiate between classification levels is viewed as important, but also difficult to achieve.	A, C
Trust between colleagues	Trust eases and streamlines inter-organisational cooperation between participants, including in classification work.	A, C
Adequate tool and process support	The use of tools can support participants in the classification process by, for example, guiding them through the steps and providing information.	A, D

### 4.2.2 Challenges in Information Classification

While several prerequisites for effective information classification were identified, the results also reveal a set of challenges connected to the classification process.

The results further show that *deciding on a level of granularity* is viewed to be a main challenge, in other words, choosing a level of detail for classification. Such as classifying a whole process or database, a low level of granularity, compared to for example single files in a database, being a high level of granularity. This was indicated by one respondent who was interviewed in Paper A, who explained that while including users of information assets in the classification workshops is an overall net positive, it can be difficult for them to understand different levels of granularity. The same respondent brought up developers as an example, who typically use a very high level of granularity when deciding on what to classify, and they typically have a difficult time understanding the purpose of using a lower level of detail. In part, this would connect to the developers not having a clear understanding of the purpose of the process, as presented in the above section. However, it could also be a result of them being too close to the information source. In general however, choosing a level of detail to classify is shown to be contextual, and difficult.

As explained in 2.3, a prerequisite for the classification to take place is to know what assets the organisation owns, however, doing so was shown to be challenging. Keeping an up-to-date registry of assets was, in Paper A, explained to be the first step in setting up the classification process. As such, having a *non-complete registry of assets* is a hindrance. One respondent in Paper A explained:

*"First of all, it is important to value the information, but the first step is to make an inventory! Often times the inventory is not very well done, and that complicates things. All of a sudden, there is data you had no idea existed [...]" - Business Developer (Paper A)*

The same respondent further explained that it is very difficult to classify or value something you do not yet know exists, and that keeping an up-to-date registry is something that is often not done.

When participants value information assets, they do so based on their own experiences and perspectives, referred to here as *actor subjectiveness*. This can be challenging, as different participants may assign different levels of value to the same asset, which can lead to lengthy discussions and disagreements. To avoid underestimating an asset, participants often choose to over-classify it, which in turn increases the cost and amount of work needed to protect the information. Some organisations have tried to reduce this challenge by developing internal tools that assist in classifying certain types of assets. However, such tools are limited in scope and cannot be applied to all assets, nor do they solve all disagreements. In some cases, these discussions stem from internal misunderstandings caused by differences in terminology and how participants interpret key terms during the workshop.

The case of such misunderstandings can be understood as a challenge connected to *discourse interpretation*. In other words, participants interpret each other differently

depending on their familiarity with jargon, the wording used, and sometimes a lack of understanding of the organisational context. This challenge was mainly described as occurring between departments.

*"Communication between departments is difficult, especially when you use the same terms but mean different things. There is confusion in the terms used. This information is secret, is it secret or very secret? You have to understand the differences. It can be the result of a cultural, competence or an 'in a hurry' barrier." – Object Owner (Paper A)*

In essence, this problem is grounded in the use of different terms and expressions during information classification workshops, where words and categories often mean different things to different parts of the organisation. This causes confusion and frustration among participants, making it harder to reach consensus on classification decisions. It can therefore be seen as a communication challenge that is not unique to classification, but that becomes particularly visible and consequential during the classification process.

Another challenge connected to communication is the *difficult to adapt guidelines* that exist related to information classification. Such guidelines target both the classification process as such, but also the tools and guiding documents, such as the classification matrix used during the process. In general, respondents explained that it is difficult to adapt best-practice guidelines. The reason for this is in part that the guidelines mostly include overarching descriptions and does not go into enough detail, and that the language used is often targeted towards subject experts. Several respondents exemplified this and connected it to both writing internal guidelines for classification, and creating classification schemes. It was exemplified that internal guidelines are written in a language that most employees do not use, one respondent explained:

*"In the world of public sector, we write regulations and guidelines in a way that is difficult to interpret and we use terms and phrases that normal persons simply does not use." - Information Security Specialist 2 (Paper A)*

The above respondent further explained that it is another communication problem, and that the interpretation of both internal and external guidelines is made even harder because they often use difficult phrasing. A similar problem is encountered when the organisations attempt to formulate descriptions for classification levels to use in the classification matrix.

As is mentioned in 2.3, the creation of a classification matrix can be difficult, especially when it comes to making *distinct differences between classification levels*. This was identified in the results, and is discussed in both Paper A and Paper C. It was shown that following guidelines and recommendations to create the classification schemes leads to generic and interpretable matrices. Respondents explain that while the classification matrices are good guiding tools, the terms used when explaining the consequence levels are important. One example brought up is how to distinguish between high monetary loss and very high monetary loss, and that it

is close to impossible to do unless there are more concrete explanations. Another example was distinguishing between limited and high value, and trying to translate it such value into the organisational classification model. Several respondents explain that it is very challenging to describe the classification levels in a clear enough manner so that most can understand their differences.

Lastly, *differentiating between risk analysis and information classification* is a recurring mention in Papers A, B and C. This is explained and discussed from mainly two perspectives. Firstly, when it comes to participants who are inexperienced with the classification process, a common way of introducing the concept is to use examples. Such examples are of a worst-case nature and are compared with one another to come up with a classification conclusion. However, in doing so, the activity becomes more of a risk analysis or assessment rather than a classification of information, meaning concepts such as risk and likelihood are included in the workshop, concepts that should be discussed in the upcoming risk analysis. Secondly, it was found to be common for the information classification to be the only step that decided what protective measures to apply to an information asset, skipping the step of risk analysis. Instead, protective measures were mapped to classification levels. It was explained that the risk analysis would be done implicitly, meaning the respondents worked with a risk-focused approach, and found a risk analysis workshop as unnecessary. This showcased a misunderstanding of the purpose of both information classification and risk analysis.

In summary, the results highlight several recurring challenges in the information classification process. Participants often struggle to determine an appropriate level of granularity and to maintain complete and up-to-date asset registries. Differences in individual experiences, referred to as actor subjectiveness, lead to inconsistent valuations and lengthy discussions. Communication issues such as differing terminology and interpretations, along with difficulties in adapting and understanding internal and external guidelines, further complicate the work. Finally, the boundary between information classification and risk analysis is frequently blurred, as the two activities are sometimes merged or used interchangeably.

**Table 3:** Challenges Identified Papers A - E

<b>Challenge</b>	<b>Description</b>	<b>Source paper</b>
Deciding on a level of granularity	It is difficult to decide on a level of detail to classify information assets	A, C
Non-complete registry of assets	Asset registries are often not complete, information assets are as a result missed or further work must be done to create an inventory	A, C
Actor subjectiveness	Experiences and individual understanding of workshop participants influence their understanding of asset value. This causes lengthy discussion and risk leading to non-linear classifications.	A, C
Discourse interpretation	Participants interpret each other, jargon, and terms used in different ways leading to misunderstandings.	A, D
Difficult to adapt guidelines	Guidelines are often written with subject experts in mind, and do not explain classification thoroughly nor in a way that beginners understand, leading to it being difficult to implement the classification process.	A, B, C, D
Distinct differences between classification levels	Classification matrices are often created with standards in mind and little customisation is made. This leads to very interpretable and non-distinguishable level explanations.	A, B, C
Differentiating between risk analysis and classification	The difference in purpose between information classification and risk analysis is generally not understood, leading to a mix of the two activities. Meaning risk is included in the classification and vice versa.	A, B, C

### 4.2.3 Supporting Information Security Risk Management and Information Classification

Building on the identified prerequisites and challenges related to information classification, it became clear that additional support is needed for the classification process. As discussed in Section 2.2, information classification provides a foundational input to ISRM, particularly in determining impact and serving as a direct input to risk analysis. Weaknesses in the classification process therefore have direct implications for the effectiveness of ISRM as a whole. For this reason, the need for support is not limited to the classification activity in isolation, but must be understood in relation to the broader ISRM process and the tools used to conduct it. This subsection therefore presents findings related to how ISRM can be supported, including the information classification process.

To understand how the information classification process could be supported, Paper D investigated practitioner needs in risk management tools. The results show that two general areas of support are desired: *automation* and *assistance*. *Automation* refers to tasks in which participants are automatically provided with an output from the tool, without requiring user input. Examples include generating reports or calculating risk scores. *Assistance*, on the other hand, refers to tasks in which users receive some form of guidance while using the tool, such as being provided with examples or explanations related to the task at hand. While Paper D focused on tool-based support, the results indicate that support is needed in these areas more broadly and is not limited to for example digital tool solutions. The findings that are most relevant for this thesis are summarised below, while a complete overview of all identified requirements can be found in Appended Paper D.

Regarding the first area of support, *automation*, respondents generally did not expect the risk management or information classification processes themselves to be automated. Instead, they argued that automation could be helpful in supporting the different activities included in these processes, especially so in the areas of *efficiency*, *accuracy* and *consistency*. Respondents indicated that automation could help address user errors by reducing repetitive input, calculating levels of risk, and generating reports, increasing *efficiency*. It was also suggested that overall *accuracy* and *consistency* between process steps could be improved by automatically transferring input from one stage to the next, thereby avoiding the need to repeat the same task. One example of this would be to automatically transfer the classification level of an asset into the risk analysis, which reduces the risk of incorrect or inconsistent information, increasing *consistency*.

Further examples included receiving automatic notifications when re-classification of an asset is due, and automatically gathering or generating values from the tool for reports. This was brought up to, again, reduce manual input. These examples were all motivated by respondents interest in saving time to put more focus on the analytical parts of classification and risk management, mentioned as the more valuable work. These suggestions target efficiency by avoiding repetitive work, accuracy by reducing user input (meaning less opportunity for error), and consistency by automatically importing previous inputs into upcoming activities where it is neces-

sary. As such, supporting classification through automation does not imply that the classification itself should be automated, but rather that some administrative steps surrounding it can be streamlined, and the administrative load could be lightened to allow more time and focus to be spent towards the decision-making.

The second area of support is *assistance*. While automation was described as a way to simplify administrative and repetitive tasks, assistance instead refers to functions that help and guide users during the process. Respondents described four main types of assistance: *learning resources*, *communication*, *external intelligence*, and *process guidance*. In terms of learning resources, respondents expressed a need for explanations of difficult steps and concepts to help participants understand how and why certain activities should be carried out. Examples included guidance on how to identify and value information assets, and explanations of information security concepts such as confidentiality. *Communication*-related assistance was described as support for using a standardised set of terminology and internal language to facilitate dialogue and ensure that all participants interpret terms in the same way, thereby avoiding confusion and misunderstandings. This was considered to be of extra importance when participants who were not as experienced in the field participated. In addition, using standardised terminology was suggested to faster allow less experienced participants to learn and understand the basics of classification and risk analysis.

*External intelligence* refers to a tool's ability to provide or import external knowledge, such as threat-intelligence information that can inform risk-related decisions, and have access to documentation from other projects. A main motivation for why this was deemed necessary is that the nature of information security is that it is ever changing. Based on this assessment, using only previous decisions and knowledge to make current decisions was deemed as inadequate, and complementing it with, for example threat-intelligence, would be helpful. Another example brought up was that other projects who have done the ISRM work already often had plenty of insights to use in the current project, and it was therefore deemed valuable to be able to access such documentation.

Lastly, *process guidance* was described as support that allows users to view information from different perspectives depending on their background, see where they are in the overall process (for instance, moving from information classification to risk analysis), and a wish for assistance in documentation. How the differences in perspective is to be realised was not mentioned, however, it was explained to be a wished for feature. Where the participants were in the overall process was explained to be a tool feature currently missing, sometimes leading to confusion on what to do in the current step, and what is to be done next.

Regarding documentation, respondents argued that it is important to be able to track previous assumptions made over time, to include reasoning and rationale of those decisions, and to keep the documentation easily accessible when re-visiting classification or risk analysis decisions. Being able to see previous decisions was mentioned to be important, as it could provide further perspectives for the current work.

As described in the above section, there are plenty of opportunities to develop support for ISRM and information classification. The final results section of this thesis will focus on what to include in the documentation practices connected to information classification. Providing such support was found to be a need from a participant perspective in Paper D, and to be an unaddressed part of the existing information classification method description outlined in chapter 2.3.

#### 4.2.4 Records in Information Classification

A main result of the information classification process is, naturally, the classification level, which indicates the protection needs and value of an information asset. However, much of the value of the process lies in the discussions that take place during workshops and in the effort to understand how the asset is of value. While the classification level is important, it represents only a simplified outcome of the process and does not capture the reasoning behind decisions made. Documenting this rationale, the arguments made, and other relevant information should therefore also be viewed as results of the classification process. In practice, however, such knowledge is rarely documented and is often forgotten once the process is completed. Existing descriptions of information classification emphasise that a record should be created and updated throughout the process, yet they do not specify what that record should contain. This lack of clarity complicates the work further for participants in classification workshops, as there is little shared understanding of what to document. As such, without a structured approach to documentation, organisations risk losing valuable insights and the reasoning behind previous decisions, as highlighted in Papers C and D. To address this gap and better support the information classification process, Paper E explored what information classification records should include and proposes a framework identifying knowledge to be captured. A summary of what to include in a record in each process step can be found in tables 4, 5 and 6.

Records connected to the classification process can be seen in the previously presented Figure 2 in section 2.3.4, where the records can be seen as outlined in red connected to the different activities. Notably, Records are created in the process steps of (1) Business Process / System Analysis, (2) Requirements and (3) Classification of Information. In process step (4) Labelling, the classification levels are applied to an asset, meaning no new record is created. Lastly, in step (5) selection of final business process / system classification, uses the created record as input. As such, there is creation of a record in steps 1, 2 and 3, no creation in step 4, and use of the record in step 5. As such, the identified knowledge was identified and categorised according to step 1, 2 and 3.

Related to what to document when it comes to information classification, two key areas of knowledge were identified, contextual knowledge and procedural knowledge. Contextual knowledge, meaning knowledge about a situation in which a task or decision occurs, including its environment, can refer to who was involved, why a decision was made, and how it was reached within a particular organisational or situational context. An example of this in relation information classification was identified to be organisational members' understanding of asset values in specific organisations settings.

Procedural knowledge instead refers to knowledge about how to carry out a particular task, such as conducting a process or applying a framework. Such knowledge is often tacit, but can be made explicit in the use of, for example, tools, methods and models. An example of tacit knowledge being made explicit is the classification method used in this thesis, explained in Figure 2, outlining and explaining how to carry out the different steps of classification. To support the classification work it would as such be beneficial to provide procedural knowledge, targeting what to document. What is to be documented however, is viewed to be contextual knowledge. The contextual knowledge that is to be gathered are described according to process steps 1, 2 and 3 below.

### **Business process / System Analysis**

Overall, respondents were in agreement that creating the record itself as a valuable task, and argued that records enable organisational knowledge to be preserved. Further, conducting classification workshops allow for creating new knowledge to include in said records, and doing so is mentioned to increase the awareness among both employees and the organisation as a whole. It is also argued that documenting and creating records improves the end result of the classification, as they could revisit previous discussions. In the Business process / System analysis step, a variety of knowledge was deemed important to collect and document. Typically, the name of the identified asset and a description of it was mentioned as important pieces to include. Additionally, what business process the asset exists in relation to was mentioned as important. Including such knowledge allows for further understanding of why the information asset provides value. Another approach to this was to categorise the information asset into one the main value-creating processes of the organisation, in this case education, and to then put it into preset subcategories. Similarly, this was done to understand where and how the asset is used. Connected to such examples, respondents explained the need to know where the asset is located, such as in what system or in what secondary asset. Additionally, an owner of the information asset, a person responsible for the asset, and potential external recipients or stakeholders were mentioned as valuable examples of contextual knowledge to include in a record. A collection of the contextual knowledge identified, tied to the Business process / System analysis step is provided in Table 4.

**Table 4:** Contextual Knowledge in Business Process/System Analysis.

Contextual knowledge documented	Explanation
Asset name	A descriptive name of the asset.
Asset description	A description of the asset.
Business process	Which business process(es) the asset is relevant to.
Person/role responsible	A statement on who/what role is responsible for the asset.
Usage	A brief description of the intended use of the asset.
Information flows	A statement on how the asset moves in and between different systems in a process.
Location in secondary asset	Where, and in which system(s) the asset is located. Such as in a service or a storage solution.
Owner of the asset	The person or role who is the owner of the asset.
External recipient	A statement on the external recipient of the asset if applicable.
Stakeholders	Stakeholders of relevance affected by the asset.

## Requirements

Documenting both internal and external requirements is something that is seldom done, and in the cases where it is, it is mostly to note what laws and other contract-based requirements exist that would affect the classification. While understandable, requirements are important related to classification and will often affect the end result. One respondent explained that as soon as personally identifiable information is handled, it must be noted as that will affect the classification level. Further, different types of sector-specific regulations were brought up, such as archiving laws and regulations. It was explained that there are cases where information must be disposed of after a certain time, which was explained as important to include in the record, given that the respondent worked in a field where this would be actionable. Another external requirement was the IT Provider agreements, the reason for why this was deemed important is that often times their collaboration contracts will dictate how both organisations are allowed to handle, for example, personally identifiable information. In terms of internal requirements, items such as internal policies and information management plans were viewed as important to document. This was further reflected in the tool-demonstrations, where an example of an internal requirement to identify and record was the internal information management plan, as is shown in Table 5.

**Table 5:** Contextual Knowledge in Requirements - Internal and External  
Requirements are exemplified with indentations

Contextual knowledge documented	Explanation
<p><i>External requirements</i></p> <p>Privacy laws and regulations</p> <p>    NIS-2</p> <p>    GDPR</p> <p>    Public access to information</p> <p>Sector-specific laws and regulations</p> <p>    Patient data laws and regulations</p> <p>    Archiving laws and regulations</p> <p>    Archives act</p> <p>    Public records act</p> <p>IT Provider Agreements</p>	<p><i>Requirements from an external source</i></p> <p>National and/or international laws regulating privacy in some sense.</p> <p>EU law enforcing cybersecurity measures and incident reporting for essential and important service providers.</p> <p>EU regulation governing data protection and privacy, giving individuals control over their personal data.</p> <p>Laws and regulations regulating public access to official documents while protecting sensitive information.</p> <p>National and/or international laws and regulations regulating sector-specific requirements.</p> <p>Laws and regulations managing and protecting patient journal information, ensuring traceability and secure handling of patient data.</p> <p>National and international laws and regulations that dictate the retention and management of records.</p> <p>Dictates the preservation and management of public records for long-term archiving.</p> <p>Governs transparency and archiving of public documents to maintain public access.</p> <p>Statement on how the information asset can be handled in relation to external providers of IT services to the organisation. An example of this is service level agreements (SLAs).</p>
<p><i>Internal requirements</i></p> <p>Internal policies</p> <p>Disaster recovery plan</p>	<p><i>Requirements from an internal source</i></p> <p>Policies stemming from within the organisation, such as ones touching on organisational privacy, information security and data retention. An example affecting the classification could be, for example, certain access-control requirements to particular assets.</p> <p>Strategy for restoring systems and data after disruptions to ensure business continuity. This can affect, for example, storage requirements and in turn, the classification of identified assets.</p>

Continued on next page

Table 5 – continued from previous page

Contextual knowledge documented	Explanation
Information management plan	Internal guidelines on structuring, storing, and managing information efficiently. This can affect the classification level by, for example, limiting the use of certain identified assets.

### Classification of Information

As for the last record creating step, classification of information, few knowledge items to add were mentioned. Those that were mentioned however, are substantial. First, all respondents agreed that the classification level should be recorded as this is the main outcome of the process. Second, most respondents mentioned that the rationale for the classification decision should be included in the record. One respondent explained:

*"It's kind of about making sure there is room for justifications and, in a way, that you can demonstrate reflections — basically, reflections that occurred before defining a value in some way, right? That there is clarity, so you can go back to the classification documentation and see on what premises this decision was reached, even a year later." - Respondent 10 (Paper E)*

The same respondent further explained that reaching consensus in a classification workshop is as important as the actual classification level. Understanding how and why the group came to such consensus is information that is equally as important as the actual outcome, and should as such be recorded.

Other respondents pressed on the importance of the classification activity, and explained it to be the most important step. Not only is it opportunity for cross-departmental collaboration and a way of increasing the security awareness of the organisation, but it was also explained to be opportunity for participants to further understand what information they use in the organisational processes. Lastly, one respondent pressed on the need for documentation practices:

*"Yes, well, if you haven't documented it, you haven't done it. I mean, it's like this, we can sit here and talk as much as we want, but I mean... You might have a "picture" memory so you remember everything, but the third person who is participating does not, and if you leave the organisation then it [the rationale] no longer exists." - Respondent 13 (Paper E)*

The above respondent further explained that creating an organisational memory of why decisions were made, and the rationale and background to such decision, are important keep. Especially so in terms of re-classification, and for the sake of transparency.

**Table 6:** Contextual Knowledge in Classification Results.

<b>Contextual knowledge documented</b>	<b>Explanation</b>
Classification Level	The level of classification of the asset received from a confidentiality, integrity and availability perspective.
Rationale for classification decision	A summary statement on the rationale of the classification decision, i.e., on what grounds/basis the classification decisions were taken.

This chapter presents an analysis and discussion of the results introduced in Section 4. The discussion is structured around the strategic, tactical, and operational levels of organisational planning and the coordination and collaboration between them, as illustrated in Figure 1. Within this structure, the chapter first examines the identified prerequisites for information classification, followed by the challenges associated with conducting classification in practice, and finally the types of support considered necessary to strengthen both information classification and ISRM. These aspects are discussed across the three planning levels, while also considering the distinction between wide and narrow planning and the coordination between organisational levels.

Following, the chapter presents the theoretical and practical contributions of the work, and concludes with a discussion of limitations and directions for future research.

### 5.1 Levels of Planning

#### Strategic

At the strategic level, the role of organisational planning is to articulate the purpose, direction, and long-term intent of information classification. As explained in section 2.1, the strategic level concerns the why of organisational activities, establishing overarching objectives and aligning them with broader organisational goals. For information classification, this means defining why classification is necessary, what value it provides, and how it supports the organisation's overall information security ambitions. It should, however, not state how information classification is supposed to be conducted.

The analysis shows that several prerequisites (see Table 7) for effective classification are rooted at the strategic level, one of them being to *understand the purpose of classification*. This applies both to the participants in a classification workshop at an operational level and to the management and board, who operate at a strategic level. Although the strategic level does not determine who should participate in the process or how specific activities should be carried out, it does shape how the classification activity is framed within the organisation. This could be challenging for the classification as such, as if the board and senior management do not understand the purpose, or why classification is important, framing it and including it in the long-term goals of the organisation may be difficult. In addition, if the board has little or no insight into how the organisation creates value, the understanding cannot easily be translated into the lower operational levels, making effective classification difficult.

The strategic level also shapes the conditions that enable collaboration, particularly by fostering interpersonal and interdepartmental trust. While trust can manifest operationally during workshops between participants, the roots of trust often lie in organisational culture, which starts at the top (Nel & Drevin, 2019). If the organisation does not cultivate an environment in which actors feel confident sharing perspectives or challenging assumptions, the classification process risks becoming superficial or dominated by a small group of voices. As such, strategic leadership plays an important role in fostering an organisational culture where participants feel safe to share perspectives and challenge assumptions. Such an environment supports open dialogue and strengthens *trust between colleagues*, which in turn can improve the quality of classification discussions.

A challenge to consider is the *difficult to adapt guidelines* and translating them to organisational practice (Niemimaa & Niemimaa, 2017). Guidelines and standardisation documents often provide high-level frameworks that outline how activities and processes should be carried out (Tehler, 2023), but they must be tailored to the organisation's context, processes, and ways of working. This challenge can be viewed from both a strategic and a tactical perspective. Strategically, the organisation must decide which standards to adopt and how these align with its goals and values. Tactically, the difficulty would instead lie in interpreting the chosen standard and translating it into concrete practices. Therefore, while an operational problem might stem from the tactical level, the root cause may ultimately stem from strategic decisions about which standards to follow, which is considered to be the case when it comes to *difficult to adapt guidelines*.

Regarding support, the categories identified in Section 4 primarily concern enabling and carrying out classification in practice, and are therefore positioned at the tactical level in this analysis. Strategic planning instead contributes by providing direction and clarity about why information classification is carried out and what value it is expected to provide. This is not because support is unimportant at this level, but because the forms of support identified in the empirical material are primarily intended to assist the planning and execution of information classification at the tactical and operational level, rather than to shape its overarching purpose. The empirical material does not indicate that strategic planning is supported in the form of, for example, digital tools or process guidance, instead, its role is identified to provide direction and clarity regarding why information classification is carried out and what value it is expected to provide.

### **Tactical**

As explained in section 2.1, the tactical level is intended to translate the strategic directives into guidance that enable the organisation to conduct information classification in practice, or simply, to enable the operational level. This includes deciding on how the process should be carried out, what tools should be used, and how the organisation should interpret and apply standards and legal requirements. In other words, the tactical level translates the strategic directives and bridges them to the operational level. In classification, this would mean that each activity present in Figure 2 should be planned so that it can be carried out in the operational level.

A key prerequisite at this stage is the use of *heterogeneous teams*. There is some nuance to this however. While the strategic level might articulate the need for different perspectives in classification, it is the tactical level that would put this into action by identifying and exemplifying, for example, which roles, departments, and expertise areas should be represented in a classification workshop. This would likely include a mix of technical, financial, operational and security perspectives to ensure that the classification process benefits from a broad understanding of asset value. However, it is important to distinguish between the tactical and operational level related to this prerequisite, as the tactical level would not decide the individual to participate, but instead outline that the activity should include people from different departments. The operational level would then decide who to include based on their role.

In a similar sense, a *shared terminology* (Ekelhart et al., 2007; Wangen & Snekenes, 2013) should be addressed in a tactical manner by outlining and defining key terms related to, for example, the classification matrix (see Figure 3). Establishing a shared understanding of essential concepts will facilitate and enable the classification process. However, it is unrealistic to expect that all relevant terms can be predefined before the workshop. Therefore, fundamental terminology connected to security concepts and classification principles should be set at a tactical level, while additional terms that arise during the workshop should be addressed in the operational stage. This would require feedback from the operational level to the tactical one, which is further discussed in Section 5.2.

While establishing a *shared terminology* can support communication among workshop participants, they must also be able to distinguish between and *understand classification levels*. This is a tactical prerequisite, since the tactical layer should enable the operational layer by providing guidance for carrying out the classification process. Supplying tools such as a classification matrix aligns with this purpose. However, addressing this prerequisite is challenging, largely due to how classification levels are formulated within classification matrices. On the one hand, levels must be simple enough for all members of the organisation to recognise and differentiate. On the other hand, they must be formulated with enough specificity and complexity to support accurate classification. Achieving this balance is difficult, and thus, although understanding classification levels is an important prerequisite, it is simultaneously a significant challenge to formulate them. Suggestions on how to create a classification matrix for a specific setting can be found in, for example, Bergquist et al. (2021).

As a last prerequisite positioned at a tactical level is providing *adequate tool and process support* to carry out the classification activities. This prerequisite was mainly identified from users at the operational level, who mainly requested digital tools to support them throughout the process. Mainly, the arguments surrounding the guiding process support came from novice users who felt unsure of how to carry out both classification and risk management overall. Interestingly, there was little expectation to get help with the actual classification, but rather having a tool guide them through the process, with them being in charge of decisions. Accommodating this from a tactical perspective can prove to be valuable. In such a case, it would

likely be useful to cooperate with the operational level to more clearly identify user needs in the organisational context. It should also be mentioned, however, that tools and process support do not necessarily mean only digital tools. One example of tactical process support is Figure 2, which explains each step of the classification process and how it is to be carried out. Other tools, such as the classification matrix (Figure 3), are necessary for the classification process to be done at all and should also be constructed at the tactical level. Without these tools or means in place, it will be difficult to carry out the classification process.

Concerning tactical challenges, the most prevalent ones identified are *deciding on a level of granularity*, *difficult to adapt guidelines* and a *non-complete registry of assets*. Relating to the absence of a complete and up-to-date registry of information assets, this is viewed to be a tactical challenge that materialises mainly at the operational level, but which stems from a strategic one. From a strategic perspective, organisations are expected to articulate the importance of knowing and understanding their information assets through directives. At the tactical level, that intent must be translated into a process or tool that enables the identification and maintenance of an asset registry. When this tactical support is lacking or incomplete, the consequences become visible during the operational level, where classification workshop participants might struggle to determine what should be classified and at what granularity. In this sense, the absence of a complete asset registry showcases how operational difficulties in information classification can be traced to insufficient tactical preparation, shaped by earlier strategic priorities.

The challenge of *deciding on a level of granularity* influences how information classification is carried out in practice (Bergström et al., 2021). From a tactical perspective, organisations should therefore prepare for how different levels of granularity can be applied during classification workshops. This may include outlining what low- and high-granularity approaches entail, describing their implications, and providing examples of when each approach might be appropriate, as well as offering process support for both. In practice, however, the decision regarding granularity often emerges during the initial stages of a classification workshop at the operational level, and is not always a straightforward choice between high- or low-level approaches. As discussed in Section 2.3.3, a low-level approach is most commonly adopted, yet even when systems are used as the primary unit of classification, participants must still decide how information within those systems should be grouped or separated. This involves judgment about what information should be bundled into a single asset and what should be treated separately. Providing clear guidance for such decisions is difficult, as organisations differ in the types and combinations of information they handle, and choices regarding granularity are influenced by participants' understanding of the asset, its context, and its perceived criticality.

As the last challenge identified to be of a tactical nature is *difficult to adapt guidelines* (Bergström et al., 2021; Park et al., 2010). The intent is for the tactical level to create support for the operational level by translating standardisation and guideline documents that are to be used in the operational level. However, standards and guidelines are often intentionally generic to provide coverage for a wide variety of organisations, and, as such, translating general directives into often very specific or-

organisational circumstances is challenging. It should be noted, however, that it is an expected and necessary task. The challenge was shown to be true for both internal and external guidelines, especially in the Swedish public sector organisation interviewed in Paper A. Respondents mentioned that they are required to use a specific type of language when authoring internal guidelines and supporting documents that few people tend to understand, further complicating this step. In Paper A, several respondents also explained that existing internal documents contain matrices or definitions that are too vague, ultimately resulting in guesswork when determining a classification level. Although respondents acknowledged that an organisation cannot describe everything, they emphasised the need for clearer guidance and more accessible formulations. Both of these reflections point to the challenge of *difficult to adapt guidelines*, as not only a matter of translating standards into organisational practice, but it also relates to how guidelines are written, how terms are defined, and how examples are constructed.

In terms of support, both categories of *automation* and *assistance* are positioned at a tactical level. Automation is aimed at improving the *accuracy*, *consistency*, and *efficiency* of information classification. From a tactical perspective, *automation* can support mainly administrative tasks connected to the information classification process by reducing repetitive input if possible, in part generate reports and copy and paste data that has been input into a potential system used in the classification process. This is of course, dependent on what kind of tool the organisation is using, and in some cases, these supports might not be applicable. Further support could also provide automatic reminders for when reclassification is supposed to be done. Importantly, *automation* does not intend to automate the decision-making of information classification, but rather to reduce the administrative burden and free up more time for discussions and interpretation of value. Decisions regarding classification levels will, as such, continue to rely on the workshop participants and their interpretations of information asset value. How such support is to be designed or implemented into an organisation's current tools is not addressed in this research, however, such design belongs to the tactical level from a planning level perspective.

*Assistance* support, in contrast, targets understanding, learning, and communication, including *learning resources*, *process guidance*, *communication* support, and *access to external intelligence*. Learning resources and process guidance can support classification workshop participants, particularly novices, in understanding the purpose of classification, the steps involved in the process, and distinctions between, for example, classification and subsequent risk analysis. *Communication* could, for example, support by providing shared terminology or guidance where needed. Access to external intelligence, such as regulatory information or domain-specific knowledge, could further support participants in situating classification decisions. However, identifying this type of knowledge is part of the information classification process, and as such, it might have limited application. As with *automation*, *assistance* support is prepared at the tactical level but primarily materialises at the operational level, where the classification process is carried out.

Lastly, an example of *assistance* support was presented in Section 4.4: a structured approach to what should be documented and retained in the classification record, here referred to as *documentation support*. The *documentation support* is intended to be aligned with, or form part of, the *assistance* support, as participants in classification workshops can use the suggested structured approach to identify which contextual knowledge should be gathered. By doing so, more information is made available as a basis for the classification decision. In addition, documenting the recommended contextual knowledge is useful for future classification workshops. In subsequent iterations, participants can look back at previous decisions and understand on what premises they were made, rather than only seeing the outcome of a decision without any indication of why it was taken. This also enables reflection on whether conditions relevant to the classification have changed, or whether they remain unchanged, and it is therefore reasonable for the classification to remain as is. This reduces guesswork, as there is no need to investigate how or why previous decisions were made, and it also reduces reliance on the memory of individuals who participated in earlier iterations. As with the rest of the *assistance* support, it is positioned at a tactical level, as the support is decided upon and developed at that level, but used at an operational one.

### Operational

The operational level is where the classification process is carried out and where the activities can draw on preparations made in the tactical layer to enable valuable classification. As discussed above, some of the identified prerequisites and challenges will be revisited and discussed at the operational level. The reason is that while preparations are made at the levels above, the prerequisites and challenges sometimes materialise during the actual classification activity. As such, the operational level takes a classification workshop participant's perspective on the prerequisites, challenges, and support.

At the operational level, an important prerequisite to take into consideration is that classification workshop participants should have an *organisational understanding*. For classification to be valuable, participants should understand how information assets support organisational processes and organisational value creation, as this understanding shapes their assessment of each information asset's value. If that understanding is thorough, the opportunity for more precise classification is higher. This is, however, a difficult prerequisite to plan for, as it largely depends on the knowledge of individuals in the organisation. It is viewed to be an operational prerequisite as it is a requirement for a valuable classification. It could, however, partly be addressed at the tactical layer, where information about the prerequisite could be outlined in the process guidance.

Similar to participants having an *organisational understanding*, they must also *understand the purpose of information classification*. As explained in Section 4.2, if workshop participants do not understand the purpose of classification, the activity can easily turn into a risk analysis, where discussions begin to include concepts such as likelihood and threat. Avoiding this is important, as the purpose of classification is to assess the value of information assets, not to, for example, analyse the probabil-

ity of threats. In addition, including risk-related concepts implies that an asset only has value in situations where a threat or risk is present, which is not the intention of classification. Understanding that risk analysis follows later in the ISRM process is therefore important for classification workshop participants, as it frames how they approach the classification task before entering the workshop. This, however, was shown to be challenging in paper C. As such, mirroring this prerequisite is the challenge of *differentiating between risk analysis and classification*, positioned at both the strategic and operational planning levels.

A further prerequisite at the operational level is the use of *shared terminology* (Wangen & Snekenes, 2013). This prerequisite also appears at the tactical level, as part of the terminology can be prepared in advance through guiding documents and explanations of key concepts, such as confidentiality or information asset. Having a baseline of commonly understood terms is likely to improve communication during the workshop and reduce misunderstandings. However, it is not possible to define all terminology beforehand, and terms will inevitably arise during the workshop that participants interpret differently. When this occurs, it becomes necessary to discuss the meaning of such terms to ensure a shared understanding. Identifying when these differences exist is not always straightforward, which makes this an operational challenge in *discourse interpretation* as well as a prerequisite in *shared terminology*. While some preparation can support this, the operational level ultimately requires active clarification and negotiation of terminology as part of the workshop process. The challenges positioned at the operational level are *deciding on a level of granularity*, *actor subjectiveness*, *discourse interpretation*, *distinct differences between classification levels*, and *differentiating between risk analysis and classification*. Deciding on an appropriate level of granularity becomes an operational challenge because it is at this level that the decision is ultimately taken. As discussed earlier, at the tactical layer, even if tactical preparation outlines possible approaches, the actual decision depends on the specific context of the information asset, the knowledge participants bring to the workshop, and the resources available to conduct the classification. There is rarely a single correct answer, and the choice often reflects a negotiation between different perspectives and interpretations. An example of this is mentioned in Section 4.2, where a respondent mentioned that developers want a very high level of detail, given that they work very close to the information asset, while a manager is inclined to instead classify at a lower level. This makes granularity a recurring challenge during the operational execution of the classification process.

*Actor subjectiveness* is one of the most frequently mentioned challenges in the empirical material and previous literature, and it is an inherent part of information classification (Bergström et al., 2021; Kaarst-Brown & Thompson, 2009). It is positioned at the operational level because it is during the workshop that individual experiences, roles, and perspectives shape how participants assess the value of information assets. These subjective judgments become visible in discussions taking place, including the decision-making of a classification level, where they can lead to differing interpretations, lengthy discussions, or tendencies to over- or under-classify assets. As such, subjectiveness is not only an unavoidable aspect of classification

but also a central factor influencing how the process unfolds in practice. However, it is also a great part of why the classification process provides value. Without discussions based on subjectivity and different views on asset value, the resulting classification level would not be based on a nuanced understanding.

*Discourse interpretation*, or challenges in communicating (Ahmad et al., 2015), also emerges at the operational level. Even when terminology has been partly prepared at the tactical stage, as per the *shared terminology* prerequisite, workshop participants may still interpret words, categories, or examples differently depending on their professional backgrounds and organisational experiences. These differences often surface only during the workshop, when participants discuss assets or requirements and realise that the same term carries different meanings across departments. Such misunderstandings can lead to confusion, delays, or parallel conversations that must be clarified before the group can move forward. For this reason, *discourse interpretation* is positioned as an operational challenge. It emerges in the moment of interaction, and its impact is connected to how participants communicate, discuss and reach classification decisions.

A further operational challenge concerns the difficulty of *distinguishing between classification levels* during the workshop. Even when the organisation has prepared a classification matrix, participants still struggle to interpret the level descriptions and translate them into concrete consequences for the information assets being discussed. This is particularly apparent when consequence levels are phrased in general or abstract terms, leading to differing interpretations of what they entail, and how they differ, in practice. Such ambiguity becomes apparent when participants attempt to classify assets, and disagreements arise, for example, over which level best reflects the asset's value or what the differences between the levels really are. For this reason, the challenge of identifying distinct differences between classification levels is positioned at the operational level, as it is during the execution of the classification activity that the clarity, or lack of clarity, in the classification becomes apparent, affecting the decision-making.

The final challenge placed at the operational level is *differentiating between risk analysis and classification*. Despite the intent for these activities to remain separate, participants may inadvertently introduce risk-related concepts such as likelihood, threat or risk into the classification discussion. An example of such an introduction was when novices were introduced to information classification. Workshop facilitators used concrete examples to help inexperienced participants understand the classification task, yet these examples often relied on worst-case scenarios or risk-based reasoning. As a result, the examples introduce risk concepts into the discussion, leading participants to frame the activity as a risk analysis rather than an assessment of information asset value. When this occurs, the workshop shifts away from the intended focus on assessing asset value towards evaluating potential risks, a topic that belongs in the subsequent risk analysis step. This challenge is positioned at the operational level because it materialises through discussions during the workshop, directly influencing how participants interpret the task and shaping the final classification outcome.

Regarding support, similarly to the strategic level, no supportive tools have been positioned at an operational level. This is because support and means are implemented and used at the operational level, while they are created at the tactical level. This is further discussed in Section 5.4. In the below Table 7, a summary of each challenge, prerequisite and support can be viewed in relation to the organisational levels of planning.

**Table 7:** Prerequisites, Challenges and Support, Positioned in Relation to Organisational Planning Levels

Planning Level	Prerequisite	Challenge	Support
<b>Strategic</b>	Understand the purpose of classification	Difficult to adapt guidelines	
	Trust between colleagues		
<b>Tactical</b>	Heterogeneous teams	Deciding on a level of granularity	Automation
	Shared terminology	Difficult to adapt guidelines	Assistance
	Understand classification levels	Incomplete registry of assets	Documentation
	Adequate tool and process support		
<b>Operational</b>	Understanding of organisational value-creation	Deciding on a level of granularity	
	Understand the purpose of classification	Actor subjectiveness	
	Shared terminology	Discourse interpretation	
		Differentiating between risk analysis and classification	

## 5.2 Coordination and Collaboration Between Planning Levels

As indicated in the analysis and summarised in Table 7, several prerequisites and challenges identified in this thesis are positioned across more than one organisational planning level. This reflects the need for coordination and collaboration across levels to address challenges in organisational information classification. In this context, coordination describes alignment across planning levels, and collaboration refers to joint efforts between actors. As illustrated by the decomposition and coordination

arrows in Figure 1, planning and execution are not strictly linear, but involve ongoing coordination across the hierarchical levels (Große, 2019). Challenges that become visible at the operational level are often the result of insufficient or unclear preparation at the strategic level, where planning decisions are made before classification activities are carried out in practice. However, this is difficult to know before the process is carried out, and as such, feedback is necessary to address potential issues.

At the same time, it is indicated that effective collaboration between planning levels is not limited to top-down direction. While strategic and tactical planning are important in enabling operational classification, feedback from operational practice is equally important for refining preparation at higher levels. As described by von Solms and von Solms (2006), planning and execution can be understood as part of a control cycle, where directives start at a strategic level, are translated in the tactical layer, and are carried out as a process in the operational layer. Feedback then flows back from the operational practice to inform tactical and strategic decision-making. In the context of information classification, such feedback may concern, for example, how well a classification matrix supports distinguishing between classification levels, how usable guidelines are in practice, or to what extent documentation support enables the capture of relevant contextual knowledge. In this sense, the operational classification workshops are not the end of planning, but rather a point of application for a plan that can then be reiterated and improved through feedback.

To further explain the collaboration and overlap between planning levels, the distinction between narrow and wide planning (Große, 2019; Schmidt & Wilhelm, 2000), as explained in Section 2.1, is useful. Narrow planning includes the preparatory work carried out before execution, such as defining processes and providing the operational team with the means to be successful. In the context of information classification, this type of planning would primarily take place at the strategic and tactical levels, planning how to carry out each step of the process, based on set directives. An example of such planning would be Figure 2, where every classification activity is outlined and explained. In doing so, the participants of the classification workshop can implement the narrow plans when carrying out the process. Wider planning, in contrast, would refer to planning that includes the actions or activities where the decisions are made, or, in the case of classification, where the classification process is carried out. This form of planning spans all levels, but becomes visible at the operational level during classification workshops, where participants apply the means created in the strategic level to specific assets and organisational contexts. Viewed through this lens, many of the challenges identified in the analysis can be understood as points where narrow planning meets the limits of what can be specified and prepared in advance. While strategic and tactical planning can provide direction and support, they cannot fully anticipate the contextual nuances and interpretations required during classification. As a result, wide planning remains a necessary part of the classification process, particularly when dealing with issues such as granularity and terminology. As indicated, some preparation can be made at the tactical level regarding this, however, not all terminology or nuances of granularity can be covered in supportive documents or tools. This would help ex-

plain why some prerequisites are difficult to fulfil entirely through preparation, and why certain challenges persist despite extensive planning efforts in a narrow sense. Additionally, in Figure 1, wide and narrow planning both cover the operational level. This relates to the difficulty of defining what does and does not constitute the classification-level decision. The preliminary planning that happens at the tactical level is clearly of a narrow sense in that it is preparatory, outlining how to carry out the process to take a decision. However, at the operational level, the line between narrow and wide planning is difficult to differentiate. There are decisions made in the classification workshop that do not affect the classification-level decision, such as deciding on a level of granularity and gathering, for example, requirements that affect the decision. Such decisions and gathering of information build the base of a decision, however, whether it is part of decision-making is not apparent.

Overall, it can be argued that effective information classification will depend on coordination and collaboration across planning levels. Strategic planning provides purpose and legitimacy through high-level directives, tactical planning translates this intent into support, and operational practice conducts information classification by carrying out the process, leading to a classification decision. Feedback between levels is essential for identifying shortcomings in preparation and for refining support over time. Recognising these dependencies and the need for coordination between planning levels is therefore key to understanding both why challenges persist in information classification and how organisations can address them through collaboration across levels, and in doing so, identifying where and how information classification can be supported.

### 5.3 Research Contributions

This thesis contributes to the understanding of information classification in several ways.

First, the thesis contributes theoretically by adapting the concepts of multi-level planning (Große, 2019) to the domain of information classification. While multi-level planning has previously been applied in other contexts, such as emergency response planning, it has not previously been used to analyse classification practices. Examining prerequisites, challenges, and support across strategic, tactical, and operational levels shows that classification cannot be fully understood as an isolated operational activity. Instead, it is shaped by decisions and assumptions made across planning levels. As a result, challenges observed in the operational carrying out of the classification process can stem from strategic decisions or tactical support, suggesting that effective classification depends on coordination and collaboration across levels. In addition, the application of the adapted multi-level planning model (see Figure 1) as an analytical framework constitutes a methodological contribution. The framework was used to structure the thesis-level analysis (See Section 5.4) and to synthesise findings across Papers A-E. In doing so, it enabled an analysis of how identified prerequisites, challenges, and support relate to different planning levels. This demonstrates how the multi-level planning framework can be used within qualitative information security research.

Second, the thesis contributes to information classification by detailing organisational prerequisites and challenges that shape information classification in practice. Through analysing Papers A-D included in this thesis (see Section 4.2.1 and 4.2.3), a set of prerequisites that enable meaningful classification and recurring challenges that hinder it are identified and analysed. While some of the identified challenges were already known, such as actor subjectiveness and difficult to adapt guidelines (see, for example, (Bergström et al., 2021; Kaarst-Brown & Thompson, 2009; Niemimaa & Niemimaa, 2017), they were in this work confirmed and further explained. This contribution provides a foundation for further understanding and supporting information classification.

Third, the thesis contributes to an existing classification method by addressing the underdeveloped part of documentation in the information classification process. Building on the structured classification method proposed by Bergström et al. (2021), a gap was identified related to the recording of contextual knowledge and decision rationale generated during classification workshops. Existing research and standards tend to emphasise the final classification level as the primary output (Bergström et al., 2021; Bradford et al., 2022; Tankard, 2015). However, the findings presented in this thesis (see Section 4.4) show that much of the value of classification lies in the discussions and interpretations that precede and shape the decision itself. By developing and proposing a structured approach to documenting such reasoning and associated contextual knowledge, the thesis extends and complements the existing classification method by describing documentation practices and demonstrating the importance of keeping a record that goes beyond a classification level. The proposed approach was further discussed and refined through expert panel validation (see Section 3.3.4), which supports its practical relevance and applicability in organisational settings. In this way, the thesis not only identifies a missing element in current classification methods but also provides guidance on how to address it.

Fourth, the thesis work challenges the existing assumptions that subjectivity in classification workshops is primarily a weakness or issue to be eliminated (Bergström et al., 2021; Kaarst-Brown & Thompson, 2009; Sajko et al., 2006). While subjective judgment has often been framed as a source of inconsistency or error, the findings demonstrate that collaborative interpretation and contextual reasoning are key to producing meaningful classification decisions. Subjectivity is therefore reconceptualised not only as a limitation or challenge, but as an important component of the classification process that contributes valuable organisational knowledge. Meaning, it is a necessary part of a better understanding of the value of information assets and a nuanced classification decision. At the same time, it is recognised that subjectivity can be challenging, and it must be addressed in organisations by using a meaningful approach.

Lastly, the thesis contributes to the ongoing discussions on automation in information classification. While some research promotes automated approaches that aim to reduce or eliminate human involvement (such as Ignaczak et al. (2026)), the findings in this work indicate that classification in organisational practice depends heavily on contextual understanding and human judgment. Meaning, humans are a critical part of understanding the value of organisational assets, and in turn, are

necessary for classification. Rather than replacing human involvement, automation is better positioned to support administrative tasks related to classification, rather than automating them completely. In this sense, the thesis contributes to the ongoing discussion by arguing for a more nuanced positioning of automation in relation to human judgment in information classification.

## 5.4 Practical Contributions

The findings of this thesis also have practical relevance for organisations working with information classification. The following section outlines the main practical contributions structured across the strategic, tactical, and operational planning levels.

### Strategic

The strategic level should lay the foundation for effective information classification by defining its purpose, shaping how it is framed within the organisation, and creating conditions that enable collaboration and trust. Factors such as how well leadership understands the organisation and which standards are adopted can influence, and sometimes complicate, the work done at lower planning levels. Such complications have previously been shown, for example, by Niemimaa and Niemimaa (2017), who describe how an information security policy on information classification, based on best-practice guidelines, proved difficult to implement in practice. One of the key takeaways from that study is that managers need to translate guidelines to the organisational context and recognise that general procedures and best practices are seldom directly applicable to operational work without an understanding of local practices and ways of working. This points to the importance of having managers with an *understanding of the purpose of information classification*, in the organisation.

This implication is also consistent with established information security management literature, which emphasises the role of senior management in enabling effective translation of strategic directives into tactical planning. For instance, von Solms and von Solms (2006) and Whitman and Mattord (2022) both highlight that successful information security management depends on leadership understanding and commitment at the strategic level. In the context of information classification, this suggests that strategic actors should focus on providing clear direction and legitimacy for classification activities, while allowing tactical and operational levels the flexibility needed to adapt classification to organisational practice.

### Tactical

It is worth noting that the tactical level of planning plays an important role in determining whether information classification can be carried out meaningfully in an organisational context. While strategic planning establishes the purpose of classification, and classification workshop participants at the operational level ultimately carry out the process, it is at the tactical level that strategic intentions are translated

into the supports that shape how classification is to be conducted. This aligns well with descriptions of planning levels and their respective intentions, as explained, for example, by White (2024) and Whitman and Mattord (2022). The effects of some of the challenges and prerequisites identified at the tactical level, such as *deciding on a level of granularity*, *understanding classification levels*, and providing *adequate tool and process support*, while positioned as tactical, do not become apparent until the classification process is carried out at the operational level. However, when these challenges and prerequisites are not addressed, resulting in classification failures, these failures may be better understood, at least in part, as consequences of insufficient tactical preparation rather than failures at the operational level.

From a practical perspective, this suggests that organisations should place great emphasis on the tactical work surrounding information classification. Doing so would include making decisions about how classification should be approached in practice, what level of granularity is appropriate for different types of information assets, and how standards or guidelines should be interpreted in relation to local processes and ways of working, similar to what's explained in (Niemimaa & Niemimaa, 2017). The findings also indicate that leaving such questions unresolved or assuming they can be addressed during classification workshops places a burden on classification workshop participants, which could increase the likelihood of inconsistent classification outcomes. Tactical planning should therefore aim to reduce unnecessary uncertainty by providing usable guidance, while at the same time acknowledging that not all ambiguity can be eliminated by support, as the actual classification decision is subjective in nature. Examples of such guidance could be digital tools, but also customised classification matrices, similar to what (Bergquist et al., 2021) did in their customisation of a classification matrix to Swedish municipalities. In regard to digital tools, current information classification tools do not meet their needs very well, as outlined in a recent study by (Bergström, 2023). In that study, it was identified that most tools used in a Swedish public sector context use spreadsheets and document templates, and that most users have chosen the tool they use because there were no other suitable alternatives, indicating that there is room for improvement and further investigation.

In addition, as discussed in relation to heterogeneous teams, tactical preparation should account for the interpretive and collaborative nature of information classification. Since classification decisions often require negotiation between participants with different perspectives, tactical planning should not only focus on creating tools but also on designing processes that support interaction during classification activities. This includes planning for heterogeneous participation, establishing a shared terminology, and providing forms of support that help participants understand the purpose and structure of the process. Notably, shared terminology was identified as a prerequisite, a challenge, and a wished-for form of support. This reflects the central role the tactical level has in enabling classification, while also highlighting the difficulty of addressing it in practice. Similar challenges related to terminology and shared understanding have been identified in information security and risk management research over the past decade (some examples being: (Bergström et al., 2019; Schmidt, 2023; Wangen & Snekenes, 2013; Wheeler, 2011)), suggesting that while

the issue is well recognised, it remains difficult to address in organisational settings.

Additionally, automating administrative aspects of the classification process could also lead to less time spent on overhead and allow for more time to be spent on discussion and interpretation, leading to classification decisions, which, in paper D, was viewed as the more valuable work. What parts of classification to automate, or how to include such automation in digital tools, has not been investigated in this research. Lastly, the tactical preparation for information classification should be treated as an iterative activity, where guidance, tools, and support are continuously refined based on experiences from operational classification workshops.

### **Operational**

The operational level represents the point at which information classification is applied and where preparations made at the tactical levels are put into action. A central implication is the importance of facilitating and structuring classification workshops. As shown in the analysis, classification largely depends on collaboration and discussion. The operational practice should therefore ensure that workshops are actively facilitated, with attention given to keeping discussions focused on the value of information assets rather than drifting into related activities such as risk analysis. Facilitation can also help manage time, ensure that different perspectives are heard, and guide participants toward shared decisions, particularly when disagreements arise. Further, the analysis indicates that subjectivity is an inherent and necessary part of information classification. As has been explained, participants bring different experiences, responsibilities, and understandings of information asset value, and these differences contribute to the quality of the classification outcome. From a practical perspective, this suggests that classification should not aim to eliminate subjectivity. Instead, providing space for participants to express and discuss their views supports more nuanced decisions and reduces the risk of classifications being based on a single dominant perspective. It is, however, important that the reasoning for decisions are documented, as is suggested in Section 4.4, and in previous research (Beckers et al., 2014). In doing so there is the ability to revisit and reflect on previous decisions and why they were made.

As discussed in Section 5.3, earlier research often posits subjectivity as an issue that must be resolved, and that the solution would be to reduce or remove subjective judgments, such as in (Bergström et al., 2021; Kaarst-Brown & Thompson, 2009; Sajko et al., 2006). In the case of this research, subjectivity has been explained to be a key part of classification decisions, and allowing for dialogue to take place is key in achieving a good understanding of the asset value, and in turn, a well-substantiated classification decision. However, conducting classification with never-ending dialogues is not a good use of resources, and as such, a suggested approach would be to understand subjectivity as necessary, while facilitating discussions to not become too lengthy, especially so on information assets that are considered less valuable.

Another contribution concerns the need to allow time for clarification and shared understanding during workshops. Although shared terminology and guidance can

be prepared at the tactical level, differences in how terms, categories, or examples are interpreted will inevitably emerge in practice. This is, in part, reflected in the classification scheme and how it is formulated. Fibikova and Müller (2011) mentions that writing a good classification scheme includes fulfilling the paradox of making it complicated enough to allow for precise classification, and simple enough for everyone to use. This perspective has been reflected in this research, such as in Paper A and Paper C, where this challenge is brought up by respondents. To mitigate this, classification should allow time for participants to clarify terminology, align their understanding, and revisit assumptions when needed, but also discuss how they view the differences between classification levels. In addition, tactical support should be prepared to define shared terminology, even though this support might be limited to concepts related to the classification activity itself, in line with suggestions from Paper D.

Maintaining a clear distinction between information classification and risk analysis is important at the operational level. As demonstrated in the analysis and shown in Papers A and C, discussions during classification workshops may inadvertently introduce risk-related concepts such as likelihood or threat, especially when participants are inexperienced, and examples are introduced. One way to address this could be to include explicit reminders of the purpose of classification and its place within the broader information security and risk management process. This helps ensure that classification remains focused on assessing information asset value, with risk analysis addressed as a subsequent activity.

Finally, it is worth highlighting the importance of using operational experience as feedback for continuous improvement. Challenges encountered during classification workshops will likely reveal gaps or ambiguities in tactical preparation, such as unclear guidance or insufficient support. From a practical perspective, outcomes and experiences from operational classification should therefore be documented and reflected upon, and used to refine tactical guidance, tools, and support over time.

## 5.5 Limitations

As with all research, this thesis has a number of limitations that should be considered when interpreting its findings. First, most of the empirical data has been collected in the context of Swedish public sector organisations. As such, the results are shaped by this context and may reflect specific conditions present in the Swedish public sector. The findings may therefore not transfer directly to other organisational settings, such as private-sector organisations, where priorities and ways of work may differ. That said, the recurring challenges identified suggest that several of the issues addressed are not unique to a single organisational context. Nevertheless, conducting similar studies in other national or sectoral settings would be valuable to further explore potential differences and similarities.

A second limitation relates to the qualitative approach used throughout the thesis. The included studies relied on semi-structured interviews, thematic analysis, and expert validation to investigate how information classification is understood from the perspectives of subject experts and classification workshop participants. This

approach was chosen to gain an in-depth understanding of respondents' experiences and perspectives. However, it also means that the results do not provide any statistical generalisation or quantitative measurements. The thesis does not, for example, assess how common the identified challenges are at a larger scale. As such, the results should be understood as providing analytical and conceptual insights rather than statistical proof.

Third, relating to documentation support, the thesis proposes a structured approach to supporting documentation in information classification. However, this support has not been evaluated in organisational use. The contextual knowledge suggested to be gathered is grounded in empirical findings and validated through expert panels, but the thesis has not evaluated the proposed structured approach. As such, the contribution should be understood as conceptual rather than as a fully evaluated operational solution.

A final limitation of the thesis concerns the distribution of the empirical material across organisational planning levels. While the overall purpose of the thesis was to create knowledge about information classification in relation to strategic, tactical, and operational levels, most of the empirical material was gathered from respondents situated close to the operational and tactical levels. As such, the perspectives gained primarily reflect the experiences of practitioners involved in conducting or supporting information classification in practice, such as information security specialists and managers. As a result, strategic-level perspectives are less prominently represented in the empirical material. Although strategic considerations are analysed and discussed in the thesis, they are to a large extent gained from operational and tactical perspectives rather than being examined directly. This may limit the depth of insight into how information classification is understood, prioritised, and governed at the strategic level.

## 5.6 Future Research

The findings and limitations of this thesis point to several directions for future research on information classification and its role in organisational information security work. An initial direction concerns subjectivity and interpretation in classification work. While this thesis shows that subjectivity is an inherent and valuable part of information classification, further research is needed to better understand how subjectivity can be supported and structured in practice. Future studies could, for example, investigate facilitation techniques or tools that help classification workshop participants articulate and document their reasoning. Such work could contribute to a more nuanced understanding of how subjectivity can be used as a resource while mitigating some of the challenges associated with reaching shared decisions.

Another avenue for future research concerns the individual challenges identified in this thesis. While this work identifies and describes several recurring challenges in information classification, it does not aim to propose detailed solutions for them. Instead, the thesis provides a foundation of challenges, clarifying how and why these challenges arise in practice. Future research could therefore take these challenges as starting points and investigate them in more depth, either individually or in focused

combinations. Future work could, for example investigate how to keep complete asset registries for classification. Such research would be interesting, especially in the age of large language models and with how much information is generated in organisations.

Similar to the identified challenges, the two general areas of support, automation and assistance, could be further investigated. The results present a structured overview of practitioner needs related to tool support when working with information security risk management and information classification. Future research could treat these identified needs as a starting point for the development of support for information classification and, importantly, examine whether and how such support is perceived as useful in classification workshops. Verifying the usefulness of such support in classification workshop settings could help ensure that developed support aligns with how classification is actually carried out in practice.

As a last research direction, future research could more directly address strategic-level perspectives on information classification. As noted in the limitations of this thesis, most empirical material is drawn from operational and tactical contexts. Studies focusing on senior management and strategic decision-makers could investigate how information classification is framed and prioritised at the strategic level and how it is linked to organisational goals. It would also be interesting to investigate how strategic assumptions influence classification practices at the lower levels of planning. Such research would complement the findings of this thesis and further deepen the understanding of classification as a multi-level organisational activity.

---

## CONCLUSION

---

This section concludes the thesis by summarising its contributions in light of the research purpose and research questions. It also reiterates the overall significance of the findings for organisational information classification.

This work was motivated by the observation that, despite its foundational role in information security risk management, information classification has been overlooked in research, especially in an empirical sense, and while standards and guidelines describe what information classification is intended to achieve, there is a limited understanding of how classification is carried out in organisational practice.

The purpose of this thesis was *to create knowledge about the relevance of information classification within the strategic, tactical, and operational levels of an organisational context*. To fulfil this purpose, the research first investigated the prerequisites and challenges associated with the information classification process in an organisational context. The research then examined the need for support in information security risk management and information classification, and addressed one such need through proposing a structured approach to documentation. Finally, the findings were analysed in relation to the strategic, tactical, and operational levels of planning.

The main theoretical contribution of this thesis is the understanding of information classification as a multi-level organisational activity. By using and adapting the concepts of multi-level planning (see Figure 1) to information classification research as an analytical framework, and applying it to classification prerequisites, challenges, and support, the thesis work shows that information classification cannot be adequately understood as a purely operational task. Instead, collaboration and coordination between planning levels are necessary for effective classification. For example, many challenges encountered in information classification workshops do not originate at the operational level where they become visible, but are instead rooted in strategic and tactical work and preparation. Importantly, the operational application of support should not be understood as the final step of planning, but as an opportunity to provide feedback that can inform and refine future planning and support. At the same time, not all challenges related to information classification can be addressed solely through planning, as parts of the classification process are inherently interpretive and challenging in their own right. Subjectivity is one such example.

While existing research often treats subjective judgment primarily as a challenge to be minimised or eliminated, the findings of this thesis indicate that subjectivity is an inherent and important part of classification work in organisational practice. Classification decisions are shaped by the perspectives and experiences of the workshop participants, and subjective interpretations allow different forms of organisational

---

knowledge to be brought into the classification process. This is important for understanding the value of information assets in their specific organisational contexts. At the same time, subjectivity can, and likely will, introduce challenges related to decision-making, particularly in collaborative workshop settings. Rather than viewing subjectivity as something to be removed entirely, the thesis shows that it is a valuable asset in classification workshops. However, it is recognised that subjective judgements are challenging, and a structured approach to managing subjectivity is necessary. By positioning subjectivity as both a resource and a challenge, the thesis offers a more nuanced understanding of subjective judgment as an important part of information classification.

Regarding practical contributions, the first research question, *what are the prerequisites and challenges with information classification in organisational practice?*, investigated how organisational information classification is enabled and hindered. The results identified both prerequisites, such as organisational understanding, the use of heterogeneous teams, and awareness of the purpose of classification, and challenges, including difficulties in choosing a level of granularity, non-complete asset registries, and difficulties in adapting standards and guidelines to local organisational contexts. This contribution provides organisations and practitioners with an overview of conditions that shape information classification beyond the immediate execution of classification workshops. By making these prerequisites and challenges explicit, the thesis supports practitioners in understanding what must be prepared, and what challenges might be encountered, which allows for better planning. It can also help organisations recognise that many issues encountered during classification workshops are not isolated operational problems but are connected to the classification preparation.

The second research question focused on support by asking, *how can the practice and documentation of organisational information classification be supported?*. The findings indicate two main avenues of support: automation and assistance. Automation can simplify repetitive and administrative tasks, such as transferring information between process steps or providing timely notifications, while assistance provides users with explanations, examples, and process guidance to improve understanding. In practical terms, this contribution clarifies what types of support are perceived as meaningful in information classification. Further, to support documentation, a structured approach to documenting the classification process was developed and validated using an expert panel. In doing so, it contributes practical support classification workshop participants can use to document classification decisions.

Given the above contributions, there are some interesting avenues for further research. This thesis has been conducted primarily in a Swedish public-sector setting, investigating how information classification is carried out. Regarding prerequisites and challenges, conducting similar studies in the private sector to investigate whether there are any differences would be of interest, given that there are likely other ways to prioritise resources. Regarding support, future research could investigate, for example, the use of classification matrices and their role in the classification workshop setting. As indicated in Paper C, matrices are often overlooked and ignored, even though they are supposed to serve as the key guiding tool throughout the classifica-

---

tion workshop. Investigating why this is the case and potential ways forward could be of great value. Furthermore, assessing the structured support for documentation in real-life classification workshop settings, and further refine the approach in practical applications would be of value. Lastly, studies that more directly addresses the strategic-level role in classification and how the strategic framing of classification affects the operational classification process would be of great interest.

To sum up, this thesis responds to calls for more empirical research on the, in many ways, overlooked but very important topic of information classification. By investigating information classification in organisational practice, the thesis contributes to a clearer understanding of how organisations approach and carry out classification work. Furthermore, it expands the current knowledge of information classification, positioning it as a multi-level organisational practice shaped by coordination and collaboration across strategic, tactical, and operational levels. In doing so, the work represents a step towards a deeper understanding of information classification as an organisational practice. At the same time, the research presented in this work stresses that much remains to be done to further understand and support information classification, pointing to both important and promising directions for future research.



---

## REFERENCES

---

- Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management*, *35*(6), 717–723. <https://doi.org/10.1016/j.ijinfomgt.2015.08.001>
- Alavi, M., & Leidner, D. E. (2001). Knowledge management and knowledge management systems: Conceptual foundations and research issues. *MIS quarterly*, *25*(1), 107–136. <https://doi.org/10.2307/3250961>
- AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & security*, *99*, 102030. <https://doi.org/10.1016/j.cose.2020.102030>
- Allmark, P., Boote, J., Chambers, E., Clarke, A., McDonnell, A., Thompson, A., & Tod, A. M. (2009). Ethical issues in the use of in-depth interviews: Literature review and discussion. *Research Ethics*, *5*(2), 48–54. <https://doi.org/10.1177/174701610900500203>
- Allouche, M. K., & Berger, J. (2011). Collaborative Multi-Level Plan Monitoring. *Journal of Defense Resources Management*, *2*(2), 13.
- Azungah, T. (2018). Qualitative research: Deductive and inductive approaches to data analysis. *Qualitative research journal*, *18*(4), 383–400. <https://doi.org/10.1108/QRJ-D-18-00035>
- Baghrmian, M., & Coliva, A. (2019). *Relativism*. Routledge.
- Barraza de la Paz, J. V., Rodríguez-Picón, L. A., Morales-Rocha, V., & Torres-Argüelles, S. V. (2023). A systematic review of risk management methodologies for complex organizations in industry 4.0 and 5.0. *Systems*, *11*(5), 218. <https://doi.org/10.3390/systems11050218>
- Beckers, K., Heisel, M., Solhaug, B., & Stølen, K. (2014). ISMS-CORAS: A structured method for establishing an ISO 27001 compliant information security management system. *Engineering Secure Future Internet Services and Systems: Current Research*, 315–344. <https://doi.org/10.13140/RG.2.2.18280.67842>
- Bergquist, J.-H., Tinet, S., & Gao, S. (2021). An information classification model for public sector organizations in sweden: A case study of a swedish municipality. *Information & Computer Security*, *30*(2), 153–172. <https://doi.org/10.1108/ICS-03-2021-0032>
- Bergström, E. (2023). Tools supporting information security risk management in practice. In P. Bednar, F. Zaghoul, C. Welch, A. Nolte, M. Rajanen, A. S. Islind, H. V. Hult, A. Ravarini, & A. M. Braccini (Eds.), *9th international conference on socio-technical perspective in information systems development, stpis* (pp. 146–159, Vol. 3598). CEUR-WS.
- Bergström, E., Karlsson, F., & Åhlfeldt, R.-M. (2021). Developing an information classification method. *Information & Computer Security*, *29*(2), 209–239. <https://doi.org/10.1108/ICS-07-2020-0110>

- 
- Bergström, E., Lundgren, M., & Ericson, A. (2019). Revisiting information security risk management challenges: A practice perspective. *Information and Computer Security*, 27(3), 358–372. <https://doi.org/10.1108/ICS-09-2018-0106>
- Bergström, E., & Åhlfeldt, R.-M. (2014). Information classification issues. In K. Bernsmed & S. Fischer-Hübner (Eds.), *Secure it systems* (pp. 27–41). Springer International Publishing. [https://doi.org/10.1007/978-3-319-11599-3\\_2](https://doi.org/10.1007/978-3-319-11599-3_2)
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative research journal*, 9(2), 27–40. <https://doi.org/10.3316/QRJ0902027>
- Bradford, M., Taylor, E. Z., & Seymore, M. (2022). A view from the ciso: Insights from the data classification process. *Journal of Information Systems*, 36(1), 201–218. <https://doi.org/10.2308/ISYS-2020-054>
- Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative research in psychology*, 3(2), 77–101. <https://doi.org/10.1191/1478088706qp063oa>
- Burnard, P. (1991). A method of analysing interview transcripts in qualitative research. *Nurse education today*, 11(6), 461–466. [https://doi.org/10.1016/0260-6917\(91\)90009-Y](https://doi.org/10.1016/0260-6917(91)90009-Y)
- Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing octave allegro: Improving the information security risk assessment process* (tech. rep.). Software Engineering Institute.
- Collard, G., Ducroquet, S., Disson, E., & Talens, G. (2017). A definition of information security classification in cybersecurity context. *2017 11th International Conference on Research Challenges in Information Science (RCIS)*, 77–82. <https://doi.org/10.1109/RCIS.2017.7956520>
- Crotty, M. J. (1998). The foundations of social research: Meaning and perspective in the research process. *The foundations of social research*, 1–256. <https://doi.org/10.4324/9781003115700>
- Davenport, T. H. (1993). *Process innovation: Reengineering work through information technology*. Harvard Business Press.
- Denzin, N. K., & Lincoln, Y. S. (2011). *The sage handbook of qualitative research* (4th ed.). Sage.
- Dhillon, G., & Backhouse, J. (2001). Current directions in is security research: Towards socio-organizational perspectives. *Information systems journal*, 11(2), 127–153. <https://doi.org/10.1046/j.1365-2575.2001.00099.x>
- Disterer, G. (2013). Iso/iec 27000, 27001 and 27002 for information security management. *Journal of Information Security*, 4(2). <https://doi.org/10.4236/jis.2013.42011>
- Dubois, A., & Gadde, L.-E. (2002). Systematic combining: An abductive approach to case research. *Journal of business research*, 55(7), 553–560. [https://doi.org/10.1016/S0148-2963\(00\)00195-8](https://doi.org/10.1016/S0148-2963(00)00195-8)
- Ekelhart, A., Fenz, S., Klemen, M., & Weippl, E. (2007). Security ontologies: Improving quantitative risk analysis. *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, 156a–156a.
- Eloff, J. H., Holbein, R., & Teufel, S. (1996). Security classification for documents. *Computers & Security*, 15(1), 55–71. [https://doi.org/10.1016/0167-4048\(95\)00023-2](https://doi.org/10.1016/0167-4048(95)00023-2)

- 
- European Union Agency for Cybersecurity (ENISA). (2023). RM/RA Tools [Accessed: 2024-02-11]. <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/%20current-risk/risk-management-inventory/rm-ra-tools>
- Evans, N., & Price, J. (2020). Development of a holistic model for the management of an enterprise's information assets. *International Journal of Information Management*, 54, 102193.
- Everett, C. (2011). Building solid foundations: The case for data classification. *Computer Fraud & Security*, 2011(6), 5–8. [https://doi.org/10.1016/S1361-3723\(11\)70060-4](https://doi.org/10.1016/S1361-3723(11)70060-4)
- Fallis, D. (2015). What is disinformation? In *Library Trends. Exploring Philosophies of Information* (pp. 401–426, Vol. 63). Johns Hopkins University Press. <https://doi.org/10.1353/lib.2015.0014>
- Fenz, S., & Ekelhart, A. (2011). Verification, validation, and evaluation in information security risk management. *IEEE Security & Privacy*, 9(2), 58–65. <https://doi.org/10.1109/MSP.2010.117>
- Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, 22(5), 410–430. <https://doi.org/doi:10.1108/IMCS-07-2013-0053>
- Fibikova, L., & Müller, R. (2011). A simplified approach for classifying applications. In N. Pohlmann, H. Reimer, & W. Schneider (Eds.), *Isse 2010 securing electronic business processes: Highlights of the information security solutions europe 2010 conference* (pp. 39–49). Vieweg+Teubner. [https://doi.org/10.1007/978-3-8348-9788-6\\_4](https://doi.org/10.1007/978-3-8348-9788-6_4)
- Flowerday, S., & Von Solms, R. (2005). Real-time information integrity= system integrity+ data integrity+ continuous assurances. *Computers & Security*, 24(8), 604–613. <https://doi.org/10.1016/j.cose.2005.08.004>
- Furlong, P., & Marsh, D. (2010). A skin not a sweater: Ontology and epistemology in political science. In *Theory and methods in political science* (3rd ed.). Palgrave Macmillan.
- Gerber, M., & von Solms, R. (2005). Management of risk in the information age. *Computers & security*, 24(1), 16–30. <https://doi.org/10.1016/j.cose.2004.11.002>
- Ghernaouti-Helie, S., Simms, D., & Tashi, I. (2011). Protecting information in a connected world: A question of security and of confidence in security. *2011 14th International Conference on Network-Based Information Systems*, 208–212. <https://doi.org/10.1109/NBiS.2011.38>
- Goundar, S. (2012). Research methodology and research method. In *Cloud computing* (pp. 1–47, Vol. 1). Research Gate Publications.
- Gritzalis, D., Iseppi, G., Mylonas, A., & Stavrou, V. (2018). Exiting the risk assessment maze: A meta-survey. *ACM Comput. Surv.*, 51(1), 1–30. <https://doi.org/10.1145/3145905>
- Große, C. (2019). Sources of uncertainty in Swedish emergency response planning. *Journal of Risk Research*, 22(6), 758–772. <https://doi.org/10.1080/13669877.2018.1459796>

- 
- Guba, E. G., Lincoln, Y. S., et al. (1994). Competing paradigms in qualitative research. In *Handbook of qualitative research* (pp. 105–117, Vol. 2). California, Sage Publications.
- Halcomb, E. J., & Davidson, P. M. (2006). Is verbatim transcription of interview data always necessary? *Applied nursing research*, *19*(1), 38–42. <https://doi.org/10.1016/j.apnr.2005.06.001>
- Haufe, K., Colomo-Palacios, R., Dzombeta, S., & Brandis, K. (2022). A process framework for information security management. *International Journal of Information Systems and Project Management*, *4*(4), 27–47. <https://doi.org/10.12821/ijispm040402>
- Heras-Saizarbitoria, I., & Boiral, O. (2013). Iso 9001 and iso 14001: Towards a research agenda on management system standards. *International journal of management reviews*, *15*(1), 47–65. <https://doi.org/10.1111/j.1468-2370.2012.00334.x>
- Hsu, C., Backhouse, J., & Silva, L. (2014). Institutionalizing operational risk management: An empirical study. *Journal of Information Technology*, *29*(1), 59–72. [https://doi.org/10.1007/978-3-319-29269-4\\_6](https://doi.org/10.1007/978-3-319-29269-4_6)
- IBM. (2023). *Cost of a data breach report 2023* (tech. rep.) (Accessed: 2024-05-11). IBM Security.
- Ignaczak, L., Martins, M. G., da Costa, C. A., & Kunst, R. (2026). A value-based approach for information classification. *International Journal of Information Security*, *25*(1), 9. <https://doi.org/10.1007/s10207-025-01174-1>
- ISO/IEC 27000. (2018). *Information technology - security techniques - information security management systems - overview and vocabulary* (Standard No. ISO/IEC 27000:2018). International Organization for Standardization. Geneva, CH. <https://www.iso.org/standard/73906>
- ISO/IEC 27001. (2022). *Information technology - cybersecurity and privacy protection - information security management systems - requirements* (Standard No. ISO/IEC 27001:2022). International Organization for Standardization. Geneva, CH. <https://www.iso.org/standard/27001>
- ISO/IEC 27002. (2022). *Information security, cybersecurity and privacy protection - information security controls* (Standard No. ISO/IEC 27002:2022). International Organization for Standardization. Geneva, CH. <https://www.iso.org/standard/75652.html>
- ISO/IEC 27005. (2022). *Information security, cybersecurity and privacy protection - guidance on managing information security risks* (Standard No. ISO/IEC 27005:2022). International Organization for Standardization. Geneva, CH. <https://www.iso.org/standard/80585.html>
- Johnson, L. M., & Schulte, J. D. (2004). Job: Security. 7 steps for hipaa compliance: Taking a proactive stance is your top job for effective information security. *Healthcare Financial Management*, *58*(10), 46–50. <https://pubmed.ncbi.nlm.nih.gov/15524033/>
- Kaarst-Brown, M. L., & Thompson, E. D. (2009). Cracks in the security foundation: Employee judgments about information sensitivity. *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, 145–151. <https://doi.org/10.1145/2751957.2751977>

- 
- Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing*, *72*(12), 2954–2965. <https://doi.org/10.1111/jan.13031>
- Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS quarterly*, 67–93. <https://doi.org/10.2307/249410>
- Ku, C.-Y., Chang, Y.-W., & Yen, D. C. (2009). National information security policy and its implementation: A case study in taiwan. *Telecommunications Policy*, *33*(7), 371–384. <https://doi.org/10.1016/j.telpol.2009.03.002>
- Leming, R. (2015). Why is information the elephant asset? an answer to this question and a strategy for information asset management. *Business Information Review*, *32*(4), 212–219. <https://doi.org/10.1177/0266382115616301>
- Lim, W. M. (2025). What is qualitative research? an overview and guidelines. *Australasian marketing journal*, *33*(2), 199–229. <https://doi.org/10.1177/14413582241264619>
- Liu, M., Shore, M., Yeoh, W., Jiang, F., & Zeadally, S. (2025). Toward effective cybersecurity management: A hierarchical process model with performance assessment. *Journal of Cybersecurity*, *11*(1). <https://doi.org/10.1093/cybsec/tyaf020>
- Longhurst, R. (2003). Semi-structured interviews and focus groups. *Key methods in geography*, *3*(2), 143–156. <https://hdl.handle.net/10289/15973>
- Lundgren, M. (2020). *Making the dead alive: Dynamic routines in risk management* [Doctoral dissertation, Luleå University of Technology].
- MacQueen, K. M., McLellan, E., Kay, K., & Milstein, B. (2008). Team-based codebook development: Structure, process, and agreement. In G. Guest & K. M. MacQueen (Eds.), *Handbook for team-based qualitative research* (pp. 119–135). AltaMira Press.
- Mattord, H. J., & Wiant, T. (2016). Information system risk assessment and documentation. In *Information security* (pp. 69–111). Routledge. <https://doi.org/10.4324/9781315288697>
- Maxwell, J. A. (2013). *Qualitative research design: An interactive approach* (3rd ed.). Sage.
- Mays, N., & Pope, C. (2000). Assessing quality in qualitative research. *BMJ*, *320*(7226), 50–52. <https://doi.org/10.1136/bmj.320.7226.50>
- METI, M. (2025). Guidelines on the roles expected of cyber infrastructure providers [Accessed: 2025-12-09]. [https://www.meti.go.jp/english/press/2025/1030\\_001.html](https://www.meti.go.jp/english/press/2025/1030_001.html)
- Metin, B., Duran, S., Telli, E., Mutlutürk, M., & Wynn, M. (2024). It risk management: Towards a system for enhancing objectivity in asset valuation that engenders a security culture. *Information*, *15*(1), 55. <https://doi.org/10.3390/info15010055>
- MSB. (2020a). Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter [Accessed: 2025-12-05]. <https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-6-foreskrifter-om-informationssakerhet-for-statliga-myndigheter.pdf>

- 
- MSB. (2020b). *Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter [the swedish civil contingencies agency's regulations on government agencies security information security]* (Report) (Accessed: 2021-11-02). Myndigheten för samhällsskydd och beredskaps författningssamling. <https://www.msb.se/siteassets/dokument/regler/forfattningar/msbfs-2020-6-foreskrifter-om-informationssakerhet-for-statliga-myndigheter.pdf>
- MSB. (2021). Arbeta systematiskt med informationssäkerhet och cybersäkerhet [Accessed: 2022-01-26]. <https://metodstod-informationssakerhet.msb.se/>
- MSB. (2023). Klassningsmodell [Accessed: 2023-12-03]. <https://www.informationssakerhet.se/metodstodet/utforma/#klassningsmodell>
- National Institute of Standards and Technology. (2004). Standards for security categorization of federal information and information systems. *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, 199*, 122.
- National Institute of Standards and Technology. (2018). Nist special publication 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy Joint Task Force. *National Institute of Standards and Technology: Gaithersburg, MD, USA*.
- Nel, F., & Drevin, L. (2019). Key elements of an information security culture in organisations. *Information & Computer Security, 27*(2), 146–164. <https://doi.org/10.1108/ICS-12-2016-0095>
- Nieves, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security. *NIST special publication, 800*(12), 101. <https://doi.org/10.6028/NIST.SP.800-12r1>
- Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems, 26*(1), 1–20. <https://doi.org/10.1057/s41303-016-0025-y>
- Oates, B. J. (2006). *Researching information systems and computing*. SAGE Publications Inc.
- Orb, A., Eisenhauer, L., & Wynaden, D. (2001). Ethics in qualitative research. *Journal of nursing scholarship, 33*(1), 93–96. <https://doi.org/10.1111/j.1547-5069.2001.00093.x>
- Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organizations: Research approaches and assumptions. *Information systems research, 2*(1), 1–28. <https://doi.org/10.1287/isre.2.1.1>
- Paananen, H., & Siponen, M. (2023). Organization members developing information security policies: A case study. *ICIS 2023: Proceedings of the International Conference on Information Systems. Association for Information Systems*. [https://aisel.aisnet.org/icis2023/cyber\\_security/cyber\\_security/14/](https://aisel.aisnet.org/icis2023/cyber_security/cyber_security/14/)
- Park, W.-S., Seo, S.-W., Son, S.-S., Lee, M.-J., Kim, S.-H., Choi, E.-M., Bang, J.-E., Kim, Y.-E., & Kim, O.-N. (2010). Analysis of information security management systems at 5 domestic hospitals with more than 500 beds. *Healthcare informatics research, 16*(2), 89–99. <https://doi.org/10.4258/hir.2010.16.2.89>
- Quist, A. S. (1993). *Security classification of information* (tech. rep.). Oak Ridge K-25 Site, TN (United States). <https://doi.org/10.2172/6934153>

- 
- Rees, J., & Allen, J. (2008). The state of risk assessment practices in information security: An exploratory investigation. *Journal of Organizational Computing and Electronic Commerce*, 18(4), 255–277. <https://doi.org/10.1080/10919390802421242>
- Rodway, P., Schepman, A., & Lambert, J. (2012). Preferring the one in the middle: Further evidence for the centre-stage effect. *Applied Cognitive Psychology*, 26(2), 215–222. [10.1002/acp.1812](https://doi.org/10.1002/acp.1812)
- Sajko, M., Rabuzin, K., & Bača, M. (2006). How to calculate information value for effective security risk assessment. *Journal of Information and Organizational Sciences*, 30(2), 263–278. <https://doi.org/10.31341/jios>
- Saldaña, J. (2021). *The coding manual for qualitative researchers* (4th). SAGE Publications Inc.
- Scarantino, A., & Piccinini, G. (2010). Information without truth. *Metaphilosophy*, 41(3), 313–330. <https://doi.org/10.1111/j.1467-9973.2010.01632.x>
- Schmidt, G., & Wilhelm, W. E. (2000). Strategic, tactical and operational decisions in multi-national logistics networks: A review and discussion of modelling issues. *International Journal of Production Research*, 38(7), 1501–1523. <https://doi.org/10.1080/002075400188690>
- Schmidt, M. (2023). Information security risk management terminology and key concepts. *Risk management*, 25(1), 2. <https://doi.org/10.1057/s41283-022-00108-8>
- Scott, W. R., & Davis, G. F. (2016). *Organizations and organizing: Rational, natural and open systems perspectives*. Routledge. <https://doi.org/10.4324/9781315663371>
- Shamala, P., & Ahmad, R. (2014). A proposed taxonomy of assets for information security risk assessment (ISRA). *2014 4th World Congress on Information and Communication Technologies (WICT 2014)*, 29–33. <https://doi.org/10.1109/WICT.2014.7077297>
- Shamala, P., Ahmad, R., Zolait, A., & Sedek, M. (2017). Integrating information quality dimensions into information security risk management (ISRM). *Journal of Information Security and Applications*, 36, 1–10. <https://doi.org/10.1016/j.jisa.2017.07.004>
- Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (isra). *Computers & Security*, 57, 14–30. <https://doi.org/10.1016/j.cose.2015.11.001>
- Shedden, P., Ahmad, A., Smith, W., Tscherning, H., & Scheepers, R. (2016). Asset identification in information security risk assessment: A business practice approach. *Communications of the Association for Information Systems*, 39(1), 15. <https://doi.org/10.17705/1CAIS.03915>
- Shedden, P., Smith, W., & Ahmad, A. (2010). Information security risk assessment: Towards a business practice perspective. *Proceedings of the 8th Australian Information Security Management Conference*, 119–130. <https://doi.org/10.4225/75/57b6769334787>
- Shivayogi, S. K. (2025). Data classification methodologies and implementation. *Journal of Computer Science and Technology Studies*, 7(5), 202–210. <https://doi.org/10.32996/jcsts.2025.7.5.26>

- 
- Silverman, D. (1998). Qualitative research: Meanings or practices? *Information systems journal*, 8(1), 3–20. <https://doi.org/10.1046/j.1365-2575.1998.00002.x>
- Silverman, D. (2015). *Interpreting qualitative data* (6th ed.). Sage.
- Singh, K. P., Rishiwal, V., & Kumar, P. (2018). Classification of data to enhance data security in cloud computing. *2018 3rd International conference on internet of things: Smart innovation and usages (IoT-SIU)*, 1–5. <https://doi.org/10.1109/IoT-SIU.2018.8519934>
- Spinellis, D., Kokolakis, S., & Gritzalis, S. (1999). Security requirements, risks and recommendations for small enterprise and home-office environments. *Information Management & Computer Security*, 7(3), 121–128. <https://doi.org/10.1108/09685229910371071>
- Stake, R. E. (1995). *The art of case study research*. Sage Publications Inc.
- Swartz, N. (2007). Data management problems widespread. *Information Management*, 41(5), 28.
- SVT. (2025). En miljon svenskers personuppgifter publicerade på darknet [Accessed: 2025-12-5]. <https://www.svt.se/nyheter/inrikes/experten-en-miljon-svenskers-personuppgifter-publicerade-pa-darknet>
- Tankard, C. (2015). Data classification—the foundation of information security. *Network Security*, 2015(5), 8–11. [https://doi.org/10.1016/S1353-4858\(15\)30038-6](https://doi.org/10.1016/S1353-4858(15)30038-6)
- Tatar, Ü., & Karabacak, B. (2012). An hierarchical asset valuation method for information security risk analysis. *International Conference on Information Society (i-Society 2012)*, 286–291.
- Tehler, H. (2023). *Introduktion till risk och riskhantering* (First). Lund: Lunds University.
- Thapa, D., & Haj-Bolouri, A. (2023). Demystifying philosophy for information systems researcher. *29th Annual Americas Conference on Information Systems, AMCIS 2023*.
- Walsham, G. (1995). The emergence of interpretivism in is research. *Information systems research*, 6(4), 376–394. <https://www.jstor.org/stable/23010981>
- Van de Ven, A. H. (2016). Grounding the research phenomenon. *Journal of Change Management*, 16(4), 265–270. <https://doi.org/10.1080/14697017.2016.1230336>
- Wangen, G., Hallstensen, C., & Snekkenes, E. (2018). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, 17(6), 681–699. <https://doi.org/10.1007/s10207-017-0382-0>
- Wangen, G., & Snekkenes, E. (2013). A taxonomy of challenges in information security risk management. *Proceeding of Norwegian Information Security Conference/Norsk informasjonssikkerhetskonferanse-NISK 2013-Stavanger, 18th-20th November 2013*. <https://doi.org/10.1007/s10207-017-0382-0>
- Veiga, A. D., & Eloff, J. H. (2007). An information security governance framework. *Information systems management*, 24(4), 361–372. <https://doi.org/10.1145/1655168.1655170>

- 
- Veritas. (2020). The uk 2020 databerg report revisited [Accessed: 2022-10-17]. [https://www.veritas.com/content/dam/www/en\\_us/documents/at-a-glance/AG\\_uk\\_databerg\\_report.pdf](https://www.veritas.com/content/dam/www/en_us/documents/at-a-glance/AG_uk_databerg_report.pdf)
- Wheeler, E. (2011). *Security risk management: Building an information security risk management program from the ground up*. Elsevier.
- White, G. (2009). Strategic, tactical, & operational management security model. *Journal of Computer Information Systems*, 49(3), 71–75. <https://doi.org/10.1080/08874417.2009.11645326>
- White, G. (2024). Security literacy model for strategic, tactical, & operational management levels. *Information Security Journal: A Global Perspective*, 33(6), 626–634. <https://doi.org/10.1080/19393555.2024.2307632>
- Whitman, M. E., & Mattord, H. J. (2019). *Management of information security* (Sixth). Cengage Learning.
- Whitman, M. E., & Mattord, H. J. (2022). *Principles of information security* (Seventh). Cengage Learning.
- von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- von Solms, R., & von Solms, S. B. (2006). Information security governance: A model based on the direct–control cycle. *Computers & security*, 25(6), 408–412. <https://doi.org/10.1016/j.cose.2006.07.005>
- Zins, C. (2007). Conceptual approaches for defining data, information, and knowledge. *Journal of the American society for information science and technology*, 58(4), 479–493. <https://doi.org/10.1002/asi.20508>
- Åhlfeldt, R.-M., Spagnoletti, P., & Sindre, G. (2007). Improving the information security model by using TFI. *New Approaches for Security, Privacy and Trust in Complex Environments*, 73–84.







# Problems in information classification: insights from practice

Problems in  
information  
classification

Simon Andersson

*Department of Computer Science, Electrical and Space Engineering,  
Luleå University of Technology, Luleå, Sweden*

449

Received 18 October 2022  
Revised 19 January 2023  
28 February 2023  
2 March 2023  
Accepted 3 March 2023

## Abstract

**Purpose** – This study aims to identify problems connected to information classification in theory and to put those problems into the context of experiences from practice.

**Design/methodology/approach** – Five themes describing problems are discussed in an empirical study, having informants represented from both a public and a private sector organization.

**Findings** – The reasons for problems to occur in information classification are exemplified by the informants' experiences. The study concludes with directions for future research.

**Originality/value** – Information classification sustains the basics of security measures. The human-organizational challenges are evident in the activities but have received little attention in research.

**Keywords** Information classification, Risk assessment, Information security

**Paper type** Research paper

## 1. Introduction

Organizations need to know what information assets they own and how valuable they are for their business to apply protection against threats (Bergström *et al.*, 2019). It allows the organization to prioritize which assets to protect first and decide how to protect them. Such protection is important, as a compromise of information in terms of confidentiality, integrity or availability can cause financial, brand and reputational damage (Tankard, 2015). For organizations to work with the management of information security, they can use an information security management system (ISMS), such as the ISO/IEC 27000 Series (ISO Central Secretary, 2018), a family of standards recommending best practices for managing information security risks. A key part of an ISMS is asset management which includes the identification and valuation of information, with a core activity being information classification (Bergström and Anteryd, 2018).

The activity of information classification builds the base for protecting valuable assets and is the foundation of risk management. The classification results in a list of ranked assets, indicating their importance and value in terms of their criticality to the organization (Agrawal, 2017). ISO 27002:2017 (ISO Central Secretary, 2017) describes its objective as an activity that is necessary to *ensure that information receives an appropriate level of protection in accordance with its importance to the organization*. Once the classification of assets is set, the result act as input into the risk assessment where classified information is required to



© Simon Andersson. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licences/by/4.0/legalcode>

The support from Interreg Aurora to the ISSUES project is gratefully acknowledged.

Information & Computer Security  
Vol. 31 No. 4, 2023  
pp. 449-462  
Emerald Publishing Limited  
2056-4961  
DOI 10.1108/ICS-10-2022-0163

analyze, prioritize and manage risks and apply protection (Bergström and Åhlfeldt, 2014; Everett, 2011; Webb *et al.*, 2014). Thus, it is an essential piece of risk analysis and management within organizations (Bergquist *et al.*, 2021; Everett, 2011; Gerber and Von Solms, 2005). According to Veritas (2015), 54% of data in organizations are unclassified and unlabeled; the result is difficulties in effectively spending and using organizational resources as there is no possibility of applying protection to assets you do not know exist. Statistics from Kaspersky (2021) show that 10% of computers were subject to an attack during the year 2020, further showing the need for security measures.

Identifying and classifying information is not straightforward, and problems occur (Bergström and Åhlfeldt, 2014), leading to failures of the risk assessment and risk management activities if not accomplished (Shedden *et al.*, 2016; Webb *et al.*, 2014). Guidelines and standards, e.g. ISO 27002:2:2017 (ISO Central Secretary, 2017) and NIST 800–60 (Stine *et al.*, 2008), provide best-practice recommendations for information classification. Organizations often use and follow such standards; however, as they are necessarily adaptable and written with a general scope in mind, it leads to struggles in interpreting them as they are intentionally generic and provide little guidance on how to adopt them (Bayuk, 2010; Siponen, 2006). Further, organizations find it challenging to translate the standards into an organizational context and to turn them into concrete actions (Niemimaa and Niemimaa, 2017).

The occurrence of human-organizational problems in information classification has previously been identified (Bergström and Åhlfeldt, 2014), and further investigation has been suggested (Bergquist *et al.*, 2021). This paper presents an analysis of problems to shed light on them from a practice point of view. Thus, the study aims to identify and suggest future research activities connected to information classification in organizations.

**2. Research design**

This study is based upon qualitative data (Fossey *et al.*, 2002) in two forms, i.e. secondary (previous research) and primary (empirical data). The search for secondary data in articles was done using Google scholar and Scopus. See Table 1 for keywords and synonyms used. The first screening was applied to identify relevant articles, i.e. those describing problems and/or challenges in information classification. After that, the secondary data, i.e. the text in the articles, were analyzed using an open-coding approach (Burnard, 1991). Such analysis can, as such, follow a non-cross-sectional format (Mason, 2017), i.e. the categories emerged from the texts rather than were formulated beforehand.

The categorization of the secondary data resulted in the formulation of five problems; those problems then guided the empirical data collection. The identified problems were named: Deciding on a level of granularity, non-complete registry of assets, actor subjectiveness, discourse interpretation problems and difficult to adapt guidelines. An example of a quote and open coding can be seen in Table 2, paired with the relevant articles used to formulate the identified problems.

Keywords	Synonyms
Information classification	Asset classification, Data classification, Information asset classification
Challenges	Issues, Problems
Information security	Cyber security, Data security

**Table 1.**  
Search words

**Source:** Created by author

Example of quote	Open coding	Articles used	Identified problem
<p>“... but it is clear that many are struggling with granularity and the implications of it” (Bergström and Åhlfeldt, 2014, p. 34)</p> <p>“An analysis is always just as good as the data it is based upon, and most risk management approaches are of little use without a reliable asset inventory” (Fenz <i>et al.</i>, 2014)</p> <p>“Subjective Scoring Methods and Risk Matrices have been claimed to add their own sources of error in an ISRM (Hubbard, 2020; Anthony (Tony) Cox, 2008). Such as compressing ranges (Anthony (Tony) Cox, 2008), presumption of regular intervals, e.g. different people at different levels in an organization will rate scales differently (Hubbard, 2020)” (Wangen and Snekkenes, 2013, p. 5)</p> <p>“The need for a security ontology, a ‘common language’ for IS professionals to ease communication and help achieve a common understanding of IS across companies and borders.” (Wangen and Snekkenes, 2013)</p> <p>“As collections of canonical practices, they ‘inevitably and intentionally omit the details’ (Brown and Duguid, 1991, p. 40), making them too abstract to be directly applicable to a specific organizational context.” (Niemiinaa and Niemiinaa, 2017, p. 12)</p>	<p>Organizations have difficulties deciding on a level of granularity</p> <p>A complete registry is needed to achieve good risk management results</p> <p>Depending on previous experiences, roles, framing etc. one tends to interpret and value risk and value of/to assets differently</p> <p>Not understanding each other properly will lead to problems in discussions and interpretations of discourse</p> <p>Guidelines are difficult to interpret and adapt as they often omit details</p>	<p>(Bergström and Åhlfeldt, 2014; Fibikova and Müller, 2011; Shedden <i>et al.</i>, 2016)</p> <p>(Bergström <i>et al.</i>, 2019; Bergström and Åhlfeldt, 2014; Fenz <i>et al.</i>, 2014; Leming, 2015)</p> <p>(Bergström <i>et al.</i>, 2019; Bergström <i>et al.</i>, 2021; Bergström and Åhlfeldt, 2014; Anthony (Tony) Cox, 2008; Fenz <i>et al.</i>, 2014; Hubbard, 2020; Kaarst-Brown and Thompson, 2015; Sajko <i>et al.</i>, 2006; Wangen and Snekkenes, 2013)</p> <p>(Ahmad <i>et al.</i>, 2015; Arhin and Wiredu, 2018; Richmond <i>et al.</i>, 2005; Shedden, 2016; Wangen and Snekkenes, 2013)</p> <p>(Bayuk, 2010; Bergström, 2020; Bergström <i>et al.</i>, 2021; Brown and Duguid, 1991; Niemiinaa and Niemiinaa, 2017; Fibikova and Müller, 2011; Ghernaouti-Helle <i>et al.</i>, 2011; Park <i>et al.</i>, 2010)</p>	<p>Deciding on a level of granularity non-complete registry of assets</p> <p>Actor subjectiveness</p> <p>Discourse interpretation</p> <p>Difficult to adapt guidelines</p>

Source: Created by author

**Table 2.**  
Example of coding and relevant articles used to formulate problems

The five categorized problems then guided the data collection which was conducted within a private sector organization that provides information security consultancy services and within a public authority organization with its main task positioned in IT. Using private and public-sector organizations allowed different actors to provide insight from varying viewpoints. The respondents were found in collaboration with a representative from the organizations' information security department.

A semi-structured approach was applied in the collection of empirical data (Fontana *et al.*, 2000). The five identified problems were thus representing the themes for data collection, which contained open-ended questions investigating the categorized problems of information classification. The open-ended questions allowed the informants to formulate their answers freely (Adams, 2015; Pedersen *et al.*, 2016) while making it possible for them to focus on the topics. The interviews lasted between 28 and 72 min and were recorded and later verbatim transcribed, i.e. word for word (Halcomb and Davidson, 2006). The analysis of the transcribed empirical data can be described as a thematic text analysis (Clarke *et al.*, 2015). The analysis of the empirical data identified, interpreted and searched for patterns which explained experiences in relation to the categories of problems (Clarke *et al.*, 2015). Expressions from the respondents have been used to add additional insights and understanding from practice to problems (Alhojailan, 2012). Table 3 shows an overview of the respondents, their position in the organization, the length of the interview, the abbreviation used in the analysis and which sector they belong to.

**3. Asset management and information classification**

For organizations to work with risk management, they can use an ISMS to minimize adverse events by assessing potential risks and assigning appropriate security measures where necessary (Shameli-Sendi *et al.*, 2016). An ISMS describes methods organizations can use to secure their assets and consists of a collection of policies, procedures and guidelines based on best practices (ISO Central Secretary, 2018; Niemimaa and Niemimaa, 2017). Within such a framework, asset management is considered to be a crucial part and includes the identification and valuation of information. The intent of asset management is to know what information exists and to value that information, with a core activity being information classification. The classification is, in turn, a crucial part of risk analysis (Gerber and Von Solms, 2005). The information classification results in a valuation of information assets in terms of confidentiality, integrity and availability. This valuation indicates how information can be, e.g. handled, stored and potential consequences in the case of a compromise (Bergström and Anteryd, 2018). The classified assets act as the primary input to the risk analysis, which is needed to understand what kind of protection to apply.

**Table 3.**  
Overview of  
informants

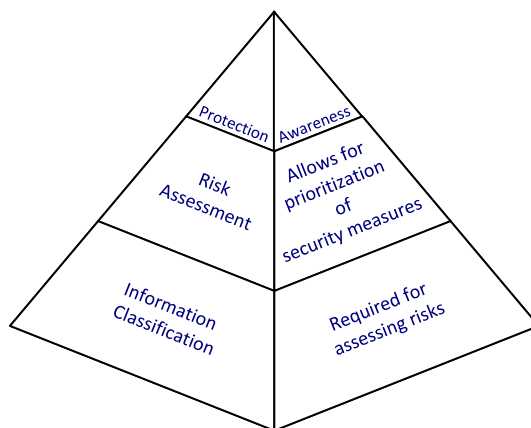
Position	Length of interview	Abbreviation	Sector
Business Developer	60 min	BD	Private
Senior Information Security Consultant	1 h 12 min	SISC	Private
Senior Consultant/IT-Archivist	28 min	SC/ITA	Private
IT-Archivist	40 min	ITA	Private
Information Security Specialist	42 min	ISS	Public
Object Owner	40 min	OO	Public
Information Security Specialist 2	36 min	ISS2	Public
Information and Data-protection coordinator	35 min	IDPO	Public

**Source:** Created by author

Conducting information classification is often done with the use of a classification scheme that contains a chosen number of consequence levels and definitions of each level in terms of confidentiality, integrity and availability (Bergquist *et al.*, 2021). It is necessary to define the stated levels clearly; not doing so can result in uneven classifications if there is too much room for interpretation. Each asset then receives a classification based on how valuable its confidentiality, integrity and availability are to the organization. The value is based on the potential consequence of information compromise. Typically, organizations divide consequences into sections such as financial and reputational consequences (Tankard, 2015). Doing so allows for a clearer view of how compromised assets might affect the organization to be gained. Additionally, classifying the asset from different perspectives, such as from a business continuity perspective or a reputational perspective shows the value of the asset from different viewpoints. With a classification in place, it allows the organization to gain knowledge of the identified assets' value in terms of how critical they are to business practices, how to prioritize them for the application of protection and to what extent the organization should spend resources to keep them protected (Agrawal, 2017). If the information classification is not considered a critical activity, it can lead to problems with the risk assessment. If there are shortcomings with the classification, it will reduce the possibility of adequately protecting the organizational assets as less knowledge is available, leading to less informed decisions (Shedden *et al.*, 2016; Webb *et al.*, 2014). Further, it also means that assets that should have been identified will remain unidentified. Thus, the organization is unaware of how to prioritize it for protection and what amount of resources is necessary to spend to keep it secure. Figure 1 showcases a thought-model of dependencies between information classification, risk assessment and applied protective measures, displaying the activity on the left side and its purpose on the right.

#### 4. Insights from practice on information classification problems

The paper addresses five problems categorized as relevant for information classification: deciding on a level of granularity, non-complete registry of assets, actor subjectiveness, discourse interpretation and difficult to adapt guidelines. They are first explained one-by-one



Source: Created by author

Figure 1.  
Dependencies  
between information  
classification, risk  
assessment and  
protection

---

from a theoretical perspective and then put into the context of experiences in the following section which presents and discusses empirical data.

*Deciding on a level of granularity*, to find an appropriate level of detail of the identified information, has been found to be a challenge (Bergström and Åhlfeldt, 2014; Shedden *et al.*, 2016). A high level of granularity means that the classification is done on every single file. Such an approach provides a detailed view of assets. A low level of granularity means that classifying assets is based on a whole system or a complete process as a cohesive unit. Naturally, the latter approach is less resource-intensive and might explain why a default approach in many organizations is to apply a low level of granularity (Shedden *et al.*, 2016). Such an approach might seem useful at the time. However, it can result in failures to identify important components of a system or a process, consequently leaving the organization with unidentified risks and assets that remain unprotected (Shedden *et al.*, 2016). Deciding on a level of granularity might be considered a simple task, but it is a critical choice for the remaining classification. The decision to use a high or low level of granularity will impact measures needed to protect the asset. A low level of granularity will thus reduce the needed resources while accepting a higher level of risk, given that assets can remain unidentified. Fibikova and Müller (2011) conclude that no straightforward suggestion can guide organizations in making the decision of granularity. Such a decision depends on the specific circumstances of each organization's business. Additionally, the asset value and risks tied to organizational assets change over time, further complicating the decision (Fibikova and Müller, 2011).

The data from informants highlight specific issues related to decisions on the level of granularity. One informant state that they start from a vast base of information that ranges from single documents to batches. The informant continues to describe that an overview and knowledge of the information base is needed:

We cannot classify information side by side, object by object. There has to be some sort of batching made. However, it is also important to understand that sometimes we have to break the batches. This is something that you learn as you reiterate the process – SISC.

Informants also describe that involving staff close to or responsible for a system is a cause for problems. One example an informant brings up is system developers, who tend to add a high level of granularity:

Developers for example, they bring a database-model and starts to classify each row with an extreme amount of detail with timestamps etc. It is not necessary to be at that level; you have to think about it logically. – ISS

With the problem of being too close to the information source in focus, the informant further explained that one major challenge is the dialogue between them, i.e. the information security specialists and the system developers. How can one find a satisfying level of granularity when one part focuses on bits and pieces and the other to gain a bigger picture view? The informant continued to reflect on experiences and explained that there is a benefit in bringing in another role into the decision-making, e.g. a person with a better understanding of how the information assets in the system at hand impacts the core business. Such a person can aid in the dialogue, the informant says, for example, by explaining and exemplifying how the information matters beyond the core system. Thus, understanding how and why it needs to be classified becomes clearer.

When interpreting the problem of deciding on a level of granularity in relation to the insights from practice, it can be discerned that such decisions are still problematic. It also indicates insight as to why a lower level of granularity tends to be an initial choice for organizations, e.g. allocating resources is a challenge, the starting point is troublesome and

the dialogues between the different roles are challenging. Communication between different actors is previously identified as causing problems, for example, due to information overload (too much information), low interest among actors and inappropriate language based on whom you are addressing (Cacciattolo, 2015). This study indicates a “catch-22” moment due to the mutually conflicting and simultaneous dependent elements in information assets, e.g. if you choose details, you risk losing the overview and vice-versa. Thus, improving the dialogues across and between actors are one area in need of more studies, e.g. questions to reflect on how communication about the rationale related to the core businesses could improve information classification. One approach could be to agree on basic knowledge exchange practices, for example drawing from knowledge management approaches for perspective making and perspective taking (Boland and Tenkasi, 1995). Another approach to assisting in the choice of granularity-decisions could be to investigate the issue through an information- and knowledge-centric perspective using a genre-based approach (Padyab, Päivärinta, and Harnesk, 2014; Yates and Orlikowski, 1992).

*Non-complete registry of information assets* means that there is no complete collection of identified assets. A registry of information assets is a way for organizations to keep track of what information they own and how it is valued and managed (Leming, 2015). Even though it is of value, a common problem within organizations is an incomplete or even lacking record of information assets (Bergström and Ahlfeldt, 2014). A complete registry, or at least a satisfying one, is seen as a fundamental part of good risk management (Leming, 2015). Part of the problem with maintaining an inventory is the scope, size and rate of internal and external change (Rees and Allen, 2008). Such changes can refer to the creation and removal of information. Naturally, the larger the organization, the more resource-intensive the task of keeping it up to date is. As the risk assessment aid protection of organizational assets based on what is in the registry, keeping an inventory alive is essential; without a complete risk registry, most risk management approaches will be less effective (Fenz *et al.*, 2014).

Data from informants show that keeping a registry of information assets up to date is a challenge; the study also highlights uses for a registry other than keeping up to date with the organizationally owned information. Informants reflected on the problem of incomplete registries:

First of all, it is important to value the information, but the first step is to make an inventory! Often times the inventory is not very well done, and that complicates things. All of a sudden, there is data you had no idea existed [...] – BD

The informant continues to explain the importance of understanding the organization’s assets and expands on the need for a registry. The informant explains that a registry is required to conduct the information classification properly and argues further that it is difficult to classify and value something you are unaware of. Additionally, the informant describes that the information security work starts with identifying, categorizing and making an inventory of information assets:

It all starts with the work connected to information classification. Sometimes the inventory is there, and at some organizations, it is not there at all. – SISC

One informant also explains an additional benefit of having an up-to-date inventory, namely, that it can be used as a means of communication between management and employees. Using it this way, the informant explains that everyone gets involved and can understand the value of the information they are working with. Consequently, raising security awareness in the organization. The informant says that updating the registry is a rare opportunity to discuss potential consequences of leakage of information and to share experiences of such events.

Analyzing the problem of a non-complete registry of information assets, when put into the context of practice, it can be found that keeping it up to date is resource demanding. New (unknown) information assets that appear later in the information classification put the actors into trouble. The challenge to keep the registries updated may relate to the allocation of resources but may also relate to an organization that accepts a high level of granularity. That is, such decisions may support one activity but may cause problems at a later stage. The additional benefit of updating the registry identified in this study, i.e. to use it to aid involvement and interactions between different roles, is an interesting approach that needs to be studied further.

*Actor subjectiveness* can be described as the idea that humans can have the same experience but different understandings of that experience (Thorburn and Stolz, 2020). Subjectiveness is often affected not only by external sources, such as culture, norms and similar factors, but also by an individual's awareness of social, economic and legal contexts (Kaarst-Brown and Thompson, 2015). Differing opinions on the correct value of a certain information asset is a common topic of competing arguments between actors. Subjective judgments in the classification activities can lead to the well-known problem of inconsistent classifications (Bergström and Åhlfeldt, 2014; Bergström et al., 2021; Fenz et al., 2014; Sajko et al., 2006), and this problem is often overlooked in practice and is under-researched.

In the investigation for this study, it was found that subjectiveness is indeed an issue. When asked about what challenges appear when conducting information classification activities several informants mention subjectiveness. One informant elaborates on the problem and explains that when a disagreement over a classification occurs, it is often followed by a lengthy discussion resulting in over-protecting assets. The informant explains:

[. . .] then you have to argue for your standpoint. As long as there is no documentation done that says a decision has been made there are a lot of discussions. We at IT who work with protecting this information are put into a difficult situation. This means that in most cases you put a higher level of protection than necessary just to be on the safe side. – IDPO

The informant continues to describe that the results of over-protection is higher costs, not just monetary but also in time. The informant gives examples, such as costs tied to upgrades of a system that is accepted to handle a higher level of protection will be higher, the update will be more extensive and simply more complex. Further, another informant mentions that a tool has been developed to get around the extensive discussions regarding different opinions about asset values:

It is very good to have a tool that contains questions, there won't be a lot of discussion and time can be spent on discussing other matters, not the classification itself [. . .] If the tools are configured well, you can save quite a lot of time when it comes to the classification as many hours can be spent on discussion if the group does not agree. – ISS2

The use of the tool has, according to the informant, not only saved them a lot of time and resources but also, in a way, reduced subjective judgment when deciding on the classification levels. The informant explained that the tool's content of requirements for information assets has made the classification process more effective. However, not all assets can be classified, and not all discussions are solved using the tool. The same informant mentions that information classification activities are a great way to connect with other departments as often, they are done cooperatively with other departments. As a result of different backgrounds between departments, the risk of misunderstandings and different interpretations of asset value is high, but the tool has assisted with better communication.

When analyzing the problem of actor subjectiveness in light of the practice, the consequence that it leads to lengthy discussions and argumentation becomes evident. Actor subjectiveness also leads to inconsistent classification. The empirical study points toward

over-protection being a typical solution to feeling safe when opposing arguments for an asset value are suggested. In response to subjectivity leading to lengthy discussions, one organization reduced the time spent on such discussions by using a self-developed tool. Subjectivity is viewed as a negative trait; however, different opinions are expressions of different experiences, and speaking them out allows for nuanced views of the information assets and their value. This study indicates that subjectiveness can, if organized and structured, become a benefit in information classification. Yet, lengthy discussions of every asset will not be beneficial, but allowing actors to express different arguments in some cases may provide a better understanding of the information classification problems and raise organizational security awareness.

*Discourse interpretation* is the action of interpreting someone's speech or piece of writing about a particular, usually serious, subject (Cambridge, 2022). As such, it is part of communication as a movement of information from a source through a channel to a destination (Arhin and Wiredu, 2018; Shannon, 1948). Information security is an interdepartmental effort rather than tied to only an IT department (Ahmad *et al.*, 2015). Thus, communication between departments is essential for the interdepartmental effort to be effective. Communicating guidelines, frameworks or manuals has proved to be problematic. Telling an employee within an organization, in writing or by voice, to read a security-guideline handbook does not necessarily mean that the employee has been communicated to (Richmond *et al.*, 2005). When communicating with others on, e.g. a departmental level, issues can appear as a cause of several factors, some tied to knowledge sharing and organizational communication. Common problems are low motivation and interest, inappropriate language, information overload, technological problems and insufficient non-verbal communication, thus causing problems with the interpretation of a particular discourse (Cacciattolo, 2015; Riege, 2005).

The study shows that discourse interpretation is both common and challenging. It is by informants deemed very important to be able to communicate between stakeholders; however, it is also expressed to be difficult in a variety of ways. One informant mentions that part of the communication issues they experience is a result of several factors, like the language used, this involves jargon, e.g. department-specific terms and interpretations, a lack of understanding of the context and difficulties of understanding each other when using only digital support. It is, according to several informants, important to ask questions in a way that can be easily understood and interpreted. Further, several informants stated that the terms used are of great importance for better understanding the topics at hand:

You write statements and guidelines with a language that can be very difficult to understand and use terms that employees simply do not use. – ISSC2

Communication between departments is difficult, especially when you use the same terms but mean different things. There is confusion in the terms used. This information is secret, is it secret or very secret? You have to understand the differences. It can be the result of a cultural, competence or an “in a hurry” barrier. – OO

We prefer to solve everything digitally, it is little effort and reaches a large amount of people [. . .] but [. . .] It is difficult to formulate in writing so that everyone can understand, the co-workers will understand the message in different ways. – IDPO

The above excerpts highlight problems encountered by informants in the information classification but are also challenges regarding communication in general. In essence, the problems are grounded on the use of different expressions and terms, which mean different things to different roles and departments.

According to many informants, the language used is an influencing factor for whether there would be an understanding of each other when communicating about information classification activities. Plain explanations to also understand the context is something that was perceived as supporting communication. However, there can be regulations in public sector organizations that force actors to apply a certain type of language, for examples using words that are seldom used by the public. Often, confusion and misunderstandings occur because a term is interpreted in different ways, depending on how it is established as a jargon within a certain knowledge domain.

*Difficult to adapt guidelines* is another categorized problem (Bayuk, 2010; Bergström *et al.*, 2021; Park *et al.*, 2010). Standards such as ISO/IEC 27002 (ISO Central Secretary, 2017) are a commonly used base for organizations to create guidelines. Standards, though, describe the activities holistically, meaning it is not a blueprint for how to apply them in organizations. One example of a problem is the difficulty of creating classification schemes that follow organizational requirements while still being usable (Bergström, 2020; Fibikova and Müller, 2011; Ghernaoui-Helie *et al.*, 2011). It is also concluded that there is a gap between formal and actual processes in information security management, which information classification is part of (Bergström *et al.*, 2021). Adopting best-practice into organizations has been stated as being difficult, not necessarily in the writing of policies but in implementing it in a way that is sensitive to the context of the organization and its local ways of working (Niemimaa and Niemimaa, 2017).

The expressions from informants indicate that organizations struggle to interpret and adapt best-practice guidelines. Both internal and external guidelines regarding information classification are according to informants difficult to interpret. One informant speaks about requirements for how to write descriptions and guidelines:

In the world of public sector, we write regulations and guidelines in a way that is difficult to interpret and we use terms and phrases that normal persons simply does not use. – ISS2

Informants having the experience writing guidelines, such as the definitions of different security levels that should later be used as a reference for other actors when conducting classification activities, express the difficulty:

You get into discussions where you look at consequences in terms of physical, psychological and financial. Will this asset be in what our model (classification scheme) is a limited value or high value? Where do we draw the lines? That is often the main discussion [ . . . ] Often times the differences between levels are quite vague and it is challenging to describe the levels in a clear manner. – ISS2

Addressing the same issue, another informant states that one problem is the formulation, description and definitions of those levels and the terms used in them. Using terms such as “great effect” is very interpretable and difficult to describe. According to the informant, this often leads to classifications that are one step above necessary as there is a fear of classifying assets too low. This reflection gets confirmed by another informant that explains that internal documents to guide the classification activities exist, but they are difficult to use and vague in their descriptions. This results in guesswork to reach a classification. The informant understands that an organization cannot describe everything in documents but describes the problem of interpretations:

You can't explain everything, but you can help by writing easy generic matrices. I sometimes see explanations of classifications to be 'results in high level of monetary loss'. What is high? And what is low? You have to help out with these things. – SISC

Giving examples are, by several informants, stated to be helpful, but, if too detailed, actors will try to replicate the examples instead of using them as guidelines for the classification. One informant concludes that while it is important to use examples for actors unfamiliar with the process, it is also important not to make examples too specific.

The problems with adapting guidelines are analyzed in this study as related to those being too complicated or general. Even though the informants are aware of the necessity to transform guidelines to the organization's requirements, they express a wish of them being more specific. The informants also describe the paradox of using examples: they cannot be too specified, but not too general either. Further studies of interest could include how to provide good and usable examples.

## 5. Concluding on further research

This paper presents five problems identified related to information classification and sheds light on how those problems are experienced in practice. The problems were as follows: *deciding on a level of granularity, non-complete registry of assets, actor subjectiveness, discourse interpretation and difficult to adapt guidelines*. Empirical data from two types of organizations, i.e. public and private, was collected to shed light on the practice in relation to the problems, thus addressing the purpose which was to identify future research directions. Solving the problems within information classification is no simple task. However, as the problems that have been presented here indicate, research beyond technical challenges can help organizations to classify their assets. This paper, thus suggests a number of directions for further studies, namely:

- Research addressing the problems of choosing a level of granularity could involve perspective-making and perspective-taking (Boland and Tenkasi, 1995), thereby highlighting for example communication practices. Related to the problem it would be interesting to investigate communicative genres to identify critical information (Päivärinta, 2001).
- The problem of having a non-complete registry of assets could be a base for studies of how different roles in an organization, such as managers and developers, apply different lenses of worldviews (Checkland, 2000) that guide communication.
- Research targeting if and how actor subjectiveness can be organized and structured to allow informed decision-making would benefit the classification work. Such studies could alter how experiences are perceived as a negative trait and turn it into a base of best practices.
- Investigations addressing the problem of discourse interpretation could focus the work done in groups and workshops, for example including interpersonal response behaviour in teams (Sonalkar *et al.*, 2012). Additionally, further investigation on how to define, not absolute, but operative terms in multi-departmental organizations is of interest to tackle this problem.
- The problem of difficult to adapt guidelines could be a base for user-oriented research focusing on how to formulate functional guidelines that meet realistic behaviour in the workplaces. Behaviour design or nudging (Thaler and Sunstein, 2009), for example, could add to the understanding of how guidelines could be adapted to organizational behaviour.

## References

- Adams, W.C. (2015), "Conducting semi-structured interviews", *Handbook of Practical Program Evaluation*, pp. 492-505.
- Agrawal, V. (2017), "A framework for the information classification in ISO 27005 standard", *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, New York, NY, IEEE, pp. 264-269, ISBN: 978-1-5090-6644-5, doi: [10.1109/CSCloud.2017.13](https://doi.org/10.1109/CSCloud.2017.13).

- Ahmad, A., Maynard, S.B. and Shanks, G. (2015), "A case analysis of information systems and security incident responses", *International Journal of Information Management*, Vol. 35 No. 6, pp. 717-723.
- Alhojailan, M.I. (2012), "Thematic analysis: a critical review of its process and evaluation", *West East Journal of Social Sciences*, Vol. 1 No. 1, pp. 39-47.
- Anthony (Tony) Cox, L. Jr (2008), "What's wrong with risk matrices?", *Risk Analysis: An International Journal*, Vol. 28 No. 2, pp. 497-512.
- Arhin, K. and Wiredu, G.O. (2018), "An organizational communication approach to information security", *The African Journal of Information Systems*, Vol. 10 No. 4, p. 1.
- Bayuk, J.L. (2010), "The utility of security standards", *44th Annual 2010 IEEE International Carnahan Conference on Security Technology*, pp. 1-6, doi: [10.1109/CCST.2010.5678676](https://doi.org/10.1109/CCST.2010.5678676).
- Bergquist, J.-H., Tinet, S. and Gao, S. (2021), "An information classification model for public sector organizations in Sweden: a case study of a Swedish municipality", *Information and Computer Security*, pp. 2056-4961, doi: [10.1108/ICS-03-2021-0032](https://doi.org/10.1108/ICS-03-2021-0032).
- Bergström, E. (2020), "Supporting information security management: developing a method for information classification", PhD thesis. University of Skövde.
- Bergström, E. and Åhlfeldt, R.-M. (2014), "Information classification issues", *Secure IT Systems*, in Bernsmed, K. and Fischer-Hübner, S. (Eds), Springer International Publishing, Cham, Vol. 8788, pp. 27-41, ISBN: 978-3-319-11598-6 978-3-319-11599-3, doi: [10.1007/978-3-319-11599-3\\_2](https://doi.org/10.1007/978-3-319-11599-3_2).
- Bergström, E. and Anteryd, F. (2018), "Information classification policies: an exploratory investigation", p. 15.
- Bergström, E., Karlsson, F. and Åhlfeldt, R.-M. (2021), "Developing an information classification method", *Information and Computer Security*, Vol. 29 No. 2, pp. 209-239, ISSN: 2056-4961, 2056-4961, doi: [10.1108/ICS-07-2020-0110](https://doi.org/10.1108/ICS-07-2020-0110).
- Bergström, E., Lundgren, M. and Ericson, Å. (2019), "Revisiting information security risk management challenges: a practice perspective", *Security Risk Management Challenges: A Practice Perspective*, Information & Computer Security.
- Boland, R.J., Jr. and Tenkasi, R.V. (1995), "Perspective making and perspective taking in communities of knowing", *Organization Science*, Vol. 6 No. 4, pp. 350-372.
- Brown, J.S. and Duguid, P. (1991), "Organizational learning and communities-of-practice: toward a unified view of working, learning, and innovation", *Organization Science*, Vol. 2 No. 1, pp. 40-57.
- Burnard, P. (1991), "A method of analysing interview transcripts in qualitative research", *Nurse Education Today*, Vol. 11 No. 6, pp. 461-466.
- Cacciattolo, K. (2015), "Defining organisational communication", *European Scientific Journal*, Vol. 11 No. 20.
- Cambridge, D. (2022), "Meaning of discourse in english", available at: <https://dictionary.cambridge.org/dictionary/english/discourse>
- Checkland, P. (2000), *Soft Systems Methodology: A Thirty Year Retrospective*, Systems Research and Behavioral Science.
- Clarke, V., Braun, V. and Hayfield, N. (2015), "Thematic analysis", *Qualitative Psychology: A Practical Guide to Research Methods*, pp. 222-248.
- Everett, C. (2011), "Building solid foundations: the case for data classification", *Computer Fraud and Security*, Vol. 2011 No. 6, pp. 5-8.
- Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. (2014), "Current challenges in information security risk management", *Information Management and Computer Security*, Vol. 22 No. 5, pp. 410-430, doi: [10.1108/IMCS-07-2013-0053](https://doi.org/10.1108/IMCS-07-2013-0053), 0968-5227.
- Fibikova, L. and Müller, R. (2011), "A simplified approach for classifying applications", *ISSE 2010 Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2010 Conference*, in Pohlmann, N., Reimer, H. and Schneider, W. (Eds), Wiesbaden, Vieweg+Teubner, pp. 39-49. ISBN: 978-3-8348-9788-6, doi: [10.1007/978-3-8348-9788-6\\_4](https://doi.org/10.1007/978-3-8348-9788-6_4).

- Fontana, A. and Frey, J.H., *et al.* (2000), "The interview: from structured questions to negotiated text", *Handbook of Qualitative Research*, Vol. 2 No. 6, pp. 645-672.
- Fossey, E., Harvey, C., McDermott, F. and Davidson, L. (2002), "Understanding and evaluating qualitative research", *Australian and New Zealand Journal of Psychiatry*, Vol. 36 No. 6, pp. 717-732.
- Gerber, M. and Von Solms, R. (2005), "Management of risk in the information age", *Computers and Security*, Vol. 24 No. 1, pp. 16-30.
- Ghernaoui-Helie, S., Simms, D. and Tashi, I. (2011), "Protecting information in a connected world: a question of security and of confidence in security", *2011 14th International Conference on Network-Based Information Systems, IEEE*, pp. 208-212.
- Halcomb, E.J. and Davidson, P.M. (2006), "Is verbatim transcription of interview data always necessary?", *Applied Nursing Research*, Vol. 19 No. 1, pp. 38-42.
- Hubbard, D.W. (2020), *The Failure of Risk Management: Why It's Broken and How to Fix It*, John Wiley and Sons.
- ISO Central Secretary (2017), *Information Technology – Security Techniques – Code of Practice for Information Security Controls*, Standard ISO/IEC 27002:2017 International Organization for Standardization, Geneva, CH.
- ISO Central Secretary (2018), *Information Technology – Security Techniques – Information Security Management, Systems – Overview and Vocabulary*, Standard ISO/IEC 27000:2018 International Organization for Standardization, Geneva, CH, available at: [www.iso.org/standard/73906.html](http://www.iso.org/standard/73906.html)
- Kaarst-Brown, M.L. and Thompson, E.D. (2015), "Cracks in the security foundation: employee judgments about information sensitivity", *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research. SIGMIS-CPR '15: 2015 Computers and People Research Conference*. Newport Beach CA USA, ACM, pp. 145-151, ISBN: 978-1-4503-3557-7, doi: [10.1145/2751957.2751977](https://doi.org/10.1145/2751957.2751977), available at: <https://dl.acm.org/doi/10.1145/2751957.2751977> (visited on 01/31/2022).
- Kaspersky (2021), "KSB\_statistics\_2020\_en.Pdf", available at: [https://go.kaspersky.com/rs/802-IJN-240/images/KSB%5C\\_statistics%5C\\_2020%5C\\_en.pdf](https://go.kaspersky.com/rs/802-IJN-240/images/KSB%5C_statistics%5C_2020%5C_en.pdf)
- Leming, R. (2015), "Why Is information the elephant asset? An answer to this question and a strategy for information asset management", *Business Information Review*, Vol. 32 No. 4, pp. 212-219, ISSN: 0266-3821, doi: [10.1177/0266382115616301](https://doi.org/10.1177/0266382115616301).
- Mason, J. (2017), *Qualitative Researching*, SAGE Publications, London.
- Niemimaa, E. and Niemimaa, M. (2017), "Information systems security policy implementation in practice: from best practices to situated practices", *European Journal of Information Systems*, Vol. 26 No. 1, pp. 1-20.
- Padyab, A., Päivärinta, T. and Harnesk, D. (2014), "Genre-based approach to assessing information and knowledge security risks", *International Journal of Knowledge Management*, Vol. 10, pp. 13-27, doi: [10.4018/ijkm.2014040102](https://doi.org/10.4018/ijkm.2014040102).
- Päivärinta, T. (2001), "The concept of genre within the critical approach to information systems development", *Information and Organization*, Vol. 11 No. 3, pp. 207-234.
- Park, W.-S., Seo, S.-W., Son, S.-S., Lee, M.-J., Kim, S.-H., Choi, E.-M., Bang, J.-E., Kim, Y.-E. and Kim, O.-N. (2010), "Analysis of information security management systems at 5 domestic hospitals with more than 500 beds", *Healthcare Informatics Research*, Vol. 16 No. 2, pp. 89-99, doi: [10.4258/hir.2010.16.2.89](https://doi.org/10.4258/hir.2010.16.2.89), ISSN: 2093-369X.
- Pedersen, B., Delmar, C., Falkmer, U. and Grønkvær, M. (2016), "Bridging the gap between interviewer and interviewee: an interview guide for individual interviews by means of a focus group", *Scandinavian Journal of Caring Sciences*, Vol. 30 No. 3, pp. 631-638, ISSN: 1471-6712, doi: [10.1111/scs.12280](https://doi.org/10.1111/scs.12280).
- Rees, J. and Allen, J. (2008), "The state of risk assessment practices in information security: an exploratory investigation", *Journal of Organizational Computing and Electronic Commerce*, Vol. 18 No. 4, pp. 255-277, ISSN: 1091-9392, doi: [10.1080/10919390802421242](https://doi.org/10.1080/10919390802421242), available at: [www.tandfonline.com/doi/abs/10.1080/10919390802421242](http://www.tandfonline.com/doi/abs/10.1080/10919390802421242) (visited on 01/31/2022).

- Richmond, V.P., McCroskey, J.C. and McCroskey, L.L. (2005), "Organizational communication for survival: making work", *Work*, Vol. 4, Allyn and Bacon.
- Riege, A. (2005), "Three-dozen knowledge-sharing barriers managers must consider", *Journal of Knowledge Management*, Vol. 9 No. 3, pp. 18-35.
- Sajko, M., Rabuzin, K. and Baca, M. (2006), "How to calculate information value for effective security risk assessment", *Journal of Information and Organizational Sciences*, Vol. 30 No. 2, pp. 263-278.
- Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. (2016), "Taxonomy of information security risk assessment (ISRA)", *Computers and Security*, Vol. 57, pp. 14-30.
- Shannon, C.E. (1948), "A mathematical theory of communication", *The Bell System Technical Journal*, Vol. 27 No. 3, pp. 379-423.
- Shedden, P., Ahmad, A., Smith, W., Tscherning, H. and Scheepers, R. (2016), "Asset identification in information security risk assessment: a business practice approach", *Communications of the Association for Information Systems*, Vol. 39, pp. 297-320, ISSN: 15293181, doi: [10.17705/1CAIS.03915](https://doi.org/10.17705/1CAIS.03915), available at: <http://aisel.aisnet.org/cais/vol39/iss1/15/> (visited on 01/31/2022).
- Siponen, M. (2006), "Information security standards focus on the existence of process, not its content", *Communications of the ACM*, Vol. 49 No. 8, pp. 97-100.
- Sonalkar, N.S., Mabogunje, A.O. and Leifer, L.J. (2012), "A visual representation to characterize moment to moment concept generation in design teams", *DS 73-1 Proceedings of the 2nd International Conference on Design Creativity Volume 1*.
- Stine, K., Kissel, R., Barker, W., Lee, A. and Fahlsing, J. (2008), *Guide for Mapping Types of Information and Information Systems to Security Categories: appendices*, Tech. rep. National Institute of Standards and Technology.
- Tankard, C. (2015), "Data classification—the foundation of information security", *Network Security*, Vol. 2015 No. 5, pp. 8-11.
- Thaler, R.H. and Sunstein, C.R. (2009), "NUDGE: improving decisions about health, wealth, and happiness", Penguin.
- Thorburn, M. and Stolz, S.A. (2020), "Understanding experience better in educational contexts: the phenomenology of embodied subjectivity", *Cambridge Journal of Education*, Vol. 50 No. 1, pp. 95-105.
- Veritas (2015), "The databerg report: see what others don't", available at: [http://info.veritas.com/databerg\\_report](http://info.veritas.com/databerg_report)
- Wangen, G. and Snekenes, E. (2013), "A taxonomy of challenges in information security risk management", *Proceeding of Norwegian Information Security Conference/Norsk informasjonsikkerhetskonferanse-NISK 2013-Stavanger*, 18th-20th November 2013, Akademika Forlag.
- Webb, J., Maynard, S., Ahmad, A. and Shanks, G. (2014), "Information security risk management: an intelligence-driven approach", *Australasian Journal of Information Systems*, Vol. 18 No. 3, pp. 1449-8618, doi: [10.3127/ajis.v18i3.1096](https://doi.org/10.3127/ajis.v18i3.1096).
- Yates, J. and Orlikowski, W.J. (1992), "Genres of organizational communication: a structural approach to studying communication and media", Vol. 29.

**Corresponding author**

Simon Andersson can be contacted at: [simon.andersson@ltu.se](mailto:simon.andersson@ltu.se)

---

For instructions on how to order reprints of this article, please visit our website:

[www.emeraldgrouppublishing.com/licensing/reprints.htm](http://www.emeraldgrouppublishing.com/licensing/reprints.htm)

Or contact us for further details: [permissions@emeraldinsight.com](mailto:permissions@emeraldinsight.com)





# To Risk Analyse, or Not to Risk Analyse: That's the Question

Erik Bergström<sup>1</sup>✉, Simon Andersson<sup>2</sup>, and Martin Lundgren<sup>3</sup>

<sup>1</sup> School of Engineering, Jönköping University, Jönköping, Sweden  
erik.bergstrom@ju.se

<sup>2</sup> Computer Science, Electrical and Space Engineering, Luleå University of  
Technology, Luleå, Sweden

<sup>3</sup> School of Informatics, University of Skövde, Skövde, Sweden

**Abstract.** Risk analysis is a key activity for organisations that are looking to protect their valuable information assets against threats, such as malicious actors. It is one of the essential parts of risk management and is used to justify and prioritise what assets require the attention of which potential security controls. Risk management, and more specifically, risk analysis, is an activity that should be performed continuously. However, recent studies indicate that this is not always the case. As such, this paper investigates risk analysis as it is performed in practice in different Swedish public sector organisations. The results are based on semi-structured interviews with 17 senior security experts, an analysis of standards, and a national method support aiming to fill the gap between standard and practice. The results are presented in three themes: how, when and why risk analysis is performed. Of note, we identify that there is an issue of overlooking specific assets or systems when establishing an organisational-wide risk profile and a general recognition of the necessity for risk analysis, albeit not always in alignment with a classic risk analysis.

**Keywords:** Risk analysis · Information security · Cybersecurity

## 1 Introduction

In short, information security can be described in a sequence where valuable information is identified and valued as assets on one end and where security controls that ensure the appropriate levels of confidentiality, integrity, and availability of those assets are selected and implemented on the other. What guides this linkage between the information assets and the security controls has been a target of research and standards alike. Perhaps the most common approach is through the use of Information Security Risk Management (ISRM), in which security controls are selected by identifying and prioritising risks towards an organisation's information assets by applying a risk analysis [10]. The result of the risk analysis is used to justify and select what techniques, i.e., security controls, should be implemented to treat the risks adequately.

© IFIP International Federation for Information Processing 2025

Published by Springer Nature Switzerland AG 2025

N. Clarke and S. Furnell (Eds.): HAISA 2024, IFIP AICT 721, pp. 107–119, 2025.

[https://doi.org/10.1007/978-3-031-72559-3\\_8](https://doi.org/10.1007/978-3-031-72559-3_8)

Risk analysis is described as the activity in which the level of risk is established [10]. The level of risk can be assessed in various ways but is often based on the likelihood of a threat (e.g., an undesired event) occurring by exploiting a vulnerability (e.g., due to a lack of a security control) and the impact that a threat would have (e.g., monetary loss) as a result. In other words, the level of risk is the product of the likelihood and impact. The level of risk can then be used to compute a cost-benefit analysis of selecting security controls [24]. A common alternative to this approach is the Annual Loss Expectancy (ALE), which uses the foundations of expected utility theory to provide a more accurate cost assessment [26]. However, both approaches and others like them, rely on access to exhaustive threat probability data [13], which is difficult to obtain in practice [26, 28]. Therefore, moving away from basing the risk analysis on quantitative probability and cost-benefit, a qualitative analysis often bases its assessment on a risk matrix instead. Here, the level of risk is ranked based on a scale (e.g., low, medium, high). Similarly, the likelihood and impact are typically also ranked by a similar scale [20]. All possible combinations of the likelihood and impact are outlined in a table (the risk matrix) and assigned a level of risk. However, qualitative risk analyses have been criticised for not being particularly accurate since they are based on experience, the judgment of the professional, and ‘what-if’ scenarios [13].

While risk analysis helps prioritise and justify the extent to which an asset should be protected, what controls to select often depends on the type of information. For example, could security controls for an asset be avoided completely if the level of risk falls within what is considered to be acceptable? While this might make sense from an economic perspective, other aspects, such as rules and regulations (e.g., GDPR and NIS in the European Union), and industry-specific guidelines (e.g., PCI-DSS and CA/Browser Forum) often list sets of security controls required for certain types of information. What role, then, does risk analysis play if the security controls can be selected from pre-defined sets (or lists) of controls based on the information type?

Relying solely on selecting security controls from a list of options has received critique as it limits the view of what threats are actually facing the organisation [7, 22]. Thereby focusing more on what controls can be implemented, rather than what controls need to be [7, 8]. Yet, as Tejay and Goel [27] wrote in their editorial piece; “*While we teach our students nuances of assessing organisational cybersecurity through a lens of classic risk analysis where assets, vulnerabilities and threats are used to compute the potential exposure to the firms, then controls are determined by rigorous cost-benefit analysis. In reality, a lack of data and the complexity of analysis drive security assessments for compliance via check-lists*” [27, p. 1]. Indeed, a recent study found that some ISRM practitioners use information types as an indicator for selecting security controls, rather than performing a classic risk analysis [12]. Furthermore, recent standards have alluded to a similar approach. For example, in NIST SP 800-37 [18], pre-defined sets of controls are assembled to address the protection needs of information based on its impact, and where classic risk analysis are performed in certain cases, such as in highly specialised environments.

Over two decades ago, Broderick [5] put forth the question of when information security risks should be managed. The accepted dogma of today is that ISRM should be continuous [10]. Managing risks is not something that is done once, but repeated on an ongoing basis to ensure relevant security of the organisation's information assets [20]. However, as indicated by recent studies and standards, this is not always the case. Therefore, adding to Broderick's [5] early work, this study sets out to study the linkage between the information assets and the security controls in practice. More specifically, this study explores when risk analysis is conducted, how it is performed, and why.

The remainder of this study is outlined as follows. The next section introduces the theory of risk analysis, which is followed by a brief presentation of our research approach. In Sect. 4, we introduce our results, i.e., risk analysis in practice. Finally, the last section presents our conclusions and future work.

## 2 Risk Analysis in Theory

A systematic approach to ISRM has long been described as the very cornerstone in information security [3]. While the exact steps and names differ between ISRM processes, they typically gravitate around three common activities, which are often collectively referred to as risk assessment: asset valuation, risk analysis, and risk treatment. In the risk assessment, the output from one activity typically serves as the input for the next. Take for example the following three common industry risk management processes [23]: NIST SP 800-30 [17], ISO/IEC 27005 [10], and OCTAVE Allegro [6]. The assessment phase in each of these three processes starts by identifying organisational information assets (tangible and intangible), and their criticality to the organisation is assessed. Knowing what information is of value to the organisation, the next step is to identify what can pose a threat to these assets' confidentiality, integrity, and availability, along with ways such threats could become a reality (usually referred to as vulnerabilities), the probability of it happening, and the potential impact thereof. Based on the result of the two previous activities, a rational decision can be made for how to best (given the available resources) address the threats and/or vulnerabilities that constitute the risk [6, 10, 17, 23].

While the risk analysis helps prioritise and justify the amount and type of security controls to implement, it is up to the ISRM practitioner to identify them. To help in this regard, there are standards which provide an extensive list of security controls to be considered, such as ISO 27001 (Appendix A) [9] and NIST 800-53 (Chapter Three) [19]. However, the selection of security controls still lies with the practitioner, which can be a challenging task even against the backdrop of a risk analysis [16] and a standardised list of available options. While it is acknowledged that choosing the most appropriate security controls (in terms of efficiently and cost-effectively assuring the confidentiality, integrity, and availability of the information assets) requires good risk insight, the NIST Risk Management Framework (RMF) [18] define two distinct approaches for selecting controls. These are the baseline control selection approach and the organisation-generated control selection approach. The latter relies on the organisation using

its own ISRM process to select controls (such as by applying a classic risk analysis) and is recommended for highly specialised systems (e.g., weapons or medical devices). As an alternative, the former of the two approaches were introduced to help organisations protect their information assets by sets of federally mandated security controls [16]. Rather than basing the selection on risk analysis, the baseline control selection approach in RMF offers a set of appropriate security controls based on an information asset valuation (what is referred to as categorisation) [18]. By determining the level of confidentiality, integrity, and availability of the information asset as having either low, moderate, or high impact on the organisation’s missions or business operations, appropriate security controls can be selected from a pre-defined baseline, as defined in NIST SP 800-53B [16].

### 3 Research Approach

This explorative paper investigates the how, when, and why of risk analysis in practice. To be able to characterise these aspects further, we set out to collect more data. In this case, we opted to interview senior information security experts in the Swedish public sector who are implementing information security in their respective organisations. In addition to these experts, we have collected documents from the site [informationssakerhet.se](http://informationssakerhet.se) [[informationsecurity.se](http://informationsecurity.se)], which offers method support, foremost intended for Swedish authorities, on how to work systematically with information security [25] and complemented these documents with interviews with some of the contributors to the site to find underlying intentions. Document studies serve to complement the interview data by providing a contextualisation, and they also shed light on how Swedish organisations could interpret ISO/IEC 27001 [9]. Finally, the combination of interviews and document studies allows for data triangulation and mitigates bias.

#### 3.1 Data Collection

Semi-structured interviews were chosen because of the study’s exploratory nature and the opportunity they offer to explore with follow-up questions [1]. An interview guide was constructed where we focused on a set of questions centred around three topics: the valuation result (as it is the input to risk analysis), the value of performing valuation and risk analysis, and the relationship between valuation and risk. The interviews started by exploring the first two topics to not impose any beliefs from the authors. A typical question from the first two topics was ‘What contextual information is important when performing a valuation,’ and from the third topic, ‘What’s your view on the relationship.’ In total, we performed 16 interviews with 17 senior security experts (who held positions such as Chief Information Security Officer (CISO), information security specialist, or similar). Fifteen of the respondents work in the Swedish public sector (in various government agencies with operational information security tasks), while the last two were contributors to the [informationssakerhet.se](http://informationssakerhet.se) site (and employed in the public sector). The interviews were performed online via conferencing software and lasted approximately 1–1.5 h each. The interviews were transcribed and

checked and encompass a total of 325 pages. An overview of the respondents can be seen in Table 1.

**Table 1.** An overview of the respondents, and the organisational size (divided into intervals to ensure anonymity for the respondents).

Respondent	Role in the organisation	Organisational size
1	Administrative Manager, IT	1001–2500
2	Security Coordinator	501–1000
3	Head of Division, IT	0–500
4	CISO	2501–5000
5	CISO	0–500
6	Information Security Specialist	501–1000
7	Information Security Specialist	5000+
8	CISO	0–500
9	CISO	5000+
10	Information Security Specialist	5000+
11	CISO	1001–2500
12	CISO	5000+
13	IT Security Manager	1001–2500
14	CISO	501–1000
15	CISO	1001–2500
16	Information Security Specialist	1001–2500
17	Information Security Specialist	1001–2500

In addition to the interview material, we used what is referred to as method support aimed at helping bridge the gap between ISO/IEC 27001 [9] and organisations seeking to implement the standard. Seven Swedish government agencies (The Swedish Civil Contingencies Agency, The Swedish Civil Contingencies Agency, The National Defence Radio Establishment, The Swedish Defence Materiel Administration, The Swedish Post and Telecom Authority, The Swedish Security Service, and The Swedish Police Authority) have jointly created the site [informationssakerhet.se](http://informationssakerhet.se) [25]. The site is aimed at supporting those who work with information security in an organisation to work more systematically. It also takes on an overall perspective, introduces all activities for any type of organisation (size of area), and supports both novices and more experienced professionals [25].

The method support offered by [informationssakerhet.se](http://informationssakerhet.se) contains four main parts or phases: (1) identify and analyse, (2) design, (3) use, and (4) follow up and improve. In addition to these phases, is there an introductory support explaining overall goals and how to use the phase. Each of the main phases

consists of a description that explicates the phase, and each phase also comes with a toolbox that consists of a set of templates that can be the basis for creating a risk matrix, a valuation matrix etc. It was launched in 2011 and has been revised several times since then. The method support encompasses 104 pages plus the toolbox.

### 3.2 Analysis

For the analysis, we adhered to the coding guidelines from Saldaña [21] that highlight the necessity of a two-cycle coding procedure. Structural coding was used for the first cycle of coding, which is especially appropriate when it is the data is from semi-structured interviews [21]. Most of the structural coding was done by two of the authors, who also created the initial categorisation version that took relationships, similarities, and differences into account [21]. Following this first stage, all authors worked together to re-code and re-classify. A synthesis during the re-coding and re-categorising resulted in the development of three themes, *how*, *when* and *why* risk analysis is performed. The material collected from informationsakerhet.se was analysed using the recommendations in [4]. Document analysis is a systematic procedure for reviewing documents [4], and in this case, we looked for evidence describing primarily the transition from valuation, how the risk analysis is portrayed and the flow between activities. This data was then coded using the themes previously identified.

## 4 Risk Analysis in Practice

In this section, the presentation of the findings has been divided into three sub-subsections: how, when, and why it (i.e., risk analysis) is done. Each subsection presents the analysis of the ISO/IEC 27001 standard [9], the informationsakerhet.se method support (hereafter simply referred to as ‘the method support’) [25], and the collected interview data.

### 4.1 How Is It Done?

It is well-known that turning standard into practice is a challenging task because activities are described in a “*general and universal manner without explaining how the practice could be accomplished in any particular organization*” [15, p.6]. The information security field has seen many papers and doctoral theses aiming to fill this gap between standard and practice [2, 11, 14]. In addition, method support, such as offered by informationsakerhet.se, has become quite extensive, particularly regarding how to perform a risk analysis [25]. The method support gives a detailed description of how to perform the activity concerning, for example, group composition, time constraints, how to develop scales and other aspects. The method support also explicates the need for several types of risk analyses on different levels, i.e. to establish a risk profile for organisation-wide information security risks and, at the same time, perform risk analysis

on individual systems or assets. Both valuation and risk analysis are recommended to be performed as a workshop activity, and each is recommended to take 3–4 h plus preparation time. It is acknowledged that many of the risks and threats are shared between systems and even between organisations, and they can be described in general terms. The method support also describes different risk analysis approaches, such as quantitative and qualitative, but recommends the qualitative approach. However, such descriptions are inclusive and could, therefore, be perceived as complex, thus instilling some doubt among readers as to which approach to choose, as opposed to describing and recommending one approach.

From the interviews, it was common amongst the respondents to conduct risk analyses in a sporadic rather than a structured “by-the-book” way. Respondent 3 explained that there is a direct connection between the results of the valuation and security controls and that the risk analysis is done in the event of a larger change. However, the same respondent also made it clear that risk analysis is not included in the otherwise systematic way of working with information security; instead, risk analysis tends to be conducted based on some trigger, such as a larger change to the information itself, the systems it resides on, or similar.

Respondent 3 explained that they are in the process of conducting a larger, organisation-wide risk analysis in order to get an overview, as they find that to be of value. More specific risk analyses will be done later on as needed, providing more details for specific assets.

Respondent 12 explained the flow from valuation to risk analysis. In their case, they start with valuation and explained that they isolate the cost of potential consequence, which is later on used in the risk analysis as input for the impact level. That is to say, the scale of valuation levels is mirrored in the risk analysis, as they have found that it is easy to simply transfer the valuation level to the risk analysis. They then identify risks and conduct the risk analysis. Notably, they do the risk analysis at a system level, and it is not tied to specific assets. It is explained that they wish to do it at an asset level but that they are missing people and resources. Hence, decreasing the granularity of the asset identification and valuation, abstracting assets to that of the systems they reside on, makes the task more efficient.

It was noted by respondent 11 that the valuation acts as a “mini-risk analysis” and that it decides whether a more comprehensive risk analysis is necessary or not. It is explained that the results of the valuation are an understanding of the asset, support for the owner of the information, and necessary security controls that should be implemented. This is based on a small gap analysis that identifies a “current” and “wished for” state.

To sum up, there is a risk that organisations that establish a risk profile for organisation-wide information security risks believe they are close enough or even think that they can omit the risk analysis on individual systems or assets because of the risk profile. This, despite that the method support explicitly states: *[a]nother disadvantage may be that businesses believe that the risk profile of the organisation is sufficient when choosing security controls and that*

*they, therefore, do not need to perform additional risk analyses for their parts. However, this is never the case [25].*

## 4.2 When Is It Done?

There are some ambiguities in the method support regarding when the risk analysis should be performed. Several passages in the method support describing that it should be performed in a more generic way, for example:

*The results of the valuation, together with the risk analysis, provide the basis for selecting adequate security controls for the information. [25], The selection of security controls is based on the valuation result and the risks identified in the risk analysis. [25], and Risk analyses also need to be carried out in connection with valuation to determine which security controls need to be implemented [25].*

There are also some mentions of a more sequential relationship between valuation and risk analysis, for example:

*In order to achieve the purpose of valuation (...) you need to carry out a risk analysis after the valuation and then implement adequate security controls. [25], and The valuation is also the input to the risk analysis that determines the protection needs of the information [25].*

In practice, respondents tend to use risk analysis in different stages of their information security work. Several times, it is mentioned that both valuation and risk analysis are good tools for organisational analysis. For example, respondent 17 argued that understanding risks is part of getting to know your organisation, and as such, they find it important. In such cases, a larger, more extensive risk analysis is done of the whole organisation, and then more specific analyses of specific assets later on. The two types of analyses are explained to complement each other. Respondent 5 mentioned that they had established an organisational-wide risk profile. Following that, smaller, more specific risk analyses that are connected to specific systems can be conducted, as the organisational risk profile is expected to have some lack of details compared to the more specific analyses.

Similarly, respondent 4 explained that they conduct their risk analysis when it is deemed needed, such as when they have something of great importance in a system. In those situations, a risk analysis is used to ensure that there is enough protection in the corresponding system. Likewise, respondent 11 explained that they redo a risk analysis if assets are moved to a new environment (e.g., from on-premise to cloud). It is clear that from an overall process perspective, there are different approaches to when the risk analysis is supposed to be performed and that there is no specific right or wrong. Like most other activities related to information security, experience is key, and the lack of a clear, explicit relationship between the activities may inhibit the decision to perform the analysis.

There might also be an issue related to what a risk-based approach entails in practice. ISO/IEC 27000 is based on a risk-based approach, and all the recommended security controls aim to decrease or eliminate risks, unlike other management system standards (e.g. quality management, (ISO 9001), and environmental management (ISO 14001)) [25]. There are some indications in the interview data that since everything is risk-based, the risk analysis itself can be seen as redundant, especially if the security controls are a consequence of a valuation.

### 4.3 Why Is It Done?

Both the standards and the method support provide a clear motivation as to why we need to perform risk analysis. Also, there are several ways to perform the analysis, which can have different aims (i.e. risk profile, etc.), and similarly, such approaches are well-motivated and well-described.

Still, the reasons as to why respondents conduct the risk analysis vary. Respondents 11 and 14 argue that risk analysis is a way to cover the gap from the current security position to a wanted security position based on a GAP analysis. That is to say, the risk analysis provides the needed context for security controls. Respondent 14 also mentions that the results of the valuation can be enough to specify security controls; however, this only applies when the valuation level is deemed low.

There is also mention of using valuation as the basis for security controls and, in those cases, not conducting a risk analysis at all. In those cases, a set of security controls is directly mapped against each valuation level. Additionally, respondents 11, 14 and 17 mentioned that a lot of risk identification is made before the “actual” risk analysis. Thus, parts of the risk analysis are done continuously, just not in a classic sense.

Often, risk analysis is conducted at a system level, i.e., not connected to specific assets. According to respondent 5, the upside of this is that the benefits of risk analysis are the most prevalent at a system level, as it provides guidance on how information should be handled to system owners and the IT department. It is further explained that little time is spent on analysing physical assets; that is to say, their focus is on IT security rather than on information security.

When asked if it would be possible to skip the risk analysis, differing opinions are explained on whether it would be possible at all and how far one would be able to get without it from an information security perspective. It is stated that:

*“In some cases, I can say that it is up to me and my role as a professional to judge if I understand and have a grip on the situation. We don't need to do a risk analysis, as I understand what to do. (Respondent 14)”*

Respondent 14 argued that the risk analysis can sometimes be skipped and can instead be implicit, based on experience and knowledge. That is to say, rather than carrying out a full risk analysis, experience alone can be enough to reach a conclusion about the level of risk and, with it, what would consequently be the appropriate security controls.

Similarly, respondent 12 argued that you would likely be able to get “*about 80% of the way towards an acceptable state of security*” by simply applying security controls based on the result of the valuation. Respondent 17 mentions the opposite, that adopting best practices and following standards without using risk analysis guidance would “*get you about 20% of the way, at the very most, 30%*”. Respondent 17 bases this comment on how the risk analysis acts as a guiding factor in how and why to implement certain security controls, and with that guidance gone, it would be difficult to correctly select the controls needed. However, both respondents believe that it is possible to select security controls based only on a pre-defined set of options, to some extent. However, the potential success of such an endeavour differs in opinion.

Respondent 17 argues that the purpose of the valuation and risk analysis is distinctly different as the valuation only decides the value of the information, and that will often persist, for example, if the information is moved. However, moving information would potentially change the risks towards it, and as such, the respondent mentioned how important it is to keep valuation and risk analysis apart. Additionally, respondent 4 argues that the risk analysis results are better suited to formulate requirements for security controls than the results of the valuation, as one can be more precise when basing the requirements on risk rather than on the appreciated value of assets.

Another example of why we need the risk analysis was discussed both by respondents and described in the method support. The issues of accumulation (when large amounts of information are stored) and aggregation (when different sets of information that are brought together create more sensitive information) that can occur at the system level can lead to a higher valuation than any identified and classified information. However, this issue might be extra challenging to identify and act on in practice.

Respondents also discuss the future of risk analysis, especially in regard to more and more external factors playing a role in dictating which security controls to implement. Examples, such as the GDPR and NIS-2, were brought up. Respondent 6, who discussed GDPR, explained that the organisation tends to get complacent and ignore risk analyses, as requirements from, e.g., laws and regulations dictate that certain security controls must be in place. Respondent 17 mentioned NIS-2 and believed it is good that security controls are being integrated into such directives, as it becomes clearer what organisations that are covered by such directives are supposed to do and how they proactively should work with risk.

## 5 Conclusions

This paper has investigated ISO 27001, a method support aiming to bridge the gap between standard and practice, and the practice through document studies and a set of interviews targeting the *how*, *when* and *why* of risk analysis.

Oftentimes, respondents request very concrete method support material, preferably tailored to the exact needs of their organisation. Being the developer of the material that aims to fill the gap between standard and practice is

not an easy task, and even in the Swedish public sector, there are significant differences between, for example, threat levels and security control needs between agencies. The material has been developed with this in mind and tries to balance being general to support different organisational needs and, at the same time, give enough guidance to organisations trying to implement their information security.

Based on the analysis, three themes emerged that investigated and captured respondents' views of *how*, *when* and *why* risk analysis is conducted in their respective organisations. The *how* theme identified that organisations establish an organisational-wide risk profile and believe they are close enough to be secure and, as such, omit the risk analysis on specific assets or systems. The *when* theme identified that there are indications that when everything is risk-based, the risk analysis can be seen to be redundant, especially so if security controls are a result of the valuation. That is to say, the risk analysis is more of an implicit than an explicit activity. The *why* theme clearly identifies that there is an understanding of the need for risk analysis, and that should be performed, just not necessarily as it is classically described.

Throughout the interviews, there were several indications that the selection of security controls was guided more by regulatory compliance rather than as a result of conducting a (classic) risk analysis. However, this could potentially create an environment where the focus will lie more on compliance with laws and regulations instead of working with risk from an internal risk analysis perspective.

This study sought to investigate something not covered well enough in previous research. The study's qualitative nature implies some apparent limitations as it is relatively small-scale and performed in the public sector of one country. We have taken a number of steps in order to address these limitations and to enhance the credibility and generalisability of the findings. We have tried to increase transparency by describing the study's scope and context and by providing a detailed account of the research design, data collection, and analysis. The sample from the group of senior security experts is limited due to the nature of the group, and we reached saturation in the responses. Furthermore, the results are drawn from a combination of interviews, document studies, and data from contributors to the documents. This approach enabled us to get an explanation of how certain practices were described and interpreted, for example.

With this paper, we would like to open up for discussion on a number of topics where risk analysis is in focus, for example, how risk analysis is perceived and used in a security landscape where laws and regulations mandate more specific security controls. There is also the question of whether more mandated security controls change the focus to compliance, and thus returning to the otherwise criticised use of checklists [7, 8, 22]. Lastly, whether or not risk analysis is perhaps moving away from being a core activity in justifying what security controls to implement (in favour of mandated or standardised pre-defined sets), and towards becoming a complementary activity that adjusts and fine-tunes this selection when needed, is also ripe for future discussion.

**Acknowledgement.** We gratefully acknowledge the grant from the Swedish Civil Contingencies Agency (MSB), project VISKA (MSB 2021-14650).

**Disclosure of Interests.** The authors have no competing interests to declare.

## References

1. Adams, W.C.: Conducting Semi-Structured Interviews, pp. 492–505 (2015). <https://doi.org/10.1002/9781119171386.ch19>
2. Bergström, E.: Supporting information security management: developing a method for information classification. Ph.D. thesis, University of Skövde (2020)
3. Blakley, B., McDermott, E., Geer, D.: Information security is information risk management, p. 97. ACM Press (2001). <https://doi.org/10.1145/508171.508187>
4. Bowen, G.: Document analysis as a qualitative research method. *Qual. Res. J.* **9**, 27–40 (2009). <https://doi.org/10.3316/QRJ0902027>
5. Broderick, J.: Information security risk management - when should it be managed? *Inf. Secur. Tech. Rep.* **6**(3), 12–18 (2001). [https://doi.org/10.1016/S1363-4127\(01\)00303-X](https://doi.org/10.1016/S1363-4127(01)00303-X)
6. Caralli, R., Stevens, J., Young, L., Wilson, W.: Introducing OCTAVE allegro: improving the information security risk assessment process. Technical report. CMU/SEI-2007-TR-012, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA (2007). <http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419>
7. Choobineh, J., Dhillon, G., Grimaila, M.R., Rees, J.: Management of information security: challenges and research directions. *Commun. Assoc. Inf. Syst.* **20**(1), 57 (2007)
8. Dhillon, G., Backhouse, J.: Current directions in IS security research: towards socio-organizational perspectives. *Inf. Syst. J.* **11**(2), 127–153 (2001). <https://doi.org/10.1046/j.1365-2575.2001.00099.x>
9. ISO/IEC 27001: Information technology - cybersecurity and privacy protection - information security management systems - requirements. Standard ISO/IEC 27001:2022, International Organization for Standardization, Geneva, CH (2022). <https://www.iso.org/standard/27001>
10. ISO/IEC 27005: Information security, cybersecurity and privacy protection - guidance on managing information security risks. Standard ISO/IEC 27005:2022, International Organization for Standardization, Geneva, CH (2022). <https://www.iso.org/standard/80585.html>
11. Lundgren, M.: Making the dead alive: dynamic routines in risk management. Ph.D. thesis, Luleå University of Technology (2020)
12. Lundgren, M., Bergström, E.: Dynamic interplay in the information security risk management process. *Int. J. Risk Assess. Manage.* **22**(2), 212 (2019). <https://doi.org/10.1504/IJRAM.2019.101287>
13. Munteanu, A.: Information security risk assessment: the qualitative versus quantitative dilemma. In: *Managing Information in the Digital Economy: Issues & Solutions-Proceedings of the 6th International Business Information Management Association (IBIMA) Conference*, pp. 227–232 (2006)
14. Niemimaa, E.: Crafting organizational information security policies. Ph.D. thesis, Tampere University of Technology, November 2017

15. Niemimaa, E., Niemimaa, M.: Information systems security policy implementation in practice: from best practices to situated practices. *Eur. J. Inf. Syst.* **26**(1), 1–20 (2017). <https://doi.org/10.1057/s41303-016-0025-y>
16. NIST 800-53B: Control baselines for information systems and organizations. Technical report, National Institute of Standards and Technology, October 2020. <https://doi.org/10.6028/NIST.SP.800-53B>
17. NIST SP 800-30: Guide for conducting risk assessments. Technical report. NIST SP 800-30r1, National Institute of Standards and Technology, Gaithersburg, MD (2012). <https://doi.org/10.6028/NIST.SP.800-30r1>
18. NIST SP 800-37: Risk management framework for information systems and organizations: a system life cycle approach for security and privacy. Technical report. NIST SP 800-37r2, National Institute of Standards and Technology, Gaithersburg, MD, December 2018. <https://doi.org/10.6028/NIST.SP.800-37r2>
19. NIST SP 800-53: Security and privacy controls for information systems and organizations. Technical report, National Institute of Standards and Technology, September 2020. <https://doi.org/10.6028/NIST.SP.800-53r5>, edition: Revision 5
20. Peltier, T.R.: *Information Security Risk Analysis*, 3rd edn. Auerbach Publications, Boca Raton (2010)
21. Saldaña, J.: *The Coding Manual for Qualitative Researchers*, 4th edn. SAGE Publications Inc., Thousand Oaks (2021)
22. Shedden, P., Smith, W., Ahmad, A.: Information security risk assessment: towards a business practice perspective. In: *Proceedings of the 8th Australian Information Security Management Conference*, 30th November 2010 (2010). <https://doi.org/10.4225/75/57B6769334787>
23. Silva, F.R.L., Jacob, P.: Mission-centric risk assessment to improve cyber situational awareness. In: *Proceedings of the 13th International Conference on Availability, Reliability and Security - ARES 2018*, Hamburg, Germany, pp. 1–8. ACM Press (2018). <https://doi.org/10.1145/3230833.3233281>
24. Spears, J.L.: A holistic risk analysis method for identifying information security risks. In: Dowland, P., Furnell, S., Thuraisingham, B., Wang, X.S. (eds.) *Security Management, Integrity, and Internal Control in Information Systems*. IIFIP, vol. 193, pp. 185–202. Springer, Boston, MA (2005). [https://doi.org/10.1007/0-387-31167-X\\_12](https://doi.org/10.1007/0-387-31167-X_12)
25. Swedish Civil Contingencies Agency: *Metodstöd för systematiskt informationssäkerhetsarbete [method support for systematic information security work]* (2020). <https://www.informationssakerhet.se/metodstodet/>
26. Taylor, R.G.: Potential problems with information security risk assessments. *Inf. Secur. J. Global Perspect.* **24**(4-6), 177–184 (2015). <https://doi.org/10.1080/19393555.2015.1092620>
27. Tejay, G., Goel, S.: Editorial: time to move away from compliance - cybersecurity in the context of needs and investments of organizations. *Org. Cybersecur. J. Pract. Process People* **2**(1), 1–2 (2022). <https://doi.org/10.1108/OCJ-05-2022-018>
28. Wangen, G., Hallstensen, C., Snekenes, E.: A framework for estimating information security risk assessment method completeness: Core Unified Risk Framework, CURF. *Int. J. Inf. Secur.* **17**(6), 681–699 (2018). <https://doi.org/10.1007/s10207-017-0382-0>









# What Makes Information Critical? Information Classification in Organizational Practice

Simon Andersson<sup>(✉)</sup> , Åsa Ericson , Johan Lugnet , and Christine Große 

Luleå University of Technology, 97187 Luleå, Sweden  
simon.andersson@ltu.se  
<http://www.springer.com/gp/computer-science/lncs>

**Abstract.** This paper investigates how information classification is conducted in practice. Despite being a foundation of risk management work, information classification remains understudied from a practical perspective. This study uses semi-structured interviews and a small-scale experiment with professionals from a consultancy firm operating at a national level to explore how information assets are identified, valued and classified. The findings show that information classification is not a purely formalized process, but a collaborative and interpretative activity in which formal models are often adapted or bypassed in favor of context-specific reasoning. Key challenges in practice include inconsistent use of terminology, subjective judgments, and the limitations of classification schemes. The study highlights a need for a shared understanding and trust among participants, which were important factors for successful classification activities, especially in inter-organizational contexts. A three-step approach is thus proposed that emphasizes the value of information in organizational processes before assessing its protection needs. This new approach contributes to a more value-oriented understanding of assets instead of viewing them solely from the perspective of loss or damage. Future research could extend the findings presented.

**Keywords:** Information classification · Information security · Risk Management · Organizational practice

## 1 Introduction

The importance of information continues to grow and is often defined as one of, if not the most critical asset of value for an organization. According to [15], information assets are essential for business processes, interactions with stakeholders, all kinds of decisions and the strategic planning of an organization. Both the importance of information as an asset and the increasing number and severity of security breaches and cyber-attacks over the last decade emphasize the necessity of properly managing and protecting the information [14, 49].

As a result, many organizations employ risk management methods to assess and reduce the associated risks [8, 21]. Usually, the approaches start with an

identification of the assets that possess value for an organization and thus should be protected. The further steps of risk management include the assessment of threats, vulnerabilities, and consequences, including a representation of concepts like the frequencies of events and conditional probabilities for different consequences given the event, together with assessments of the severity of these consequences (e.g. [32]). In addition, the identification and selection of mitigation strategies, their implementation and monitoring, the external monitoring of emerging and developing threats and the learning from incidents are part of the risk management process [23]. In this paper, the focus is on the initial step, the identification and classification of the information within an organization that is worthy of protection. As previous literature has shown, identifying (information) assets that are of value for an organization is a difficult task, which among others also include capturing intellectual ones. Leming [33] thus stresses the problem that organizations seem to know more about computers and filing cabinets than the information they contain. Today, the same can be said about a greater variety of devices, databases, and cloud services. Therefore, research has regularly emphasized that information governance, including recognizing the value of information, should be a high-level corporate function to ensure maintenance and alignment with strategic development of the organization. Despite a great body of research considering risk assessment methods, there is still a lack of empirical studies investigating how information classification is done in practice and how the value of information is assessed prior to risk assessment and management.

This study aims to fill this gap and investigates information classification as it is done in practice to better understand the main considerations of the people responsible and the use of classification models in such efforts. For this purpose, several professionals tasked with risk management in their own and other organizations participated in this study. Based on interviews and a small-scale experiment, the results show that information classification is in practice a collaborative and interpretative process where formal models are often adapted or bypassed in favor of context-specific reasoning. Moreover, it has been demonstrated that the creation of a common understanding of the criticality of information in the organizational value creation processes and an appropriate level of trust between participants in classification workshops are crucial for the practical application of information classification. This is particularly important for consulting firms as they must confront particular challenges in information classification and risk management due to their vulnerable position as subcontractors [37].

The contribution of this study is twofold. First, it offers empirical evidence on how information is classified in practice, providing valuable insights into the key challenges and possible solutions in an organizational practice. This enables a better understanding of both the problem at hand and the need for further research. Second, it proposes a renewed perspective on information classification that focuses more on the value of information assets in the value chains of organizations before determining the need for protection in terms of specific attributes.

Following this introduction, the next section provides more details on the main concepts underpinning this study, and the method section describes the

data collection and analysis. In the result section, findings from interviews and the classification experiment are presented, related to how professionals identify and assess information assets in practice, including approaches, challenges, criteria, and the role of trust. The discussion and conclusion sections complete the paper.

## 2 Information Classification

### 2.1 Key Concepts

A central feature of information is that it “represents some part of the world as being a certain way” [17]. In particular, information is an artifact that has semantic or representational content. Other research has recognized objects or documents that contain certain descriptions or summaries as such forms of representation [12]. However, further attributes are needed to distinguish between different levels of importance, that is, to classify the value of a piece of information for an organization. Information classification provides the base for subsequent risk assessments [7, 16, 47]. The first step is to identify the relevant information assets, describing which they are, how and where they are stored, who uses them, and for which tasks. In general, information is an essential prerequisite for business processes and strategic planning and decision making (see e.g. [15, 24]). Information must therefore meet the specific criteria of an organization in terms of its quality and security, for which information classification lays ground. Information assets can be tangible, in the sense that they exist in a directly observable form on items such as paper or digital documents, and intangible, such as business strategies, employee knowledge, or the reputation of an organization. In addition, important information assets can be intellectual property, such assets are often formalized in (digital) documents and stored in hardware and software systems, such as servers, clouds, databases, and networks. Users can retrieve information from those systems to a variety of devices like laptops, tablets and mobile phones. Digital information can be in textual, audio and visual forms, including documents, videos, voice recordings, emails, web sites, text and multimedia messages.

It has been shown that identifying and classifying an organization’s information assets are challenging, especially when they are abstract elements, for example, associated with the brand, reputation, and core know-how of an organization [3]. Likewise, digital information assets seem difficult to recognize. For example, a logistics company that fell victim for the NotPetya attack consequently realized that their transport management system was critical to their business [27]. Previously, the executives had seen the company’s business as purely physical. From the loss of access to their information system they learned how much the company relies on the digital systems [27]. Hence, all information asset that can be associated with organizational value should be included in the classification process. Identifying and classifying information assets, their locations and interdependencies therefore necessitates a team of different professionals from the organization.

A deeper understanding of an organization, including its purpose and how value is created, is a precondition for information classification. In addition, established models can guide information classification, for example, ISO 27002 is a widely used and known standard [29]. Common information security qualities are confidentiality, integrity, and availability, which refer to the extent to which the information is protected from disclosure by unauthorized persons; is verifiable, well-documented, and free from unauthorized alteration; and is accessible for authorized persons at the right time, in the right place and with correct permission (see e.g. [24]).

Preferably, the classification is conducted by the mentioned team responsible, often in a workshop format [7]. Valuing information is difficult, and it is often considered one of the major problems within risk management [9,18]. The classification assesses the criticality of information to core business operations, for example, by investigating replacement costs and consequences associated with the loss, compromise or leakage of information [2]. Consequence categories can be used to emphasize different effects of misuse, disclosure, alteration or loss of information, such as financial, reputational or operational consequences [6]. However, the lens of compromise and loss may be insufficient to recognize the value of information, as it implies that value only arises in the presence of risk. Such a perspective runs the risk of overlooking the strategic and enabling role that information plays in everyday operations. Therefore, valuation should ideally be done upfront and based on how information supports business processes and creates value, not just how its absence might cause damage or loss.

## 2.2 Challenges with Information Classification

As mentioned, confidentiality, integrity, and availability are common qualities in information classification (see e.g., [24]), whereby assessing their importance intends to support representing the value of the information for an organization. Often, a classification scheme detailing a few levels of impact, which a compromise of these qualities could bring to the organization, is adapted to the organization of interest [10]. However, there is a scarcity of research considering how such classification scheme can be successfully used, apart from the finding that impact levels should have speaking names in the organizational context of application [7]. In addition, the number of such levels is commonly chosen by an organization itself; typically, it ranges between three and five [29,48]. The classification includes determining the importance of each factor in the context of the organization, while the highest classification of each aspect finally determines the classification for this information asset. In addition, there is a dilemma with the design of the schemes intended to support the information classification: they need to be detailed but also understandable for information owners and users [7,19]. Too complex schemes without sufficient instructions and assessment methods can instead lead to inconsistent valuation [19] whereas too simple schemes are associated with the “bias to the middle”, that is, if unequal (e.g. three or five) alternatives are presented, users tend to choose the middle option,

similar to the “center-stage effect”, described in [41]. Additional issues that previous research has identified include weak, or a lack of, classification guidelines, insufficient inventories of assets, unclear ownership and incomplete classification processes [4, 10, 19, 20, 48].

Moreover, professionals entrusted with information classification and risk management in organizations need to legitimate their decisions and to appear confident and knowledgeable about the classifications made. That implies that trust in the role or person can play an important role in organizational information classification and risk management processes. Robinson [40] described trust as the attitude someone or a party adopts (trustor) towards somebody else or another party (trustee), such as a person, a role, an organization, a piece of information, a technical device or a system (e.g., [43]). According to [39], trust is a combination of five components: i) perceived competence, ii) objectivity, iii) fairness, iv) consistency, and v) faith (good will). In addition, it is emphasized that low performance on some attributes can be compensated by higher performance on others [39].

As indicated, information classification is associated with uncertainty in several ways. One concern is how to properly assess the criticality of information, another one is associated with the identification and assessment process within a particular context, and a third concern includes the professionals who act on behalf of an organization [23]. Furthermore, group settings may increase individually perceived uncertainty, including prevalent group values, the ambiguity of information that can emerge and the feeling of being forced into action [34]. Previous studies have shown that group decisions, whether collective or distributed, may tend to trust the opinions of experienced group members, meaning that not all alternatives are adequately considered [44]. In information classification practice, such behavior can lead to incomplete identification of information assets or over-valuing of assets that in turn imply inappropriate protection measures [4]. Consequently, this study involves a focus on trust, which also addresses the issue that trust is poorly understood from an organizational perspective [35].

## 3 Method

### 3.1 Data Collection

This study addresses the scarcity of empirical studies investigating how information classification is done in practice and how the value of information is assessed by the people responsible with the aid of classification models. For this purpose, four experienced professionals with different positions and backgrounds tasked with risk management on behalf of their organization, an information security consultancy firm, participated in this study. The consultancy firm operates at a national level and works extensively with public sector organizations, mainly in Sweden. It is of particular interest as consulting firms occupy a vulnerable position as subcontractors. As sub-contractors have access to multiple clients’ data, they are at higher risk of being targeted by cyber-attacks [38], while at the same time needing to build and maintain a reputation as a trustworthy

business partner. In addition, perspectives on information classification from a consultancy perspective were deemed interesting, as they assist others in the process, often users who are inexperienced. However, there is still a significant lack of research on specifically IT consulting firms [28]. The respondents in this study work in different locations and have different roles, but are all involved in information classification, allowing for a variety of valuable insights into the practice of information classification. Table 1 provides further details about the respondents.

**Table 1.** Respondents from an information security consultancy firm

Respondent	Length of interview	Experience in role
Business developer/project leader	60 min	> 20 years
Senior information security consultant	72 min	2 years
Senior consultant/IT-Archivist	28 min	> 20 years
IT-Archivist	40 min	1.5 years

Semi-structured interviews [1, 30] with practitioners constitute the base for this study, which is a sufficient method for investigating the outlined topic in greater detail. Semi-structured interviews facilitate the collection of opinions, values and thoughts allowing for the enrichment of a study with extensive data [30]. Semi-structured interviews are generally described as conversations with a purpose; here, the focus was on in-depth dialogues exploring the experiences of the professionals with information classification in practice.

During the interviews, a set of open-ended questions were used to guide the dialogue. Examples of such questions were: “*Could you explain how you conduct information classification?*” and “*How do you use classification models in the classification work?*”. Follow-up questions were asked when answers needed further clarification. Upon consent of the respondents, the interviews were voice-recorded and transcribed verbatim. At the end of each interview, a small-scale experiment using two different classification schemes was conducted with the purpose of observing the process of information classification done by professionals. The respondents were asked to explain their reasoning while conducting the classification, and to “think aloud” to further explain the criteria they considered. In addition, notes were taken alongside the interviews and included in the analysis.

It should be noted that the empirical material consists of 4 interviews with professionals from a single consultancy firm. While this limits the breadth and generalizability of the findings, the respondents’ extensive experience offers valuable insight into the practice of information classification.

### 3.2 Data Analysis

The analysis began while gathering the data, which is consistent with interviewing people [1]. For example, an interviewer seeks to identify hesitation or changes

of wording while conducting interviews and follow-up questions. An initial analysis was done when listening to and transcribing the recorded interviews [13]. The in-depth analysis included further a thematic analysis of the transcripts by identifying, analyzing and interpreting patterns within the data [11]. The thematic analysis included the generation of initial codes, the organization of the material into themes, and the interpretation [11, 42, 46]. The interview guide provided the starting point for coding the material. The collected textual material was then arranged by identified relationships to form cohesive themes. The descriptions and examples provided during the interviews were interpreted using the introduced theoretical perspectives, namely the identification and classification of information assets, and challenges with the information classification process including a focus on trust [31]. The thematic analysis resulted in the following themes: (i) identification and classification of information assets, considering approaches, techniques and organizational prerequisites; ii) common criteria in practice, including reflections on what makes information critical; and iii) security communication and trust, involving contemplations on interpersonal and interorganizational challenges. The interpretations made were verified by returning to the interview recordings to confirm that they were grounded in the context of the investigated topic and mirrored the respondents' own words.

## 4 Results

### 4.1 Identification and Classification of Information Assets

There was consensus among the respondents about the importance of information classification for organizations regardless of their size. However, the perceptions varied in terms of how information should be identified and classified and what variables should guide the assessment. The classification scale was perceived as a dilemma by most respondents. According to the business developer, it is vital to identify the information asset, the owner or carrier of it and the classification of confidentiality, availability and integrity (CIA) demands:

*“There are information objects and the scale of it, then there is the carrier of information, where does this information exist. This is often done within the borders of what we call information security... So, carrier of information, information object and a classification of the object... There are always variants of CIA but then you need a classification system that you agree with the customer about. Either high, medium, low or a scale of 1–5.” - Business Developer*

The Senior Information Security Consultant emphasized instead the understanding of the objectives for information classification in an organization and the completeness of the asset inventory

*“First you are to value the information, but before it is important to create an inventory of it, it is far from always that has been done fully... You must understand what the purpose is, what is it that we want to*

*achieve? It is an asset inventory and [...] a valuation of this inventory that ends with [...] a valuation of our information.”- Senior Information Security Consultant*

In addition, the Senior Information Security Consultant highlighted issues with the naming of classification levels if they are not adapted to the needs of an organization.

*“The worst scenario in a business with people is that someone dies. [And] we have handled information in a way that caused someone to lose their life. That’s the worst case; another worst case is to go out of business.*

*That is not severe, instead devastating would be better suited. If that happens it is over, goodnight!” - Senior Information Security Consultant*

All respondents highlighted that providing guiding examples would be helpful for learning and understanding the information identification and classification task, especially when it comes to examining consequences of the loss of information qualities by unexperienced employees. Another issue brought up was the level of aggregation applicable during information identification. Not only was the type of information, such as financial data of a customer, perceived as too vague, but also the relationship to process flows and the relevance for the organization were considered difficult to assess without further insight into the key processes of a specific organization.

Although the respondents stated that the ordering of the classification scale would not matter, the small experiment at the end of the interviews revealed that all of them preferred to place the assets with the highest protection demands at the top of the list followed by the others in descending order.

The results of the interviews show that forming a heterogeneous team of various professions from an organization’s different departments is a necessary precondition for performing information identification and classification. As different formal roles and responsibilities as well as individual experiences affect how the criticality of information is perceived, the classification work involves relational and knowledge complexity. This includes the representatives’ differences in reasoning and comprehension of the organization’s core values and the importance of information assets in organizational value generation along key processes. Information classification models are regularly used as communication tools facilitating negotiation and group decision-making.

## 4.2 Common Criteria in Practice

The respondents regularly helped other organizations, primarily in the public sector, with identifying and classifying information assets prior to risk analysis. Although quality criteria like confidentiality, integrity and availability are common in the information security field, all respondents explained that they often must rephrase them when talking with people in client organizations. The Business developer detailed it as follows:

*“You must ask the right questions [...] if this is secret or sensitive information if it leaks? Yes, or no. Then you might have to value how sensitive it is. And if it is important that this information is always within reach and so on.” - Business Developer*

A few main reasons were regularly mentioned by the respondents, including the experience of experts involved in the classification of information, the vocabulary that is common in some professions and the terminology that is used in a specific organization. The Senior Consultant/IT Archivist exemplified the issues:

*“If you are a system administrator and enter a classification workshop... This [the classification] is nothing that people I meet think about all the time. So, a lot of what I do also involves explaining why I do things and why I use the terms that I am using.” - IT Archivist*

The Business Developer explained the importance of establishing common ground to facilitate information identification and classification by the following example:

*“When I arrive at a new customer and mention the term document it can mean a word-document for one person, a collection of 40 appendixes and one missive for another, and for a third person it could simply be a paper. It is very important that you agree on the meaning of certain terms.” - Business developer*

The Senior Information Security Consultant confirmed that the terms confidentiality, integrity and availability are less frequently employed as assumed and argued that they are not useful in the preparatory phase of risk analysis including information identification and classification in practice. He further declared:

*“When I arrive at customers that use the terms a lot, I usually tell them that they are on the wrong track... I’ve done this for many years, and I know one thing. There is no point in classifying confidentiality [integrity and availability] 1 to 4, you will get a C2, I2 and A2, and what do you do with that?” - Senior Information Security Consultant*

Instead of such superficial classification, where neither the term nor the numbers provide sufficient clarity on how to proceed, the assessment must therefore focus on the value of the information for the specific organization looking at the information in its context and how its value comes about. However, the study results reveal that discussing different scenarios is an approach to assessing consequences. The scenarios, naturally worst-case scenarios, are then compared with each other, which refers to risk analysis rather than to information classification as a precondition for the former.

### 4.3 Security Communication and Trust

The respondents reflected on the role of trust in their work with information classification in two ways, internally and externally. The internal perspective

included trust within their organization among colleagues and the external perspective considered clients and customers of their consultancy services. Main prerequisites for trust that the respondents identified as one part's willingness to put faith in another individual, function or item, were the fulfilment of expectations regarding conducting tasks, adhering to agreements and behaving reliably. The business developer perceived that trust can be placed both on information and persons and explained it in the following way:

*“When I help customers, trust is the connection to integrity [...], how much can I trust that this information that I take part in or receive is correct and not altered, and what believe do I put in it? And if we turn around and talk about colleagues then trust is [...] the ability to have faith in that the colleagues I have do what they are supposed to do and that they will do their work in the best possible way”. - Business Developer*

Transparency and commitment to agreements were also considered important to create and enhance trust among business partners. All respondents expressed a clear distinction between trust in items, such as information, and people. Mainly, the interviewees discussed how one part's behavior affects the other part's trust in the former. When talking about trust in information, they rather reflected on one's belief in information qualities, such as accuracy, correctness and originality. The Senior Information Security Consultant emphasized the relation between information Security and trust:

*“When connecting trust with Information Security, trust lies in the quality of the information. That it is correct, available and that there is some sort of quality-protection of confidentiality that often surrounds information or a task... within information security, it [trust] is what is important, it is the ‘be-all end-all’”. - Senior Information Security Consultant*

The interviewees also provided the insight that trust is an important prerequisite in organizational and inter-organizational contexts to ease and streamline cooperations. The IT Archivist underlined the importance of a certain level of trust in such contexts:

*“If you can trust each other, it makes transactions between people and things more effective. If you assume that you can't trust anything things will be far more cumbersome and complicated.” - IT Archivist*

The results of the interviews emphasize that a common language and terminology regarding information classification and security requirements is considered a good start to build trust within the team and the organization. However, the extent to which trust in teamwork roles and responsibilities is expressed or taken for granted remains questionable.

## 5 Discussion

### 5.1 Implications for Information Identification and Classification

A few key issues can be discussed based on the analysis of the study's empirical evidence, including the complexity of the information classification task in an organizational context. To begin with, clarification of the general process steps appears necessary. Although defined as prerequisite for organizational risk analysis, the presented findings reveal that identification and classification of information tends to tamper into risk assessments, through the use of scenarios based on threats, vulnerabilities and consequence as well as probability estimations. As a consequence, the value of information in a specific organizational context, for example to enable and support core business processes and value realization, is regularly overlooked. Moreover, the task remains unstructured and overly complex as all aspects of risk analysis are involved simultaneously. Therefore, a more structured approach is advisable. The upper row of activities in Fig. 1 illustrates a three-step process related to information classification, including the identification, valuation and classification of information, in an organizational context. The first step relates to an inventory of information assets, the second one intends to create an understanding of the value of the information to the organization and the third step results in determining the protection needs of the information assets.



**Fig. 1.** A three-step process of asset identification and classification as input into risk analysis, (Newly originated by the authors).

This study has found that challenges appear in the identification step, for example, concerning the level of granularity that should be adopted, which also aligns with findings in previous research in different contexts (e.g., [4, 25, 26]). As emphasized by the empirical results, these steps preferably are conducted by a heterogenous team of various professions in a format that enables dialogue among participants and facilitates mutual understanding of the organizational values and security needs. In addition, the group also needs to discuss the level of

detail and the terminology that is appropriate in the specific organization. Moreover, the employed tools and methodology require consideration. For example, the valuation of the identified assets could be based on a mapping of key processes prepared in advance following a structures quality management approach (cf. e.g., ISO 9001). An alignment of information security and quality management can help with both identifying information assets and processes that are critical to the organization and determining the value and protection needs of those information assets [22,24]. Process models and descriptions facilitate the identification of relevant information objects and their owners, carriers, and users, as well as interrelated systems and devices, as this study's results emphasize. Moreover, such alignment is likely to improve the various professions' understanding of the purpose of information classification in particular and the impact of information security work as a facilitator of business continuity in general.

As presented above, the classification of information, that is, the determination of the targeted level of protection, is accompanied by methodological issues. For example, the selection of the classification scheme or tool and the criteria for describing the level of protection required. The information qualities of confidentiality, integrity and availability are useful for describing the level of protection that is needed from the view of these three perspectives. However, the choice of one number or word that summarizes these three different dimensions regularly appeared as the key challenge, that also leads to an oversimplification and misalignment between information classification; threat, vulnerability and risk assessments; and mitigation strategies that facilitate organizational value creation by socio-technical processes. It would therefore be advisable to document the argumentation and considerations underpinning the group decision-making during the three-step process in a sufficient manner [5] to inform the following assessments, as depicted in the lower row in Fig. 1.

Moreover, the study's findings highlight trust as a means to cope with the uncertainty and ambiguity inherent in complex problems, such as determining the criticality of assets in societal contexts to prioritize resource allocation and security measures [25]. In the study presented here, trust was put on other professionals when their behavior was perceived reasonable in relation to their formal roles and responsibilities (see also [45]). Further, the findings also show that interpersonal trust is an important factor that can facilitate relational performance (e.g., [43]), especially in interorganizational collaboration by consultancy firms and in group settings.

## 5.2 Implications for Further Research

The findings of this study indicate several remaining issues that deserve further attention. First, organizational processes and contexts, as well as the information in use, are subject to regular and dynamic changes. Therefore, asset registries are incomplete and the determination of the value and protection needs of information assets changes over time. Further empirical research could examine how organizational procedures, and methodological approaches can be designed to

better reflect the complex realities of public and private organizations. In addition, experiments on group settings and dialogue-based approaches could expand the findings presented in this study. In particular, the presented results emphasize a stronger focus on organizational value creation instead of premature risk analysis that arises when using consequence categories in information classification. Therefore, suggestions for further research include studies evaluating the applicability and usefulness of value assessments to determine the criticality of information. Inspiration can be found in the research area of critical infrastructure and vital societal function, in which infrastructure is considered critical if the survival, well-being and progress of society depend on its maintained functionality [25]. Similarly, information can be considered critical if the survival, well-being and progress of an organization (or society) depend on its maintained quality in terms of confidentiality, integrity and availability. Additional research could investigate the role of additional qualities that are gaining attention, such as privacy and truthfulness (see also [24]).

Moreover, the application of scales to describe and determine the protection needs of information assets regarding various information qualities is common but their meaningfulness has been questioned. In addition to terms that better describe the thresholds, the granularity of such scales can be subject to future research. The aggregation of the protection levels determined for each criterion into a value protection index that actually captures the significance of information under consideration remains a further area for research.

This study also reveals that providing examples was an important tool to convey the message to stakeholders involved in information classification. It could therefore be further explored whether the use of narrative or fiction-based methods of storytelling [36] can provide alternative approaches. In addition, the effects of such approaches on trust-building mechanisms among professionals may be of interest. Based on the empirical material presented, trust remains an important factor for group work and inter-organizational collaboration, especially with respect to security-related tasks conducted by consultants. Assessments include critical information, business secrets and dependencies on assets, knowledge and people. Hence, a certain level of interpersonal trust is also precondition for information classification, regardless of the involvement of internal or external professionals. Follow-up research could deepen the insights presented in this paper by analyzing how trust in partner organizations, individual professionals, information assets and different types of information systems affect the conduct of information classification and risk analysis in organizations. It could further investigate what secondary risks may arise from an inappropriate level of trust on both responsible people, implemented approaches and technical tools as well as their implications for supply chain security.

## 6 Conclusion

This paper investigated information classification as done in practice to better understand the main considerations of the people responsible, the use of classification models, and the interrelated challenges. To this end, several professionals who are regularly entrusted with such tasks in their own and other organizations, mainly in the public sector in Sweden, participated in this study.

The results highlight that a deeper understanding of an organization, including its purpose and how value is created, is necessary to perform meaningful information classification. For example, the type of information, such as financial data of a customer, and the relationship to core processes as well as the relevance for the organization were considered difficult to assess without further insight into a specific organization. In addition, the findings emphasize that a common language regarding information classification terms and security requirements helps to build trust within the team. However, the extent to which trust in teamwork roles and responsibilities is expressed or taken for granted remains a question for further investigation.

The classification of information includes determining the importance of different criteria in the context of the organization, while the highest classification of each usually determines the criticality of this information asset. However, the choice of one number or word that summarizes these different requirements regularly appeared as the key challenge, that also tended to lead to an oversimplification and misalignment between information classification; threat, vulnerability and risk assessments; and mitigation strategies. In particular, the presented study stresses a stronger focus on organizational value creation by socio-technical processes instead of premature risk analysis that arises when using consequence categories, which focus on compromise and loss, in information classification. Such a focus may overlook the strategic and enabling role that information plays in day-to-day business. Therefore, the findings underline that valuation should ideally be done upfront and based on how information supports business processes and creates value, not just how its absence might cause damage or loss.

The contribution of this study is thus twofold. First, it contributes empirical evidence on the classification of information that provides valuable insights into the key challenges and possible solutions in organizational practice. This enables a better understanding of both the problem at hand and the need for further research. Second, it offers a renewed three-step perspective on the classification of information that focuses more on the value of information assets in the value chains of organizations before determining the need for protection in terms of specific attributes.

Further research that seeks to advance the knowledge presented in this study could explore the development and evaluation of methods that better integrate value-based assessments into information classification processes. In addition, the impact of organizations' prerequisites, subcontractors in the supply chain and key narratives for problem recognition and trust building are further areas for future research. Further research could expand the study presented here with

additional empirical material and take other contexts into account, such as the private sector or international organisations.

**Disclosure of Interests.** The authors have no competing interests to declare relevant to this article's content.

## References

1. Adams, W.C.: Conducting semi-structured interviews. In: Handbook of Practical Program Evaluation, pp. 492–505 (2015)
2. Agrawal, V.: A framework for the information classification in ISO 27005 standard. In: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 264–269. IEEE (2017)
3. Ahlin, K.: Measuring the immeasurable? The intangible benefits of digital information. In: Hawaii International Conference on System Sciences, pp. 6176–6185. Hawaii International Conference on System Sciences (2019)
4. Andersson, S.: Problems in information classification: insights from practice. *Inf. Comput. Secur.* **31**(4), 449–462 (2023)
5. Andersson, S., Bergström, E., Lundgren, M., Bernsmed, K., Bour, G.: Information security risk management tools in the air traffic management domain: what are practitioners' needs? *Inf. Secur. J. A Global Perspect.*, 1–18 (2025)
6. Bergquist, J.H., Tinetti, S., Gao, S.: An information classification model for public sector organizations in Sweden: a case study of a Swedish municipality. *Inf. Comput. Secur.* **30**(2), 153–172 (2021)
7. Bergström, E., Karlsson, F., Åhlfeldt, R.M.: Developing an information classification method. *Inf. Comput. Secur.* **29**(2), 209–239 (2021)
8. Bergström, E., Lundgren, M.: Stress amongst novice information security risk management practitioners. *Intl. J. Cyber Situational Awareness* **4**(1), 128–154 (2019). <https://doi.org/10.22619/IJCSA.2019.100128>, <https://c-mric.com/100128>
9. Bergström, E., Lundgren, M., Ericson, A.: Revisiting information security risk management challenges: a practice perspective. *Inf. Comput. Secur.* **27**(3), 358–372 (2019). <https://doi.org/10.1108/ICS-09-2018-0106>
10. Bergström, E., Åhlfeldt, R.-M.: Information classification issues. In: Bernsmed, K., Fischer-Hübner, S. (eds.) NordSec 2014. LNCS, vol. 8788, pp. 27–41. Springer, Cham (2014). [https://doi.org/10.1007/978-3-319-11599-3\\_2](https://doi.org/10.1007/978-3-319-11599-3_2)
11. Braun, V., Clarke, V.: Using thematic analysis in psychology. *Qual. Res. Psychol.* **3**(2), 77–101 (2006)
12. Buckland, M.K.: Information as thing. *J. Am. Soc. Inf. Sci.* **42**(5), 351–360 (1991)
13. Denscombe, M.: EBOOK: The Good Research Guide: For Small-Scale Social Research Projects. McGraw-Hill Education (UK) (2017)
14. European Union Agency for Cybersecurity (ENISA): ENISA Threat Landscape 2024 (2024). <https://doi.org/10.2824/0710888>, [https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024\\_0.pdf](https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf)
15. Evans, N., Price, J.: Development of a holistic model for the management of an enterprise's information assets. *Int. J. Inf. Manage.* **54**, 102193 (2020)
16. Everett, C.: Building solid foundations: the case for data classification. *Comput. Fraud Secur.* **2011**(6), 5–8 (2011). <http://www.sciencedirect.com/science/article/pii/S1361372311700604>
17. Fallis, D.: What is disinformation? *Libr. Trends* **63**(3), 401–426 (2015)

18. Fenz, S., Heurix, J., Neubauer, T., Pechstein, F.: Current challenges in information security risk management. *Inf. Manage. Comput. Secur.* **22**(5), 410–430 (2014), <https://doi.org/10.1108/IMCS-07-2013-0053>
19. Fibikova, L., Müller, R.: A Simplified Approach for Classifying Applications, pp. 39–49. Vieweg+Teubner, Wiesbaden (2011)
20. Ghernaouti-Helie, S., Simms, D., Tashi, I.: Protecting information in a connected world: a question of security and of confidence in security. In: 2011 14th International Conference on Network-Based Information Systems, pp. 208–212 (2011). <https://doi.org/10.1109/NBiS.2011.38>
21. Gritzalis, D., Iseppi, G., Mylonas, A., Stavrou, V.: Exiting the risk assessment maze: a meta-survey. *ACM Comput. Surv.* **51**(1), 1–30 (2018)
22. Große, C.: Towards an integrated framework for quality and information security management in small companies (2016)
23. Große, C.: Sources of uncertainty in Swedish emergency response planning. *J. Risk Res.* **22**(6), 758–772 (2019)
24. Große, C.: Enhanced information management in inter-organisational planning for critical infrastructure protection: case and framework. In: ICISSP, pp. 319–330 (2021)
25. Große, C., Larsson, A., Björkqvist, O.: Information-flawing filters in critical infrastructure protection: the deficient information basis in a Swedish approach. *Int. J. Crit. Infrastruct.* **19**(1), 40–57 (2023)
26. Große, C., Olausson, P.M., Wallman-Lundäsen, S.: Left in the dark: obstacles to studying and performing critical infrastructure protection. *Electron. J. Bus. Res. Meth.* **19**(2), 58–70 (2021)
27. Hepfer, M., Powell, T.C.: Make cybersecurity a strategic asset. *MIT Sloan Manag. Rev.* **62**(1), 40–45 (2020)
28. Hove, C., Tärnes, M., Line, M.B., Bernsmed, K.: Information security incident management: identified practice in large organizations. In: 2014 Eighth International Conference on IT Security Incident Management & IT Forensics, pp. 27–46. IEEE (2014)
29. ISO/IEC 27002: Information security, cybersecurity and privacy protection – information security controls. Standard ISO/IEC 27002:2022, International Organization for Standardization, Geneva, CH (2022). <https://www.iso.org/standard/75652.html>
30. Kallio, H., Pietilä, A.M., Johnson, M., Kangasniemi, M.: Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *J. Adv. Nurs.* **72**(12), 2954–2965 (2016)
31. Kvale, S.: The 1,000-page question. *Q. Inq.* **2**(3), 275–284 (1996)
32. Larsson, A., Große, C.: Data use and data needs in critical infrastructure risk analysis. *J. Risk Res.* **26**(5), 524–546 (2023)
33. Leming, R.: Why is information the elephant asset? An answer to this question and a strategy for information asset management. *Bus. Inf. Rev.* **32**(4), 212–219 (2015)
34. March, J.G.: Understanding how decisions happen in organizations. *Organ. Decis. Making* **10**(2), 9–32 (1997)
35. Marcial, D.E., Launer, M.A.: Towards the measurement of digital trust in the workplace: a proposed framework. *Int. J. Sci. Eng. Sci.* **3**(12), 1–7 (2019)
36. McBeth, M.K., Jones, M.D., Shanahan, E.A.: The narrative policy framework. *Theor. Policy Process* **3**, 225–266 (2014)
37. Nyman, M., Große, C.: Are you ready when it counts? It consulting firm’s information security incident management. In: ICISSP, pp. 26–37 (2019)

38. General Data Protection Regulation: Regulation (EU) 2016/679 of the European Parliament and of the council. Regulation (EU) 679, 2016 (2016)
39. Renn, O., Levine, D.: Credibility and trust in risk communication. In: Kasperson, R.E., Stallen, P.J.M. (eds.) *Communicating Risks to the Public*. Technology, Risk, and Society, vol. 4. Springer, Dordrecht (1991). [https://doi.org/10.1007/978-94-009-1952-5\\_10](https://doi.org/10.1007/978-94-009-1952-5_10)
40. Robinson, S.L.: Trust and breach of the psychological contract. *Adm. Sci. Q.*, 574–599 (1996)
41. Rodway, P., Schepman, A., Lambert, J.: Preferring the one in the middle: further evidence for the centre-stage effect. *Appl. Cogn. Psychol.* **26**(2), 215–222 (2012)
42. Saldaña, J.: *The Coding Manual for Qualitative Researchers*, 4th edn. SAGE Publications Inc., Thousand Oaks, CA, USA (2021)
43. Söderström, E.: Trust types: an overview. *Discourses Secur. Assur. Priv.* **15**(16), 1–12 (2009)
44. Stasser, G., Kerr, N.L., Davis, J.H.: Influence processes and consensus models in decision-making groups. *Psychol. Group Influence* **2**, 279–326 (1989)
45. Svensson, Å., Lundberg, J., Forsell, C., Rönnerberg, N.: Automation, teamwork, and the feared loss of safety: air traffic controllers' experiences and expectations on current and future atm systems. In: *Proceedings of the 32nd European Conference on Cognitive Ergonomics*, pp. 1–8 (2021)
46. Vaismoradi, M., Turunen, H., Bondas, T.: Content analysis and thematic analysis: implications for conducting a qualitative descriptive study. *Nurs. Health Sci.* **15**(3), 398–405 (2013)
47. Webb, J., Maynard, S., Ahmad, A., Shanks, G., et al.: Information security risk management: an intelligence-driven approach. *Australas. J. Inf. Syst.* **18**(3) (2014)
48. Whitman, M.E., Mattord, H.J.: *Principles of Information Security*, 7th edn. Cengage Learning (2022)
49. Yadav Ph D, S.B., Dong, T.: A comprehensive method to assess work system security risk. *Commun. Assoc. Inf. Syst.* **34**(1), 8 (2014)









## Information security risk management tools in the air traffic management domain: what are practitioners' needs?

Simon Andersson, Erik Bergström, Martin Lundgren, Karin Bernsmed & Guillaume Bour

To cite this article: Simon Andersson, Erik Bergström, Martin Lundgren, Karin Bernsmed & Guillaume Bour (06 May 2025): Information security risk management tools in the air traffic management domain: what are practitioners' needs?, Information Security Journal: A Global Perspective, DOI: [10.1080/19393555.2025.2498472](https://doi.org/10.1080/19393555.2025.2498472)

To link to this article: <https://doi.org/10.1080/19393555.2025.2498472>



© 2025 The Author(s). Published with license by Taylor & Francis Group, LLC.



Published online: 06 May 2025.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)

# Information security risk management tools in the air traffic management domain: what are practitioners' needs?

Simon Andersson<sup>a</sup>, Erik Bergström<sup>b</sup>, Martin Lundgren<sup>c</sup>, Karin Bernsmed<sup>d</sup>, and Guillaume Bour<sup>d</sup>

<sup>a</sup>Computer Science, Electrical and Space Engineering, Luleå University of Technology, Luleå, Sweden; <sup>b</sup>School of Engineering, Jönköping University, Jönköping, Sweden; <sup>c</sup>School of Informatics, University of Skövde, Skövde, Sweden; <sup>d</sup>SINTEF Digital, Trondheim, Norway

## ABSTRACT

Information Security Risk Management (ISRM) activities are essential for organizations seeking to control and monitor risk. However, it is well known that doing so is difficult, and the different ISRM activities provide different challenges. To provide support, ISRM tools can be used. Such tools can come in the form of spreadsheets, document templates, or dedicated software to support either part of or the full ISRM work. Few studies have been conducted investigating the use of such tools and their necessary properties. Through semi-structured interviews with 17 security practitioners in the Air Traffic Management (ATM) domain and five validation sessions with 34 experts, this study examines the needs of security practitioners using ISRM tools. The ATM domain was chosen as the study context since they use a method built on the ISO/IEC 27005 standard, which, unlike other ISRM frameworks, does not provide tool support. The findings contain a collection of properties needed in ISRM tools. Notably, the ability to get a holistic view of risks in and toward the organization, tool flexibility, and the ability to get assistance with documentation and information exchange. We also identify that current ISRM tools do not provide enough support and suggest ways to address this.

## KEYWORDS

Air traffic management; aviation; cybersecurity; information security risk management; security practitioner



## 1. Introduction

Risk management is often described as the cornerstone of information security. It is the continuous process of identifying valuable information assets, what might negatively impact those assets and to what extent, as well as what the most effective (given the available resources) ways are to proactively or reactively address the cause of those impacts (Whitman & Mattord, 2014). As such, Information Security Risk Management (ISRM) has become an important aspect for many different types of organizations.

Even for organizations that have traditionally not been associated with information security, such as the car industry (Salin & Lundgren, 2023) and aviation industry (De Gramatica et al., 2015) – the latter of which is the context of this study. Over the years, a myriad of methodologies and (even industry-specific) standards have been developed to guide practitioners in implementing ISRM processes, often as a series of steps and activities. To be applicable in different contexts, ISRM

methodologies are often generic in nature, where the focus is on rule-based descriptions of what to do, rather than how (Njenga & Brown, 2012). However, despite the vast options of methodologies, ISRM has been reported as being difficult to implement and translate into practice (Maneerattanasak & Wongpinunwatana, 2017; Osborn et al., 2018). Especially for novices who have little or no previous experience and know-how in information security (Wangen, 2017). ISRM challenges, to name a few, include activities such as asset identification and valuation, predicting the level of risk toward assets, as well as sharing information and practical know-how between stakeholders (Bergström et al., 2019; Fenz et al., 2014). To assist in these challenges, as well as the overall ISRM methodology, various supporting tools have been developed that can further aid practitioners through the process steps and elaborate on its activities (Gritzalis et al., 2018).

As the old Chinese proverb goes: *for one's work to be done properly, one must first sharpen the tools.*

**CONTACT** Simon Andersson  [simon.andersson@tu.se](mailto:simon.andersson@tu.se)  Computer Science, Electrical and Space Engineering, Luleå University of Technology, Laboratorievägen 14, LULEÅ SE-971 87, Sweden

© 2025 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

However, research on ISRM tools is sparse (Bergström, Welch, et al., 2023), although there has been an upward trend in the last decade (Sánchez-García et al., 2023). Some examples include comparisons of tools and their characteristics (Chafiq et al., 2018; M. Ghazouani et al., 2017; Sánchez-García et al., 2023; Tiganoia et al., 2017) and models to guide practitioners in selecting appropriate tools (Gritzalis et al., 2018; Sajko et al., 2010). Even more scarce is research that focuses on what practitioners actually need from ISRM tools, as is the focus in this study. One related example is the study conducted by Bang et al. (2004) more than two decades ago, in which ISRM consultants' experience was used as the basis for a risk analysis tool architecture. Furthermore, the concept of tools in ISRM research is often used interchangeably with particular methodologies or methods (e.g., Feng and Yu (2012); Kaur et al. (2021); Shypovskiy (2023); Wicaksono et al. (2022)). In this study, however, tools are considered a supporting artifact of some shape or form, defined as “*something that helps you to do a particular activity*” (Cambridge Dictionary n.d.). That is, something – such as worksheets, document templates, software, etc.—that is designed to help practitioners implement and perform activities in an ISRM process.

While research on what practitioners need from ISRM tools may be scarce, there are indications that such insights are needed. For example, ISRM tools are often designed to conform with particular standards – typically the ISO/IEC 2700× family or the NIST 800–30 model (Sánchez-García et al., 2023) – outlining its activities in a series of steps to be followed (Gritzalis et al., 2018). While such step-by-step approaches provide a good overview of the process, they could also give the impression that the process is static and not dynamic, thus stifling the organization's flexibility (Lundgren & Bergström, 2019). Similarly, a common characteristic of many ISRM tools is that they focus on risk-level determination (e.g., by qualitative or quantitative assessments) and vulnerability and impact identification (which typically focuses on technical risks that can be automatically scanned for in a network) (Sánchez-García et al., 2023). However, not all risks are technical and could thereby create a false sense of security by only

partially covering the risks in an organization. Moreover, the tools depend on accurate input data in order to support various ISRM activities, such as determining the level of risk. The need for accurate input data must, therefore, be recognized and attained by the practitioner, something which has been shown to be difficult to do in practice (Taylor, 2015; Wangen et al., 2018).

Indeed, ISRM processes have been reported to be difficult to perform even with supporting tools at hand (Gritzalis et al., 2018; Yang et al., 2016), suggesting a gap between the tools and the needs of the practitioners using them. As such, additional work is needed to further our understanding of how tools can better aid the ISRM process to make its activities more efficient for practitioners (Wangen, 2017). This study, therefore, set out to shed additional light on the following question:

- What are security practitioners' needs from supporting ISRM tools?

The remainder of the paper is outlined as follows. Section two outlines ISRM processes and standards as well as related research on tools to aid in its activities. Section three describes the research approach and how the collected data was analyzed, while section four presents the result of the analysis. Finally, section five discusses and highlights the findings of the study and concludes these in section six.

## 2. Background

As outlined above, information security risk management is often described as a process, a series of activities to identify and mitigate risks toward an organization's valuable information assets. Standards such as the ISO 2700× family outline a series of activities to identify and value information assets, assess information security risks, select and implement relevant controls, and finally, monitor, maintain, and improve over time (2022).

Risk management standards and methodologies provide organizations with a description of how to manage risk through recommendations and best practices that tend to be normative, i.e., they say *what* to do, not *how* to do it (AL-Dosari & Fetais, 2023; Tehler, 2023; Wangen, 2017). Additionally, it

is difficult to adapt standards to the organization's local environment, i.e., turning standards into practice (Bergström, 2020; Lundgren, 2020; Niemimaa & Niemimaa, 2017). For example, while activities to identify and value the information that needs to be protected have been described as one of the cornerstones of risk management (Wangen et al., 2018), it is also described as one of the most difficult to conduct (Sajko et al., 2006). Intangible assets, such as reputation, do not always have a monetary value, and subjective judgment may affect the valuation. Similarly, a common practice in ISRM is to assess the level of risk toward the identified assets to serve as a basis for deciding what risks to mitigate and what risks to accept. However, it is not always evident how to estimate the level of risk toward the assets. Risk estimation is often expressed as a formula based on the asset's value, how vulnerable the asset is against potential threats, and how likely it is that those threats become a reality by exploiting the asset's vulnerability and causing damage to the asset (Bergström et al., 2024). However, attaining the information required to conduct such estimations is not always possible in practice (Taylor, 2015; Wangen et al., 2018).

So, while there is no shortage of different methods to pick from, completing the different stated tasks can be challenging (S. Ghazouani et al., 2014). To assist with such tasks, there is the possibility of using tool support. However, it is not clear what tool support actually implies in an ISRM context, and as such, we have kept an inclusive view of what it could be.

### 2.1. ISRM tools

In the context of ISRM, plenty of tools have been developed with different approaches to the way one conducts risk assessments, e.g., qualitative, quantitative, or semi-qualitative. Ionita et al. (2014) identified 25 tools for risk management and/or assessment, all of which use an existing methodology as a basis. More recently, Sánchez-García et al. (2023) identified 35 different tools, 20 of which use an existing model (such as ISO 2700× or NIST 800–30) with the focus of automating the risk assessment. In another study, Bergström, Welch, et al. (2023) identified 18

tools used in ISRM, 14 of which are mentioned to support the overall ISRM work, and the remaining 4 were used for specific parts of it. However, the tools identified by Bergström, Welch, et al. (2023) provide support in different ways, such as setting a structure for how to work, and do not intend to automate the risk assessment. New tools and models are continuously developed and suggested in an ISRM setting, such as Rosado et al. (2024), which developed a framework and accompanying tool focusing on business model patterns. Another example is Moukafih et al. (2024), who developed and suggested a tool specialized for the healthcare sector.

Some ISRM methodologies, such as CRAMM (Cram et al., 2019), Octave-Allegro (Caralli et al., 2007), and EBIOS, provide a tool in the form of, e.g., spreadsheets, document templates and software. In such cases, tools aim to assist organizations in the use of the corresponding methodology. For example, Octave-Allegro (Caralli et al., 2007) provides worksheets and questionnaires focusing on information assets (Alsafwani et al., 2024). The worksheets guide users throughout the risk assessment, resulting in a calculated level of risk. Commonly, tools created for ISRM processes seek a coupling with international certifiable models, such as the ISO 2700× family (Sánchez-García et al., 2023).

The support ISRM tools provided differ. Typical tool properties are automation of tasks, reducing manual work that can generate errors and creating a more streamlined way of work, i.e., guiding the user through the process (Bergström, Lundgren, et al., 2023; Gritzalis et al., 2018; Sánchez-García et al., 2023). One study indicates that the use of tools could reduce subjective judgment in information classification; in that case, the tool assists users by providing set requirements for different types of information, thus easing decisions (Andersson, 2023). Automating parts of the ISRM process is seen as a future challenge (Sánchez-García et al., 2023). More specifically, they mention challenges tied to using tools not targeting both information- and cybersecurity risks (Von Solms & Van Niekerk, 2013), the implementation of a partly or incomplete automated risk assessment (Shameli-Sendi et al., 2016), and the use of inappropriate tools that do not mitigate the predominant types of risk

in their corresponding industry (Bartoš et al., 2014).

The AI revolution may also affect ISRM tools in the future. A new strand of literature is emerging that suggests various ways to implement AI support to enhance risk management. Recent studies suggest that AI can affect most ISRM activities so that they can be performed faster, more impartial, accurately, transparent, and generally more complete, sometimes by itself and sometimes in collaboration with a user or by providing support to users (Biolcheva, 2021). More concretely, AI can, for example, facilitate the development of complete inventories of assets and provide data on asset usage in great detail (Toxirjonovich & Fozilovich, 2022), and provide real-time, up-to-date data on global and organization-specific risks, thereby enabling organizations to prioritize security controls effectively (Al Hayajneh et al., 2023).

While tools do provide support, depending on the type of tool used, there are likely to be some drawbacks. Gritzalis et al. (2018) developed a method for organizations to select an appropriate risk assessment method based on four main criteria. Based on that method, they compare ten popular ISRM methodologies where tool support is considered. They describe that simpler tools, such as spreadsheets, provide limited functionality, are found to be restrictive, and that dedicated software is preferred. However, it was also found that such software can have its own drawbacks, such as input limitations regarding what can be documented and predefined tables for information classification (Gritzalis et al., 2018). In a more general sense, tools and methodologies fail to answer fundamental questions of importance in the ISRM activities, such as how to calculate the likelihood of threats and how we separate critical and non-critical resources (Shameli-Sendi et al., 2016).

## 2.2. ISRM tools for ISO/IEC 27005

The ISO/IEC 2700× family covers the topic of Information Security Management Systems (ISMS), provides best-practice approaches and is considered to be one of the most important standards for risk assessment (Stoll, 2015). It is also the most commonly used methodology to use as a basis for tools (Ionita et al., 2014). The 2018

methodology, handling risk management is, according to previous literature, deemed to be the most complete when compared to other methodologies, such as Octave-Allegro and CRAMM (Agrawal, 2017; Wangen, 2017). Of note, 2018 does not provide specific tools to assist organizations in following their standards and guidelines (Bergström, Welch, et al. (2023)). There are, however, tools created based on the ISO/IEC 2700× family, such as TRiCK and TRiCK Lite, RiskSafe Assessment (deemed to be a methodology that provides a tool), and Smart Information Security Management System (SISMS) (European Union Agency for Cybersecurity ENISA, 2023). Such tools are created to comply with the 2018 methodology of managing risk.

## 2.3. ISRM in the air traffic management domain

Air Traffic Management (ATM) is an umbrella term for a complex system of systems. ATM is made up of both hardware and software components spread over three different types of services: Air Traffic Services (declares the maximum number of aircraft which can be accepted over a given period of time and area), Air Traffic Flow Management (matches air traffic demands with available capacity of airspace and airport resources), and Airspace Management (maximizes the most efficient use of airspace based on time-sharing and need, e.g., between military exercises and commercial flights) (Kistan et al., 2017).

In short, the main function of ATM is to ensure efficient and safe aircraft movement and prevent collisions on the ground and in the air (Nie et al., 2009). As such, coordination and monitoring of information between ATM components and its services is critical. Information, such as an aircraft's position, velocity, and identification, is often shared over wide area networks and requires integrity and availability to ensure operational safety (Costin & Francillon, 2012), but recently also to ensure the security of that information. Information security has not traditionally been emphasized in aviation. Advanced, proprietary, and commercially unavailable hardware and software have long worked as a protection mechanism in itself, much like how security in Operational Technologies has relied on a degree of physical

separation from other information technology infrastructures (Murray et al., 2017). As such, there has been a lack of standardized security management systems to help assess information security risks and requirements of ATM components and services (Labunets et al., 2014). Instead, the focus has been on safety, which, on the contrary, has enjoyed a long history of research on and implementation of standardized safety management systems in ATM (Stelkens-Kobsch et al., 2017). However, in recent years, aviation has lost its technological advantage that protected its communication in the past. For example, wide access to increasingly cheaper tools like software-defined radios has increased the potential of cyberattacks (e.g., manipulation or disruption) on ATM traffic (Strohmeier et al., 2016).

Over the years, ATM-related communication has reached its capacity and efficiency limit, yet with growing traffic demands, particularly in Europe and the United States. As a consequence, programs such as the Single European Sky ATM Research (SESAR) in Europe and the Joint Planning and Development Office for the Next Generation Air Transportation System (NextGen) in the United States were launched to modernize ATM (Casado et al., 2016). The need to work systematically and proactively with information security risks has been recognized in both these programs. For example, within the SESAR program, the SESAR ATM Security Risk Assessment Method (SecRAM) was developed and provided steps, tools and techniques to guide stakeholders across the program to perform risk assessments in a standardized way that is compatible with ISO 27005 (De Gramatica et al., 2015). In order to help non-experts considering the many stakeholders involved in developing, maintaining, and commissioning ATM components and services, SecRAM includes predefined catalogs, listing potential threats, information assets, and security controls (Johnson, 2015). More specifically, the SecRAM material consists of a guidance document which describes the methodology and how to apply it. The tools provided by SecRAM consist of catalogs in the form of a Microsoft Excel spreadsheet that contains pre-defined examples of assets, threats, vulnerabilities, and controls, as well as three different Microsoft Word templates, which

the practitioners use to document the results of their risk assessment.

While previous studies have investigated the efficiency of using such predefined catalogs when performing risk assessments (De Gramatica et al., 2015; Labunets et al., 2015), understanding the use, need, and applications of ISRM tools, however, remains largely uncharted territory.

### 3. Research approach

This study aims to delve into the rationale behind the reasons for needing tool support for ISRM. To be able to acquire an extensive collection of data, we have chosen to employ a qualitative research methodology. Hence, our aim was to identify recurring patterns in our observations rather than assessing preexisting hypotheses, we employed an inductive research strategy (Oates, 2006). By utilizing a qualitative approach, the focus is not on seeking statistical generalizations but rather on achieving saturation of the chosen topic, which is a valid approach in these particular cases (Mason, 2002). Various qualitative approaches to data collection were considered, but due to the nature of the aim, interviews were considered the most suitable. Furthermore, it was decided to focus on a specific group of individuals from the ATM domain where SecRAM is used.

#### 3.1. Data collection

Interviews are a widely recognized research method for gathering qualitative research data that can be performed in multiple ways (Oates, 2006). As the nature of this study is more explorative, semi-structured interviews were selected as they provide the possibility to pursue uncharted territory with follow-up questions (Adams, 2015). The laddering technique was used to systematize the follow-up questions (Reynolds & Gutman, 1988). When using the laddering technique, an interview guide comprising a series of open-ended questions is prepared, and the respondents are repeatedly probed with “why” questions based on their previous answers (Reynolds & Gutman, 1988). Establishing an interview setting that creates a sense of security and minimizes the likelihood

of respondents feeling threatened by the interview setting is crucial, especially when using laddering (Reynolds & Gutman, 1988). We took several measures to achieve such a setting. Firstly, one of the researchers took on the lead interviewer role, asking the majority of the interview questions in the performed interviews, allowing the other participants to take on a more observing role. This also enabled a continuity between the interviews. Secondly, we performed the interviews electronically using an online meeting software (GoToMeeting), making it possible for the whole research team to participate in the interviews while staying in the background. Using an online tool also enabled access to interviewees across Europe. Furthermore, it made it possible for the participating researchers to send questions and comments to the lead interviewer electronically without interrupting and reminding the respondent that there were more participants in the interview.

Two primary sources were used as a basis for the interview guide: (1) existing literature on ISRM tool usage and (2) SecRAM documentation, comprising seven documents totaling 120 pages. This approach ensured that our questions were grounded in both theory and real-world applications.

The interview guide (see Appendix) was structured in three parts. First, one part had introductory questions about demographics and the role of the respondents to understand the respondents' backgrounds better. Typical questions from this part were, for example, *"How long have you worked with security?"* and *"Have you worked with other ISRM methodologies than SecRAM?"*

The next part of the interview guide focused on working with SecRAM in practice. Furthermore, we focused on the activities performed as a part of ISRM, such as asset identification, and the documentation of the activities. The questions were deliberately designed to inquire about how the practitioners worked with risk management to first get a better understand of the needs they had in their work, before moving to more direct questions about tool support. Questions asked in this part of the interview were, for example, *"How did you identify the assets?"* and *"Is there anything you*

*have experienced that is particularly challenging with SecRAM?"*

In the third and final part of the interview guide, we focused more directly on tool support and returned to the questions in the second part to follow-up using the laddering technique to elicit knowledge on what tool support could provide. A typical laddering question from this part was *"Could you give an example?"*. A more specific tool question was, for example, *"What type of functionality are you missing?"*

It is well-known that it is normally very difficult to collect data in the cybersecurity domain (Baskerville et al., 2018; Cram et al., 2019; Kotulic & Clark, 2004), and perhaps even more challenging when critical infrastructure is considered. Despite this, we performed 17 interviews during the fall of 2019 with respondents who all use SecRAM as part of their job. The respondents' roles, titles and backgrounds varied. Some had more management-oriented roles (for example, as Chief Information Security Officer and IT security manager), while others had more development-oriented roles (for example, computer engineer, security engineer and aerospace engineer) or operative roles (for example, cyber security analyst and security expert). Most respondents had experience working with other ISRM methodologies, such as ISO 27005 or MAGERIT (Amutio et al., 2014). The common theme among the respondents was that they all had hands-on experience applying SecRAM in practice and assessing security risks in European ATM research and development projects. That means the respondents also shared the conditions in the domain and the terminology used. In addition, most respondents have several years of experience applying SecRAM and using an Excel tool and Word templates that support SecRAM. Respondents were recruited by one of the authors who contacted possible participants based on recommendations from experts who participated in the SESAR transversal project PJ19: Content Integration (2020).

Each interview was recorded as an audio file that a research assistant transcribed. One of the authors then examined and cross-referenced the transcriptions against the audio file. Every interview lasted approximately one hour, corresponding to 209 pages of transcribed text.

### 3.2. Data analysis

We followed the coding recommendations from Saldaña (2021) for the analysis, emphasizing the need for a two-cycle coding process. The first-cycle coding was performed by applying structural coding, which is extra suitable when the data comes from semi-structured interviews with multiple respondents (Saldaña, 2021). Structural coding leads to large segments of text that form the basis for in-depth analysis (MacQueen et al., 2008). In this case, one of the authors made most of the structural coding and prepared the first version of the categorization, where similarities, differences, and correspondence (Saldaña, 2021) were considered. After this initial step, the iterative work of re-coding and re-categorization was made as a group effort. During the re-coding and re-categorizing, a synthesis led to the development of 18 categories, ultimately leading to the development of two themes. These themes are based on what type of support users need from ISRM tools: automation and assistance. Automation refers to tasks where stakeholders are automatically provided with something from the tool without user input. For example, calculating a risk score or generating a report are examples of categories found under the theme automation. The theme assistance describes tasks where a stakeholder is provided with some type of assistance while using the tool. For example, to give examples or an overview of the task at hand. For the coding, we used the qualitative analysis software NVivo, but for the last iterations of coding, the data was moved to a word processor.

### 3.3. Validation

ISRM research often lacks validation, and scholars propose diverse methods to address this (Fenz & Ekelhart, 2011). Silverman (2015) advocates for qualitative research approaches that take “one’s findings back” (Silverman, 2015, p. 92) to see if they correspond to their experiences. Such an approach can be performed in several ways, for example, by taking it back to the respondents (Thornhill et al., 2016) or by taking it back to a panel of experts (Fenz & Ekelhart, 2011). Although an expert panel is opinion-based, it is one of the few ways to validate ISRM findings (Fenz & Ekelhart, 2011).

For the validation, we opted to widen the discussion by getting insights on the findings from a wider pool of experts in both the public and private sectors from domains other than ATM. This was done to get a cross-sector perspective and thereby improve the validity of the findings. According to the suggestions in Fenz and Ekelhart (2011), we selected a team of external experts, in this case, 10 senior experts at the Swedish Civil Contingencies Agency, all working in the same unit with systematic information security at a national level. The expert panel was held as an hour-long session divided into two parts. First, a presentation of the preliminary results, followed by a discussion of the results. After the validation, the categories were re-categorized, and ultimately, the themes, as presented in the result section, were derived.

The end results were validated through three separate expert panels and a professional risk-focused conference involving participants from both practice and academia. Two of these panels included representatives who had participated in the initial expert panel, ensuring continuity in the validation process. The third panel consisted of two representatives from a separate government agency that had not been previously involved in data collection or validation, providing an additional external perspective. Additionally, the results were validated at a professional risk-focused conference through a presentation and discussion session. The discussion session was attended by 20 participants from diverse backgrounds. This broad representation was considered valuable, as most organizations engage in some form of risk analysis. The validations of the final results and the conference presentation only led to minor adjustments, primarily in the naming of categories. In total, 5 validation sessions were conducted, with a total of 34 professionals participating.

## 4. Results and analysis

Based on the analysis, this section is divided into two themes: Automating and Assisting. Each theme presents the categories found in the analysis.

## 4.1. Automating

### 4.1.1. Efficiency

In its current form, the ISRM tool consists of Excel spreadsheets and Word templates, which are perceived as limiting, and respondents experience a lot of repetition. They exemplify that they have to answer the same or very similar questions several times over in different steps of the process, and having to manually move data between tabs of the tool, i.e., copy-pasting, this is experienced to be double-work. Several respondents express their wish for those types of activities to be automated, partly to save time and to avoid errors. It is further explained that a lot of time is spent doing things deemed unnecessary, again, such as copy-pasting information, and that a lot of time could be saved and, as a result, be spent on what is considered to be more critical activities. Another example that is brought up is to *calculate risk* levels, and respondents suggest that this could and should be automated. There would still be the necessary inputs of likelihood and impact; however, the actual automation would happen in the calculation stage of the risk level, removing one necessary step from the user and automating it for increased efficiency. It is further wished that this calculation and the corresponding likelihood and impact values are connected to the asset and risk being assessed. This would further decrease the number of inputs from users and save them valuable time.

Respondents also mentioned the need for a tool to *give timely reminders*. Reminding users of when to conduct certain tasks, such as when to re-visit a previously done risk analysis or when it is time to re-classify information. Such reminders are viewed to be helpful.

Writing reports is seen as something that could and should be automated, at least in part. There are several arguments from respondents on why this is the case, most of which are based on the interest of saving time. It is explained that it is possible to make the overall ISRM work more effective if respondents could do less of what they perceive as busy work, such as writing reports, and instead focus on the risk analysis, thus making the process more effective. There is also a wish to link the Excel sheets together to automatically *generate reports*, reducing the amount

of necessary copy-pasting. This would reduce the required amount of work to, as one respondent puts it, intelligent work in the generation of reports. Respondents also asked to have the final result generated in one single report file, and they motivated this by stating that it would be easier to share information that way, which is seen to be another issue. As is, there is often overlapping work being done in different versions of the same document. This is confusing and information tends to be diverted to places where it is not supposed to be as a result.

### 4.1.2. Accuracy

Interviewed respondents asked for the automation of tasks in a variety of ways, mainly as they believe it would limit the double-work, such as having to calculate risk and input values several times over, copying and pasting information from one tab to another in the ISRM tool, and having to manually keep track of risk assessment values such as likelihood and threat tied to a specific asset. As mentioned, one of the main reasons for this is to save time. The other reason, however, is to avoid mistakes and, as a result, increase the accuracy of the IRSM process results. This was explained by one of the respondents as:

So, a manual completion, a manual filling of the template could also generate errors because the values are normally a large number of values to be inserted, so mistakes can happen in the completion in the reporting of some values from one table to another. A supporting tool could be useful. - I10

As mentioned by the respondent, such mistakes could be avoided by automating certain tasks in the ISRM tool, such as moving information from one table to another or calculating risk levels. Doing so would reduce the number of inputs necessary and, as a result, provide fewer opportunities for inputting inaccurate information.

There are also wishes for the ability to connect the risk assessment with its corresponding primary- and supporting assets, threats, vulnerability and risk in some way. During the interviews, it was explained how users have to keep all of these factors in mind while working with the assessment, which, according to respondents, makes it difficult to focus and results in mistakes in the assessment.

A suggested solution from a respondent is to keep the different parts of the risk assessment grouped together throughout the steps. Doing so would reduce user input, remove the burden of mentally keeping track of the different parts and allow for more focus on the assessment at hand.

#### 4.1.3. Consistency

Having a *consistency* throughout the ISRM process, both *within activities*, and *between activities*, is essential for several respondents. It is explained that being able to track evaluations and assessments done in the ISRM tool throughout the different steps and making all the assessments match, i.e., making sure they are coherent with one another and look the same way, is important. If there is no consistency, respondents mention that it gets confusing and challenging to keep track of both specific assessments and how they are connected.

It helps to track the evaluations, the assessment crossing the solution. To make more coherent all the assessments. This was one of the reasons that pushed us to realise this Excel sheet. - I10

Another respondent mentions the importance of having different activities connected with one another to ensure that if a change is made in one activity, that change should automatically be applied in other relevant areas. An example here is if a countermeasure is mapped to one asset, it should show throughout the ISRM process, not only where the user input took place. One respondent explained that there was no such solution at the moment, and when they modified something in a specific task, it would impact other parts of the same document. However, as it stands, all changes must be tracked and modified by the user; a wish from respondents is that the changes should be automated.

## 4.2. Assisting

### 4.2.1. Learning resources

There is a varying degree of experience in information security and the use of the SecRAM tool and methodology amongst the respondents. Several mentioned that having the different activities of both the methodology and tool explained, as in

the purpose of specific activities but also the overall purpose of the work, is necessary. Some respondents find the tool confusing to use and are unsure of what is required from them and what the activity is supposed to result in. As a proposed solution, they wish for more guidance in each activity, i.e., a tool should *explain difficult steps* of what is supposed to be done, have examples provided, as well as guidance throughout the ISRM process and its activities. Thus avoiding guesswork and speculation about how tasks should be conducted.

The way users motivate why explanations are needed differs somewhat. Less experienced users wish to have comprehensive explanations for each ISRM step, and some want the tool to *explain concepts*. As is, there is guidance present for each step, but respondents argue that it's not enough to make them understand what to do while mentioning that more experienced users probably do not see this as a problem. They further explain that with more thorough explanations, they would not only understand the task better, but they would also avoid having to go back in the process at a later stage and re-do steps they then realize have been misunderstood, misinterpreted or simply not performed. There is also the mention of wanting more explanation regarding questions (i.e., providing information surrounding the question) in the different Excel spreadsheets provided by the tool.

Getting assistance with the overall purpose of activities and security concepts, in general, is also regarded as important. The reasons for this vary; some have had a hard time understanding the purpose of the work, some found it challenging to grasp the bigger picture of what they were doing, and as a result, had a hard time getting started. This is exemplified by one respondent who said:

As I said, I need a more detailed explanation for each chapter, but that is because I have no background. We have this good connection between template and guidance. I assume for everybody who knows what to do in security it is very easy then to fill out the different chapters because there is a short explanation. 'In this chapter, there are supporting assets and then what I have to do there. I check, then I can fill it out.' I think this is very good for everybody who has experience in security since five, ten or more years, but not for me. - (I14)

Again, some respondents had less experience than others, and they explained that this made the tool difficult to use and understand. One respondent mentioned that it was difficult to understand, e.g., the terminology being used, and another mentioned that it was difficult to understand both the purpose of the process and specific steps. A third respondent states that a detailed description of each step would be necessary in order to successfully understand and complete the task at hand.

#### 4.2.2. Communication

The terminology used in the ISRM tool is something respondents explain to be hard to understand, especially to those who were new to the methodology and cybersecurity field. It is explained that some terms, such as asset, are seldom used in other domains and that there are others, oftentimes very specific and technical concepts used in security, that remain unexplained. A respondent mentioned that getting familiar with the different terms and concepts being used was difficult. However, as time went on, they mentioned that they became less reluctant to use certain terminology. Explaining concepts and using a *standardised terminology*, i.e., making sure everyone in the organization uses and understands terms and concepts in the same way, would allow users to easily and more quickly get familiar with concepts and terms used in the security domain. This ensures that there is a common understanding of specific terms, thus avoiding misunderstandings.

External communication is explained to be difficult. The reason given for this is not the contents of the ISRM assessment report but, instead, the fact that there are no guidelines for how to distribute the document to other stakeholders and parties. That is., there is a wish for assistance in ensuring there is *secure communication* between parties that take part in the ISRM report to avoid exposing them to high levels of risk.

#### 4.2.3. External intelligence

Making decisions often requires some level of underlying knowledge or information; in the case of the respondents, there are wishes for a function that could provide external knowledge, e.g., threat intelligence.

One of the main reasons why external knowledge is described as important is the constantly changing nature of cybersecurity. A respondent explains that one can not rely only on historical information when assessing risk:

Cybersecurity nature is this; you can not rely on historical information anymore. Historical information, you used it, you assessed it, and yet you put something in place, but the threats are going to evolve. - (I5)

The collection of previous decisions and knowledge is important but should be complemented with outside information. According to the respondent, this is important given the evolution of threats over time, and having access to external knowledge can allow for better-informed decisions.

#### 4.2.4. Process guidance

Respondents ask for guidance in the ISRM process in several different ways, such as getting *different perspectives* of assets, having a *flow between activities*, i.e., making sure newer users understand how the SecRAM methodology works using in-tool support, having the tool be able to *give an overview* and to provide a way of generating and assisting with *structured documentation* based on results and decisions made.

One respondent argues that capturing knowledge from previous projects within the organization is just as important as having access to external knowledge and that internal knowledge can be re-used to better spot things related to the current assessment of risk. There is also mention of having more heterogeneous groups conducting the risk assessment together, and as a result, a wider variety of views will be available for the assessment. The respondent explains that using more heterogeneous groups would allow for other viewpoints of assets and potential vulnerabilities regarding confidentiality, integrity and availability. However, the same respondent mentions that while this would increase the time spent, as more points of view would have to be considered in the ISRM process by including viewpoints of, e.g., a lawyer, it would lead to a more comprehensive investigation and as such, a more informed decision. Lastly, there is mention of the value of being able to reflect and analyze assets together, to come up with more perspectives. There should be support for this in a tool.

Respondents wish for the steps and tasks aided by the SecRAM tool to provide a clear and distinct workflow. This is exemplified in several ways, such as respondents finding it difficult to understand what was needed for a specific activity, having to go back and forth throughout the activities as explanations were not clear enough, and a general lack of understanding of how SecRAM works. There are wishes for guidance and structure to make the work more straightforward and for a tool to support users with an understanding of how to use SecRAM as a methodology. One respondent mentioned that there is teaching and support involved when less experienced users start using SecRAM and mentioned that it would be good to have support from the tool itself to further aid with this. Such support could assist users in making sure that all necessary parts of a task have been completed and to increase their understanding of the task itself. As one respondent puts it:

I'm not thinking about expensive tools, but maybe it could be an Excel sheet with some information. That could be really good to help apply that methodology. We know that most of the steps are really automatic. Doing it on paper is not the best. - (I3)

Several respondents say that getting an overview of the ISRM process is another feature that would help them understand activities and form a complete understanding of the work. The ability to see an overview of the process and its contents would allow users to see their progress in the different steps of the process, the pieces of analysis that are completed, and what the different tasks are supposed to lead to in the end. As it stands, respondents want to provide a full picture, and they do their best not to forget specific parts of activities but find it challenging to do so.

Another way of providing process guidance is through *structured documentation* practices. As has been previously mentioned, respondents mention that process documentation is important; however, several also mention that it is their least favorite part of the ISRM work and most would like it to be automated in some sense. It further explained that it is important to track the assumptions made over time, map and connect supporting and primary assets, and state what decisions have been made on how to handle

risks. This is all important information to keep documented and easily available, as, without it, the upcoming iterations of work will be more difficult if there is no documentation on why and how decisions were taken, nor on what basis they were made. There is also a large emphasis on the importance of documenting decisions from respondents, as well as the ability to access that documentation later on. One respondent argues that having access to previous documentation throughout the process would make it easier for everyone involved, as those who are to continue the process, later on can easily identify on what grounds previous decisions have been made and provide further perspective on current assessments.

## 5. Discussion

This study provides insight into users' perceptions of the SecRAM Methodology and their views of its provided tool. More specifically, the results showcase properties that users wish would be present in ISRM tools. Validating our findings through expert sessions provided an important layer of scrutiny, ensuring that the identified ISRM tool properties align with security practitioner needs.

Firstly, regarding the two themes of automation and assisting, there seems to be a general over-belief in both scientific literature (e.g., Sánchez-García et al. (2023)) and other literature (e.g., in Forbes (Vashistha, 2021)) that it is possible to automate the risk assessment completely – or at least to a very large extent. Our study shows that the respondents do not have such expectations and that there are a great deal of tasks where users do not expect automation but rather assistance in performing the task. This was further discussed and confirmed during the validation sessions. [Table 1](#) summarizes the findings in the automation theme and outlines the categories and subcategories where automated tool support is expected. There is an obvious relation between efficiency and accuracy, for example, if a copy-paste is avoided, the possibility of a manual error is also avoided, and hence automated tasks that increase efficiency also increase accuracy. There is, however, a pedagogical point to make and emphasize both accuracy and efficiency. Initially, more such relations could be

**Table 1.** The summarised finding in the automation theme. The categories are in italics, and the subcategories belonging to a category are immediately below.

Categories and subcategories	Explanation
<i>Efficiency</i>	Category aiming at saving time by not performing double-work (e.g. copy-paste) so that more time can be spent on performing the tasks.
Calculations	It is more efficient to have for example risk calculations performed automatically.
Give timely reminders	Many revisits, e.g. previous risk analyses or valuations with certain time intervals, and reminders assist users.
Generate reports	The need for automatic collection of data located in various tabs or documents
<i>Accuracy</i>	Category aiming at the tasks where automation decreases the likelihood of errors that could arise from manual work.
<i>Consistency</i>	There is a need to have a consistent solution that automatically ties together the overall view of the ISRM process.
Between activities	Changes in one activity should affect other ISRM activities automatically.
Within activities	Changes within an activity should internally be consistent.

**Table 2.** The summarised finding in the assisting theme. The categories are in italics, and the subcategories belonging to a category are immediately below.

Categories and subcategories	Explanation
<i>Learning resources</i>	Tools should be able to assist the user with different types of help.
Explain difficult steps	Explanations should be provided for steps perceived as problematic, e.g. how to identify or value assets.
Explain concepts	Explanations should be provided for concepts perceived as difficult, e.g. the meaning of confidentiality.
<i>Communication</i>	Tools should assist the organisation and users to communicate in various ways standardised and secure.
Standardised terminology	Tools should enable and support the use of a standardised internal language.
Secure communication	Tools should provide a platform for distributing, e.g. results and reports to internal and external stakeholders.
<i>External intelligence</i>	The tool should help provide external knowledge, e.g. threat intelligence information.
<i>Process guidance</i>	The tool should assist the user with guidance throughout the process.
Different perspectives	Providing support for users to be able to view, for example, the impact on an asset differently depending on your background.
Give an overview	Users expect the tool to deliver information on where in the overall ISRM process they are and what the next steps will be.
Structured documentation	The tool should assist the user to collect and document in a structured way.

found, but as a result of our validation, they have, to the best of our ability, been minimized. Related to automation, some fundamental issues are identified in, for example, Shameli-Sendi et al. (2016) about the input to the risk assessment, e.g. the calculations of the likelihood of a threat and the separation of critical from non-critical resources that are hard to perform automatically, especially if it is a qualitative risk assessment.

Table 2 summarizes the findings in the assisting theme and outlines the categories and subcategories where there is an expectation of assistance from a tool. Several categories relate to the ISRM process, which is often perceived as hard to navigate or understand. One of the challenges with ISRM is that there are different approaches to how ISRM is implemented in practice compared to how they are described in formal processes (Alaskar et al., 2015; Lundgren, 2020; Niemimaa & Niemimaa, 2017; Njenga & Brown, 2012), and can, therefore, be hard to overview and comprehend for users.

A main gripe of respondents is having to re-do the same or similar tasks several times over, this could likely be attributed to Excel sheets being used for the different activities as they have

indeed been described as being limiting in ISRM literature (Gritzalis et al., 2018). It is, however, a convenient tool, as the Microsoft Office package is very commonly used. The SecRAM tool attempts to guide users through the different activities that make up the process through short explanations and examples; how successful this is viewed differently depending on the experience of the respondent. Respondents with more experience find the existing guidance to be good enough, while more junior respondents describe that there is a lack of guidance and that it does not assist them enough to make them understand the purpose of what they are doing or how to do it. Not very surprisingly, this indicates that less experienced users require more assistance, as was indicated and confirmed during validations. The solution to this could be to simply add more information and examples; however, it could also be to change tools to a dedicated software supporting the whole ISRM process, as is suggested by literature (Gritzalis et al., 2018) and present information and guidance in a different manner. Additionally, when presenting information, Andersson (2023) suggests that standardized terminology should be

used to allow users to interpret terms in the same way. The need for a common language has also been identified in previous studies, such as Ekelhart et al. (2007), Wangen and Snekkenes (2013), and Bergström et al. (2019), suggesting that standardized terminology is effective as a way to avoid confusion when communicating.

A very interesting observation is that less than a third of the 35 tools identified by Sánchez-García et al. (2023) cover all tasks that are to be performed in the risk assessment. Most of the tools in their study lacked partial or complete support for asset, threat or existing control identification or in the selection of an acceptable risk value. Such features have previously been identified as useful by practitioners as they could bring together supporting information about the risk assessment and thereby help identify relevant threat scenarios and reduce uncertainty (Erdogan et al., 2022). Similarly, Bergström, Welch, et al. (2023) concluded in his study on tool usage in the public sector that tools need to be more encompassing in terms of supporting tasks and that it is a disadvantage to spread the activities over several separate tools. The category process guidance elaborates on this need. The respondents, for example, need an overview of the tasks and guidance between them.

In this work, we investigated security practitioner's ISRM tool needs. The focus has been on the needs and not on how the solution can be realized. For example, the category external intelligence is one example of AI being a very suitable solution to address the need, as has been shown in the telecom industry, where a survey revealed AI can provide support for threat identification (Ebere-Uneze & Naqvi, 2024). AI could also help ISRM in various ways, for example, by providing decision support to decrease subjective judgment in most ISRM activities. AI has also been identified as a key for operational risk management, e.g., by helping identify emerging threats in the financial sector (Dewasiri et al., 2024), and for threat identification in the hospitality sector (Pipyros & Liasidou, 2025). The advances in cybersecurity operations also help ISRM as it can trigger a reevaluation of information classification or risk analysis.

## 6. Conclusion

This paper takes a step back and investigates the core reasons why we need tools supporting ISRM. We nuance the picture and show that ISRM tool users' expectations are not that all tasks must be automated and that many users require assistance instead. One reason for this might be that there are tasks that are very complex to implement.

The paper contributes to tool developers by taking a holistic view of ISRM and its tasks to identify tool users' needs and expectations of the automation level for these tasks. The paper is a starting point for continued data collection aiming to investigate further and refine the needs identified and transform them into design requirements and design principles so that the ISRM tools in the future can deliver better support to security practitioners seeking to use tools to support their work. One way of continuing this work would be to perform a broader data collection, e.g. using a survey, to get broad input on the categories. With quantitative data, we could, for example, draw conclusions on what functionalities would help out the most if implemented, and it could also be used by tool developers to prioritize.

Based on the analysis and expert validation, two themes emerged that elaborated on security practitioners' needs from supporting ISRM tools: Automating and Assisting. The Automating theme captured aspects of removing double work and increasing efficiency, such as built-in help in the tool to avoid human errors and mistakes when calculating or entering values. It was also noted that tools with such features could also help with consistency over time and between assessments. The Assisting theme captured aspects such as support and guidance for the practitioners to perform the ISRM process and its activities. These aspects strove to make the process and its activities more transparent, detailing what different concepts and terminologies entailed and clear instructions as to what was required to complete the different activities and why so as to avoid guesswork and ease communication between ISRM practitioners.

This study set out to further the research stream on practitioners' needs from supporting ISRM tools. The insights from this study present new

avenues for future research. For example, revisiting the research question in different contexts or environments can broaden the scope and further deepen our understanding of practitioners' needs from supporting ISRM tools. Additionally, exploring to what extent such tools would actually benefit practitioners is also ripe for future research.

## Acknowledgments

We gratefully acknowledge the Swedish Civil Contingencies Agency (MSB), project VISKA (MSB 2021-14650) and the funding from the SESAR JU under the EU H2020 research and innovation program (grant agreement 731765). We also gratefully acknowledge the support from Interreg Aurora to the ISSUES project.

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## Funding

The work was supported by the Interreg [20357977]; The Swedish Civil Contingencies Agency [MSB 2021-14650]; SESAR Joint Undertaking [731765].

## References

- Adams, W. C. (2015). *Conducting semi-structured interviews*. Jossey-Bass.
- Agrawal, V. (2017). A framework for the information classification in ISO 27005 standard. In *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)* (pp. 264–269). IEEE. New York, New York.
- Alaskar, M., Vodanovich, S., & Shen, K. N. (2015). Evolution of information security research on employees' behavior: A systematic review and future direction. In *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS)* (pp. 4241–4250). ISBN 147997367X. Kauai, Hawaii.
- AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach. *Electronics*, 12(17), 3629. <https://doi.org/10.3390/electronics12173629>
- Alsafwani, N., Fazea, Y., & Alnajjar, F. (2024). Strategic approaches in network communication and information security risk assessment. *Information*, 15(6), 353. <https://doi.org/10.3390/info15060353>
- Amutio, M., Candau, J., & Mañas, J. A. (2014). Magerit-methodology for information systems risk analysis and management. *Ministry of finance and public administration*. Spain.
- Andersson, S. (2023). Problems in information classification: Insights from practice. *Information & Computer Security*, 31(4), 449–462. <https://doi.org/10.1108/ICS-10-2022-0163>
- Bang, Y.-H., Jung, Y.-J., Kim, I., Lee, N., & Lee, G.-S. (2004). The design and development for risk analysis automatic tool. In *Computational Science and Its Applications-ICCSA 2004: International Conference* (pp. 491–499). Springer, Assisi, Italy. May 14–17, 2004, *Proceedings, Part I 4*.
- Bartoš, J., Walek, B., Klimeš, C., & Farana, R. (2014). Fuzzy application with expert system for conducting information security risk analysis. In *Proceedings of the 13th European Conference on Cyber Warfare and Security* (pp. 33–41). Piraeus, Greece.
- Baskerville, R., Rowe, F., & Wolff, F.-C. (2018). Integration of information systems and cybersecurity countermeasures: An exposure to risk perspective. *SIGMIS Database*, 49(1), 33–52. <https://doi.org/10.1145/3184444.3184448>
- Bergström, E. (2020). *Supporting information security management: Developing a method for information classification* [PhD thesis]. University of Skövde.
- Bergström, E., Andersson, S., & Lundgren, M. (2024). To risk analyse, or not to risk analyse: That's the question. In Nathan Clarke, Steven Furnell (Eds.), *International symposium on human aspects of information security and assurance* (pp. 107–119). Springer.
- Bergström, E., Lundgren, M., Bernsmed, K., & Bour, G. (2023). "Check, check, check, we got those" - catalogue use in information security risk management. In S. Furnell & N. Clarke (Eds.), *Human aspects of information security and assurance* (pp. 181–191). Springer Nature Switzerland. ISBN 978-3-031-38530-8.
- Bergström, E., Lundgren, M., & Ericson, Å. (2019). Revisiting information security risk management challenges: A practice perspective. *Information and Computer Security*, 27(3), 358–372. <https://doi.org/10.1108/ICS-09-2018-0106>
- Bergström, E., Welch, C., Nolte, A., Rajanen, M., Island, A. S., Hult, H. V., & Ravarini, A. (2023). Tools supporting information security risk management in practice. In P. Bednar, F. Zaghoul, & A. M. Braccini (Eds.), *9th International Conference on Socio-Technical Perspective in Information Systems Development, STPIS* (Vol. 3598. pp. 146–159). CEUR-WS. Portsmouth, United Kingdom.
- Biolcheva, P. (2021). The place of artificial intelligence in the risk management process. In *SHS Web of Conferences* (Vol. 120. pp. 1–9). EDP Sciences. Starozagorski bani (online), Bulgaria
- Cambridge University Press. (n.d). Tool. *Cambridge Dictionary*. Retrieved August 25. <https://dictionary.cambridge.org/dictionary/english/tool?q=Tool>
- Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). *Introducing OCTAVE Allegro: Improving the information security risk assessment process*. Report No.: CMU/

- SEI-2007-TR-012. Software Engineering Institute, Carnegie Mellon University.
- Casado, E., Rodriguez, R., Taboso, P., & García, J. (2016). Information security in future air traffic management systems. *Journal of Aerospace Information Systems*, 13(3), 101–112. <https://doi.org/10.2514/1.I010233>
- Chafiq, N., Talbi, M., & Ghazouani, M. (2018). Design and implementation of a risk management tool: A case study of the moodle platform. *International Journal of Advanced Computer Science & Applications*, 9(8), 2018. <https://doi.org/10.14569/IJACSA.2018.090858>
- Costin, A., & Francillon, A. (2012). Ghost in the air (traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. *Black Hat USA*, 1, 1–12.
- Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, 43(2), 525–554. <https://doi.org/10.25300/MISQ/2019/15117>
- De Gramatica, M., Labunets, K., Massacci, F., Paci, F., & Tedeschi, A. The role of catalogues of threats and security controls in security risk assessment: An empirical study with atm professionals. In *Requirements Engineering: Foundation for Software Quality: 21st International Working Conference, REFSQ 2015*. 21. (pp. 98–114). Springer, Essen, Germany. March 23–26, 2015
- Dewasiri, N., Dharmarathna, D., & Choudhary, M. (2024). Chapter 13 Leveraging Artificial Intelligence for Enhanced Risk Management in Banking: A Systematic Literature Review. In R. Singh, S. Khan, A. Kumar, & V. Kumar (Eds.), *Artificial Intelligence Enabled Management: An Emerging Economy Perspective* (pp. 197–214). Berlin, Boston: De Gruyter. <https://doi.org/10.1515/9783111172408-013>.
- Ebere-Uneze, I., & Naqvi, S. (2024). Using artificial intelligence in cyber security risk management for telecom industry 4.0. In *Proceedings of the 19th International Conference on Availability, Reliability and Security*, ARES '24, New York, NY, USA. Association for Computing Machinery. ISBN 9798400717185.
- Ekelhart, A., Fenz, S., Klemen, M., & Weippl, E. (2007). Security ontologies: Improving quantitative risk analysis. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, IEEE. Big Island, Hawaii.
- Erdogan, G., Tondel, I. A., Tokas, S., Garau, M., & Jaatun, M. G. (2022). Needs and challenges concerning cyber-risk assessment in the cyber-physical smart grid. In *Proceedings of the 17th International Conference on Software Technologies (ICSOFT 2022)*, SciTe Press.
- European Union Agency for Cybersecurity. (2023). RM/RA Tools. <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools>
- Feng, N., & Yu, X. (2012). A data-driven assessment model for information systems security risk management. *Journal of Computing*, 7(12), 3103–3109. <https://doi.org/10.4304/jcp.7.12.3103-3109>
- Fenz, S., & Ekelhart, A. (2011). Verification, validation, and evaluation in information security risk management. *IEEE Security & Privacy*, 9(2), 58–65. <https://doi.org/10.1109/MSP.2010.117>
- Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security*, 22(5), 410–430. <https://doi.org/10.1108/IMCS-07-2013-0053>
- Ghazouani, M., Medromi, H., & Moussaid, L. (2017). Design and implementation of a comprehensive information security risk management tool based on multi-agents systems. *International Journal of Applied Information Systems*, 12(7), 1–8. <https://doi.org/10.5120/ijais2017451711>
- Ghazouani, S., Faris, M., Medromi, H., & Sayouti, A. (2014). Information security risk assessment—a practical approach with a mathematical formulation of risk. *International Journal of Computer Applications*, 103(8), 36–42. <https://doi.org/10.5120/18097-9155>
- Gritzalis, D., Iseppi, G., Mylonas, A., & Stavrou, V. (2018). Exiting the risk assessment maze: A meta-survey. *ACM Computing Surveys (CSUR)*, 51(1), 1–30. <https://doi.org/10.1145/3145905>
- Hayajneh, A. A., Thakur, H. N., & Thakur, K. (2023). The evolution of information security strategies: A comprehensive investigation of infosec risk assessment in the contemporary information era. *Computer and Information Science*, 16(4), 1–1. <https://doi.org/10.5539/cis.v16n4p1>
- Ionita, D., Hartel, P., Pieters, W., & Wieringa, R. (2014). Current established risk assessment method-ologies and tools. *Technical report*, 02.
- ISO/IEC 27001. (2022). *Information technology - cybersecurity and privacy protection - information security management systems - requirements*. Standard ISO/IEC 27001: 2022. International Organization for Standardization. <https://www.iso.org/standard/27001>,
- ISO/IEC 27005. (2018). *ISO/IEC 27005: Information technology-security techniques -information security risk management*. ISO.
- Johnson, C. W. (2015). Cyber security and the future of safety-critical air traffic management: Identifying the challenges under NextGen and SESAR. In *10th IET System Safety and Cyber-Security Conference 2015* (pp. 1–6). IET. Bristol, United Kingdom.
- Kaur, G., Lashkari, Z. H., & Lashkari, A. H. (2021). *Cybersecurity risk in FinTech*. Springer International Publishing. <https://doi.org/10.1007/978-3-030-79915-16>
- Kistan, T., Gardi, A., Sabatini, R., Ramasamy, S., & Batuwangala, E. (2017). An evolutionary outlook of air traffic flow management techniques. *Progress in Aerospace Sciences*, 88, 15–42. <https://doi.org/10.1016/j.paerosci.2016.10.001>
- Kotulic, A. G., & Clark, J. G. (2004). Why there aren't more information security research studies. *Information &*

- Management*, 41(5), 597–607. <https://doi.org/10.1016/j.im.2003.08.001>
- Labunets, K., Paci, F., & Massacci, F. (2015). Which security catalogue is better for novices? In *2015 IEEE Fifth International Workshop on Empirical Requirements Engineering (EmpiRE)* (pp. 25–32). IEEE, Ottawa, Ontario, Canada.
- Labunets, K., Paci, F., Massacci, F., Ragosta, M., & Solhaug, B. (2014). A first empirical evaluation framework for security risk assessment methods in the ATM domain. *Proc. of SIDs*. Madrid, Spain.
- Lundgren, M. (2020). *Making the dead alive: Dynamic routines in risk management* [PhD thesis]. Luleå University of Technology.
- Lundgren, M., & Bergström, E. (2019). Dynamic interplay in the information security risk management process. *International Journal of Risk Assessment and Management*, 22(2), 212–230. <https://doi.org/10.1504/IJRAM.2019.101287>
- MacQueen, K. M., McLellan-Lemal, E., Bartholow, K., & Milstein, B. (2008). *Team-based codebook development: Structure, process, and agreement*. AltaMira Press.
- Maneerattanasak, U., & Wongpinunwatana, N. (2017). A proposed framework: An appropriation for principle and practice in information technology risk management. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1–6). IEEE, Langkawi, Kedah.
- Mason, J. (2002). *Qualitative researching* (second ed.). SAGE Publications Inc.
- Moukafih, N., Zhang, H., Epiphaniou, G., Maple, C., Taylor, S., & Carmichael, L. (2024). Semi-automated threat vulnerability & risk assessment (tvr) for medical devices. In *Proceedings of the 17th International Conference on Pervasive Technologies Related to Assistive Environments* (pp. 687–693). Crete, Greece.
- Murray, G., Johnstone, M. N., & Valli, C. (2017). The convergence of it and ot in critical infrastructure. *Australian Information Security Management Conference*. Perth, Western Australia.
- Nie, R.-T., Zhao, Y., & Dai, J.-H. (2009). Evaluation on safety performance of air traffic management based on fuzzy theory. In *2009 International conference on measuring technology and mechatronics automation* (Vol. 2. pp. 554–557). IEEE, Zhangjiajie, Hunan, China.
- Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European Journal of Information Systems*, 26(1), 1–20. <https://doi.org/10.1057/s41303-016-0025-y>
- Njenga, K., & Brown, I. (2012). Conceptualising improvisation in information systems security. *European Journal of Information Systems*, 21(6), 592–607. <https://doi.org/10.1057/ejis.2012.3>
- Oates, B. J. (2006). *Researching information systems and computing*. SAGE Publications Inc.
- Osborn, E., Simpson, A., & Loukas, G. (2018). Risk and the small-scale cyber security decision making dialogue—a UK case study. *The Computer Journal*, 61(4), 472–495. <https://doi.org/10.1093/comjnl/bxx093>
- Pipyros, K., & Liasidou, S. (2025). A new cybersecurity risk assessment framework for the hospitality industry: Techniques and methods for enhanced data protection and threat mitigation. *Worldwide Hospitality & Tourism Themes*, 17(1), 48–61. <https://doi.org/10.1108/WHATT-12-2024-0296>
- Reynolds, T. J., & Gutman, J. (1988). Laddering theory, method, analysis, and interpretation. *Journal of Advertising Research*, 28(1), 11–31.
- Rosado, D. G., Sánchez, L. E., Varela-Vaca, Á. J., Santos-Olmo, A., Gómez-López, M. T., Gasca, R. M., & Fernández-Medina, E. (2024). Enabling security risk assessment and management for business process models. *Journal of Information Security and Applications*, 84, 103829. <https://doi.org/10.1016/j.jisa.2024.103829>
- Sajko, M., Hadjina, N., & Pešut, D. (2010). Multi-criteria model for evaluation of information security risk assessment methods and tools. *The 33rd International Convention MIPRO*, 1215–1220.
- Sajko, M., Rabuzin, K., & Bača, M. (2006). How to calculate information value for effective security risk assessment. *Journal of Information and Organizational Sciences*, 30(2), 263–278.
- Saldaña, J. (2021). *The coding manual for qualitative researchers* (4th ed.). SAGE Publications Inc.
- Salin, H., & Lundgren, M. (2023). A gap analysis of the adoption maturity of certificateless cryptography in cooperative intelligent transportation systems. *Journal of Cybersecurity and Privacy*, 3(3), 591–609. <https://doi.org/10.3390/jcp3030028>
- Sánchez-García, H. D., Mejía, J., & Gilbert, T. S. F. (2023). Cybersecurity risk assessment: A systematic mapping review, proposal, and validation. *Applied Sciences*, 13(1), 395. <https://doi.org/10.3390/app13010395>
- SESAR 3 Joint Undertaking. (2020). *Sesar joint undertaking - content integration*. <https://www.sesarju.eu/projects/ci>
- Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, 57, 14–30. <https://doi.org/10.1016/j.cose.2015.11.001>
- Shypovskiy, U. (2023). Enhancing the factor analysis of information risk methodology for assessing cyberresilience in critical infrastructure information systems. *Political Science and Security Studies Journal*, 4(1), 25–33.
- Silverman, D. (2015). *Interpreting qualitative data* (5th ed.). Sage.
- Stelkens-Kobsch, T. H., Finke, M., & Carstengerdes, N. (2017). A comprehensive approach for validation of air traffic management security prototypes: A case study. In *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)* (pp. 1–10). IEEE, St. Petersburg, Florida, USA.
- Stoll, M. (2015). An information security model for implementing the new iso 27001. In Manish Gupta (Ed.),

- Handbook of research on emerging developments in data privacy* (pp. 216–238). IGI Global.
- Strohmeier, M., Schäfer, M., Pinheiro, R., Lenders, V., & Martinovic, I. (2016). On perception and reality in wireless air traffic communication security. *IEEE Transactions on Intelligent Transportation Systems*, 18(6), 1–20. <https://doi.org/10.1109/TITS.2016.2612584>
- Taylor, R. G. (2015). Potential problems with information security risk assessments. *Information Security Journal: A Global Perspective*, 24(4–6), 177–184. <https://doi.org/10.1080/19393555.2015.1092620>
- Tehler, H. (2023). *Introduktion till risk och riskhantering* (first ed.). Lunds University.
- Thornhill, A., Saunders, M., & Lewis, P. (2016). *Research methods for business students* (seventh ed.). Prentice Hall.
- Tiganoaia, A., Cercel, C., & Pavlíček, A. (2017). Some risk management software tools - an exploratory study. In *The European Proceedings of Social & Behavioural Sciences*. Future Academy. University of Barcelona, Spain.
- Toxirjonovich, O. N., & Fozilovich, Y. O. (2022, April). Artificial intelligence and its application in information security management. *Central Asian Journal of Theoretical and Applied Science*, 3(4), 90–97.
- Vashistha, A. (2021). *The future of risk management is automated*. <https://www.forbes.com/sites/forbestechcouncil/2021/02/25/the-future-of-risk-management-is-automated/>
- Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Wangen, G. (2017). Information security risk assessment: A method comparison. *Computer*, 50(4), 52–61. <https://doi.org/10.1109/MC.2017.107>
- Wangen, G., Hallstensen, C., & Snekenes, E. (2018). A framework for estimating information security risk assessment method completeness. *International Journal of Information Security*, 17(6), 681–699. <https://doi.org/10.1007/s10207-017-0382-0>
- Wangen, G., & Snekenes, E. (2013). A taxonomy of challenges in information security risk management. In *Proceeding of Norwegian Information Security Conference/ Norsk informasjonssikkerhetskonferanse-NISK 2013-Stavanger*, 18th-20th November 2013. Akademika Forlag, Stavanger, Norway.
- Whitman, M. E., & Mattord, H. J. (2014). *Principles of information security* (fifth ed.). Cengage Learning.
- Wicaksono, A. C., Prabowo, S., & Oktaria, D. (2022). Risk and security measurement based on ISO 27001 using FMEA methodology case study: National government agency. In *2022 1st International Conference on Software Engineering and Information Technology (ICoSEIT)* (pp. 6–11). IEEE. Virtual Conference.
- Yang, T.-H., Ku, C.-Y., & Liu, M.-N. (2016). An integrated system for information security management with the unified framework. *Journal of Risk Research*, 19(1), 21–41. <https://doi.org/10.1080/13669877.2014.940593>

## Appendix Interview Guide

The background part contained the following questions:

- We understand you have been working with SecRAM. We have read up on the SecRAM documentation, but the documentation only says so much. Perhaps you could tell us a bit about how it is to work with it in practice?
- What would you say your role is?
- What would you say your role entails?
- How long have you worked with security?
- What is your take on security?
  - Why is it important for you?
- How do you find it working with security?
- Have you worked with other ISRM methodologies than SecRAM?
  - Could you compare?
  - Is it a big part of your work?
- How does the security-related work you do fit into your day-to-day work?
  - Do you feel you have enough time for it?
- How come you have these security-related duties?

The practice part contained the following questions:

- Could you describe the SecRAM process?
- What do you think is the purpose of using SecRAM?
- Which parts of SecRAM have you completed?
  - Why is it like that?
- Which parts of SecRAM were easy?
- Which parts of SecRAM were difficult?
- Is there anything you have experienced that is particularly challenging with SecRAM?
- What could have been made more efficient?
- How did you identify the assets?
  - Did you use the catalogues?
- Apart from SecRAM, are there any other security standards or regulations your solution must adhere to?
- Do you agree with the prioritization of your project?
- Is there anything special in SecRAM that makes the security work particularly easy?
- What level of support does SecRAM provide?
- Do you feel the methodology itself provides enough support, or is something missing?
- Do you need to complement with other sources of information?
  - For example, Google, other best practices, blogs, or colleagues?
- Is there anything you would like to change in the methodology, and if so, why?
- Are there any challenges in your security-related work?
- What's your approach to working with SecRAM? Do you primarily work alone or in teams?
- How do you construct the teams? *Or*
- Why do you work alone?
- Are there always some recurring participants in the teams?
- Do you find it hard to differentiate between primary assets and supporting assets?
- Is it hard to judge and use the impact areas in practice, e.g. what is the difference between “serious loss of income” and “large loss of income”?

The third part on tool support contained two types of questions, laddering questions and more specific tool questions. Typical laddering questions from this part were:

- Could you give an example?
- Why do you think that?
- You previously mentioned that. . . could you explain why?
- Why is that difficult?

The more direct questions on tools were:

- What type of functionality are you missing?
- How can tools better support your security-related work?
- In what way could . . .*[insert ISRM activity here]*. . . be performed better if there were tool support?



V



# The importance of records in information classification – “if you have not documented it, you have not done it”

Information &  
Computer  
Security

Simon Andersson

*Department of Computer Science Electrical and Space Engineering,  
Luleå University of Technology, Luleå, Sweden, and*

Erik Bergström

*Department of Computer Science and Informatics,  
School of Engineering, Jönköping University, Jönköping, Sweden*

Received 8 April 2025

Revised 3 July 2025

1 September 2025

12 December 2025

Accepted 21 January 2026

## Abstract

**Purpose** – This paper aims to examine what contextual knowledge should be documented during the information classification process and how such knowledge can be structured to support information security risk management. Although many tools support documentation of basic classification outputs, they often lack functionality for capturing decision rationales or supporting classification discussions to be kept in a record.

**Design/methodology/approach** – The study used a qualitative approach. Data were collected through 16 semi-structured interviews with information security professionals and observations of 14 tool demonstrations. A thematic analysis was conducted and guided by an existing classification method based on ISO/IEC 27002.

**Findings** – The study identifies a range of contextual knowledge that practitioners consider important to document, including the classification level, decision rationale and responsible roles. Furthermore, it proposes a structured approach consisting of recommended contextual knowledge to include in a classification record, which may serve as a starting point for organisations conducting information classification. Finally, the study contributes procedural knowledge by clarifying how classification decisions are documented and what information should be retained.

**Originality/value** – This study addresses an identified gap in both research and practice by specifying what contextual knowledge should be documented during information classification. It provides practical guidance for improving documentation practices and highlights opportunities for tool development in information classification.

**Keywords** Information Classification, Information Security Risk Management, Information Security, Documentation, Records

**Paper type** Research paper

---

© Simon Andersson and Erik Bergström. Published by Emerald Publishing Limited. This article is published under the Creative Commons Attribution (CC BY 4.0) licence. Anyone may reproduce, distribute, translate and create derivative works of this article (for both commercial and non-commercial purposes), subject to full attribution to the original publication and authors. The full terms of this licence may be seen at <http://creativecommons.org/licences/by/4.0/>

**Funding:** The authors gratefully acknowledge the Swedish Civil Contingencies Agency (MSB), project VISKA (MSB 2021–14650). This study was supported by the Myndigheten för Samhällsskydd och Beredskap (No. 2021–14650).



Information & Computer Security  
Emerald Publishing Limited  
2056-4961  
DOI 10.1108/ICS-04-2025-0124

## 1. Introduction

Most, if not all, organisations must manage information security risks to avoid, for example, operational, financial or reputational damage (Whitman and Mattord, 2022). Managing risk is particularly important in the public sector, where risk realisation can not only disrupt essential services and erode public trust but also cause consequences that extend beyond the organisation itself, causing societal effects (van Laere and Lindblom, 2019). Organisations can adopt information security risk management (ISRM) frameworks, which offer structured approaches to mitigate and reduce risk (Gritzalis *et al.*, 2018). ISRM generally centre around three key activities forming the process of risk assessment: asset identification and classification, risk analysis and risk treatment (Silva and Jacob, 2018; ISO/IEC 27005, 2022). These activities are interdependent, with each step relying on the output of the previous one, underscoring the importance of reliable inputs at every stage. That is, an organisation identifies and classifies an asset, followed by a risk analysis targeting threats to that asset. Finally, the organisation will have to either accept the level of risk or implement security controls to lower it.

A critical input for risk analysis is the classification of assets based on their value to the organisation, known as information classification (Gerber and Von Solms, 2005; Tankard, 2015). If the information classification process is not performed correctly, it could lead to unreliable input to the risk analysis and, consequently, inaccurate risk management, following the principle of “garbage in, garbage out” (Shamala *et al.*, 2017, p. 2). If the classification is not conducted at all, organisations risk consequences beyond the loss of input to the risk analysis. In several countries, public sector organisations are legally required to work systematically with information security. For example, in Sweden, regulations stipulate that public authorities must work in a risk-based manner by classifying their information assets, identifying risks, and applying and monitoring appropriate security measures (MSB, 2020). Similarly, in Japan, subcontractors are required to establish and apply information classification to be considered for government contracts (METI, 2025).

Despite its importance, information classification is still an understudied area (Shedden *et al.*, 2016; Bergquist *et al.*, 2021), and it is widely recognised as a challenging process, with difficulties such as subjective judgments, deciding which security aspects (for example, confidentiality, integrity and/or availability) to consider, choosing the right level of granularity for classifying assets and determining what information to include in the classification (Andersson, 2023; Shedden *et al.*, 2016; Fibikova and Müller, 2011; Whitman and Mattord, 2022; Grimaila and Fortson, 2007). In other words, classification contains several challenges besides making a classification decision.

Although the literature on information classification is limited, some contributions address the classification process. For instance, Bergström *et al.* (2021) developed a method based on ISO/IEC 27002 (2022). Other studies, such as Bergquist *et al.* (2021), investigated tools and specific parts of the classification process, while Bradford *et al.* (2022), examined the process and provided general insights from security managers. What these contributions have in common, whether describing the process or only parts of it, is that none address what should be documented and kept in a record during the classification process in any depth. This is problematic, as records are essential for understanding why classification decisions were made and which factors were considered. Such understanding is particularly important for reclassification and for providing input to the risk analysis.

While we do know that some aspects of the classification process must be documented, such as the final classification value assigned to an asset, existing research does not provide comprehensive guidance on what else should be documented. Current literature, such as Bergström *et al.* (2021), suggests that a record should be created but does not explicate its

---

contents. A concept similar to records is that of documents, which can be understood as carriers of knowledge (Alavi and Leidner, 2001), or as records that have been further contextualised and formalised. Although the terms “record” and “document” are often used interchangeably, in this paper, a record refers specifically to the knowledge gathered throughout the execution of a process. The process of creating the record we refer to as “documenting”.

The value of records aligns with key concepts in knowledge management, where they are seen as vehicles for capturing, sharing and reusing organisational knowledge (Alavi and Leidner, 2001; Yeo, 2018). In particular, contextual knowledge, such as organisational members’ understanding of asset values in a specific organisational setting, can be preserved through structured documentation and be used to support future decisions (Nunes *et al.*, 2009). Capturing contextual knowledge helps ensure that important insights are not lost over time, which aligns with knowledge management efforts to promote continuity and shared understanding across the organisation (Nonaka *et al.*, 2000). Procedural knowledge, on the other hand, refers to the knowledge of how to perform a specific task (Anderson and Crawford, 1995), such as tasks or activities in the information classification process. To clarify the difference between the two in the context of information classification, we argue that contextual knowledge refers to what type of knowledge is to be gathered, and procedural knowledge is how to gather it. To support the collection of such knowledge, a knowledge management strategy can be formulated, which is a statement on how knowledge should be gathered and used. Using such a strategy has been shown to improve decision-making performance (Willman *et al.*, 2022).

Records connected to ISRM have, in previous literature, been explained to be important for several reasons. Keeping up-to-date records is considered to be a cornerstone of good information security management (Mattord and Wiant, 2016), this is achieved by documenting, sharing and verifying the outcomes of different security processes to ensure that well-informed choices are made (Barraza de la Paz *et al.*, 2023). Records are also essential in the event of audits or when revisiting risk analyses and classifications, as information security experts must be able to understand the reasoning for earlier decisions (Beckers *et al.*, 2014).

In other sectors, such as healthcare and engineering, records containing decision rationale are considered as standard. Clinical records, for example, track a patient’s condition and communicate the actions made, as well as the reasoning behind them, to other members in a care team (Kuhn *et al.*, 2015). Similarly, in engineering, capturing design rationale (for instance, why an IT-artifact is designed the way it is) is viewed to be critical (Bracewell *et al.*, 2009). Both domains show how records support accountability, motivate decision-making, and provide a history of previous rationale. However, this type of approach has not yet been adopted in classification, and investigating what to document and add to a record in the information classification process has largely remained unaddressed in research.

The lack of guidance regarding records in information classification is a significant problem in practice. In contrast to other parts of the ISRM process, such as risk analysis and risk treatment, where established frameworks clearly describe what should be documented, for example, in a risk registry, there is no comparable guidance for information classification. As a result, practitioners are left without clear instructions on what to document beyond the classification result. This often leads to inconsistent records, where only the final classification level is captured while the rationale and contextual knowledge behind the decision are overlooked.

Addressing this gap is important, as inadequate records reduce transparency and hinder the reuse of underlying reasoning for past decisions, both of which are essential during reclassification or audit. Poor documentation practices can also undermine organisational risk management and increase exposure to the growing frequency and severity of cyber

threats, given the current risk landscape (ENISA, 2024; Orlando, 2021). An example of this is Capita, a UK outsourcing company that was the target of a cyberattack and later fined £14m for failing to ensure the security of personal data affected by the breach. Part of the reason the breach was successful was noted to be a failure of proper systematic ISRM work (ICO, 2025).

Without a structured approach to documenting in the classification process, organisations risk inconsistent practices and an inability to build on past insights. This lack of clarity can also lead to a loss of organisational knowledge, especially when members involved in classification are replaced, resulting in the loss of past understanding of decisions. In other words, documenting more than just the classification result is important, yet there is a lack of understanding of what contextual knowledge to actually gather.

As such, the aim of this paper is to address how to support risk analysis with reliable and structured input from the information classification process. Given the aim, this study set out to shed light on the following question:

- Q1. What contextual knowledge should be documented in the information classification process?

The remainder of this paper is structured as follows: Section 2 provides an overview of the information classification process, contextual and procedural knowledge, knowledge management strategy, the use of records in ISRM and tool use in ISRM. Section 3 explains the research approach and the methods used to gather and analyse the data. Section 4 presents the results. Section 5 then discusses and emphasises the study's key findings, and finally, Section 6 offers the concluding insights.

## 2. Background

The process of information classification is described in standards, such as ISO/IEC 27002 (2022) and the NIST Risk Management Framework (NIST RMF) (NIST, 2018), it is also described in different national supporting documents in, for example, the UK (Cabinet Office, 2024) and Sweden (MSB, 2023). The mentioned resources describe the classification process in a holistic sense and a normative manner, that is, they explain *what* should be done and are vague at best in *how* to do it (Tehler, 2023; Wangen *et al.*, 2018). While the normative approach is understandable, as part of the purpose of a standard is to provide general advice and best practices for organisations to adopt and adapt, information classification is known to be a difficult process to implement in an organisation (Niemimaa and Niemimaa, 2017). Why this is the case likely differs between organisations; however, classifying assets has been noted to be difficult (Andersson, 2023; Fenz *et al.*, 2014; Fibikova and Müller, 2011; Bergström *et al.*, 2021; Kaarst-Brown and Thompson, 2009).

The information classification process is often conducted in a workshop setting with a group of individuals who have varying levels of expertise and familiarity with the information asset being classified (Bergström *et al.*, 2021). Doing it in a workshop allows for a more nuanced view and understanding, leading to more informed classification decisions. However, as previously mentioned, the contextual knowledge and rationale are seldom documented or included in a record as a result of the classification.

Bergström *et al.* (2021) expanded on the ISO 27002 standard by developing a method based on a low-granularity approach, where an entire system or business process is classified. This is also described as the most common approach in practice (Fibikova and Müller, 2011). While the method refers to records being kept and created, it offers little guidance on what those records should include beyond the name of an asset, requirements, and the classification result. In addition, it does not mention the documentation of decision

---

rationale, which is considered an important part of information security management (Mattord and Wiant, 2016; Barraza de la Paz *et al.*, 2023). An adapted version of the ISO/IEC 27002 method, expanded by Bergström *et al.* (2021), is presented in Figure 1, and the five main steps are briefly explained:

- (1) *Business Process/System Analysis*: Within a business process/system, primary assets, such as information related to customers, and secondary assets, such as servers, are identified, as well as their use, roles and context. This creates an inventory that serves as the foundation for classification.
- (2) *Requirement Identification*: Internal and external requirements are identified. Internal requirements refer to, for example, internal policies and external requirements refer to, for example, laws and regulations, such as the General Data Protection Regulation (GDPR). Both types of requirements should be documented.
- (3) *Classification of Information*: Classification levels are assigned using a classification matrix based on a description of the potential consequence of a loss of confidentiality, integrity and availability. The results are documented and connected to each asset.
- (4) *Labelling of Information*: The records containing the classification results and other information are archived, and a decision is taken on whether to label the asset. If yes, it is labelled according to its classification.
- (5) *Selection of Final Business Process/System Classification*: The business process or system inherits the highest classification level among its assets and is classified accordingly.

### 2.1 Contextual and procedural knowledge

Knowledge is often discussed as being either explicit or tacit. Explicit knowledge, according to Nonaka *et al.* (2000), is readily and easily communicated through structured means, such as documents and manuals, and can be expressed in a systematic language. Tacit knowledge, however, is personal, experiential, and difficult to formalise.

Contextual knowledge refers to knowledge about a situation in which a task or decision occurs, including its environment (Nunes *et al.*, 2009; Brezillon and Pomerol, 1999). This can include who was involved, why a decision was made and how it was reached within a particular organisational or situational context (Nunes *et al.*, 2009; Davenport and Prusak, 1997; Greenberg, 2001). In the case of information classification, contextual knowledge may include what shapes the participants' understanding of asset value in classification workshops, their understanding of the use of specific assets and the rationale behind a certain classification decision. Contextual knowledge is often not readily observable from the outside and must be captured and made explicit for reuse. In other words, for classification outcomes to remain meaningful, they must be conducted within the organisational context and take it into consideration, and the contextual knowledge must be documented to support future reclassification and to allow for traceability.

Procedural knowledge can be defined as knowledge about how to perform a specific task, such as conducting a particular process or applying a specific framework (Georgeff and Lansky, 1986; Anderson and Crawford, 1995). Such knowledge can be made explicit in, for example, guidelines, documents or as part of a workflow in a tool. In the context of information classification, procedural knowledge is partially reflected in existing models and frameworks, for example, in the method developed by Bergström *et al.* (2021) based on ISO/IEC 27002 (2022), which outlines key steps in the classification process. As previously described and shown in Figure 1, however, such models do not provide explicit procedural

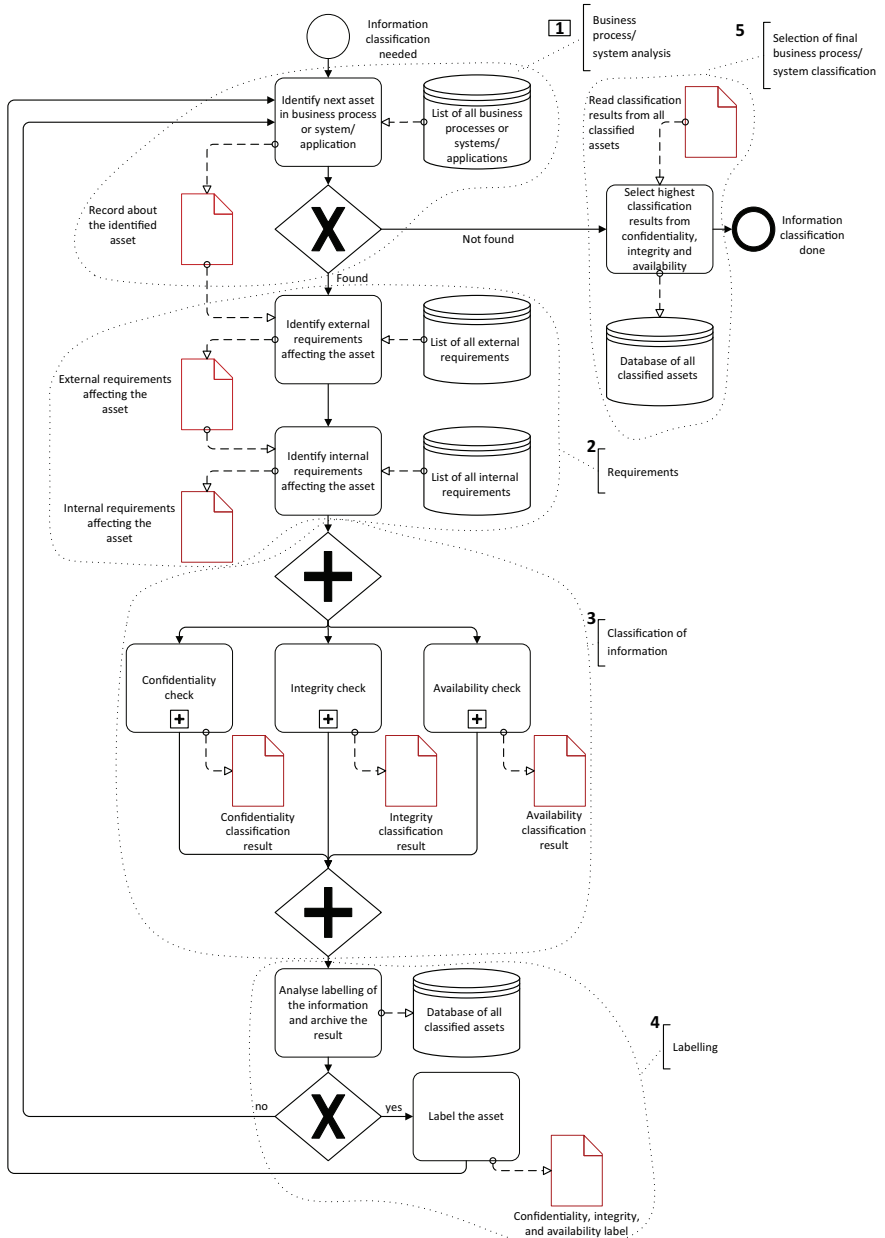


Figure 1. A low granularity approach to information classification, the record highlighted in red – Adapted from (Bergström et al., 2021) based on ISO/IEC 27002

---

guidance on what should be documented throughout the classification process. That is, while they describe how to perform classification, they lack specificity about how to capture contextual knowledge during the process.

In the classification process, contextual knowledge often emerges through discussion among participants in classification workshops, based on their understanding of organisational processes and information assets. This knowledge also resides in the individuals involved in the classification activity. However, without procedural knowledge specifying what should be documented, the contextual knowledge may remain undocumented or only partially captured. As a result, decision rationale and organisational details affecting the decision may be lost, leading to incomplete inputs for subsequent risk analysis. Providing procedural guidance on documentation practices can help organisations capture contextual knowledge more consistently as part of the classification process.

### 2.2 Knowledge management strategy

A knowledge management strategy is essentially a statement of how knowledge is to be captured and used, and [Jennex \(2010\)](#) found that implementing one can improve decision-making. Although the strategy is not itself the reason for creating a record, it shapes what is included, and these choices should be justified through use-cases that illustrate the purpose of collecting knowledge. According to [Willman et al. \(2022\)](#), a knowledge management strategy typically identifies the intended users of knowledge, the forms of information to be captured, the sources from which knowledge is drawn, and how it will be represented, stored and supported technologically. It also establishes organisational commitment, metrics for evaluating use, and processes for ongoing feedback and adjustment.

In the context of information classification, such a strategy would clarify not only what knowledge should be captured but also why it should be captured, by contextualising each classification record in a use-case. Such an approach supports, for example, reclassification, enables auditability and facilitates novices in a classification workshop.

### 2.3 Records in information security risk management

Documenting processes and activities is essential for understanding what actions were taken, how they were performed and what the outcomes were ([Conklin and Yakemovic, 1991](#)). In an Information Security Management System (ISMS), records involve the identification, documentation, updating, and controlling of informations that is determined to be necessary for the functions of the ISMS, including ISRM ([Haufe et al., 2016](#); [ISO/IEC 27001, 2022](#)). Furthermore, [ISO/IEC 27001 \(2022\)](#) emphasises that the required extent of records will vary across organisations, stating that records should be sufficiently available to confirm that processes are carried out as intended. What this means in practice, however, is not stated.

In ISMS, records are used both as input to processes and as outputs or deliverables generated by said processes ([Suhaimi et al., 2014](#)). One example is that the results of information classification are used as the main input for the risk analysis. Keeping records up-to-date is not only a recommended practice ([Johnson and Schulte, 2004](#)) but is also essential for effective information security management. Records that are the outcome of a process should contain the rationale behind decisions, which is especially valuable when revisiting risk analysis results to understand why specific security controls were chosen ([Beckers et al., 2014](#); [Barraza de la Paz et al., 2023](#)). Additionally, thorough records and support external audits by allowing the organisation to clearly present and justify its decisions, making the decision-making process transparent to other security experts ([Beckers et al., 2014](#)). According to [Fung et al. \(2003\)](#), comprehensive records serve as evidence that security officers have acted professionally and competently. Along with other factors,

comprehensive records are also a key success factor in information security and risk management (Mattord and Wiant, 2016; Sillaber and Breu, 2015).

Existing literature on records in ISRM processes focuses on the one hand, on the use of existing records and, on the other, on creating and updating records throughout the risk management process, meaning documenting. In two such cases, user involvement has been studied (Sillaber and Breu, 2015; Spears and Barki, 2010). When using records on systems and previous risk assessments, high-quality information, meaning it is accurate and complete, improves the reliability of risk assessments by providing clear, current details for informed decision-making. This reliability is further supported by records that include a clear description of a business process or asset used as the basis for the assessment, often created in part by users with in-depth knowledge of the system or process (Sillaber and Breu, 2015; Spears and Barki, 2010). In this way, records play an important role in managing risk and supporting the ISRM process.

The ISRM process is iterative in nature (Whitman and Mattord, 2022), and revisiting previously made decisions in the different steps is a natural action. This is known to be good practice, as the value of information may change over time. As a result, it is necessary to revisit the classification process (Everett, 2011). If a reclassification is not done, it could result in an outdated view of the criticality of assets to the organisation. However, if records containing contextual knowledge from previous iterations exist, the classification level and basis for decisions can be evaluated and discussed rather than starting from scratch. This further cements the need for records and procedural knowledge on what they should include in information classification.

Ngoepe (2014) investigated the role of records within risk management and found that the success of risk management is partly dependent on the accuracy of records, as decisions must be made on accurate and complete information. In addition, it was identified that if nothing is documented, it is difficult to prove that it happened and that relying on human memory is a dangerous practice. Further, Ngoepe (2014) identified risks related to the lack of records, for example, the inability to find mission-critical information, lack of records of who knows what and when, and a loss of proof of ownership, rights and obligations.

In information classification, there is no method or approach describing what should be documented apart from the results of the classification, that is, the final classification level. This makes the process susceptible to the risks described by Ngoepe (2014). However, previous research suggests that support regarding both the documentation and records is an area that needs to be addressed (Bergström, 2023; Grimaila and Fortson, 2007; Sillaber and Breu, 2015).

#### 2.4 Tool support in information security risk management

One way of supporting the ISRM process and information classification is through the use of tools. What a tool entails in the context of ISRM has previously been discussed in for example Bergström (2023) and Gritzalis *et al.* (2018), who define tools as either dedicated software for conducting ISRM activities or more rudimentary supports, such as spreadsheets or templates used in ISRM work (Gritzalis *et al.*, 2018; Wangen *et al.*, 2018). Different tools provide different types of support. Typical properties of dedicated tools include task automation, reduction of manual work, minimisation of user input to limit the possibility of user errors, and the creation of a more streamlined workflow that guides users through an ISRM activity or process (Gritzalis *et al.*, 2018; Sánchez-García *et al.*, 2023).

While rudimentary supports like spreadsheets are seen as helpful, they are often considered restrictive, and dedicated tools are generally preferred (Gritzalis *et al.*, 2018). However, even dedicated tools are not without limitations. Gritzalis *et al.* (2018) identified

---

that input constraints, meaning what can be documented, are often seen as limiting. Similarly, [Lundgren and Bergström \(2019\)](#) investigated stress among practitioners working in an ISRM process. In that study, respondents used a specific tool for information classification, and the tool was found to be inflexible in terms of documenting classification results. These examples suggest that although tools can offer some structure, they often lack sufficient functionality to support comprehensive documentation practices. Notably, one common feature, minimising user input to reduce errors, may inadvertently hinder the ability to document important ISRM and classification details ([Gritzalis et al., 2018](#)).

Few overviews of ISRM tools exist. For example, [European Union Agency for Cybersecurity \(ENISA\) \(2023\)](#) provides a list of tools related to risk management methods. In addition, [Sánchez-García et al. \(2023\)](#) identified 25 tools for risk management and risk assessment, while [Bergström \(2023\)](#) found 18 tools related to ISRM. There is, however, little literature on ISRM tools in general and even less so on tools targeting information classification specifically. The reason why there are so few tools targeting information classification could be that ISRM tools include information classification as an activity. However, there is a distinct lack of research exploring tools that focus on both ISRM and classification aspects and even more so on tools that support documentation practices. This gap suggests that further exploration and development in these areas could be beneficial to risk management overall.

### 3. Research approach

This study aimed to investigate what contextual knowledge should be documented in the information classification process. Given the explorative nature of this endeavour, we opted to use a qualitative research approach ([Lim, 2024](#)). Choosing a qualitative approach meant that we aimed to identify recurring patterns in our collected data and looked for saturation in answers rather than trying or assessing a pre-existing hypothesis ([Oates, 2006](#)). To conduct our data collection, we used semi-structured interviews as our main approach, given the explorative nature of the study. In addition, we participated as observers in tool demonstrations aimed at supporting classification and risk management.

#### 3.1 Data collection

The main data collection method used were semi-structured interviews ([Adams, 2015](#)). The reasoning for using semi-structured interviews was, in part, that they are characterised by asking open-ended questions, allowing respondents to formulate their answers freely; this was perceived as beneficial given the explorative approach ([Kallio et al., 2016](#)). Semi-structured interviews also allow the researcher to ask follow-up questions when investigating unexplored territory ([Reynolds and Gutman, 1988](#)). An interview guide was created before the interviews, including questions surrounding the information classification process as such, and more specifically, what respondents deem to be the main results of the classification and what they find important to document. This allowed respondents to freely formulate their answers surrounding the general process and what they perceived to be the results before we more specifically asked them what they documented and what they considered to be important to include in a record. Finally, semi-structured interviews were deemed to be a good fit for the study in terms of gathering and understanding contextual knowledge described by respondents, as explained in [Kallio et al. \(2016\)](#); [Magaldi and Berler \(2018\)](#); [Ruslin et al. \(2022\)](#).

To follow ethical guidelines for in-depth and semi-structured interviews, we took several steps based on [Allmark et al. \(2009\)](#). Each interview began with a brief introduction explaining the agenda, how the data would be used, and explaining the respondents' right to

withdraw at any time. We also asked for consent to record the interview both before and after starting the interview, ensuring informed consent. To maintain privacy, all identifying details, like respondents' names and their organisations, were removed from the transcripts and replaced with pseudonyms. The transcription was done *verbatim*, word for word (Halcomb and Davidson, 2006).

In total, we interviewed 16 respondents regarding records connected to information classification. All respondents had some sort of managing role connected to information security work, such as a Chief Information Security Officer (CISO), Information Security Specialist or IT security manager. We perceived the roles of the respondents as relevant to the study, as they were the persons responsible for the records and documentation outputs of the process. The interviews all lasted between 1 and 1.5 h and were conducted using conferencing software in an online setting. A summary of the respondents and their roles can be seen in Table 1. In addition to the interviews, we also participated as observers in 14 tool demonstrations aimed at supporting organisations in areas such as governance, risk and compliance (GRC) management. Each session involved a live walkthrough of the tool via screen sharing, during which the presenters demonstrated its use in real time. Importantly, we did not use or evaluate the tools ourselves as our role was strictly observational.

The selection of tools was carried out in collaboration with a Swedish national interest group focused on risk analysis, comprising 22 members from both industry and academia. Tool selection was guided by the ENISA list of Risk Management tools [European Union Agency for Cybersecurity (ENISA), 2023] and additional suggestions from members of the interest group. The demonstrations were hosted by the interest group, with tool developers invited to present and answer questions. Each session followed a consistent structure: a walkthrough of the tool's interface and features, followed by a Q&A session. These sessions enabled us to explore the tools in greater depth and allowed us to ask questions such as, "Practically, how does the tool support classification?" which were of a more procedural nature. However, we also asked questions of a contextual nature, such as, "How do you capture external requirements in practice?" The reason for asking questions of a contextual nature was to investigate what contextual knowledge is being captured in existing tools. The

**Table 1.** An overview of the respondents and their organisational role and size

Respondent	Role in the organisation	Organisation size
1	Information security specialist	1001–2500
2	Information security specialist	1001–2500
3	Administrative manager, IT	1001–2500
4	Security coordinator	501–1000
5	Head of division, IT	0–500
6	CISO	2501–5000
7	CISO	0–500
8	Information security specialist	501–1000
9	CISO	0–500
10	CISO	5000+
11	Information security specialist	5000+
12	CISO	1001–2500
13	CISO	5000+
14	IT security manager	1001–2500
15	CISO	501–1000
16	CISO	1001–2500

**Source(s):** Authors' own work

demonstrations also allowed us to get access and insight into proprietary tools, which would have been difficult otherwise. We used a combination of screenshots and text to document the fields in the respective tool used to capture contextual knowledge.

An overview of the different tools, their intended area of use, nation of origin, and intended national or international use can be seen in [Table 2](#). We include the international use column to reflect the practical considerations in terms of language availability. Several tools, for example, were only available in Swedish. The tools are not mentioned by name, as this study did not aim to evaluate individual tools, and some were proprietary or subject to copyright restrictions. The tools have no connection to the respondents we interviewed, and the two should be viewed as separate and complementary data collection activities. By observing which documentation fields were consistently implemented in the tools, we gained additional insight into what procedural knowledge tool developers have included to assist with documenting the information classification process.

### 3.2 Data analysis

In our analysis, we followed Saldaña's thematic analysis coding guidelines ([Saldaña, 2021](#)), which recommend a two-cycle approach to qualitative coding. For the initial cycle, we employed structural coding, which is particularly suited to data gathered through semi-structured interviews ([Saldaña, 2021](#)). The initial coding structure was based on the main activity categories in [Figure 1](#): "Business Process / System Analysis", "Requirements", "Classification of Information", "Labelling" and "Selection of Final Business Process/System Classification". In this first cycle, we used these activity categories as codes and grouped excerpts from the interview transcripts under them based on what type of activity or process step they related to. This helped us identify where and in what step of the classification process records were used and described by the respondents.

In the second cycle, we reviewed and re-evaluated the initial coding to better reflect the focus of the study. We also used the contextual knowledge gathered from the tool demonstrations as input in the second coding cycle. During this stage, we removed

**Table 2.** An overview of the tools presented, their intended area of use, country of origin and if the tool is intended for national or international use

Tool	Intended area of use	Country of origin	International use
Tool 1	GRC	Sweden	X
Tool 2	GRC	Sweden	X
Tool 3	Incident management	Sweden	
Tool 4	GRC	USA	X
Tool 5	Risk management	Israel	X
Tool 6	GRC	Sweden	X
Tool 7	GRC/ISMS	Sweden	
Tool 8	Risk management	Sweden	
Tool 9	Risk management	France	X
Tool 10	GRC	USA	X
Tool 11	GRC	Slovakia	X
Tool 12	Information classification	Sweden	
Tool 13	Issue/project tracking – Showcased as a risk management tool	Australia	X
Tool 14	GRC	Luxembourg	X

**Source(s):** Authors' own work

---

“Labelling” and “Selection of Final Business Process/System Classification”, as these steps do not typically produce a record, but rather use one as input. We retained and slightly adjusted the remaining three categories, which became: “Business Process / System Analysis”, “Requirements” and “Classification Results”. Within each of these final categories, we then coded more specifically for record types and parts of records mentioned by respondents, such as asset type, rationale and responsible role. As an example, one respondent explained how they document the reasoning behind classification decisions. Such a quote was initially coded under “Classification of Information” and later recategorised under “Classification Results”, with the specific code of “Rationale for classification decision”. All coding was done manually in Microsoft Word using comment and highlighting features to mark and compare coded excerpts.

### 3.3 Validation

In ISRM research, validation is often missing (Fenz and Ekelhart, 2011). One way of validating ISRM research is presenting research results to a panel of experts (Fenz and Ekelhart, 2011; Thornhill *et al.*, 2016). Although an expert panel is opinion-based, it remains one of the few ways to validate ISRM findings (Fenz and Ekelhart, 2011).

In this paper, the preliminary results were brought to a panel of 14 information security experts with roles such as CISO and Senior Information Security Consultant. The choice of participants was done in accordance with the suggestions in Fenz and Ekelhart (2011). The participants represented organisations from both the private and public sectors, which allowed for a wide variety of experiences and knowledge to provide feedback. The session lasted for about one hour, starting with a presentation of the purpose and the presentation of the results, followed by a Q&A. A typical question that was asked and discussed were: “Do you think our results could improve the classification work?”. In a similar sense to the semi-structured interviews, the session was recorded with everyone’s consent and later transcribed *verbatim*. The validation session primarily strengthened the validity of the findings, and provided information for the use-cases.

## 4. Results and analysis

Based on the analysis, this section presents findings from the interviews and tool demonstrations, structured around the coding categories: Business Process/System Analysis, Requirements and Classification Results. Within each phase, we identify what practitioners and tool developers consider important to document. Each subsection begins with perspectives from interview respondents, followed by relevant observations from the tool demonstrations, and concludes with a table summarising the contextual knowledge identified as necessary for that category. The findings provide a structured view of what contextual knowledge is considered important to capture during the information classification process. At the end of each subchapter, a purpose and a brief use-case example are provided to illustrate the use in gathering the contextual knowledge.

### 4.1 Business process/system analysis

Respondents describe creating records in the business process/system analysis as a valuable task. Organisational knowledge is preserved not only through the records themselves but also through the collaborative discussions and analyses leading to their creation. These activities are said to increase awareness among both employees and the organisation, and improve the end result of the classification.

A variety of information found necessary to document by respondents, aside from the actual asset itself, were identified. In particular, respondents mentioned the importance of personally identifiable information (PII). Some respondents have internal tools they use to

document if the asset being classified does indeed include PII, often by a checkbox or a drop-down menu. Others use, for example, an Excel sheet developed by the organisation internally, and document information they perceive as important in a free-text field. However, it was explained that most of the time, this free-text field does not exist, and they have to manually create it by themselves and come up with the contextual knowledge to document. It is noted, however, that while the free-text fields are used, they tend to be quite scarce with information; respondent 6 explained:

[...] there is a small box where you have to fill in a description of the classification object so that, yes, you define some kind of contextual information, even if that information is usually quite scarce. – Respondent 6

Other respondents discussed contextual knowledge; for example, respondents 4 and 5 explained that it could be a detailed description of an asset and how it connects to a specific *process*. The same respondents also note that contextual descriptions, such as how assets relate to organisational processes, can support and further the understanding of the asset during classification by providing additional information and context.

Respondent 15 explained that they always document the main process the asset is used in, such as education, administration, or research. They then put the asset in a more specific process or sub-process, such as administering students; thus, it can be identified where the asset is used. Furthermore, what the asset contains is documented, such as PII of certain types, and lastly, its *location in a secondary asset*, that is, in which system it resides. In a similar sense, respondent 8 presses on the need to include the *information flow* of the identified asset, meaning, how the asset moves between systems/secondary assets during its lifecycle.

The tool demonstrations showcased pieces of records that respondents did not discuss, such as who the potential *external recipient* would be, the *location in the secondary asset*, the *purpose of the asset*, the *stakeholders* of relevance and the *person/role responsible* for the asset. The manner in which these are entered are text fields, which are then connected to the identified asset, and it will follow the asset throughout the classification and risk analysis.

#### *Purpose and use-case example:*

During a classification workshop, participants are to assess the potential consequences of confidentiality, integrity, or availability loss for a specific asset. By having the contextual knowledge in [Table 3](#), such as information flows, business processes, stakeholders and asset location, the team can more accurately determine the asset's organisational criticality. For example, knowing that the asset is used in both admissions and financial processes, and that it flows through multiple systems, may shift the classification towards a higher classification. The documented context ensures that the classification decision is grounded in how the asset functions in practice. After the classification, this contextual knowledge supports future reclassification and the inclusion of novices by allowing them to quickly understand the asset's purpose and organisational importance without having to reconstruct that understanding from scratch.

## 4.2 Requirements

Documenting *external and/or internal requirements* are only described to be done by some respondents, and it is mentioned to be connected to either laws or other contract-based requirements made with outside actors. They do, however, have a big effect on the classification as such. For example, if the asset includes, for example, PII, then that will have to be taken into consideration in the classification. This is brought up by respondent 5, who explains that as soon as they handle PII, they also have to comply with the regulations stated by the GDPR. The same respondent also mentions that contextual information they gather in

**Table 3.** Contextual knowledge in the business process/system analysis

Contextual knowledge documented	Explanation
Asset name	A descriptive name of the asset
Asset description	A description of the asset
Business process	Which business process(es) the asset is relevant to
Person/role responsible	A statement on who/what role is responsible for the asset
Usage	A brief description of the intended use of the asset
Information flows	A statement on how the asset moves in and between different systems in a process
Location in secondary asset	Where, and in which system(s) the asset is located. Such as in a service or a storage solution
Owner of the asset	The person or role who is the owner of the asset
External recipient	A statement on the external recipient of the asset if applicable
Stakeholders	Stakeholders of relevance affected by the asset

**Source(s):** Authors' own work

the first step, "Identify asset", can sometimes point towards laws they must adhere to, such as the Swedish law "Public Access to Secrecy", or other *privacy laws and regulations*. Another example of a requirement that can affect classification is brought up by respondent 6, who explains that, due to *archiving laws and regulations*, there are cases where information and documents must be disposed of, something that must be considered during the classification process. There is also mention of agreements with outside stakeholders that must be taken into consideration. One example being *IT provider agreements*, and investigating what their contracts mention regarding, for example, handling PII and similar assets.

Pertaining to the requirements section, the tool demonstrations showcased a variety of internal and external requirements present in tools that were not mentioned by respondents. In the tool demonstrations, examples were often used with generic requirements, such as the GDPR, *sector-specific laws and regulations*, or how the information management plan would have to be taken into consideration, for example.

*Purpose and use-case example:*

When classifying, workshop participants must consider the laws and regulations that affect the asset. Using the requirement types listed in Table 4, the team can identify relevant mandatory constraints, such as PII-related obligations, retention rules from archiving legislation, or internal access-control policies. These requirements can influence the level of strictness required for classification. For example, if the asset is subject to or includes regulated patient information, specific confidentiality and integrity levels must be taken into consideration. The documented requirements, therefore, provide justification for adjusting the classification level, which might otherwise be overlooked. After classification, this documentation provides a record of why certain requirements influenced the outcome, supporting audits and compliance reviews.

#### 4.3 Classification results

Respondents who discussed the classification results mentioned that the actual *classification level*, such as "level 3", is a key output. The same level is later used in the risk analysis, and respondents make it clear that it is important to document. However, respondents 8, 10 and 13, stress that classification involves more than just assigning a level and emphasise the

**Table 4.** Contextual knowledge in Requirements – Internal and external requirements are exemplified

Contextual knowledge documented	Explanation
<i>External requirements</i>	
Privacy laws and regulations NIS-2	<i>Requirements from an external source</i> National and/or international laws regulating privacy in some sense EU law enforcing cybersecurity measures and incident reporting for essential and important service providers
GDPR	EU regulation governing data protection and privacy, giving individuals control over their personal data
Public access to information	Laws and regulations regulating public access to official documents while protecting sensitive information
Sector-specific laws and regulations	National and/or international laws and regulations regulating sector-specific requirements
Patient data laws and regulations	Laws and regulations managing and protecting patient journal information, ensuring traceability and secure handling of patient data
Archiving laws and regulations	National and international laws and regulations that dictate the retention and management of records
Archives act	Dictates the preservation and management of public records for long-term archiving
Public records act	Governs transparency and archiving of public documents to maintain public access
IT provider agreements	Statement on how the information asset can be handled in relation to external providers of IT services to the organisation. An example of this is service level agreements (SLAs)
<i>Internal requirements</i>	
Internal policies	<i>Requirements from an internal source</i> Policies stemming from within the organisation, such as ones touching on organisational privacy, information security and data retention. An example affecting the classification could be, for example, certain access-control requirements to particular assets
Disaster recovery plan	Strategy for restoring systems and data after disruptions to ensure business continuity. This can affect, for example, storage requirements, and in turn, the classification of identified assets
Information management plan	Internal guidelines on structuring, storing and managing information efficiently. This can affect the classification level by, for example, limiting the use of certain identified assets

**Source(s):** Authors' own work

importance of documenting the rationale behind decisions, and the roles responsible. As Respondent 10 explains:

It's kind of about making sure there is room for justifications and, in a way, that you can demonstrate reflections — basically, reflections that occurred before defining a value in some way, right? That there is clarity, so you can go back to the classification documentation and see on what premises this decision was reached, even a year later". – Respondent 10

Respondent 10 further described classification as a collaborative process where reaching consensus is as important as the *classification level* itself. Including the *rationale for classification decisions* allows users to revisit and understand why a decision was made.

Respondent 15 explains that they have an internal tool that supports and encourages the documentation of rationale and perspectives of consequence (such as health, reputation and/or core business functions) by including text fields targeting those areas.

Respondent 7 emphasised the awareness-raising effect of classification workshops and explained that a classification workshop brings together different stakeholders, offering a rare opportunity to reflect on the value of the information being processed. This contributes to increased awareness of what types of information the organisation uses and manages.

Many respondents highlighted the classification activity as the most important step in the classification process. Not only does it produce the classification level, but it also brings together internal stakeholders. Respondent 7 describes it as one of the few opportunities for organisational reflection on the value of information. Such discussions are said to foster information security awareness, both individually and organisationally. Respondent 7 also noted that participants gained a better understanding of the types of information in organisational processes. According to Respondent 15, the discussion surrounding the classification creates a form of “collective memory” that, if documented, helps the organisation remember and build on previous discussions. Respondent 13 further explained:

Yes, well, if you haven’t documented it, you haven’t done it. I mean, it’s like this – we can sit here and talk as much as we want, but I mean [...] You might have a “picture” memory so you remember everything, but the third person who is participating does not, and if you leave the organisation then it [the rationale] no longer exists. – Respondent 13

The tool demonstrations did not highlight any additional information to be documented, but confirmed the importance of documenting both the classification level and rationale.

*Purpose and use-case example:*

During classification workshops, the participants determine the classification level. Capturing the rationale described in Table 5, including the arguments raised, potential consequences and perspectives considered, supports the team in making a well-founded and transparent decision. This also prevents having to do all of the work again in future classification sessions by making it clear what reasoning led to the chosen level. As such, the rationale becomes part of the classification result itself, ensuring that the assigned level is not just a number but an argued-for conclusion. After classification, this rationale serves as an organisational memory that supports reclassification, avoids repeated arguments, and can help novices understand the reasoning behind earlier decisions.

## 5. Discussion

A central finding in this study is that while classification decisions are often documented in some sense in most organisations, contextual knowledge surrounding such decisions is only partially captured, if at all. Respondents consistently emphasised that documenting only the classification level is insufficient to support reclassification. Instead, they highlight the importance of also documenting, for example, contextual knowledge of specific assets,

**Table 5.** Contextual knowledge in the classification results

Contextual knowledge documented	Explanation
Classification level	The level of classification of the asset received from a confidentiality, integrity and availability perspective
Rationale for classification decision	A summary statement on the rationale of the classification decision, that is, on what grounds/basis the classification decisions were taken

**Source(s):** Authors’ own work

---

internal and external requirements, and the rationale for making a classification decision. Even when the classification process is defined, such contextual knowledge is often not captured.

A possible explanation for this shortcoming is a gap identified in this study, namely, the lack of comprehensive guidance on what should be documented during the classification process. While existing methods, such as the one proposed by [Bergström et al. \(2021\)](#) based on [ISO/IEC 27002 \(2022\)](#), outline the main steps of a classification process, they provide little guidance on what the contents of the classification record should be. The lack of guidance may contribute to the variability observed in practice, where decisions are often based on subjective judgement but with limited documented contextual knowledge ([Andersson, 2023](#); [Shedden et al., 2016](#)). This study extends existing methods by identifying contextual knowledge that practitioners and tool developers consider essential to capture, and provides procedural knowledge in the form of a structured overview of what to document during a classification process. In doing so, we address a gap in current methods and offer a more complete view of how the information classification process can be supported.

A recurring mention in our findings is to record contextual knowledge, such as the rationale behind decisions and the roles of participants. Respondents emphasised the value of maintaining records that capture the discussions and reflections made during workshops, as these help preserve organisational memory, ensure transparency, and keep the rationale of decisions. The mention of such records aligns with assertions made by [Barraza de la Paz et al. \(2023\)](#) and [Beckers et al. \(2014\)](#), claiming that rationale is important for revisiting and justifying security choices during audits or future reviews. Similarly, [Sillaber and Breu \(2015\)](#) stresses the importance of documentation and its contribution to ISRM work.

While contextual knowledge is valuable in itself, there is also an argument to make surrounding how it is produced by the workshop participants. Classification workshops are viewed as an activity that increases information security awareness and understanding, indicating that while contextual knowledge is an important output, meaning the record, its creation is just as important. This suggests a “the journey is the goal” type of approach, where the value lies not only in the record itself but also in the activities and discussions that lead to its creation. In a similar setting, [Lundgren and Bergström \(2019\)](#) identified a scenario where the contextual information of assets found through analysis could potentially be more valuable than their actual valuation.

Our study also highlights additional organisational benefits of the information classification process. While the primary output of information classification is often understood to be the assigned classification level ([Bergström et al., 2021](#); [Tankard, 2015](#); [Bradford et al., 2022](#)), respondents emphasised two other key outcomes: a deeper understanding of the information being processed and an increased level of security awareness, both at the individual and organisational level. Both benefits are attributed to the participation of different stakeholders within the organisation in discussions during the information classification workshops, where the group discusses and reflects on the value of information. The workshops are stated to be one of the few moments where it is feasible and fitting to do so. In other words, users participate in security processes and, as a result, gain increased organisational awareness, which aligns with the findings in earlier work focusing on including organisational members in security processes ([Spears and Barki, 2010](#)). These workshops, while valuable for fostering awareness, also produce contextual knowledge that is important to document and preserve.

The approach that we propose in this work helps guide and focus classification by offering the procedural knowledge needed for each step of the classification process, and the

---

contextual knowledge on what to consider documenting during the classification. In doing so, an organisation can create a structure for documenting the activity and create a record that can be retrieved and reused during reclassification.

The tool demonstrations provided further insight into how classification records are currently structured in practice. Many tools include predefined fields for assets and regulatory requirements [in line with (Gritzalis *et al.*, 2018)], however, they offer limited support for capturing decision rationale and contextual discussions, both of which respondents emphasised as important for transparency and reclassification. While tools in their current form assist in structuring classification documentation, they still lack functionalities that respondents consider necessary. These gaps may contribute to variations in documentation practices, as some respondents rely on the structured input fields provided by tools, while others create additional fields and document contextual knowledge to compensate for missing functionalities. This became particularly evident among respondents who reported using spreadsheets rather than proprietary software. In addition, while the tools primarily support the organisation of classification records, they do little to assist users in making the actual classification decisions. In other words, there is a lack of functional tools that support decision-making in information classification.

Our findings include a variety of items to include in a record that tools could support. It is worth mentioning, however, that the structure we suggest does not require an advanced tool, it could be realised in a text file or a spreadsheet and support organisations with a structure when creating their records. However, as seen in other research [e.g. Gritzalis *et al.* (2018) and Bergström (2023)], a better scenario would likely be to integrate our proposed structure into a tool that covers the whole ISRM process rather than having a specific tool only for information classification.

Finally, the results of this study were validated through the use of a panel of information security experts. In the validation session, the experts confirmed that the contextual knowledge elements identified in the study reflected their own experiences with information classification and were aligned with the practical challenges they encounter in their work, thereby confirming their practical relevance.

### 5.1 Limitations

The results of this study are generalisable in the sense that they highlight types of contextual knowledge that practitioners commonly consider important to document. However, they are not directly applicable to all organisations or all asset types without adaptation to specific organisational contexts. Some elements of the proposed record structure are likely to be of greater value to certain organisations than others, depending on their size, sector, and maturity of information security practices.

The findings also reflect the perspectives of a limited set of respondents, primarily CISOs and information security specialists, and observations of a selected number of tools. A broader sample, including additional organisational roles and sectors, may have yielded a wider range of perspectives and potentially expanded the list of contextual knowledge identified.

Concerning the data collection, there is a potential bias. The interviews were conducted with only Swedish representatives, and the tools are predominantly from Sweden and Europe, even though four continents are represented in the study. All the tools and respondents that were interviewed followed an existing information classification model based on the ISO/IEC 27002 standard. We did not find any inconsistencies based on the country of origin.

---

## 6. Conclusion

This study explored which types of contextual knowledge should be recorded during the information classification process. In doing so, it contributes procedural knowledge by outlining how organisations can identify and document such knowledge when conducting information classification. Using an existing model based on ISO/IEC 27002 as a frame of reference, we examined how contextual knowledge is currently captured in practice and identified knowledge elements that security practitioners and tool developers consider essential to document.

A key takeaway is that current classification models provide little guidance on what should be documented beyond the final classification level. This gap could be a reason why documentation practices differ so much in practice, both in what is documented and how they do it. At the same time, the collaborative nature of classification workshops presents an opportunity for reflection, shared understanding and increased security awareness. However, without structured approaches to capture the contextual knowledge that emerges in these settings, much of the potential value of these insights risks being lost. To address this, we propose a structured approach consisting of recommended contextual knowledge to document, which can serve as a starting point for integration into an organisation's classification process. Each part of the structured approach is linked to a use-case example, illustrating why the associated contextual knowledge should be captured and how it can be used.

The paper contributes to practitioners who conduct information classification as part of their profession by suggesting contextual knowledge that could be captured during the classification process more extensively than what is currently described in literature and standards. In doing so, organisations can get a better basis for classification decisions. In addition, the gathered knowledge will follow the asset to the risk analysis, thereby providing a better basis for starting that work. The contribution could also support practice and future development of guidelines and standards.

In addition, for research, it showcases that there is a clear need for developing guidelines on what to document throughout the classification process and, in doing so, providing some much-needed structure to the practice. Finally, the study highlights that there is a lot of value to be found in classifying information when adopting a “the journey is the goal” approach, resulting in increased security awareness both as an organisation and as individuals and at the same time probably producing a better classification output. In addition, the results of this study could be of value to tool developers, as it offers insight into the contextual knowledge that is collected and the missing functionality of existing tools.

Future research could focus on further developing existing methods to include structured documentation practices. One approach to this could be to develop standardised templates that could be integrated into existing ISRM tools to ease the administrative burden and assist users in determining what to capture during record creation. Another topic of interest is investigating how tools can assist users in making classification decisions, not just support them by gathering more contextual knowledge. A last suggestion for future research is to investigate how different types of gathered contextual knowledge affect the classification decision.

## References

- Adams, W.C. (2015), “Conducting semi-structured interviews”, *Handbook of Practical Program Evaluation*, Wiley Online Library, pp. 492-505.
- Alavi, M. and Leidner, D.E. (2001), “Knowledge management and knowledge management systems: conceptual foundations and research issues”, *MIS Quarterly*, Vol. 25 No. 1, pp. 107-136.

- Allmark, P., Boote, J., Chambers, E., Clarke, A., McDonnell, A., Thompson, A. and Tod, A.M. (2009), "Ethical issues in the use of in-depth interviews: literature review and discussion", *Research Ethics*, Vol. 5 No. 2, pp. 48-54.
- Anderson, J.R., and Crawford, J. (1995), *Cognitive Psychology and Its Implications*, wh freeman, New York, NY.
- Andersson, S. (2023), "Problems in information classification: insights from practice", *Information and Computer Security*, Vol. 31 No. 4, pp. 449-462.
- Barraza de la Paz, J.V., Rodríguez-Picón, L.A., Morales-Rocha, V. and Torres-Argüelles, S.V. (2023), "A systematic review of risk management methodologies for complex organizations in industry 4.0 and 5.0", *Systems*, Vol. 11 No. 5, p. 218.
- Beckers, K., Heisel, M., Solhaug, B., and Stølen, K. (2014), "Isms-coras: a structured method for establishing an iso 27001 compliant information security management system", *Engineering Secure Future Internet Services and Systems: Current Research*, ages, pp. 315-344.
- Bergquist, J.-H., Tinet, S. and Gao, S. (2021), "An information classification model for public sector organizations in Sweden: a case study of a swedish municipality", *Information and Computer Security*, Vol. 30 No. 2, pp. 153-172.
- Bergström, E. (2023), "Tools supporting information security risk management in practice", in Bednar, P., Zaghoul, F., Welch, C., Nolte, A., Rajanen, M., Islind, A. S., Hult, H. V., Ravarini, A. and Braccini, A. M. (Editors), *9th International Conference on Socio-Technical Perspective in Information Systems Development, STPIS, CEUR-WS*, Vol. 3598, pp 146-159.
- Bergström, E., Karlsson, F. and Åhlfeldt, R.-M. (2021), "Developing an information classification method", *Information and Computer Security*, Vol. 29 No. 2, pp. 209-239.
- Bracewell, R., Wallace, K., Moss, M. and Knott, D. (2009), "Capturing design rationale", *Computer-Aided Design*, Vol. 41 No. 3, pp. 173-186.
- Bradford, M., Taylor, E.Z. and Seymore, M. (2022), "A view from the ciso: insights from the data classification process", *Journal of Information Systems*, Vol. 36 No. 1, pp. 201-218.
- Brezillon, P., and Pomerol, J.-C. (1999), "Contextual knowledge and proceduralized context", In *Proceedings of the AAAI-99 Workshop on Modeling Context in AI Applications*, AAAI Technical Report, Orlando, FL.
- Cabinet Office (2024), "Government security classifications policy" (accessed 3 May 2025).
- Conklin, E.J. and Yakemovic, K.B. (1991), "A process-oriented approach to design rationale", *Human-Computer Interaction*, Vol. 6 No. 3, pp. 357-391.
- Davenport, T.H., and Prusak, L. (1997), *Information Ecology: Mastering the Information and Knowledge Environment*, Oxford University Press.
- ENISA (2024), "ENISA threat landscape 2024".
- European Union Agency for Cybersecurity (ENISA) (2023), "RM/RA tools".
- Everett, C. (2011), "Building solid foundations: the case for data classification", *Computer Fraud and Security*, Vol. 2011 No. 6, pp. 5-8.
- Fenz, S. and Ekelhart, A. (2011), "Verification, validation, and evaluation in information security risk management", *IEEE Security and Privacy Magazine*, Vol. 9 No. 2, pp. 58-65.
- Fenz, S., Heurix, J., Neubauer, T. and Pechstein, F. (2014), "Current challenges in information security risk management", *Information Management and Computer Security*, Vol. 22 No. 5, pp. 410-430.
- Fibikova, L., and Müller, R. (2011), *A Simplified Approach for Classifying Applications*, ages, Vieweg +Teubner, Wiesbaden, pp. 39-49.
- Fung, P., Kwok, L-F., and Longley, D. (2003), "Electronic information security documentation", in *Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003*, Vol. 21, pp. 25-31.

- 
- Georgeff, M.P. and Lansky, A.L. (1986), "Procedural knowledge", *Proceedings of the IEEE*, Vol. 74 No. 10, pp. 1383-1398.
- Gerber, M. and Von Solms, R. (2005), "Management of risk in the information age", *Computers and Security*, Vol. 24 No. 1, pp. 16-30.
- Greenberg, S. (2001), "Context as a dynamic construct", *Human-Computer Interaction*, Vol. 16 Nos 2-4, pp. 257-268.
- Grimaila, M.R. and Fortson, L.W. (2007), "Towards an information asset-based defensive cyber damage assessment process", In 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications, pp. 206-212.
- Gritzalis, D., Iseppi, G., Mylonas, A. and Stavrou, V. (2018), "Exiting the risk assessment maze: a meta", *Survey. ACM Comput. Surv.*, Vol. 51 No. 1, pp. 1-30.
- Halcomb, E.J. and Davidson, P.M. (2006), "Is verbatim transcription of interview data always necessary?", *Applied Nursing Research*, Vol. 19 No. 1, pp. 38-42.
- Haufe, K., Colomo-Palacios, R., Dzombeta, S. and Brandis, K. (2016), "A process framework for information security management", *International Journal of Information Systems and Project Management*, Vol. 4 No. 4, pp. 27-47.
- Ico, I.C.O. (2025), "Capita fined £14m for data breach affecting over 6m people".
- ISO/IEC 27001 (2022), *Information Technology – Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements. Standard ISO/IEC 27001:2022*, International Organization for Standardization, Geneva, CH.
- ISO/IEC 27002 (2022), *Information Security, Cybersecurity and Privacy Protection — Information Security Controls. Standard ISO/IEC 27002:2022*, International Organization for Standardization, Geneva, CH.
- ISO/IEC 27005 (2022), *Information Security, Cybersecurity and Privacy Protection — Guidance on Managing Information Security Risks. Standard ISO/IEC 27005:2022*, International Organization for Standardization, Geneva, CH.
- Jennex, M.E. (2010), "Implementing social media in crisis response using knowledge management", *International Journal of Information Systems for Crisis Response and Management (JIJISCRAM)*, Vol. 2 No. 4, pp. 20-32.
- Johnson, L.M. and Schulte, J.D. (2004), "Job: security 7 steps for hipaa compliance: taking a proactive stance is your top job for effective information security", *Healthcare Financial Management*, Vol. 58 No. 10, pp. 46-50.
- Kaarst-Brown, M.L., and Thompson, E.D. (2009), "Cracks in the security foundation: employee judgments about information sensitivity", In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, ACM, pp. 145-151.
- Kallio, H., Pietilä, A.-M., Johnson, M. and Kangasniemi, M. (2016), "Systematic methodological review: developing a framework for a qualitative semi-structured interview guide", *Journal of Advanced Nursing*, Vol. 72 No. 12, pp. 2954-2965.
- Kuhn, T., Basch, P., Barr, M., Yackel, T. and Of The American College Of Physicians\*, M.I.C. (2015), "Clinical documentation in the 21st century: executive summary of a policy position paper from the american college of physicians", *Annals of Internal Medicine*, Vol. 162 No. 4, pp. 301-303.
- Lim, W.M. (2024), "What is qualitative research? an overview and guidelines", *Australasian Marketing Journal*, Page, Vol. 33 No. 2, p. 14413582241264619.
- Lundgren, M. and Bergström, E. (2019), "Dynamic interplay in the information security risk management process", *International Journal of Risk Assessment and Management*, Vol. 22 No. 2, p. 212.
- Magaldi, D., and Berler, M. (2018), "Semi-structured interviews", In *Encyclopedia of Personality and Individual Differences*, Springer, pp. 1-6.

- Mattord, H.J., and Wiant, T. (2016), "Information system risk assessment and documentation", In *Information Security*, Routledge, pp. 69-111.
- Meti, M. (2025), "Guidelines on the roles expected of cyber infrastructure providers. Collected: 2025-12-09".
- MSB (2020), "Myndigheten för samhällsskydd och beredskaps föreskrifter om informationssäkerhet för statliga myndigheter. Collected: 2025-12-05".
- MSB (2023), "Klassningsmodell".
- Ngoepe, M. (2014), "The role of records management as a tool to identify risks in the public sector in South Africa", *SA Journal of Information Management*, Vol. 16 No. 1, pp. 1-8.
- Niemimaa, E. and Niemimaa, M. (2017), "Information systems security policy implementation in practice: from best practices to situated practices", *European Journal of Information Systems*, Vol. 26 No. 1, pp. 1-20.
- Nist, J.T.F. (2018), *Nist Special Publication 800-37 Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy Joint Task Force*, National Institute of Standards and Technology, Gaithersburg, MD, USA.
- Nonaka, I., Toyama, R. and Konno, N. (2000), "Seci, ba and leadership: a unified model of dynamic knowledge creation", *Long Range Planning*, Vol. 33 No. 1, pp. 5-34.
- Nunes, V.T., Santoro, F.M. and Borges, M.R. (2009), "A context-based model for knowledge management embodied in work processes", *Information Sciences*, Vol. 179 No. 15, pp. 2538-2554.
- Oates, B.J. (2006), *Researching Information Systems and Computing*, SAGE Publications Inc., London.
- Orlando, A. (2021), "Cyber risk quantification: investigating the role of cyber value at risk", *Risks*, Vol. 9 No. 10, p. 184.
- Reynolds, T.J. and Gutman, J. (1988), "Laddering theory, method, analysis, and interpretation", *Journal of Advertising Research*, Vol. 28 No. 1, pp. 11-31.
- Ruslin, R., Mashuri, S., Rasak, M.S.A., Alhabsyi, F. and Syam, H. (2022), "Semi-structured interview: a methodological reflection on the development of a qualitative research instrument in educational studies", *IOSR Journal of Research and Method in Education (IOSR-JRME)*, Vol. 12 No. 1, pp. 22-29.
- Saldaña, J. (2021), *The Coding Manual for Qualitative Researchers*, SAGE Publications Inc., Thousand Oaks, CA, USA, 4th edition.
- Sánchez-García, I.D., Mejía, J. and San Feliu Gilabert, T. (2023), "Cybersecurity risk assessment: a systematic mapping review, proposal, and validation", *Applied Sciences*, Vol. 13 No. 1, p. 395.
- Shamala, P., Ahmad, R., Zolait, A. and Sedek, M. (2017), "Integrating information quality dimensions into information security risk management (isrm)", *Journal of Information Security and Applications*, Vol. 36, pp. 1-10.
- Shedden, P., Ahmad, A., Smith, W., Tscherning, H. and Scheepers, R. (2016), "Asset identification in information security risk assessment: a business practice approach", *Communications of the Association for Information Systems*, Vol. 39 No. 1, p. 15.
- Sillaber, C., and Breu, R. (2015), "Using stakeholder knowledge for data quality assessment in is security risk management processes", In *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*, pp. 153-159.
- Silva, F., and Jacob, P. (2018), "Mission-centric risk assessment to improve cyber situational awareness", In *Proceedings of the 13th International Conference on Availability, Reliability and Security*, pp. 1-8.
- Spears, J.L. and Barki, H. (2010), "User participation in information systems security risk management", *MIS Quarterly*, Vol. 34 No. 3, pp. 503-522.

- Suhaimi, A.I.H., Goto, Y. and Cheng, J. (2014), "An information security management database system (ismds) for engineering environment supporting organizations with ismss", *IEICE Transactions on Information and Systems*, Vol. E97.D No. 6, pp. 1516-1527.
- Tankard, C. (2015), "Data classification—the foundation of information security", *Network Security*, Vol. 2015 No. 5, pp. 8-11.
- Tehler, H. (2023), *Introduktion till Risk Och Riskhantering*, Lunds University, Lund: first edition.
- Thornhill, A., Saunders, M., and Lewis, P. (2016), "Research methods for business students", Prentice Hall, London, seventh edition edition.
- van Laere, J. and Lindblom, J. (2019), "Cultivating a longitudinal learning process through recurring crisis management training exercises in twelve swedish municipalities", *Journal of Contingencies and Crisis Management*, Vol. 27 No. 1, pp. 38-49.
- Wangen, G., Hallstensen, C. and Snekkenes, E. (2018), "A framework for estimating information security risk assessment method completeness", *International Journal of Information Security*, Vol. 17 No. 6, pp. 681-699.
- Whitman, M.E., and Mattord, H.J. (2022), *Principles of Information Security*, Cengage Learning, seventh edition.
- Willman, L., Jennex, M.E. and Frost, E.G. (2022), "Using knowledge management to improve the effectiveness of data fusion centers", *International Journal of Knowledge Management (IJKM)*, Vol. 18 No. 1, pp. 1-16.
- Yeo, G. (2018), *Records, Information and Data*, Facet Publishing.

#### Corresponding author

Simon Andersson can be contacted at: [simon.andersson@ltu.se](mailto:simon.andersson@ltu.se)





Department of Computer Science, Electrical and Space Engineering  
Division of Digital Services and Systems

---

ISSN 1402-1544

ISBN 978-91-8142-008-1 (print)

ISBN 978-91-8142-009-8 (pdf)

Luleå University of Technology 2026

