UNIVERSITY
OF SKÖVDE

THESIS PROPOSAL

A METHOD FOR INFORMATION CLASSIFICATION

ERIK BERGSTRÖM
Informatics

A METHOD FOR INFORMATION CLASSIFICATION

[Keywords]

THESIS PROPOSAL

A METHOD FOR INFORMATION CLASSIFICATION

[Keywords]

ERIK BERGSTRÖM
Informatics

UNIVERSITY
OF SKÖVDE

Erik Bergström, 2017

Title: A Method for Information Classification
[Keywords]

University of Skövde 2017, Sweden
www.his.se

Printer: Printers name, Printers location

ISBN XXX-XX-XXXX-XX-X
Dissertation Series, No. Number (Year)

ABSTRACT

In the highly digitalized world in which we live today, information and information systems have become key assets to organizations. These assets need to be managed properly because it is difficult to safeguard assets that an organization does not know exist and does not know the value they offer. In an Information Security Management System (ISMS), asset management is an important activity as it aims at identifying, assigning ownership and adding protection to information assets. Within asset management, one activity is information classification that has the objective to ensure that information receives an appropriate level of protection in accordance with its importance to the organization. In practice, this is usually done using a classification scheme, and the result is handled as input to the risk analysis. Information classification is a well-known practice for all kind of organizations, both in the private and public sector, and is included in different variants in standards such as ISO/IEC 27002, COBIT and NIST-SP800.

However, information classification has received little attention from academia, and many organizations are struggling with the implementation. Little is known about the reasons behind why it is problematic, and how to address such issues. Furthermore, the existing methods, described in, e.g., standards do not provide a coherent and systematic approach to information classification. The short descriptions in standards, and literature alike, leave out important aspects needed for many to adopt any kind of information classification. For instance, there is a lack of detailed descriptions regarding (1) overview of procedures, and concepts, (2) which roles are involved in the classification, and how they interact, (3) how to tailor the method for different situations and (4) a framework that structures and guides the classification. If information classification is not implemented in an organization, the organization might not know what information they possess, what the value of the information is, but even if it is implemented, an unclear approach can lead to information being under or overvalued, which, in turn, lead to under or overprotected information.

This thesis aims to increase the applicability of information classification by devising a method for information classification in ISMS that draws from established standards and practice. In order to address this aim, a Design Science Research (DSR) study has been performed in five cycles. The contributions so far include an identification of issues and enablers for information classification and propose a component-based method for information classification. Furthermore, eighth design principles underpinning an information classification method are presented. Additionally, an outline for further research is provided, where the objectives are to further develop the method by addressing the context around information classification (the risk analysis and security controls), and by adding usage views to the method. Finally, a security declaration as an addition to the information classification method is outlined as a complement for tying security controls to the information

classification scheme.

SAMMANFATTNING

Click here to add your text

ACKNOWLEDGEMENTS

Click here to add your text

PUBLICATIONS

Click here to add your text

PUBLICATIONS WITH HIGH RELEVANCE

1. 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.
2. Bergström, E., & Åhlfeldt, R.-M. (2015). Information Classification Enablers. In J. Garcia-Alfaro, E. Kranakis, & G. Bonfante (Eds.), *Foundations and Practice of Security: 8th International Symposium, FPS 2015, Clermont-Ferrand, France, October 26-28, 2015, Revised Selected Papers* (pp. 268-276). Cham: Springer International Publishing.
3. Bergström, E., Åhlfeldt, R.-M., & Anteryd, F. (2016). *Informationsklassificering och säkerhetsåtgärder*. IIT Technical Reports, HS-IIT-TR-16-002.
4. Bergström, E., Karlsson, F., & Åhlfeldt, R.-M. (2018) *Devising an Information Classification Method.* Going to be submitted to Information and Computer Security: Emerald Publishing Limited. (Preliminary draft included).
5. Lundgren, M., & Bergström (2017). *The Interplay: Classification, Risk, and Controls.* Submitted to Journal of Information Assurance and Security. (Submitted paper included)

PUBLICATIONS WITH LOWER RELEVANCE

1. Åhlfeldt, R.-M., Andersén, A., Eriksson, N., Nohlberg, M., Bergström, E., & Fischer-Hübner, S. (2015). *Kompetensbehov och kompetensförsörjning inom informationssäkerhet från ett samhällsperspektiv.* IIT Technical Reports, HS-IIT-TR-15-001.

CONTENTS

CHAPTER 1
INTRODUCTION

With the move to the information society, organizations have become dependent on information technology for creating value. With this growing dependability of information combined with the rapid increase in the amount of information organizations need to handle, the continual decrease in storage costs, the increased usage of cloud services, bring your own device, combined with an endless stream of new exploits paints a problematic picture for information security. In the last decade, information security breaches have started to make it to the headlines of most major newspapers on a frequent basis. The costs associated with malicious breaches are expected to increase to more than 2 trillion USD by 2019, which is a quadrupling since 2015, and an expected 2.2% of the world's total GDP in that year (Moar, 2015).

To counteract breaches, information security is applied. Information security can be defined as *"means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide - (A) integrity [...] (B) confidentiality [...] and (C) availability"* (44 U.S. Code § 3542(b)(1), 2002). Information security is a broad concept and consists of security measures that are both technical and administrative. To manage information security, a management system, or Information Security Management System (ISMS) such as the ISO/IEC 27000 series can be used. ISO/IEC defines ISMS as *"that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security"* (ISO/IEC 27002, 2013 p. 2). ISMS is normally built on a standard that in turn stems from *"generally accepted principles"*, or *"best practices"* (M. Siponen & Willison, 2009). With the continuously evolving threats, organizations face pressure to adopt ISMS (Hsu, Lee, & Straub, 2012), but many organizations also do so to address different legal or contractual demands (Gerber & von Solms, 2008) or because they are required to do so due to compliance requirements from governments (Smith, Winchester, Bunker, & Jamieson, 2010).

Traditionally, much effort has been directed at developing the technical aspects of information security (M. Siponen & Oinas-Kukkonen, 2007), where the socio-technical aspects were neglected (Ashenden, 2008). Therefore, in this work, the focus is on administrative security, that includes, e.g., policies, standards, and procedures (Åhlfeldt, Spagnoletti, & Sindre, 2007). More specifically, the focus is on information classification, which is an important part of asset management, where information is valued concerning the loss of, e.g., confidentiality, integrity or availability. This is important, because if an organization does not know the value or the information they possess, they might not know

how to protect it properly. The classified information then serves as input to the risk assessment, where risks are identified and expressed in terms of the combination of consequence and likelihood (ISO/IEC 27005, 2013). Following the risk assessment, the security techniques needed to fulfill the levels of protection needed are put in place.

In the following sections, the problem space is presented following with the aims and objectives for the thesis. This is followed by a summary of the contributions, related research, and the delimitations of the work so far. Finally, an outline of the thesis is provided.

1.1 PROBLEM SPACE

Information classification is a well-established practice that originates from the military. The probably most well-known classification scheme comes from the US military, where the levels top secret, secret, and unclassified information are used (Bayuk, 2010). Information classification is a practice recommended to be used in a number of ISMS standards, for example, in the ISO/IEC 27000-series, and in the Control Objectives for Information and Related Technologies (COBIT) framework, where it is referred to as data classification. Information classification is also included in other management standards, such as in the American NIST-SP800, and in the Payment Card Industry Data Security Standard (PCI-DSS) (Niemimaa & Niemimaa, 2017). Furthermore, information classification is a mandatory activity for government agencies in a number of countries, for instance in the UK (Cabinet Office, 2013), Australia (Australian Government, 2014), and Sweden (MSBFS 2016:1, 2016). In the private sector, information classification is also a well-established activity due to legal requirements, e.g., for protecting personally identifiable information (Raman, Beets, & Kabay, 2014). With the introduction of EU's General Data Protection Regulation (GDPR) in 2018, information classification is expected to gain further momentum as organizations need to identify and value their information to avoid breaches and large fines (Mansfield-Devine, 2016).

Despite this relatively wide-spread adoption of information classification, according to a Forrester report, information classification is an overlooked activity among security and risk professionals (Kindervag, Shey, & Mak, 2015), something also acknowledged in existing research (Oscarson & Karlsson, 2009). The identification of information assets is described as a challenge for many organizations (Bunker, 2012; Ku, Chang, & Yen, 2009), as is the decision of the information value (Aksentijevic, Tijan, & Agatic, 2011; Al-Fedaghi, 2008), which is the objective with asset management and information classification.

The classification process has been described as problematic in a general way, and many organizations struggle to perform the classification (Collette, 2006; Ghernaouti-Helie, Simms, & Tashi, 2011; Glynn, 2011; Hayes, 2008; Kane & Koppel, 2013). The exact causes why it is problematic have been investigated from several perspectives, however, no coherent view on such causes appear in the literature. One reason is the military tradition that is believed to be non-transferable to a corporate setting (Bayuk, 2010; Gantz & Philpott, 2013; Grandison et al., 2007; Jafari & Fathian, 2007; Lindup, 1995; D. B. Parker, 1996; Donn B. Parker, 1997; Ramasamy & Schunter, 2006) that has led to a focus on the confidentiality aspect. Consequently, confidentiality has been prioritized over integrity and availability when it comes to information classification (Gantz & Philpott, 2013).

Baškarada (2009) described that one of the inhibitors is actually developing the classifications itself, however without providing any details on exactly why it is so. Niemimaa and Niemimaa (2017) followed the implementation of information classification in an organization and saw that "*the standard described the practice of information classification in a general and universal manner without explaining how the practice could be accomplished in any particular organization*". In other words, they address the gap of turning the standard into policy, which then is turned into organizational practice.

Another challenge with information classifications is a subjective judgment that leads to inconsistent classifications (Baškarada, 2009; Booysen & Eloff, 1995; Eloff, Holbein, & Teufel, 1996; Ku et al., 2009; D. B. Parker, 1996). This might be due to too complex schemes (D. B. Parker, 1996) or because the scheme does not fit the business's needs (Donn B. Parker, 1997). The subjective judgment in information classification refers to the lack of an explicit process and criteria for deciding on the value of the information in question. In practice this means that two individuals might classify the same type of information differently, which leads to situations where information might get under- or overclassified and hence not receives that right level of protection. The subjective judgment in information classification refers to the lack of an explicit process and criteria for deciding on the value of the information in question. Thompson and Kaarst-Brown (2005) argued that a number of aspects come into play when information is classified, such as social and cultural perspectives as well as a person's awareness of organizational, economical, legal and social contexts. The challenge of subjective judgment is an area often ignored, both in practice and research. As a result, it creates tension between the classification schema, implemented information security controls, and the information that employees are using (Kaarst-Brown & Thompson, 2015).

In the field of Information Systems Security, abbreviated ISS (or ISsec), the research practice has not matured as other Information Systems (IS) disciplines, and both from a theoretical, and empirical perspective the field is behind IS (M. Siponen, Willison, & Baskerville, 2008). Hence, subsequent work has started to introduce more socio-technical aspects and theoretically justified work (Willison & Warkentin, 2013).

In this work, a way forward is proposed for organizations struggling with the classification by suggesting a method for information classification. The focus is on the classification process itself, associated descriptions, and the context around information classification.

1.2 AIMS AND OBJECTIVES

The overall aim of the work is to *increase the applicability of information classification by developing a method for information classification in information security management systems*. In order to address this aim, a set of objectives have been specified:

- O1. Identify and characterize the inhibitors and enablers in the information classification process.
- O2. Develop design principles that support the development of a method.
- O3. Develop a method for information classification.

During the design process the aim and objectives have changed slightly, but broadly the focus is the same as when the thesis project started. Initially, there was a tighter relationship to the ISO/IEC 27002 (2013) standard and literature associated with that standard. In the beginning, much attention was directed to problems at a Swedish county council as the first interviews were performed there. These interviews showed some gaps that initially were found interesting, but after subsequent interviews with other actors, the gaps identified were in fact greater than originally expected. For example, one of the initial objectives was to clarify the information classification process as described in ISO/IEC 27002, but as time passed and knowledge about the causes of the problem grew, it was clear that it was not only a process model that lacked but rather a method for information classification.

The first objective, O1, targets the general area of information classification. Even though information classification is a well-known activity for valuing information, it is under-researched, and much is not known about what the issues are and what can be done about them.

The main outcome designed in this thesis is a method for information classification. The method intends to be a method possible to adopt for any organization wishing to implement information classification as a part of their ISMS.

1.3 CONTRIBUTIONS

The main contributions of this thesis are the identification and characterization of the inhibitors and enablers for information classification, design principles underpinning the method, and the method for information classification.

This section will be developed further for the final thesis. For the thesis proposal, the results can be seen in Chapter 5.

1.4 RELATED RESEARCH

The work in the information classification domain is fragmented, both regarding publication year and in which area the work is published. Even though searches for information classification returns a large number of publications mentioning information classification, security classification or data classification (see more in Chapter 2.4 for a discussion on the difference between the terms), most publications are not about the classification process, but rather mentions it. Information classification research, in general, is limited (Oscarson & Karlsson, 2009) with few research contributions focusing on the classification process itself. Several authors, e.g., Eloff et al. (1996); Feuerlicht and Grattan (1989); Kwo-Jean, Shu-Kuo, and Chi-Chun (2008); D. B. Parker (1996), provide guidelines, frameworks or models with varying degree of detail for how to classify information. Fibikova and Müller (2011) describe two alternative approaches to classifying information, a process-oriented approach and an application-oriented approach. The process-approach takes it stance from business-processes in an organizations, and describes a way of classifying information based on the process (Fibikova & Müller, 2011). Similarly, if the organization does not use a process-view, applications can be seen as a starting-point, and the information present in an application is used as an onset for classification (Fibikova & Müller, 2011).

Fernando and Zavarsky (2012) propose a categorization with thresholds to enable an organization to handle parts of the information lifecycle such as the disposal of data. The goal with the proposed additions to the Information Lifecycle Management (ILM) will handle more than just the disposal phase of the ILM, and will not take an approach where the value of the data is calculated to find out if it is going to be disposed or not.

Several of the contributions predate the commonly used ISO 27000-series standard where many organizations take their stance from today, but they still contribute to the overall understanding of the information classification process and its related issues. There are also some studies describing how to handle issues in the classification process (Collette, 2006), practical tips for implementing classification (Glynn, 2011), and why it needs to be done (Everett, 2011), but it is unclear whether these studies are peer-reviewed or not.

Much research is also performed in the areas that relate to or make an impact on the information classification process. Automatic classification, using, for instance, different techniques from machine learning and linguistics seem to be a growing field. Some examples are Virtanen (2001) that proposes a solution for reclassification where previous data is used to recalculate the classification automatically. An approach with the same intent is presented by DuraiPandian and Chellappan (2006) and Hayat, Reeve, Boutle, and Field (2006). Access control mechanisms and models are researched in a number of ways, for example, on giving access to more fine-grained data, which it is important since it enforces the information classification when access is to be granted to a specific piece of information. There is also

research about the labeling part of the information classification process, and topics include, for instance, what the label should consist of (see e.g. Blazic and Saljic (2010), and Collette (2006)), and problems related to how labeling are implemented (see e.g. Winkler (2011), and Fibikova and Müller (2011)).

1.5 DELIMITATIONS

As previously mentioned, there are several suggestions for automatic information classification, but here only manual classification is considered. Manual information classification is to the best of my knowledge the most well-used practice, and to date, no organization using any type of automatic classification tool has been encountered. Many times when there is an issue, an easy fix is to implement some tool or technology, but in this work, the stance from Everett (2011) is followed, that information classification is very much a human, and process problem. The argument used is that even if a technology fix was enough, there are not any tools available that can classify based on phrases or keywords without the need for manual intervention.

Furthermore, information classification is considered a group activity, as opposed to security classification that is more of a one-man-show (Axelrod, Bayuk, & Schutzer, 2009). In other words, this work takes a stance on that there are several individuals with a variety of competences that are involved in the classification of information.

As previously mentioned, labelling is related to the information classification processes the consequence of a classification is that a label is applied to the information. This is also the classical picture of information classification, where a document has been labeled with a big red stamp statin the information is TOP SECRET. The same applies to all information, and as most information in an organization is electronic, labeling is a serious problem as all information in an organization that is classified should be labeled. This means all data or at least, all data not classified at the lowest level should be labeled (e.g., the lowest level OFFICIAL in the UK does not require a label (Cabinet Office, 2013). In practice, the data can be found everywhere, which means, e.g., in databases, log data, and documents spread across different platforms using different file systems. The issue of adding the label to a specific piece of information is many times of technical nature. A label is an addition of meta-data that need to be inserted in files, sentences in files or cells in a database. These aspects are not considered in this thesis, but the labeling activity is included.

Finally, the handling routines that follow as a consequence of a classification is delimited to be included in the method devised, and suggestions on how to use them or how to develop them are not included. The reasons behind this are that they are first and foremost extremely organization specific. The layout of a typical handling routine is a direct mapping of security controls to a specific consequence level when handling, processing, storing and communicating (ISO/IEC 27002, 2013).

1.6 THESIS OUTLINE

The rest of the thesis proposal is organized as follows. In chapter 2, a brief introduction to Information Security Management, information classification, security classification, and related standards is introduced. In chapter 3, the method theory is described, followed by chapter 4 where the research design is presented. Chapter 5 outlines the results, followed by chapter 6 that presents the method for information classification. Finally, chapter 7 reveal the conclusions and introduce future work.

CHAPTER 2
BACKGROUND

This chapter introduces information security management, and tries to make some sense of the alphabetical soup currently best describing the wide flora of standards, frameworks and best practices for information security management (Tomhave, 2005). Furthermore, background information on information classification, and the related security classification and data classification, as well as literature to information classification, is presented.

2.1 INFORMATION SECURITY MANAGEMENT

Traditionally, information security has been viewed as a technical matter (M. Siponen & Oinas-Kukkonen, 2007), where organizational and societal norms were taken for granted, but this is no longer the case (Coles-Kemp, 2009). The socio-technical nature of the field has largely been neglected, however, challenges related to human aspects of information security management has started to attract more attention (Ashenden, 2008), and today, researchers are increasingly interested in understanding information security management (Niemimaa & Niemimaa, 2017).

It is hard to exactly define what information security management is because of the combination of the social and the material within information security (Coles-Kemp, 2009). It is, however, commonly believed that information security needs to be managed in a structured way, and this is normally referred to as Information Security Management (ISM), that can be described as "*[p]rotecting information assets through defining, achieving, maintaining, and improving information security effectively is essential to enable an organization to achieve its objectives, and maintain and enhance its legal compliance and image. These coordinated activities directing the implementation of suitable controls and treating unacceptable information security risks are generally known as elements of information security management* (ISO/IEC 27000, 2014, p. 12). A similar definition comes from OECD "*[s]ecurity management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. […] Information system and network security policies, practices, measures and procedures should be coordinated and integrated to create a coherent system of security"* (Organisation for Economic Co-operation and Development, 2002 p. 12). To reach these objectives, a management system is implemented to get a structured approach. To implement a management system is a common way in other areas as well, such as for quality management (ISO 9000), and environmental management (ISO 14000). In the area of information security, an Information Security Management System (ISMS) can be seen to consist "*of the policies, procedures, guidelines, and associated resources and activities,*

collectively managed by an organization, in the pursuit of protecting its information assets" (ISO/IEC 27000, 2014, p. 13).

Without ISMS, there is a possibility that the security controls are not working together or that some aspects of information security are left out. One of the main reasons for choosing to use ISMS is that it tries to take an overall approach to information security so that no aspect is left out or missed in the implementation of information security. Sometimes the term Information Systems Security Management (ISSM) is used synonymously with ISMS, but in this work, the latter term will be used.

2.2 INFORMATION SECURITY MANAGEMENT STANDARDS

Many organizations have implemented a large number of different security controls as a part of their information security work, trying to keep the organization secure. There are currently more than 1000 standards (Department for Business, 2013) in the information security field focusing on different aspects, from technical standards to comprehensive standards covering broader areas of information security, as with, for example, information security management standards.

One example of a well-known and a well-used ISMS is the ISO 27000-series, which among other things offer best-practice recommendations for initiating, implementing and maintaining ISMS. The ISO 27000-series stems from the '90s and the British standard BS7799. The BS7799 standard consisted of two parts, where part one was about best practices for information security management, and ISO/IEC adopted it and released as ISO/IEC 17799, "Information Technology - Code of practice for information security management" (Kokolakis & Lambrinoudakis, 2005). Part two of the BS7799 standards focused on the implementation of ISMS and were adopted as ISO/IEC 27001 "Information Security Management Systems - Requirements" (Kokolakis & Lambrinoudakis, 2005). The ISO/IEC 17799, was renamed and released as ISO/IEC 27002:2005 in 2005 to align with the ISO 27000-series, and updated in 2013 to ISO/IEC 27002:2013. There are more than 20 published standards in the 27000-series, and more are under development. The standards that primarily relate to the work in this thesis are ISO/IEC 27000 (2014), ISO/IEC 27001 (2013), ISO/IEC 27002 (2013), and ISO/IEC 27005 (2013).

Closely related to ISMS in some aspects are the Information Technology Service Management (ITSM) standards, for example, the Information Technology Infrastructure Library (ITIL), Control Objectives for Information and Related Technology (COBIT) and the ISO/IEC 20000 series (IT Service Management and IT Governance). There is, however, a trend towards refining ITSM, and for example, ITIL v2 contained a separate security management publication, whereas ITIL v3 did not, due to the existence of other ISMS standards (Clinch, 2009). Similarly, for COBIT, that takes an overall approach to the processes on an organizational level give references to other standards (such as the ISO/IEC 27000 series) for details (Mataracioglu & Ozkan, 2011).

Another standard that relate to the field is The Open Group Information Security Management Maturity Model (O-ISM3) (The Open Group, 2017). O-ISM3 is compatible with the ISO 27000-series but uses a different approach where O-ISM3 aims at defining and measuring what people do in activities that support security and does not consider a large number of security controls as in ISO/IEC 27001 (The Open Group, 2017).

In the US, the Federal Information Security Management Act of 2002 (FISMA), is a federal law that recognizes the importance of information security to US economic and national security interests (NIST, 2017a). The National Institute for Science and Technology (NIST) provide the details for how to manage information security in a set of standards ranging from

the management perspective to detailed descriptions of security controls for specific standards. According to FISMA. There is a large overlap between FISMA and ISO 27000, but FISMA can be considered more encompassing in total (Gikas, 2010).

ISMS is a mandatory activity for many organizations due to legal regulations, for instance, in Japan, ISO/IEC 27001 is mandated for many government contracts (Gillies, 2011), in the US, all federal agencies, and all contractors and others sources need to adhere to FISMA (Gikas, 2010), and in Sweden all government agencies (MSBFS 2016:1, 2016).

2.3 INFORMATION CLASSIFICATION

In ISMS, asset management is a central activity since it establishes ownership of all organizational assets. The assets are identified by doing an inventory of all assets such as software, physical assets (for example, computers, and network equipment), services (for example, heating, lightning, power, and air-condition), people and their skills and experience, intangibles such as the reputation and image of the organization, and the information in the organization (ISO/IEC 27002, 2013). The information can be found in many places in the organization, and take different shapes. After the inventory, ownership or responsibility is designated to all assets and guidelines are set up for acceptable use of the assets. Based on how important the asset is in terms of business value or security classification, levels of protection need to be identified (ISO/IEC 27002, 2013). The information identified as an asset should be classified according to its value, and criticality to the organization. Normally, a classification scheme uses categories in a hierarchical model, where each category is associated with procedures for how to handle the information, and what protection mechanisms, it requires. An organization should not use too many classification categories as complex schemes may become harder and uneconomic to use (ISO/IEC 27002, 2013), and a typical organization might have between three and five categories in a hierarchy (Axelrod et al., 2009).

The information classification can change over time, for example; an annual report from a stock market company contains very sensitive information before it is published, but the information classification changes at the point of publication. When the information classification is changed, a reclassification is performed. It is important that the classification is up-to-date, otherwise, the information might be under- or overprotected. If the information is overprotected, it can lead to higher costs since more security controls are needed. There are also other consequences with overclassification of information, such as unintended operational consequences that are hindering people from doing their job when metadata is used to label information that in turn hinders them from accessing the information (Everett, 2011), or when information is overclassified to protect the asset owners (L. P. Taylor, 2013). Underclassification, on the other hand, means that the information is not as protected as it should be and that it is more exposed than it should.

The input to information classification is information, but there are different approaches to both how to identify the information assets, and on what granularity the information should be evaluated. The granularity of classification is debated, but a lower level, e.g., every file or even sentences in a text document, can enable access to information (Alqudah & Nair, 2011; Burnap & Hilton, 2009), but grouping information types or categories of information decreases the amount of classification (Fibikova & Müller, 2011; ISO/IEC 27002, 2013). Generally, it is also easier to protect for instance an entire database if all the information in it have the same classification (Blyth & Kovacich, 2006), and to set access controls that match the classification.

Contrary to look with high granularity at the information, other approaches are to classify networks (Collette, 2006), business processes or applications (Fibikova & Müller, 2011). These approaches are similar and consider bigger chunks of information and take a stance

from the highest information value that is included in, e.g., a system, and consequently, protect the system based on the highest level found. These approaches primarily classify according to information in a process or applications/systems have some advantages as it can be done more rarely, and as a collaborative task bringing in more specialist competencies. The drawbacks are that some information might be overclassified as all information in the process/application/system will inherent the highest classification from the identified information types. This approach of using a higher granularity has been used successfully in most Swedish governmental agencies, as well as in private organizations, e.g., Daimler Financial Services (Fibikova & Müller, 2011).

2.4 SECURITY AND DATA CLASSIFICATION

Information classification is sometimes referred to as security classification or data classification, and these concepts are sometimes treated as overlapping or separated in literature depending on context. They could also cater to different types of information. The concepts are also used synonymously in some literature, for example, in Montesino and Fenz (2011). Several claim that the concepts are variable and sometimes uninformative. An attempt trying to define a new definition has been made by Collard, Ducroquet, Disson, and Talens (2017). The same authors also claim that COBIT is the only standard speaking about data classification, and that it is unclear if COBIT consider the additional value found through information (Collard et al., 2017). Searches for the term data classification also give many false positives (Bergström & Åhlfeldt, 2014) as it is used to describe other types of classification than information classification. There are however a great number of papers describing data classification as information classification, e.g. Collette (2006), Everett (2011), Glynn (2011), and Photopoulos (2008), and the terms have been treated as synonymous in this work.

Information, data and security classification aims at protecting information against security breaches, but generally, security classification refers to information where a loss affects the national security. Security classification is also referred to as classified information, and most countries in the world have developed classification schemes for handling information related to national security (Kaarst-Brown & Thompson, 2015). Wikipedia (2017) provides an impressive list with the equivalent of classification markings for more than 100 countries.

Security classification relates more to the classification of information with a low granularity as discussed in Chapter 2.3, but more critical information, requiring more extreme handling routines and security controls. The approach to security classification as well differs as it is more seen as a one-man-show (Axelrod et al., 2009). Furthermore, there is more focus on the confidentiality aspect in security classification (Gantz & Philpott, 2013), and, e.g., integrity and availability are handled ancillary. With high-level granularity for confidentiality, it is hard to imagine how, for instance, high-level availability requirements are implemented on the same system or application.

From a security control perspective, security classifications are more likely to include a mapping between how confidential the information is and how it should be protected. This is evident by looking at, e.g., national laws regulating how information should be protected, e.g., via FISMA in the US, where classification is done in accordance with FIPS Publication 199 (National Institute of Standards and Technology, 2004). Then security controls are applied in accordance with FIPS Publication 200 (National Institute of Standards and Technology, 2006), and NIST Special Publication 800-53 (National Institute of Standards and Technology, 2015). In Sweden, the security act refers to both information classification, and security classification, where the security classification for higher levels of confidentiality has a direct mapping to security controls (SOU 2015:25, 2015).

In this work, the theoretical foundation draws from security classification, data classification and information classification, because we want to propose a method which is applicable to

any kind of organisation, but the term information classification will be used throughout the work, and hence, data classification and security classification can be seen as included in the broader term information classification.

2.5 INFORMATION CLASSIFICATION PRACTICE

ISMS themselves are based on best practices (Niemimaa & Niemimaa, 2017), and organizations face institutional pressures to adopt such practices (Hsu et al., 2012). This pressure to comply comes from e.g., legislation or to meet the constantly evolving threats facing organizations as discussed earlier. However, turning standards into practice is easier said than done, and many scholars have recognized a gap between formal and actual processes in information security management (Njenga & Brown, 2012; Shedden, Smith, & Ahmad, 2010; M. Siponen, 2006; R. G. Taylor & Brice, 2012). Nevertheless, the gap between standard, and practice in the area of information classification has not attracted much attention from scholars. One notable work is from Niemimaa and Niemimaa (2017), that studied the translation from ISS best practice on information classification into a local policy and how that was turned into practice at an organization. This study found that the ISS best practice prescriptions were insufficient for local action and that they offered a plan that fell short because of the complexity of actual organizational life (Niemimaa & Niemimaa, 2017). One aspect of this is the general lack of information classification competence among employees in organizations, and the increased need of it is seen as one of the future trends in a study by Åhlfeldt et al. (2015).

Most scholarly literature in the area has focused on security classification, and research on classification used by other organizations than the ones handling information critical to national security is virtually non-existent (Thompson & Kaarst-Brown, 2005). This was also the conclusion of a study trying to identify information classification practices online (Mikkelinen, 2015).

Information classification is a mandatory activity for government agencies in many countries, such as in the UK (Cabinet Office, 2013), Australia (Australian Government, 2014), and Sweden (MSBFS 2016:1, 2016). Furthermore, it is well-established in the private sector due to legal requirements, e.g., for protecting personally identifiable information (Raman et al., 2014), or to be eligible to be a sub-contractor to the government (Cabinet Office, 2013). A survey into cybersecurity breaches with more than 1000 respondents in the UK revealed that 58% of all large firms, and 46% of firms overall covered classification in their security policies (Department for Culture, 2016), but it is unclear how many of these firms, in reality, has turned their policy into practice. The classification practice in Swedish public sector has also been investigated, and in 2014, 43% of the government agencies used information classification, and another 24% were working on implementing it (Swedish Civil Contingencies Agency, 2014). A similar result was presented in a study by Bergström, Åhlfeldt, and Anteryd (2016), where 57% of the government agencies replied that they were using information classification. In Swedish municipalities, the situation is dire, and in 2015, only 75 of 241 municipalities that answered an information security survey (there are 290 municipalities in total) used information classification, but of those 75 municipalities, only 10 did it on a regular basis (Swedish Civil Contingencies Agency, 2015). The survey also showed varying responsibility for who is responsible for the classifications, and that 58% of the municipalities did not use a method for information classification (Swedish Civil Contingencies Agency, 2015).

CHAPTER 3
METHOD THEORY

The theoretical foundation of this thesis is built on the concept of method, and this chapter describes the method concept and methods in ISS. Information Systems is an area where there has been an ongoing discussion of the definition for years (G. Dhillon, 2007), add security, and it becomes worse. One including a way of viewing the ISS concept is to secure on three levels that continuously interact: the technical, formal and informal (G. Dhillon, 2007). The technical level consists of, e.g., the hardware, software and network infrastructure; the formal level consists of, e.g., policies, standards, and procedures that are driven by the informal level that consists of, e.g., awareness, beliefs and culture (Åhlfeldt et al., 2007).

There are many terms related to ISS, such as, IT security, ICT security, information security, and computer security that are used more or less synonymously, but throughout this thesis, ISS is used as it clearly includes the organizational aspects of information security.

3.1 METHOD CONCEPT

Methods are widely debated concepts in the area of Information Systems Development (ISD) (Cronholm & Ågerfalk, 1999), and many scholars have tried to define the concept of method (Brinkkemper, 1996; Checkland, 1981; Goldkuhl, Lind, & Seigerroth, 1998). The method concept in the area of ISS is not clearly defined or elaborated, and concepts such as framework, model, process, and approach are used as synonyms for an ISS method (Kolkowska, 2013). Methods in the ISS field are underdeveloped compared to the IS field (M. Siponen et al., 2008), and here, we adopt the same reasoning as in Kolkowska (2013), where the similarities between the IS and ISS fields are embraced, as methods in IS support the design and development of an IS, and methods in ISS support the design and development of an ISS.

Much confusion can be generated when mixing the use of the terms method and methodology, and the IS literature contains many examples of this (Wynekoop & Russo, 1995). In an IS context in Europe, the term method is used to describe a systematic procedure of conducting systems development, and methodology refers to the study of methods, whereas in North America, the term methodology is used as the term methods in Europe (Iivari, Hirschheim, & Klein, 2000). In this thesis, the term method is used the European way, i.e., method refers to the outcome developed in this thesis, and methodology refers to the research approach used to develop the method.

When analyzing descriptions of what a method is, there is a reoccurring pattern of similar elements in them. To exemplify, the following method definition from Jayaratna (1994) states that method is *"an explicit way of structuring one's thinking and actions. Methodologies contain model(s) and reflect particular perspectives of 'reality', based on a set of philosophical paradigms. A methodology should tell you 'what' steps to take and 'how' to perform those steps but most importantly the reasons 'why' those steps should be taken, in a particular order"* (as cited in Cronholm and Ågerfalk (1999)). Fitzgerald, Russo, and Stolterman (2002) describe method as a *"coherent and systematic approach, based on a particular philosophy of systems development, which will guide developers on what steps to take, how these steps should be performed and why these steps are important in the development of an information system"*.

Although the method concept is used slightly different, some components of what a method should constitute emerge. First, there must be a set of procedures to perform, that is explicit, coherent and systematic. Secondly, there is a philosophy or perspective that represent the method's rationale. Finally, a method includes models or means of representing the method. In other words, a method should be able to answer the "how", "why", and "what". A method should have a prescriptive character that explains what to do in different situations to arrive at certain goals (Goldkuhl et al., 1998).

A method can be seen as a "whole" consisting of different "parts" (Cronholm & Ågerfalk, 1999). "Whole" is a monolithic view where the method is integrated and dependable, and the antipole of this is "parts" or "fragments" that are independent and separated from each other (Röstlinger & Goldkuhl, 1994). Many times, neither is preferable, and combination between the two is preferred. This is referred to as "method components" (Röstlinger & Goldkuhl, 1994). The "method components" should be component-based, separated, adaptable, modifiable, combinable, exchangeable and reusable (Röstlinger & Goldkuhl, 1994). A method component can be seen as a self-contained part of a method expressing how to transform one or several inputs into a defined output. This modular view of method means that these components can be exchanged for other components that produce the same type of result. This view also makes it tailorable and flexible, i.e., possible to fit different situations (Karlsson & Ågerfalk, 2009).

Drawing from this, we align with the method definition put forward by Goldkuhl et al. (1998), where a method is organized as a set of method components, that includes the parts *procedure*, *notation*, and *concepts*. The *procedures* describe how to work, i.e., meta concepts such as processes, activities, and information flow. The *notation* is the representational guidelines, semantics, and syntax. The procedure and notation are tightly coupled, and *concepts* could be seen as the overlapping parts of procedure and notation (Goldkuhl et al., 1998). The method components that can be seen as activities that put together is a *framework*. The *co-operation forms* refer to the people involved and their roles. The *perspective* is the conceptual and value basis of the method and can be implicitly or explicitly expressed in the method (Goldkuhl et al., 1998). Figure 3.1 illustrates the relationship between the parts of the method.

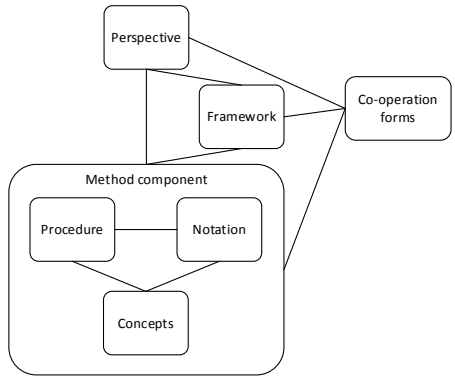

Figure 3.1: Relationship between method component, perspective, framework and co-operation forms. Adapted from (Goldkuhl et al., 1998).

3.2 METHOD REQUIREMENTS

As the aim of this thesis is to devise a method for information classification, and taking into consideration the method concept discussion in chapter 3.1, a number of method requirements have been defined to outline what needs to be included in a method.

The method requirements are:

MR1. The information classification method needs to include a set of procedures, concepts, and notations to solve and document that solves defined tasks of information classification.
MR2. The information classification method needs to be based on method components to make it tailorable to different situations.
MR3. The information classification method needs to include a suitable framework that structure and guides the performance of method components.
MR4. The information classification method needs to include a set of roles and how these roles are to interact.
MR5. The information classification method needs to include an explicit perspective that guides the information classification work.

MR1 is motivated by the shared understanding (Brinkkemper, 1996; Checkland, 1981; Goldkuhl et al., 1998) that a method consists of three interrelated parts, the procedures, concepts, and notation. The procedures to perform in information classification can be, e.g., the identification of internal or legal requirements. The concepts relate to important aspects of the problem domain, such as confidentiality, integrity and availability, and the information assets. Notation refers to the need to express the method for information classification using representational guidelines, semantics, and syntax.

MR2 draws from Goldkuhl et al. (1998), that a method consists of method components with defined inputs and outputs, and from Karlsson and Ågerfalk (2009) that these components make the method possible to fit different situations, i.e., tailorable and flexible. For information classification, this takes form, e.g., in labeling that could be implemented very differently depending on what type of information it is or how it is stored or transmitted. Furthermore, the identification of systems or processes can differ significantly in different organizations, and the method needs to account for this kind of requirements.

MR3 focuses on the framework as put forward by Goldkuhl et al. (1998). The role of the framework is to structure and guide the performance of method components, and how they relate to each other. An example is that the identification and classification could be seen as both iterative and using a waterfall model.

MR4 is derived from the co-operation forms as described by Goldkuhl et al. (1998). In an information classification context, this means that the people involved in the identification of information assets and the classification of them.

MR5 addresses the perspective as put forward by Goldkuhl et al. (1998), which is how the method designer views the problem domain. The perspective provides the rationale for each method component. This also aligns with Brinkkemper (1996) that stated that each method is grounded in the way of thinking, making a method a normative construction. In this context, an example is that the method for information classification needs to reflect the practice.

3.3 INFORMATION CLASSIFICATION METHODS

There are several established standards and frameworks describing information classification, for example, COBIT 5, ISO/IEC 27001:2013, ISA 62443-2-1:2009, and NIST SP 800-53 Rev. 4 (NIST, 2017b). Additionally, there are guidelines or supporting documentation to aid the implementation of information classification available from, e.g., Andersson et al. (2011), and Cabinet Office (2013). In this chapter, the standards and guidelines are analyzed from the perspective of the method requirements outlined in chapter 3.2.

3.3.1 ISO/IEC 27002

The ISO/IEC 27001 (2013) describes the requirement of implementing information classification, and the ISO/IEC 27002 (2013) standard provides a two pages description on the implementation of information classification. Looking from the perspective of MR1, the standard does provide a set of procedures and concepts guiding the implementation, but the process provided is briefly described.

From the perspective of MR2, the description in the standard provides some guidance as it separates information classification, labeling, and handling of assets in separate chapters. It also states that it should be consistent across the whole organization and its processes. In the classification scheme, the recommendation is to consider CIA, and any other requirement considered for the information. Also, an example of a classification scheme in four levels for confidentiality is given.

In relation to MR3, there is a mention of a life-cycle, and that the classification results should be updated in accordance with changes in the value, sensitivity, and criticality. Additionally, there should be criteria for review of the classification over time, and there is an emphasis on this as otherwise, information will be under- or over-protected, but no details are given on how this is achieved. Furthermore, when looking at the components, an appropriate set of procedures for labeling and handling should be provided. Finally, the standard describes taking business needs and as well as legal requirements into account.

For MR4, ISO/IEC 27002 gives recommendations that the information asset should be accountable and that the classification should give people who deal with information guidance on how to protect it, i.e., handling guidelines.

There is a clear organizational perspective matching MR5, and a description of what will happen if classification is not implemented correctly. Furthermore, there is a rationale for labeling and handling, and also for classification where it is suggested to group information with similar protection needs to reduce the need for case-by-case risk analysis and custom design of security controls.

Combined, it can be said that ISO/IEC 27002 balances between giving concrete advice on how to implement information classification, and still stay on a general level to be applicable for all.

3.3.2 COBIT 5

Control Objectives for Information and Related Technologies (COBIT) is a framework for IT government and governance created by ISACA (formerly Information Systems Audit and Control Association). COBIT is generally described on a higher level than, e.g., ISO/IEC 27001 (Mataracioglu & Ozkan, 2011), and the framework itself also reference standards in association to its own descriptions (e.g., from ISO/IEC 27001 and ITIL). COBIT labels information classification as data classification.

COBIT uses a process-oriented approach, and a starting point is to define information and system ownership (ISACA, 2012). The outputs are data classification guidelines, data security and control guidelines, and data integrity procedures, i.e., the focus is more on the ISM process. For aiding the actual implementation of COBIT, one can turn to, e.g., Etges and McNeil (2006), that outlines the process and the requirements for classification. The ownership can be done in a business impact analysis, where the most critical information is identified primarily, but subsequently, all information in the organization is identified.

From the perspective of MR1, COBIT does not provide a graphical overview of the classification process, but Etges and McNeil (2006) provide an overview, as shown in Figure 3.2.

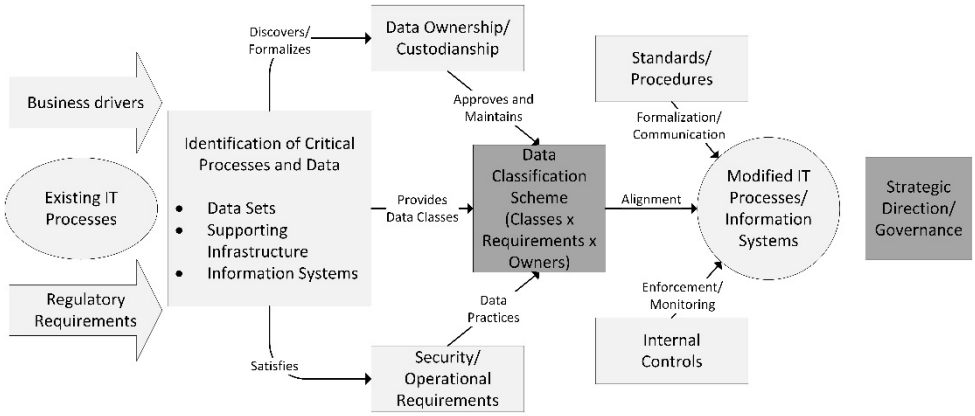

Figure 3.2: The data classification process, redrawn from Etges and McNeil (2006).

MR1 is partly satisfied by the process overview and descriptions provided by Etges and McNeil (2006), but a detailed explanation of the process is not provided. Furthermore, it is unclear how the data classification scheme activity is applied in practice. Also, by looking at Figure 3.1, after the classification scheme is used, processes or information systems are modified with input from internal controls and standards/procedures. In ISO/IEC 27000, this would imply that security controls are adopted, which is the step after the risk analysis, and not a part of information classification. The process is built around a number of requirements related to e.g. access and authentication, ownership, confidentiality, integrity, privacy, availability, auditability and data retention. In COBIT, the risks are considered more as a part of e.g. access and authentication, and what needs to be considered in terms of security controls. ISACA (2012) outlines four activities: (1) provide policies and guidelines for classification, (2) define, maintain and provide appropriate tools, techniques and guidelines to provide effective security and controls over information and information

systems in collaboration with the owner, (3) create and maintain an inventory of information including a listing of owners, custodians and classifications, (4) define and implement procedures to ensure the integrity and consistency of all information stored in electronic form.

MR2 is about how tailorable the method is, but with the high-level description of the process, that outlines what could be seen as components, it could be said that it is tailorable, but how tailorable it is in practice is unclear.

MR3: As COBIT is described on a higher level, much specifics are left out, but still in some aspects more detailed descriptions than in e.g. ISO/27002 are provided. In the activity where information is identified, the recommendations include to consider *"content types (procedures, processes, structures, concepts, policies, rules, facts, classifications), artefacts (documents, records, video, voice), and structured and unstructured information (experts, social media, email, voice mail, RSS feeds)"* (ISACA, 2012 pp. 160). Furthermore, the actual classification should be based on a content classification scheme, and sources of information should be mapped to the classification scheme. The information sources should be collected, collated and validated based on information validation criteria (e.g., understandability, relevance, importance, integrity, accuracy, consistency, confidentiality, currency and reliability).

MR4 targets the roles involved in classification, and in COBIT, the ownership role is important, as the owner is responsible for the classification. Etges and McNeil (2006) also mentions that the data is stored in systems that are complex and managed by an IT department, that also implement security controls to protect the information. The gap between the business side, and the IT department is normally bridged by the Chief Security Officer (CSO), but Etges and McNeil (2006) point out that the CSO is not responsible. ISACA (2012) outlines stakeholders in relation to information in general, and classifies in three groups: information producers, information custodians, and information consumers.

MR5 also has a relation in COBIT, and it is suggested that all information should be classified, and the classification should be performed with enterprise-wide consistency.

3.3.3 FIPS PUBLICATION 199

The Standards for Security Categorization of Federal Information and Information Systems (National Institute of Standards and Technology, 2004) might be included later on for the final version of the thesis.

3.3.4 METHOD SUPPORT FROM MSB

The Swedish Civil Contingencies Agency (MSB) publishes a method support that covers all aspects of ISMS from preparation, implementation to continual improvement. It is developed to complement the ISO/IEC 27000 series of standards with explanations on how to implement it in practice (Swedish Civil Contingencies Agency, 2016).

On a general level, the documentation describes three activities in information classification: to identify information assets, to identify requirements, and to classify information. An overview of this process can be seen in Figure 3.3.

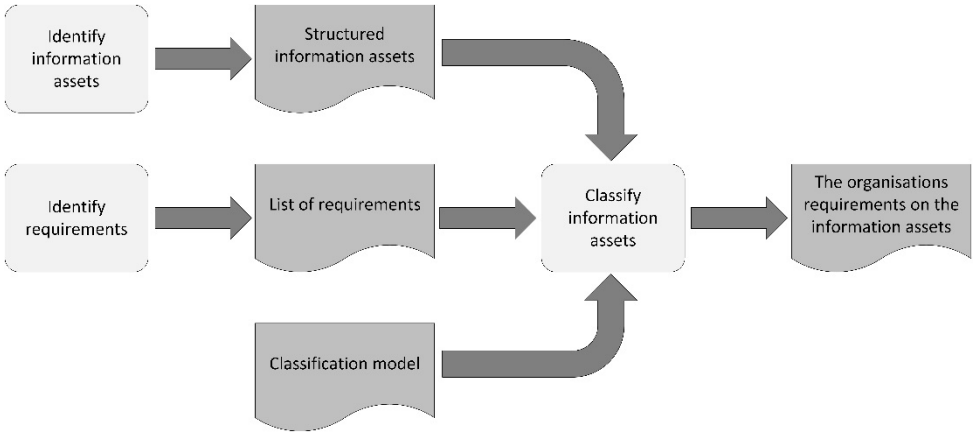

Figure 3.3: Flow model of business analysis, adapted from Andersson et al. (2011).

Looking from the perspective of MR1, there is a set of procedures, concepts, and notations as a starting point. Also, an appendix is included in the document, that gives a template for how to structure the information assets. This template includes a description of the information asset, a date for when the classification was performed, and who is the system/information owner. Furthermore, the participants (name, role, and contact information) in the classification is mentioned together with a free-text-boxes for filling in a description of the information asset, IT support, and limitations.

The method is based on activities that can be seen as components as described by MR2, but it is hard to judge how tailorable they are.

From the perspective of MR3, there is also guidance on the structure, and it is described as the identification of information assets, and the identification of requirements can be made in parallel. Both these tasks produce an output, which is fed together with the classification model into the actual classification of information. Furthermore, the activities can be seen as components.

For MR4, little is mentioned, but it is recommended not to be more than ten persons at the classification, otherwise, it is hard to handle the discussions. Also, it is mentioned that lawyers in the organization can help out with the identification of legal requirements.

Regarding MR5, there is a clear focus on taking business processes as a starting point, and thereby, identify information assets in these business processes.

3.3.5 GOVERNMENT SECURITY CLASSIFICATIONS

GSC (Cabinet Office, 2013) describes how the classification in the UK is implemented. This might be included later on for the final version of the thesis.

Furthermore, a comparison between the methods for information classification will be included in a more comprehensible format such as e.g. a table for the final version of the thesis.

CHAPTER 4
RESEARCH DESIGN

This chapter presents the research design, which is the research approach, and the research methods used. Furthermore, it introduces the overall research paradigm adopted in this thesis project.

4.1 RESEARCH APPROACH

As the IS field shows a great diversity in the problems addressed, the theoretical foundations, and the methods to collect, analyze and interpret data (Benbasat & Weber, 1996), the different underlying philosophical paradigms are important to convey (Oates, 2006). To better explain the decisions on why, how and what has been performed in this thesis, it is also important to introduce some of the underlying philosophical stances in order to clarify why some choices have been made.

A research paradigm can be seen as *"the set of activities a research community considers appropriate to the production of understanding (knowledge) in its research methods or techniques"* (Hevner & Chatterjee, 2010, p. 7). A research paradigm can be seen to consist of the following components: *ontology*, *epistemology*, *methodology*, and *method*s (Scotland, 2012). Ontology, or the way in which the world is viewed, and the epistemology, which is the ways in which knowledge can be acquired from differs in the IS field (Oates, 2006). In the multi-paradigmatic IS field (Vaishnavi & Kuechler, 2004), the traditional paradigm has been positivism (Oates, 2006; G. Walsham, 1995), but interpretative research is a well-established strand in the field (G. Walsham, 2006). In the ISS field the situation is similar, and until the end of the 1990s, the majority of ISS research was from a positivist perspective (Gurpreet Dhillon & Backhouse, 2001). However, the technical orientation in the majority of traditional ISS methods leads to solutions being implemented in organizations that are neither adapted nor accepted, and therefore, there is a need to increase practitioners' and researchers' understanding of the fundamentals of ISS (M. T. Siponen, 2005). Hence, there is a call for more interpretative studies in the ISS field (McFadzean, Ezingeard, & Birchall; M. T. Siponen, 2005).

Interpretative research is focused on understanding a phenomenon by including the individual's perspective, to investigate the interaction among individuals and the historical and cultural contexts (Creswell, 2009). Interpretivism can be seen to bring into consciousness hidden social forces and structures (Scotland, 2012). An interpretative approach to ISS offers advantages as it can bring a holistic view into the problem domain *"especially within the*

scope of networked organizational forms, instead of the simplistic, one-dimensional, explanation, more suitable for hierarchically structured organizations" (Gurpreet Dhillon & Backhouse, 2001).

The *methodology* adopted is the Design Science Research (DSR) methodology (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007). Design is central in DSR to develop an artifact, something the IS field is increasingly concerned with (S. D. Gregor & Jones, 2007). Several scholars including Orlikowski and Iacono (2001), and Benbasat and Zmud (2003) argue that historically, too little research has focused on artifacts, its effects, context, and capabilities. The term artifact describes something artificial that is constructed by humans, and as something not occurring naturally (Simon, 1996). In the context of DSR, artifacts can be constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems) (Alan R. Hevner, Salvatore T. March, Jinsoo Park, & Sudha Ram, 2004; March & Smith, 1995; Oates, 2006). Furthermore, DSR creates and evaluates artifacts that are "*intended to solve identified organizational problems*" (Alan R. Hevner et al., 2004 p. 77), which information classification is a clear example of according to, e.g., Niemimaa and Niemimaa (2017).

The research process was structured according to the DSR process model put forward by Peffers et al. (2007). There are several similar notable DSR alternatives within IS and engineering (e.g. A. R Hevner, S T March, J Park, & S Ram, 2004; Nunamaker, Chen, & Purdin, 1991; Takeda, Veerkamp, Tomiyama, & Yoshikawam, 1990; J G Walls, G R Widmeyer, & O A El Sawy, 1992). Peffers et al. (2007) was chosen because the approach is consistent with DSR processes suggested in earlier DSR papers within information systems and engineering, and because the phases included in the model are well described.

In the context of DSR, it can be noted that DSR also can be seen as its own research paradigm (S. Gregor & Hevner, 2013; Alan R. Hevner et al., 2004). Another example is Vaishnavi and Kuechler (2004) that contrasts positivist and interpretative to *design*. Oates (2006) contrasts positivist, interpretative and critical realism, but argues that all three paradigms can use design science as a methodology.

A number of research *methods*, which can be seen as the specific techniques for how the data is collected and analyzed have been adopted in order to reach the aim and objectives. In interpretative research, there is often a strong connection to qualitative data collection and qualitative data analysis (Oates, 2006). Therefore, in each of the DSR cycles, research methods reflecting the interpretative approach were adopted. Scotland (2012) argues that it implies that there is a need for research methods that yield insight and understanding of behavior, that can help to explain actions from the participant's perspective, and which do not dominate the participants. Therefore, suitable qualitative methods include, e.g., open-ended interviews, open-ended questionnaires, and open-ended observations. An overview of the adopted research methods in the respective DSR cycles can be seen as an overview in Table 4.1.

4.2 DESIGN SCIENCE RESEARCH

As mentioned previously, the methodology adopted for this thesis is DSR as described by Peffers et al. (2007). According to the model by Peffers et al. (2007), each DSR cycle contains six phases: (1) problem identification and motivation, (2) define the objectives for a solution, (3) design and development, (4) demonstration, (5) evaluation, and (6) communication.

4.2.1 DSR THEORY

There are different views on theory in the IS field, but one way of viewing it is to follow the classification of theories from S. D. Gregor and Jones (2007), that identifies five interrelated

types of theories: (1) theory for analyzing, (2) theory for explaining, (3) theory for predicting, (4) theory for explaining and predicting, and (5) theory for design and action. All types inform the theory for design and action, but the theory for explaining and predicting and the theory for design and action have the strongest relationship. This strong relationship exists because "*[k]nowledge of people and information technology capabilities informs the design and development of new information systems artefacts*" (S. D. Gregor & Jones, 2007 p. 629). In practice, this knowledge and capabilities serve as input to the design process, otherwise, it is implied that design is a random process (Kuechler & Vaishnavi, 2012). In design theory, where an artifact is constructed, two intertwined aspects are in focus, the development process knowledge and what the artifact should look like when built, i.e., the design principles (S. Gregor, 2002). Kuechler and Vaishnavi (2012) emphasize the importance that the process of developing the artifact is informed by either practice-based insight or theory. Similarly, it is put by Sarker and Lee (2002), that the theory behind a design theory should be academic theory or practitioner theory-in-use.

Hence, it is important that the method developed is informed by theory. Method itself is a complicated topic as explicated in Chapter 3.1 and 3.2, and the very design of a method needs to adhere to theory, hence the MR. To address the MR, design principles (DP) have been developed. These DP are based on existing knowledge within the ISS field or empiric experiences. As the method devised is for information classification, it needs to be informed by the field. Here, the standards such as ISO/IEC 27002, and frameworks like COBIT are seen as kernel theories (as in, e.g., Shrestha (2015)). The methods used to collect data in the DSR cycles also reflect the collection of practice-based insight, e.g., by observations or interviews, and in turn, informs the DP. Some of the work that is yet to be performed will be based on practice theory (see Chapter 5.3), and stakeholder theory (see Chapter 5.4).

The DPs have been formulated at different points in time, as results of following the DSR methodology. Below is a list of DP identified so far, but for motivations on why, and when they were formulated, see Chapter 5.

- DP1. The method for information classification should be compatible with ISO/IEC 27002 information classification code of practice.
- DP2. The starting point for the information classification method should be a process or system/application.
- DP3. The process in the information classification method should be described using a well-known and accepted notation.
- DP4. The information classification method should describe how the output of an information classification should be documented in a structured way.
- DP5. The information classification method should be empirically grounded to not deviate too far from established practices.
- DP6. The information classification method should have identified stakeholders to give usage views for information classification stakeholders.
- DP7. The information classification method should be constructed using components and be flexible to fit different organizational needs.
  - DP7.1. The method components should be compatible with ISO/IEC 27002 information classification code of practice.

4.2.2 METHODOLOGICAL CONSIDERATIONS

Initially, when the thesis project started, the intended research path was to perform one soft case study as described by Geoff Walsham (1993) and follow this up with four action case studies at a Swedish County Council (SCC) targeting different aspects of information classification. One of the action cases was expected to focus on developing a conceptual model of the information classification process. This plan was dropped when the focus

changed to a broader perspective and when the decision was taken to focus on the development of an artifact, the information classification method.

When the objective is to build an artifact, Action Research (AR) is a clear alternative methodology to DSR. AR is an established methodology (see, e.g., Baskerville (1999); Checkland and Holwell (1998)) in the IS field. There are elements in the AR methodology that clearly follow a similar path as DSR, e.g., there is a focus on practical issues, it follows an interactive approach, there are multiple data generation methods, and collaboration with practitioners (Oates, 2006). Furthermore, AR and DSR share some of the same advantages and disadvantages (see chapter 4.2.3 for more details).

The main reason for adopting DSR instead of AR is that AR has more emphasis on change, and requires close collaboration with practitioners. Throughout the thesis project, there has not been one organization in focus, but rather a mix of actors on different levels. At the beginning of the thesis project, the plan was to work closely to SCC, develop a method, and follow the implementation of it using AR. This plan was however abandoned fairly quickly, both because it could be harder to argue generalization of the results, and because the time plan of the thesis deviated from the SCCs time plan. Furthermore, when the thesis work started, more organizations showed interest in participating to varying degrees, which led to a decision to generalize the project, include more actors and to use DSR. Other key reasons why not to use AR was that the formulation of the objectives of the thesis, and the design and development were performed without the involvement of external actors. Rather organizations performed action regarding giving input to issues regarding information classification, demonstration, and evaluation in the DSR cycles.

4.2.3 DSR CRITIQUE

This chapter will introduce some of the issues with DSR raised in, e.g., Oates (2006) in the final version.

4.2.4 RESEARCH CONTEXT

The context in which this project has been carried out is primarily in the public sector. The public sector is organized differently in various countries and offer different services. In Sweden, where most of the work for this thesis has been carried out, the public sector is rather big and influential, and is primarily organized in government agencies, county councils, and municipalities. To cover as many facets as possible on practice, a broad approach has been selected, and input from a national level, from government agencies, from county councils, municipalities, and private organizations have been included in the work at different points.

Sweden differs from most other countries in how government agencies are organized. The ministries (or governmental departments) are headed by a minister and are divided into governmental agencies (or bureaus or offices) that handle a specific sector of public administration. The difference is that in Sweden, the governmental agencies are not a part of a department like most other countries. Ministers in Sweden are not allowed to decide on activities in the government agencies directly, so this kind of decisions must be made by the government. In practice, this entails a larger degree of autonomy for government agencies, with a lesser degree of central control. This has practical implications, e.g., ISM as it is recommended that all government agencies follow ISO/IEC 27001, and ISO/IEC 27002, and implement information classification (MSBFS 2016:1, 2016), but not exactly how to do so. In other words, it is up to the individual government agency to select their own approach including the classification scheme. This has led to proliferation, and many agencies have developed their own practice based on ISO/IEC 27002. In combination with the principle of

public access to official records, Swedish government agencies make good study objects as access to their underlying guidelines should be publicly available upon request.

There are currently 442 government agencies divided into six categories (Statistics Sweden, 2017), but of which 238 were included in this work. The excluded government agencies are primarily embassies and consulates abroad (107), Swedish general courts, general administrative courts and special courts (e.g., labor court, migration court, and the court of patent appeals) (84), and the National Pension Funds (6). The included government agencies (sv. förvaltningsmyndigheter) represents a wide range of functions for the society, including the Swedish Armed Forces, Swedish Economic Crime Authority, the Swedish Tax Agency, the Swedish Police, the Swedish Civil Contingencies Agency, the Swedish Pensions Agency, and the Swedish Transport Administration. Many of the included government agencies handle systems and information that are critical to society, but most of them handle little information that could be expected to cause exceptionally grave damage to national interests (compare to Top Secret in the previously discussed security classifications).

The government agencies provide services on a national level within specifically defined areas that are defined by the Government of Sweden through 8 ministries. Information security is primarily handled by the Ministry of Justice that is principal for the Swedish Civil Contingencies Agency (MSB, Myndigheten för Samhällsskydd och Beredskap in Swedish). MSB is responsible for issues concerning, e.g., public safety, emergency management and civil defense when no other agency or authority has a responsibility, before, during and after emergencies or crisis's (Swedish Civil Contingencies Agency, 2017a). One of MSB:s responsibilities is to support and coordinate the societal work on information, and cybersecurity through the Office of Cybersecurity and Critical Infrastructure Protection (Swedish Civil Contingencies Agency, 2017b). One section in this office is the Information Security Governance Section that supports governmental agencies, municipalities, county councils, and private organizations with advice, aid in risk and threat analyses, and maintain support documentation for aiding the implementation of ISMS (Swedish Civil Contingencies Agency, 2017b). Since MSB is in charge of these tasks, they have a national perspective on ISMS implementation and thereby, influence information classification practices in Swedish organizations. There are other government agencies involved in developing practices related to classification, but primarily, to security classification, i.e. the different branches related to the Ministry of Defence (e.g., the Swedish Armed Forces, the National Defence Radio Establishment, and the Swedish Defence Materiel Administration). In their context, they are more likely to handle top secret information that could damage Sweden, and thus fall under other laws, such as the Security Act (SOU 2015:25, 2015). Their ideas and practices are however, included in the study as they are government agencies (included in the previously mentioned 238 government agencies).

There are 20 self-governing local authorities called county councils in Sweden. The county council studied in this thesis is referred to as Swedish County Council (SCC), and is among the largest in Sweden with over 50.000 employees distributed over many municipalities. County councils in Sweden have three main tasks, to provide public healthcare, public transport and to promote regional development regarding providing culture and increasing growth. In order to do so, the counties needs to provide a wide array of IT services to a heterogeneous group of users. With a centralized IT organization handling tens of thousands of PCs and servers, it is a challenging environment to implement ISMS. Furthermore, the healthcare sector is interesting from an information security perspective, as more and more cybercriminals are targeting higher-value records such as health-related personally identifiable information (IBM Security, 2016), which affect the county councils.

There are 290 municipalities in Sweden, and three municipalities are preliminary included in this work. The municipalities are responsible for providing, e.g., childcare, primary and secondary schools, elderly care and emergency services (excluding police). Like with SCC,

services have to be provided to a heterogeneous group of users. All municipalities, and county councils belong to the Swedish Association of Local Authorities and Regions (SKL), which have developed a tool for aiding information classification. In 2015, 58% of all municipalities lacked a method for information classification (Swedish Civil Contingencies Agency, 2015).

4.2.5 DSR CYCLES IN THIS THESIS

The identification of issues and enablers for information classification, the development of the information classification method, and the design principles underpinning the method have been performed in five DSR cycles. Each of the DSR cycles had a specific focus and utilized different methods and data collection techniques to reach the intended results. Table 4.1 gives an overview of the focus, methods, and data collection used in each of the DSR cycles.

DSR cycle	Focus	Methods and data collection
1	Focus on deepening our understanding of the domain, and on identifying information classification issues and enablers found in theory and practice.	Systematic literature reviews (on inhibitors and enablers). Email survey, interviews and document collection (government agency survey).
2	Focus on the information classification process, and devising an information classification method.	DSR in three cycles using results from DSR cycle 1 complemented with observations and interviews.
3	Focus on the context around information classification, the relation to risk analysis and security controls.	Literature review, interviews, and document collection.
4	Focus on how usage views can be used to decrease the subjective judgment in the information classification process.	Literature review, interviews, and document collection.
5	Focus on a complement to the information classification scheme that ties classification to security controls.	Literature review, interviews, and document collection.

Table 4.1: Summary of focus, research methods, and data collection for each of the DSR cycles.

Figure 4.1 presents an overview of thesis project, where an overview of the results that evolved in each of the cycles. The dashed boxes each represent a DSR cycle, and the solid boxes represent a main activity in the DSR cycle. The figure also highlights the relationship (the solid arrows), between the activities and which activity primarily informed the next.

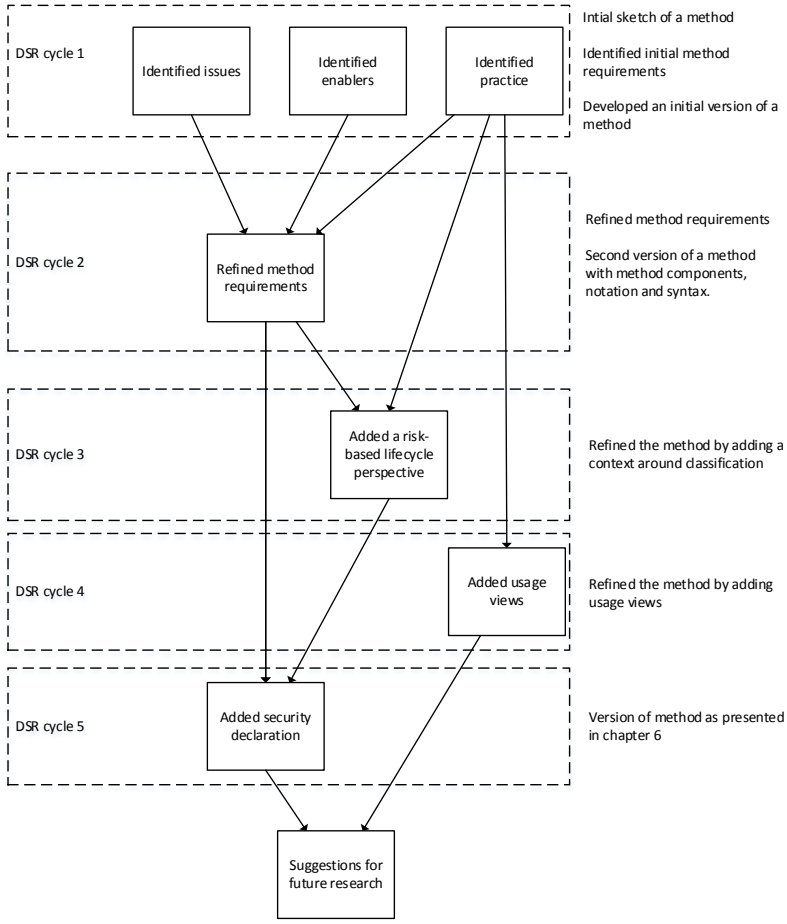

Figure 4.1: The overall research process of the development of the information classification method.

CHAPTER 5
RESULTS

This chapter discusses the results presented in this thesis, as well as their implications for future research. The results are presented according to the respective DSR cycle. To increase transparency, each DSR cycle is presented according to the phases as described by Peffers et al. (2007).

5.1 DSR CYCLE 1 – THE DOMAIN

The focus in the first DSR cycle was on deepening the understanding of the domain, and addressing issues found early in the research process. Furthermore, attention was directed at the process, and the need of a graphical overview of the information classification process.

5.1.1 PROBLEM IDENTIFICATION AND MOTIVATION

Initial interviews and discussions with three senior information security responsible from the SCC took place, and they presented some challenges with the classification process. Issues included the classification scheme itself, and discussions on, e.g., number of levels, and wording in the scheme. Also, the process itself, the relation to risk analysis, and issues on subjective judgment were discussed. As a complement, the author also participated in a work-group within SIS/TK-318 (Swedish Standards Institute/Technical Committee 318, Information Security). The work-group worked on an addition to the standard to address the hurdles of implementing ISMS in organizations by proposing a simplified ISMS, including a more pragmatic view of information classification. In this group, there were representatives from both public and private sector. The issues addressed in this group were very similar to the discussions with the SCC, and early ideas formed around what needed to be addressed in the area of information classification to increase the applicability of the standard. These initial ideas primarily circled around the lack of a model describing the information classification process, number of levels in the scheme, and the relation to risk analysis and security controls.

With this in mind, two literature reviews were initiated, one focusing on information classification issues, and the other one on information classification enablers. Both literature reviews reveal a fragmented landscape covering many aspects ranging from technical to organizational issues and enablers. However, when looking at the results from the perspective of Glynn (2011), where technology can help, but ultimately classification is a subjective business often best done as a collaborative task, it is easier to see some patterns forming around some of the inhibitors and enablers that are especially important.

Information classification guidelines in organizations are too generic (see, e.g., Baškarada (2009); Bayuk (2010) or Janczewski and Xinli Shi (2002)) or too complex (see, e.g., Ghernaouti-Helie et al. (2011). The same applies to the classification scheme that also can be too complex (see, e.g., Donn B. Parker (1997) or Saxby (2008)) or too limited that leads to a development of local practices within organizations (see, e.g., Seifert and Relyea (2004) or Feinberg (2004)). In other words, there is a problem translating the standard into guidelines and organizational practice on a balanced level that fit organizational needs.

To better understand the practice, and anchor it in practice, an email survey was sent out to all government agencies in Sweden. This email survey contained questions about their practices, but also a call to send their internal guidelines for information classification. The details on the email survey can be found in Bergström et al. (2016). Furthermore, six groups of employees in the SCC with a total of 22 employees performing information classification were observed and complemented with four group interviews. These observations made it clear that there was a problem with subjective judgment. In the observations, all groups performed a classification on the same process, but the groups ended up with different results for the same information types. To dig deeper into the reasons why this happened, the observations were immediately followed up by group interviews (that will be added as appendices). Three of the groups were with the employees performing the observation, and the last group was the managers. It was clear that the process itself was difficult to understand, and they spent much time discussing the process, interpretation of information types, wording in the scheme and when asking about if the process could benefit from a graphical description could help out, a security coordinator answered: *"definitely... then it would be possible to follow the information asset [through the process]... That would make it much easier"*.

With this as a backdrop, the initial problem identification and motivation were expressed as: information security managers and the actors doing the actual classification lack a generic information classification method with associated descriptions.

5.1.2 DEFINE THE OBJECTIVES FOR A SOLUTION

Initially, much attention was directed at visualizing the classification process using a model. The focus was on identifying the activities in classification, and structuring the overall flow of the activities in the method. In the first version of the model, no special attention was directed to the modelling language used. Furthermore, an outline of method requirements were formulated.

5.1.3 DESIGN AND DEVELOPMENT

The first version of the model was developed as a flow model, assuming information classification has a clearly defined start and end. The main aim was to get the process as described in the text by ISO/IEC 27002 (2013) but complemented with input from practice described as a model. For example, it is not clearly described in ISO/IEC 27002 (2013) that internal and external requirements affect the classification process, but this was added from practice. In an effort to focus on the classification scheme itself, the consequences of the classification, i.e., the connection to handling guidelines and the labeling were excluded to make the model simpler. The model used the language from Swedish Civil Contingencies Agency (2009) as it is the basis for most Swedish Governmental agencies as well as SCC, which helps in the validation. The language was however ancillary at this point as capturing the process, and the flow was the focus. The first embryo of a model was developed by the author, but it was fed into a group modeling exercise with the author and one of the supervisors. This led to the development of the flow model that is presented in Figure 5.1.

The flow model is read from the activity “Identify process or system”, and ends with handing over the result to the risk analysis.

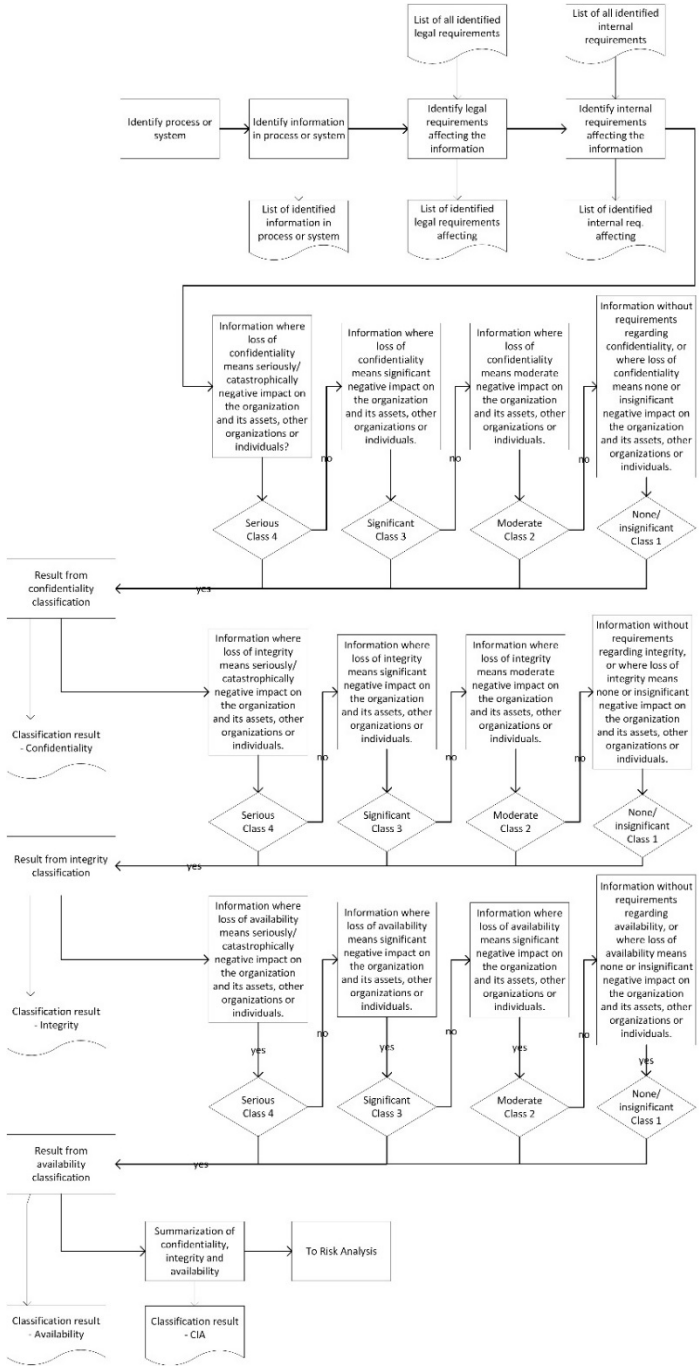

Figure 5.1: The initial flow model, developed to visualize the information classification process. This model was primarily based on the guidelines from MSB (Swedish Civil Contingencies Agency, 2009).

5.1.4 DEMONSTRATION

The first demonstration was held internally at the University. The author presented the model and explained the flow by giving an example to a process modeling expert.

5.1.5 EVALUATION

At the first evaluation with the process modeling expert, the discussion that followed made it evident that it would be beneficial to use a more powerful notation that can express choices. Another benefit of changing the notation is that it would enable to structure the process into sub-processes, and thereby reduce the complexity of the overall process. Furthermore, in the first evaluation, the lack of the excluded labeling and connection to handling guidelines was discussed. If they are excluded, the method will not be compliant to the current standards or practice, and therefore, it was decided to include them in DSR cycle 2.

5.1.6 COMMUNICATION

The process model developed in the first DSR iteration was deemed incomplete, and too premature to be communicated to other audiences. Instead, as much of the initial effort was directed at understanding the area of information classification, and the fact that the area is under-researched, three publications were written, focusing on issues (Bergström & Åhlfeldt, 2014), enablers (Bergström & Åhlfeldt, 2015), and classification practices in Swedish governmental agencies including a comparison with three countries (Bergström et al., 2016). The latter was ordered by MSB as a report to be used as input to their work on upgrading the methodological support for ISMS implementation, especially with a focus on the relationship between information classification and security controls.

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.

Bergström, E., & Åhlfeldt, R.-M. (2015). Information Classification Enablers. In J. Garcia-Alfaro, E. Kranakis, & G. Bonfante (Eds.), *Foundations and Practice of Security: 8th International Symposium, FPS 2015, Clermont-Ferrand, France, October 26-28, 2015, Revised Selected Papers* (pp. 268-276). Cham: Springer International Publishing.

Bergström, E., Åhlfeldt, R.-M., & Anteryd, F. (2016). *Informationsklassificering och säkerhetsåtgärder*. IIT Technical Reports, HS-IIT-TR-16-002.

The results were also communicated orally and via email in a series of dialogues, where background information on progress was sent continuously to MSB, both as a part of the ordered study, but also because of interest shown by MSB to stay informed. Furthermore, the results were communicated at the annual Swedish IT Security Network for Ph.D. Students (SWITS) in 2014, where the issues in the information classification process were presented. Furthermore, at SWITS 2015, the enablers were presented.

5.2 DSR CYCLE 2 – THE METHOD

In the second DSR cycle, DSR was used as a methodology as the process of developing the components for information classification. This cycle (DSR cycle 2) consists of three cycles, but here, these three cycles will be presented together at each phase. The reason for this is that all cycles in DSR study 2 were iterations on the method components constituting the method for information classification.

5.2.1 PROBLEM IDENTIFICATION AND MOTIVATION

The main problem addressed in this cycle is the same as in DSR cycle 1: information security managers and the actors doing the actual classification lack a generic information classification method with associated descriptions. As concluded in the evaluation of DSR cycle 1, the method would benefit from changing the notation to a more powerful one that could also express choices. Also, as not all components were in place in the first DSR cycle, the information classification method was incomplete. Furthermore, little focus on the associated descriptions was spent in DSR cycle 1, and to make the method complete; this aspect was considered more thoroughly in this DSR cycle.

5.2.2 DEFINE THE OBJECTIVES FOR A SOLUTION

In the first iteration, the focus was on developing a method addressing the issues encountered in DSR cycle 1. It was decided to adopt a new notation. This was formulated as DP3: the process in the information classification method should be described using a well-known and accepted notation and is transformed from MR1.

Discussions with a modeling expert of the aim with the method lead to search for alternative means of representation. This was fed into a review of different options, and primarily Unified Modeling Language (UML) and Business Process Model and Notation (BPMN) were considered. UML is object-oriented and stems from software engineering, and BPMN is process-oriented. Both UML and BPMN would be possible to use as they both support modeling of business processes, but BPMN was decided as it has a primary goal of being understandable by all business stakeholders (Peixoto et al., 2008). Furthermore, BPMN has seen a big increase in use in both industry and academia over the past years and seen by many as the de facto standard for process modeling (Dijkman, Hofstetter, & Koehler, 2011).

The initial flow model that came from DSR cycle 1 was extensive and detailed, but to proceed with the conversion to BPMN, the structure of the process model needed to be reworked, and components needed to be identified to make it manageable, that target MR2 and MR3. At this point, in the first cycle, DP7 was formulated: the information classification method should be constructed using components and be flexible to fit different organizational needs. This DP stems from the practice because the initial flow model did actually not allow for changes. The rework of the process model started by identifying skeletons of method components (targeting MR2). In the second cycle, the focus was turned to the descriptions of the method. This meant providing detailed descriptions of the method components that are anchored in explicit definitions and goals, i.e., a perspective. That, in turn, means MR3 primarily, and MR5 were in focus, but also MR1 was touched. In the third and final cycle, the objective was to make the method more generic to fit different organizational needs, an international context and fit both in public and the private sector. In practice, that means addressing MR2. That implies that not only DP7, and DP1, were in focus, but also DP7.1: the method components should be compatible with ISO/IEC 27002 information classification code of practice, was formulated to highlight the importance of the connection to ISO/IEC 27002. Furthermore, DP6: the information classification method should have identified stakeholders to give usage views for information classification stakeholders, was transformed from MR4.

5.2.3 DESIGN AND DEVELOPMENT

In the first cycle, the initial flow model was used as input, together with ISO/IEC 27002 (2013), and how information classification is used in practice. That meant a number of DPs were addressed throughout the cycles. As a first step, following DP3 (targeting MR1), the notation was changed to BPMN using the recommendations in Dumas, La Rosa, Mendling, and Reijers (2013). With the change to BPMN, it was also possible to structure the process

into sub-processes and reduce the complexity of the process following DP7 (targeting MR3). That also meant that the components were possible to identify and separate more clearly. The method was also complemented with the work-flow from how the model is applied in practice following DP5. This meant to include some additions to what is included in the standard, such as the importance of highlighting internal and external requirements in addition to legal requirements.

In the second iteration, we mainly address the textual description of the method was revised to clarify and add details to the activities. That meant addressing DP2 by changing the method so that it is clearer that the input to the method should be an information type in a business process or a system/application.

In the third iteration, the descriptions were updated to follow the confidentiality scheme example based on four levels given in ISO/IEC 27002 (2013) (p. 16), as opposed to the earlier versions using the proposed scheme from Oscarson and Karlsson (2009). This update addresses DP1 and DP7.1. Moreover, a description on the stakeholders was added as given in DP6 (targeting MR4). The stakeholder identification came from a review of the supporting documentation from the government agencies that were collected in DSR cycle 1. The stakeholders were clustered by the type of roles and assigned to the respective method component accordingly. This can be seen as an initial input to DSR cycle 4, where MR4 and DP6 are addressed more in-depth. Finally, a clarification of the connection to the handling guidelines was added in the textual description of the model (addressing DP1).

5.2.4 DEMONSTRATION

The demonstration in the first cycle was done at a workshop organized by the Swedish Civil Contingencies Agency. The theme of the workshop was on information classification and the connection to security controls. The workshop was attended by approximately 55 senior information security experts from around 45 organizations in the public sector. In the second cycle, the demonstration was performed to get input from academia, and this time it took place at the annual SWITS with around 75 attendees. In these two cycles, the demonstrations followed a protocol where the demonstration and evaluation were performed as two separate sessions, and where the method was presented by describing the tasks in the method components, and by giving an example of a generic information type utilizing the method. In the first demonstration the focus was more on the components and the relationship between components, and in the second demonstration, after the method was improved, the focus included more of the descriptions of the method.

In the third iteration, the method was demonstrated for three different organizations (and one more is still left to perform). The selected organizations were the Swedish Civil Contingencies Agency, one government agency, SCC, and the one left to demonstrate to is a private information security consultant company. These organizations were selected to demonstrate the method at different types of organizations. The purpose with choosing a variety of organization was to make the method design less context-specific, i.e., that the method should be applicable to any organization. These demonstrations were all performed following a protocol where the method was sent one week in advance to the organizations. At the demonstration, the method was presented by giving a generic example of an information type flowing through the method components, explaining the tasks in each component along with the stakeholders involved in each component.

5.2.5 EVALUATION

The selection of evaluation activities for each DSR cycle was motivated by the method's maturity and how it evolved. As the maturity of the artifact increased, the evaluation became more complex.

The first and second evaluation was performed using expert panel discussions. The purpose of the first expert panel was to get a broad input from a national and government agency perspective. This was important since the method developed in both DSR cycle 1 and in the first cycle of DSR cycle 2 mainly focused on how the process is described in the standard and our perception on how it is used in practice. This evaluation gave an account for how the method was interpreted by potential adopters and thus, valuable input in the development of the descriptions of the method components. The second iteration targeted academia and had an international perspective. In this evaluation, the focus was on adapting the method to suit an international context. This primarily lead to the objective of changing the method to use the ISO/IEC 270002 examples as opposed to the variant used in Sweden, and the textual descriptions were changed to be less vague as there were some ambiguities in the naming of the tasks.

The third and final evaluation was carried out using expert interviews at three (one additional is planned in the near future) organizations with a total of 5 (so far) participants. The selection of organizations were motivated by assessing different perspectives: a national perspective, a regional perspective, a government agency perspective, and a private organization perspective. All interviews followed the same protocol: which was designed based on the guidelines put forward by Bryman and Bell (2011). All experts received a summary of the protocol before the interviews, containing a short background, aim, and objective, together with the method. This was done to provide a background and to prepare them for the interview, allowing them to become familiar with the method. The first validation was with three senior security specialists at MSB working with the national perspective on systematic information security management. After this validation, the method was complemented so that it is clear that also external requirements should be identified. Following this, the method was validated by a CISO at a government agency. This validation led to a clarification on the connection between specific requirements and a standardized classification value. Following this, the method was validated by a senior security strategist in SCC, that said "*I don't think it is hard to identify with the method, I think this is how I have perceived and understood the process*" when questioned about the method in relation to how they work with information classification. A discussion on the difficulties in identifying the information types, and on what level information types should be classified followed, but we have intentionally left that discussion out since it will differ greatly between organizations and no standard recommendation can be given. Additionally, the limitation regarding DP2, and possible starting points were discussed.

Here, a description of the fourth and final evaluation with the private organization will be inserted.

5.2.6 COMMUNICATION

Throughout the cycles, there has been a continious exchange of information with the Swedish Civil Contingencies Agency to update them on the progress of the method. Moreover, the demonstrations, in primarily cycle 1, and 2, are in fact communication as they included many actors from both public sector and academia.

One publication has been written, but not published yet, as a part of the work performed in this cycle:

> Bergström, E., Karlsson, F., & Åhlfeldt, R.-M. (2018) *Devising an Information Classification Method*. Going to be submitted to Information and Computer Security: Emerald Publishing Limited. (Preliminary draft included).

5.3 DSR CYCLE 3 – THE RISK PERSPECTIVE

The third DSR cycle focus on the context around information classification by tying risk analysis and security controls closer to information classification through a life-cycle perspective. The literature normally describes information classification as input to risk analysis sequentially followed by security controls (ISO/IEC 27001, 2013; Spears & Barki, 2010; Straub & Welke, 1998). In both DSR cycle 1 and 2, interviews touching the subject of the relation to risk analysis and security controls revealed that the exact nature of these relations is vague in practice. When turning to the literature, it is recognized that there is a gap between formal and actual processes (Alaskar, Vodanovich, & Shen, 2015; Niemimaa & Niemimaa, 2017; M. Siponen, 2006), but the interplay, i.e., how they affect each other in practice largely remains a question. For example, the direct relationship between information classification and security controls is a practice in some encountered organizations, but this relation is not well-described in literature, even though there is a direct link as the consequence of a classification is handling guidelines (i.e., security controls).

The research performed in this cycle is divided into two steps. The first step is more exploratory and aims at describing the relations. It was performed by developing a challenge-based perspective based on a literature review on information classification, and risk analysis literature. The challenges found were used to develop an interview guide for semi-structured interviews. The interviews were performed as four in-depth interviews with four government agencies assumed a sequential onset as described in literature and standards. The questions centered on the relations (information classification to risk analysis, risk analysis to information classification, risk analysis to security controls, security controls to risk analysis, information classification to security controls, and security controls to information classification). The result reveals that three of the four agencies describe a sequential onset where for instance the direct relation from information classification to security controls should not exist. However, all of the agencies show examples of all the previously mentioned relations. The results so far are still in development, but the initial results are presented in:

> Lundgren, M., & Bergström (2017). *The Interplay: Classification, Risk, and Controls.* Submitted to Journal of Information Assurance and Security.

From this section and on, the descriptions reflect what is going to be performed, and the text before rather reflect what has been done. The next step is to use practice theory (Feldman & Orlikowski, 2011) as a lens for investigating the relations further. The preliminary idea is to do follow-up interviews with the organizations in step one and to complement with private sector organizations. Additionally, in the first step only security managers were interviewed, so also other employees should be included. Additionally, document studies will be employed to get a triangulation of the data.

From an information classification perspective, the work in this cycle will help describe the context around information classification more clearly, and possibly describe a process on how risk analysis and security controls can aid the classification instead of being an isolated process.

5.4 DSR CYCLE 4 – THE USAGE VIEW

The focus in this cycle will be on how usage views can be employed to decrease the subjective judgment in the information classification process. Two aspects of classification are expected to investigate in this DSR cycle. Firstly, in DSR cycle 2, the roles, or stakeholders, involved in the classification will be investigated further as the role description was limited in that

cycle. Secondly, the focus will turn to the classification scheme to see how views on the classification can be used to aid classification. This cycle primarily targets MR4 and MR5.

The initial idea is to use stakeholder theory to identify stakeholders involved and affected by classification. Stakeholder theory was introduced in the strategic management literature by Freeman (1984), as a set of interest groups affected by an organization's objectives. Since the first introduction, stakeholder theory has evolved and has been accepted in other areas, for example in IS (Pouloudi, 1999). Based on the suggestions from Flak and Rose (2005), the initial focus will be on identification and classification of stakeholders.

After this, the focus will be on the classification scheme itself and on how different views can aid different roles in understanding what level an information type should be classified on. To give an example, the highest level of the confidentiality aspect is put as "*[d]isclosure has a serious impact on long-term strategic objectives or puts the survival of the organization at risk*" in ISO/IEC 27002 (2013 p. 16), and in the US, the National Institute of Standards and Technology (NIST) put it as "*[t]he unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals*" (National Institute of Standards and Technology, 2004 p. 6).

In several of the interviews, the topic on how low, moderate and high impact of, e.g., confidentiality, is discussed. For example, in Sweden, four levels are the most commonly adopted practice, where e.g., the highest level of the confidentiality aspect reads like "*[i]nformation where loss of confidentiality means seriously/catastrophically negative impact on the organization and its assets, other organizations or individuals*" (Oscarson & Karlsson, 2009 p. 9). The other levels of the scheme replace *seriously/catastrophically* with *significant*, *moderate* or *none or insignificant*. The interviews reveal many discussions around the hardships of judging if it is, e.g., *seriously* or *significant*, but also the views of judging the severity from different angles. As, e.g., in both the NIST and Swedish example, the organization, and individuals are mentioned, and in the Swedish example, other organizations are mentioned. That implies that there can be different severity for different actors, which leads to confusion. A concrete example of this came from the discussions with SCC in DSR cycle 1, where it was discussed if a patient record would lose the confidentiality: for the individual, that could be catastrophic, but for the organization, it could be an insignificant impact. This balance has been perceived as problematic, and extensions in the descriptions were asked for as a complement to the classification scheme.

Furthermore, in the demonstration of the first iteration in DSR cycle 2, the question on the wording in classification scheme came up, and a senior security strategist with experience from implementing classification in both public and private sector organizations said: "*don't care about the names, call them 1, 2, 3 and 4, or colour code them. That is not what is important!*". From his experience, this question is irrelevant as when classification experience increases, the wording does not matter.

This dichotomy towards the question of the text in the scheme is not very surprising as, with experience, the need for it decreases. However, as many roles are involved in the classification, another approach introducing different views on the consequence of a loss is proposed to be developed to help aid employees classifying information.

The aim in this cycle is not to develop a better wording in the scheme that competes with NIST, ISO/IEC 27001 or MSB, but rather to complement with other scales that can be easier to interpret for most employees. Initial thoughts are to review the material collected from the government agencies and review what practices can be found on this matter, and complement them with additional organizations. Initial searches show that there are some promising ideas that could be further investigated and ordered thematically. For instance, mapping levels of consequence against the consequences it would incur in the organizational

hierarchy. In other words, it can be hard for employees to judge if the consequence of a loss of confidentiality for an information type is catastrophic or serious, but it could potentially be easier to choose correctly if the consequence is mapped to reflect the organizational hierarchy to see if, e.g., top-level management, middle management or operational level employees are affected. Similarly, depending on the background and role of the person involved in the classification, other areas such as the economic impact or environmental impact of a loss could help guide the classification.

These thematic categories will be developed to reflect different roles and sectors that can be validated in a broad range of organizations.

The identification of the stakeholder's targets MR4 and the view targets MR5. This has been transformed into DP6*:* the information classification method should have identified stakeholders to give usage views for information classification stakeholders.

5.5 DSR CYCLE 5 – THE SECURITY DECLARATION

The focus in this cycle will be on how a security declaration (tentative name) can be used to complement the information classification method. The aim is to build from the results in DSR cycle 3, where it is already clear that a direct relation between information classification and security controls exist. The interviews performed so far in DSR cycle 3 indicate that security controls can be used as a decision-basis for selecting the classification level, in contrast with how the information security process if most often described. The idea is to make this implicit relation explicit by developing a declaration that can be seen as a mirror image of the classification scheme, but with levels of security controls instead. In other words, the levels of the consequence of loss of confidentiality, integrity and availability is mapped to levels of security controls.

The ideas in this cycle also draw from interviews with SCC that saw a need for this kind of complement early on. Furthermore, the need for it was highlighted at a MSB workshop in DSR cycle 2, where an initiative of twelve government agencies involved in fighting serious organized crime was presented (GOB-satsningen in Swedish). The twelve government agencies had a number of deliverables and one of them related to information classification as they had incompatible classification schemes that inhibited the exchange of information. Their approach was to create a new scheme that is mapped against their internal schemes and complement it with common handling guidelines and routines for labeling. The new scheme only related to the confidentiality aspect as that security aspect was in focus for the exchange of information. Also, looking at how requirements for security controls are handled in security classification, it is observable that this practice can be implemented.

When sharing information between organizations, the classification scheme itself only states how valuable the information is to the organization, based on the own organization's needs, but not how it is protected. For the receiving organization, that means that they know how valuable the information is for the sending organization, but not how to protect it. This is an issue also identified by e.g. Y. Cherdantseva and Hilton (2013), that argues consensus use of classification schemes, but that it is hard to achieve, and that ultimately it does not imply the same level of protection. Y. Cherdantseva and Hilton (2013) presents a Reference Model of Information Assurance & Security (RMIAS), that is similar to what is proposed with the security declaration. The differences lie in the execution, where RIMAS try to be very generic and suitable for "*purposes such as education, benchmarking, consultancy, the facilitation of communication, security policy development and others*" (Yulia Cherdantseva, 2014 pp. 287), and which is based on the security development life cycle, information taxonomy, security goals and security measures. The security declaration will primarily be based on

parts of the information taxonomy, focus on CIA, and connect the security controls from an information classification perspective.

The security declaration also relates to the Information Sharing Traffic Light Protocol (ISTLP) (ENISA, 2013), that is developed by the European Union Agency for Network and Information Security (ENISA) as a protocol for sharing information between different countries Computer Emergency Response Teams (CERT). ISTLP focus on the usage of the information sent between organizations, and describe four levels of how the information can be shared and used. In essence, the security declaration adopt some of this thinking, but the focus is on the protection aspects.

This problem is an effect of the decentralized approach in Sweden where government agencies are more independent than most other countries. Compared to national initiatives in, e.g., the UK (Cabinet Office, 2013), the Swedish situation is different, but it highlights a fundamental issue with information classification. The classification only tells the value, and on what level information is classified, not how it is protected. For most organizations, the actual level, and the process of deciding this level is only a starting point, because the end-goal is the protection of the information. By connecting the classification scheme to security controls, the role of the risk analysis might be challenged, which is an issue that needs to be addressed in this work.

The aim of this DSR cycle is not to develop standardized levels of security controls or to address the need for national standards for security controls. The aim is to develop a proof-of-concept that can be used by organizations for mapping their classification scheme to security controls on a more general level by highlighting the benefits of doing so from an information classification perspective.

CHAPTER 6
A METHOD FOR INFORMATION CLASSIFICATION

Joseph G Walls, George R Widmeyer, and Omar A El Sawy (1992) argues a design theory should have two characteristics, a theoretical base and explicit guidance for practitioners. Hence, this chapter will present the method for information classification more in-depth. The results from the DSR cycles will be elaborated and presented so that practitioners could use the chapter as a basis for implementing classification in an organization.

The method as a result from DSR cycle 2 will not be presented here as it is not published yet.

CHAPTER 7
CONCLUSIONS AND FUTURE WORK

This chapter will be included in the final version of the thesis.

REFERENCES

REFERENCES

U.S. Code: Title 44 - PUBLIC PRINTING AND DOCUMENTS, CHAPTER 35—COORDINATION OF FEDERAL INFORMATION POLICY, SUBCHAPTER III—INFORMATION SECURITY, § 3542 - Definitions, (2002).

Aksentijevic, S., Tijan, E., & Agatic, A. (2011). *Information security as utilization tool of enterprise information capital*. Paper presented at the MIPRO, 2011 Proceedings of the 34th International Convention.

Al-Fedaghi, S. (2008). *On Information Lifecycle Management*. Paper presented at the Asia-Pacific Services Computing Conference, 2008. APSCC '08. IEEE.

Alaskar, M., Vodanovich, S., & Shen, K. N. (2015). *Evolvement of Information Security Research on Employees' Behavior: A Systematic Review and Future Direction*. Paper presented at the System Sciences (HICSS), 2015 48th Hawaii International Conference on.

Alqudah, B. I., & Nair, S. (2011). TOWARD MULTI-SERVICE ELECTRONIC MEDICAL RECORDS STRUCTURE. In S. C. G. Suh, Varadraj P.; Tanik, Murat M. (Ed.), *Biomedical Engineering* (pp. 243-254): Springer New York.

Andersson, H., Andersson, J.-O., Björck, F., Eriksson, M., Eriksson, R., Lundberg, R., . . . Starkerud, K. (2011). *Verksamhetsanalys*. Myndigheten för samhällsskydd och beredskap.

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, *13*(4), 195-201. doi:http://dx.doi.org/10.1016/j.istr.2008.10.006

Australian Government. (2014). *Information security management guidelines - Australian Government security classification system Version 2.2*. Attorney-General's Department, Retrieved from https://www.protectivesecurity.gov.au/informationsecurity/Documents/INFOSECGuidelinesAustralianGovernmentSecurityClassificationSystem.pdf.

Axelrod, C. W., Bayuk, J. L., & Schutzer, D. (2009). *Enterprise Information Security and Privacy*: Artech House.

Baškarada, S. (2009). Analysis of Data. In *Information Quality Management Capability Maturity Model* (pp. 139-221): Vieweg+Teubner.

Baskerville, R. L. (1999). Investigating information systems with action research. *Communications of the AIS, 2*(3), 4.

Bayuk, J. (2010). *The utility of security standards*. Paper presented at the 2010 IEEE International Carnahan Conference on Security Technology (ICCST).

Benbasat, I., & Weber, R. (1996). Research Commentary: Rethinking "Diversity" in Information Systems Research. *Info. Sys. Research, 7*(4), 389-399. doi:10.1287/isre.7.4.389

Benbasat, I., & Zmud, R. W. (2003). The identity crisis within the is discipline: defining and communicating the discipline's core properties. *Mis Quarterly, 27*(2), 183-194.

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.

Bergström, E., & Åhlfeldt, R.-M. (2015). Information Classification Enablers. In J. Garcia-Alfaro, E. Kranakis, & G. Bonfante (Eds.), *Foundations and Practice of Security: 8th International Symposium, FPS 2015, Clermont-Ferrand, France, October 26-28, 2015, Revised Selected Papers* (pp. 268-276). Cham: Springer International Publishing.

Bergström, E., Åhlfeldt, R.-M., & Anteryd, F. (2016). *Informationsklassificering och säkerhetsåtgärder*. Retrieved from Skövde:

Blazic, A. J., & Saljic, S. (2010). *Confidentiality Labeling Using Structured Data Types*. Paper presented at the Fourth International Conference on Digital Society.

Blyth, A., & Kovacich, G. L. (2006). Security Standards. In *Information Assurance* (pp. 235-240): Springer London.

Booysen, H. A. S., & Eloff, J. H. P. (1995). Classification of objects for improved access control. *Computers & Security, 14*(3), 251-265. doi:http://dx.doi.org/10.1016/0167-4048(95)00001-O

Brinkkemper, S. (1996). Method engineering: engineering of information systems development methods and tools. *Information and Software Technology, 38*(4), 275-280. doi:http://dx.doi.org/10.1016/0950-5849(95)01059-9

Bunker, G. (2012). Technology is not enough: Taking a holistic view for information assurance. *Information Security Technical Report, 17*(1–2), 19-25. doi:http://dx.doi.org/10.1016/j.istr.2011.12.002

Burnap, P., & Hilton, J. (2009). *Self Protecting Data for De-perimeterised Information Sharing*. Paper presented at the Third International Conference on Digital Society, 2009. ICDS '09. .

Cabinet Office. (2013). *Government Security Classifications April 2014 Version 1.0 – October 2013*. Cabinet Office, Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf.

Checkland, P. (1981). Systems thinking, systems practice.

Checkland, P., & Holwell, S. (1998). Action Research: Its Nature and Validity. *Systemic Practice and Action Research, 11*(1), 9-21. doi:10.1023/a:1022908820784

Cherdantseva, Y. (2014). *Secure* BPMN-a graphical extension for BPMN 2.0 based on a reference model of information assurance & security*. Cardiff University,

Cherdantseva, Y., & Hilton, J. (2013, 2-6 Sept. 2013). *A Reference Model of Information Assurance & Security*. Paper presented at the Availability, Reliability and Security (ARES), 2013 Eighth International Conference on.

Clinch, J. (2009). *ITIL V3 and Information Security*. Best Management Practice For Portfolio, Programme, Project, Risk and Service Management. Clinch Consulting.

Coles-Kemp, L. (2009). Information security management: An entangled research challenge. *Information Security Technical Report, 14*(4), 181-185. doi:http://dx.doi.org/10.1016/j.istr.2010.04.005

Collard, G., Ducroquet, S., Disson, E., & Talens, G. (2017). *A definition of Information Security Classification in cybersecurity context.* Paper presented at the 11th International Conference on Research Challenges in Information Science (RCIS), 2017

Collette, R. (2006). Overcoming obstacles to data classification [information security]. *Computer Economics Report (International Edition), 28*(4), 8-11.

Creswell, J. W. (2009). *Research Design Qualitative, Quantitative, and Mixed Methods Approaches* (Third edition ed.). Thousand Oaks, CA: SAGE Publications Inc.

Cronholm, S., & Ågerfalk, P. J. (1999). *On the concept of method in information systems development*.

Department for Business, I. S. (2013). *UK cyber security standards: research report*. Retrieved from

Department for Culture, Media & Sport,. (2016). *Cyber Security Breaches Survey 2016 Main Report*. Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf

Dhillon, G. (2007). *Principles of information systems security: text and cases*: John Wiley & Sons.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal, 11*(2), 127-153. doi:10.1046/j.1365-2575.2001.00099.x

Dijkman, R., Hofstetter, J., & Koehler, J. (2011). *Business Process Model and Notation*: Springer.

Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. (2013). *Fundamentals of Business Process Management*. Berlin Heidelberg: Springer Berlin Heidelberg.

DuraiPandian, N., & Chellappan, C. (2006, 0-0 0). *Dynamic information security level reclassification.* Paper presented at the Wireless and Optical Communications Networks, 2006 IFIP International Conference on.

Eloff, J. H. P., Holbein, L. R., & Teufel, S. (1996). Security classification for documents. *Computers & Security*, *15*(1), 55-71.

ENISA. (2013). *Security certification practice in the EU: Information Security Management Systems - A case study, v.1, October 2013*. Retrieved from

Etges, R., & McNeil, K. (2006). Understanding data classification based on business and security requirements. *ISACA Information Systems Control Journal*, *5*.

Everett, C. (2011). Building solid foundations: the case for data classification. *Computer Fraud & Security*, *2011*(6), 5-8. doi:http://dx.doi.org/10.1016/S1361-3723(11)70060-4

Feinberg, L. E. (2004). FOIA, federal information policy, and information availability in a post-9/11 world. *Government Information Quarterly*, *21*(4), 439-460. doi:http://dx.doi.org/10.1016/j.giq.2004.08.004

Feldman, M. S., & Orlikowski, W. J. (2011). Theorizing Practice and Practicing Theory. *Organization Science*, *22*(5), 1240-1253. doi:10.1287/orsc.1100.0612

Fernando, D., & Zavarsky, P. (2012). *Secure decommissioning of confidential electronically stored information (CESI): A framework for managing CESI in the disposal phase as needed*. Paper presented at the 2012 World Congress on Internet Security (WorldCIS).

Feuerlicht, J., & Grattan, P. (1989). The role of classification of information in controlling data proliferation in end-user personal computer environment. *Computers & Security*, *8*(1), 59-66. doi:http://dx.doi.org/10.1016/0167-4048(89)90040-0

Fibikova, L., & Müller, R. (2011). A Simplified Approach for Classifying Applications. In N. R. Pohlmann, Helmut; Schneider, Wolfgang (Ed.), *ISSE 2010 Securing Electronic Business Processes* (pp. 39-49): Vieweg+Teubner.

Fitzgerald, B., Russo, N., L., & Stolterman, E. (2002). *Information Systems Development: Methods-in-Action*. New York: McGraw-Hill Higher Education.

Flak, L. S., & Rose, J. (2005). Stakeholder governance: Adapting stakeholder theory to e-government. *Communications of the Association for Information Systems*, *16*(1), 31.

Freeman, R. E. (1984). *Strategic management : a stakeholder approach*. Boston :: Pitman.

Gantz, S. D., & Philpott, D. R. (2013). Chapter 2 - Federal Information Security Fundamentals. In S. D. P. Gantz, Daniel R. (Ed.), *FISMA and the Risk Management Framework* (pp. 23-52): Syngress.

Gerber, M., & von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security*, *27*(5–6), 124-135. doi:http://dx.doi.org/10.1016/j.cose.2008.07.009

Ghernaouti-Helie, S., Simms, D., & Tashi, I. (2011). *Protecting Information in a Connected World: A Question of Security and of Confidence in Security*. Paper presented at

the 14th International Conference on Network-Based Information Systems (NBiS).

Gikas, C. (2010). A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. *Information Security Journal: A Global Perspective, 19*(3), 132-141. doi:10.1080/19393551003657019

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal, 23*(4), 367-376. doi:doi:10.1108/17542731111139455

Glynn, S. (2011). Getting To Grips With Data Classification. *Database and Network Journal, 41*(1), 8-9.

Goldkuhl, G., Lind, M., & Seigerroth, U. (1998). Method integration: the need for a learning perspective. *IEE Proceedings - Software, 145*(4), 113-118. doi:10.1049/ip-sen:19982197

Grandison, T., Bilger, M., O'Connor, L., Graf, M., Swimmer, M., Schunter, M., . . . Zunic, N. (2007). *Elevating the Discussion on Security Management: The Data Centric Paradigm*. Paper presented at the 2nd IEEE/IFIP International Workshop on Business-Driven IT Management, BDIM.

Gregor, S. (2002). Design theory in information systems. *Australasian Journal of Information Systems, 10*(1).

Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *Mis Quarterly, 37*(2), 337-356.

Gregor, S. D., & Jones, D. (2007). The anatomy of a design theory. *Journal of the Association for Information Systems, 8*(5), 312-335.

Hayat, Z., Reeve, J., Boutle, C., & Field, M. (2006). *Information security implications of autonomous systems*. Paper presented at the Proceedings of the 2006 IEEE conference on Military communications, Washington, D.C.

Hayes, J. (2008). Have data will travel - [IT security]. *Engineering & Technology, 3*(15), 60-61.

Hevner, A., & Chatterjee, S. (2010). *Design Research in Information Systems: Theory and Practice*: Springer Publishing Company, Incorporated.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28*(1), 75-105.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *Mis Quarterly, 28*(1), 75-105.

Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional Influences on Information Systems Security Innovations. *Information Systems Research, 23*(3-part-2), 918-939. doi:10.1287/isre.1110.0393

IBM Security. (2016). *IBM X-Force Threat Intelligence Report 2016*. Retrieved from Somers, NY:

Iivari, J., Hirschheim, R., & Klein, H. K. (2000). A Dynamic Framework for Classifying Information Systems Development Methodologies and Approaches. *Journal of*

Management Information Systems, 17(3), 179-218. doi:10.1080/07421222.2000.11045656

ISACA. (2012). *COBIT 5 Enabling Processes*. Rolling Meadows, IL.: ISACA.

ISO/IEC 27000. (2014). Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary. In: ISO/IEC.

ISO/IEC 27001. (2013). Information technology – Security techniques – Information security management systems – Requirements. In: ISO/IEC.

ISO/IEC 27002. (2013). Information technology – Security techniques – Code of practice for information security controls. In: ISO/IEC.

ISO/IEC 27005. (2013). Information technology – Security techniques – Information security risk management. In: ISO/IEC.

Jafari, M., & Fathian, M. (2007). Management Advantages of Object Classification in Role-Based Access Control (RBAC). In I. Cervesato (Ed.), *Advances in Computer Science – ASIAN 2007. Computer and Network Security* (Vol. 4846, pp. 95-110): Springer Berlin Heidelberg.

Janczewski, L., & Xinli Shi, F. (2002). Development of Information Security Baselines for Healthcare Information Systems in New Zealand. *Computers & Security, 21*(2), 172-192. doi:http://dx.doi.org/10.1016/S0167-4048(02)00212-2

Jayaratna, N. (1994). *Understanding and Evaluating Methodologies: NIMSAD, a Systematic Framework*: McGraw-Hill, Inc.

Kaarst-Brown, M. L., & Thompson, E. D. (2015). *Cracks in the Security Foundation: Employee Judgments about Information Sensitivity*. Paper presented at the Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, Newport Beach, California, USA.

Kane, G., & Koppel, L. (2013). Chapter 1 - Information Protection Function One: Governance. In G. K. Kane, Lorna (Ed.), *Information Security* (pp. 1-11). Boston: Elsevier.

Karlsson, F., & Ågerfalk, P. J. (2009). Towards Structured Flexibility in Information Systems Development: Devising a Method for Method Configuration. *Journal of Database Management (JDM), 20*(3), 51-75. doi:10.4018/jdm.2009070103

Kindervag, J., Shey, H., & Mak, K. (2015). *The Future Of Data Security And Privacy: Growth And Competitive Differentiation*. Retrieved from Cambridge, MA.:

Kokolakis, S., & Lambrinoudakis, C. (2005). ICT Security Standards for Healthcare Applications. *The European Journal for the Informatics Professional, V1*(4), 47-54.

Kolkowska, E. (2013). *A method for analyzing value-based compliance in systems security*. (PhD), Örebro University, Örebro.

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. doi:http://dx.doi.org/10.1016/j.telpol.2009.03.002

Kuechler, W., & Vaishnavi, V. (2012). A Framework for Theory Development in Design Science Research: Multiple Perspectives. *Journal of the Association for Information Systems, 13*(6).

Kwo-Jean, F., Shu-Kuo, L., & Chi-Chun, L. (2008). A study on e-Taiwan information system security classification and implementation. *Computer Standards & Interfaces, 30*(1-2), 1-7. doi:http://dx.doi.org/10.1016/j.csi.2007.07.001

Lindup, K. R. (1995). A new model for information security policies. *Computers & Security, 14*(8), 691-695. doi:http://dx.doi.org/10.1016/0167-4048(96)81709-3

Mansfield-Devine, S. (2016). Data classification: keeping track of your most precious asset. *Network Security, 2016*(12), 10-15. doi:http://dx.doi.org/10.1016/S1353-4858(16)30116-7

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decis. Support Syst., 15*(4), 251-266. doi:10.1016/0167-9236(94)00041-2

Mataracioglu, T., & Ozkan, S. (2011). Governing information security in conjunction with COBIT and ISO 27001. *International Journal of Network Security & Its Applications, 3*(4), 111-116.

McFadzean, E., Ezingeard, J.-N., & Birchall, D. Anchoring information security governance research: sociological groundings and future directions.

Mikkelinen, N. (2015). *Analysis of information classification best practices.* University of Skövde, Skövde.

Moar, J. (2015). *CYBERCRIME AND THE INTERNET OF THREATS*. Retrieved from Basingstoke, UK:

Montesino, R., & Fenz, S. (2011, 22-26 Aug. 2011). *Information Security Automation: How Far Can We Go?* Paper presented at the Availability, Reliability and Security (ARES), 2011 Sixth International Conference on.

Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet, (2016).

National Institute of Standards and Technology. (2004). FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems. In *The National Institute of Standards and Technology (NIST)*. Gaithersburg, MD: National Institute of Standards and Technology.

National Institute of Standards and Technology. (2006). FIPS Publication 200: Minimum Security Requirements for Federal Information and Information Systems. In *The National Institute of Standards and Technology (NIST)*. Gaithersburg, MD: National Institute of Standards and Technology.

National Institute of Standards and Technology. (2015). NIST Special Publication 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations. In *The National Institute of Standards and Technology (NIST)*. Gaithersburg, MD: Technology.

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. doi:10.1057/s41303-016-0025-y

NIST. (2017a). FISMA BACKGROUND. Retrieved from http://csrc.nist.gov/groups/SMA/fisma/overview.html

NIST. (2017b). *Framework for Improving Critical Infrastructure Cybersecurity (Draft Version 1.1)*. Retrieved from Gaithersburg, MD.:

Njenga, K., & Brown, I. (2012). Conceptualising improvisation in information systems security. *European Journal of Information Systems, 21*(6), 592-607. doi:10.1057/ejis.2012.3

Nunamaker, J. F., Chen, M., & Purdin, T. D. M. (1991). Systems Development in Information Systems Research. In (Vol. 7). Journal of Management Information Systems Development.

Oates, B. J. (2006). *Researching Information Systems and Computing*. London: Sage.

Organisation for Economic Co-operation and Development. (2002). OECD guidelines for the security of information systems and networks: Towards a culture of security.

Orlikowski, W. J., & Iacono, C. S. (2001). Research commentary: Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact. *Information Systems Research, 12*(2), 121-134.

Oscarson, P., & Karlsson, F. (2009). *A National Model for Information Classification*. Paper presented at the AIS SIGSEC Workshop on Information Security & Privacy (WISP2009), Phoenix, AZ, USA.

Parker, D. B. (1996). The classification of information to protect it from loss. *Information Systems Security, 5*(2), 9-15.

Parker, D. B. (1997). The strategic values of information security in business. *Computers & Security, 16*(7), 572-582. doi:http://dx.doi.org/10.1016/S0167-4048(97)80793-6

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *J. Manage. Inf. Syst., 24*(3), 45-77. doi:10.2753/mis0742-1222240302

Peixoto, D., Batista, V., Atayde, A., Borges, E., Resende, R., & Pádua, C. (2008). *A comparison of BPMN and UML 2.0 activity diagrams.* Paper presented at the VII Simposio Brasileiro de Qualidade de Software.

Photopoulos, C. (2008). Chapter 2 - Data Classification. In C. Photopoulos (Ed.), *Managing Catastrophic Loss of Sensitive Data* (pp. 15-45). Burlington: Syngress.

Pouloudi, A. (1999, 1999). *Aspects of the stakeholder concept and their implications for information systems development.* Paper presented at the Systems Sciences, 1999. HICSS-32. Proceedings of the 32nd Annual Hawaii International Conference on.

Raman, K., Beets, K., & Kabay, M. E. (2014). Developing Classification Policies for Data Sixth Edition. In *Computer Security Handbook* (Vol. Vol. 1, pp. 1885-1903): John Wiley & Sons, Inc.

Ramasamy, H. V., & Schunter, M. (2006). *Multi-Level Security for Service-Oriented Architectures*. Paper presented at the Military Communications Conference, 2006. MILCOM 2006. IEEE.

Röstlinger, A., & Goldkuhl, G. (1994). *Generisk flexibilitet – På väg mot en komponentbaserad metodsyn*. Retrieved from Presenterat på VITS Höstseminarium 1994. Institutionen för datavetenskap, Linköpings universitet:

Sarker, S., & Lee, A. S. (2002). Using a positivist case research methodology to test three competing theories-in-use of business process redesign. *Journal of the Association for Information Systems, 2*(1), 7.

Saxby, S. (2008). News and comment on recent developments from around the world. *Computer Law & Security Review, 24*(2), 95-110. doi:http://dx.doi.org/10.1016/j.clsr.2008.01.013

Scotland, J. (2012). Exploring the philosophical underpinnings of research: Relating ontology and epistemology to the methodology and methods of the scientific, interpretive, and critical research paradigms. *English Language Teaching, 5*(9), 9.

Seifert, J. W., & Relyea, H. C. (2004). Do you know where your information is in the homeland security era? *Government Information Quarterly, 21*(4), 399-405. doi:http://dx.doi.org/10.1016/j.giq.2004.08.001

Shedden, P., Smith, W., & Ahmad, A. (2010). *Information security risk assessment: towards a business practice perspective*. Paper presented at the Australian Information Security Management Conference 2010.

Shrestha, A. (2015). *Development and evaluation of a software-mediated process assessment approach in IT service managment.* University of Southern Queensland,

Simon, H. A. (1996). *The sciences of the artificial* (Third Edition ed.): MIT press.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Commun. ACM, 49*(8), 97-100. doi:10.1145/1145287.1145316

Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *SIGMIS Database, 38*(1), 60-80. doi:10.1145/1216218.1216224

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management, 46*(5), 267-270. doi:http://dx.doi.org/10.1016/j.im.2008.12.007

Siponen, M., Willison, R., & Baskerville, R. (2008). Power and practice in information systems security research. *ICIS 2008 Proceedings*, 26.

Siponen, M. T. (2005). An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems, 14*(3), 303-315. doi:10.1057/palgrave.ejis.3000537

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of Power: A Study of Mandated Compliance to an Information Systems Security "De Jure" Standard in a Government Organization. *Mis Quarterly*, *34*(3), 463-486.

SOU 2015:25. (2015). *En ny säkerhetsskyddslag [A New Security Act]*. Retrieved from Stockholm:

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *Mis Quarterly*, *34*(3), 503-522.

Statistics Sweden. (2017). Välkommen till det allmänna myndighetsregistret. Retrieved from http://www.myndighetsregistret.scb.se/Default.aspx

Straub, D. W., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *Mis Quarterly*, *22*(4), 441-469. doi:10.2307/249551

Swedish Civil Contingencies Agency. (2009). *Modell för klassificering av information - rekommendationer [A model for classification of information - recommendations]*. Retrieved from

Swedish Civil Contingencies Agency. (2014). *En bild av myndigheternas informationssäkerhetsarbete 2014 – tillämpning av MSB:s föreskrifter [A picture of governmental agencies work with information security 2014 - application of the Swedish Civil Contingencies Agency guidelines]* (978-91-7383-478-0). Retrieved from https://www.msb.se/Produkter--tjanster/Publikationer/Publikationer-fran-MSB/En-bild-av-myndigheternas-informationssakerhetsarbete-2014/

Swedish Civil Contingencies Agency. (2015). *En bild av kommunernas informationssäkerhetsarbete 2015 [A picture of the municipalities work with information security 2015]* (978-91-7383-619-7). Retrieved from https://www.msb.se/RibData/Filer/pdf/27967.pdf

Swedish Civil Contingencies Agency. (2016). Introduktion [Introduction]. Retrieved from https://www.informationssakerhet.se/metodstod-for-lis/introduktion/

Swedish Civil Contingencies Agency. (2017a). MSB – Swedish Civil Contingencies Agency. Retrieved from https://www.msb.se/en/About-MSB/

Swedish Civil Contingencies Agency. (2017b). Verksamheten för cybersäkerhet och skydd av samhällsviktig verksamhet [The Office of Cybersecurity and Critical Infrastructure Protection]. Retrieved from https://www.msb.se/sv/Om-MSB/Organisation/Organisation/Avdelningar/Avd-for-utveckling-av-samhallsskydd/Verksamheten-for-cybersakerhet-och-skydd-av-samhallsviktig-verksamhet/

Takeda, H., Veerkamp, P., Tomiyama, T., & Yoshikawam, H. (1990). Modeling Design Processes. *AI Magazine*, *11*(4), 37-48.

Taylor, L. P. (2013). Chapter 8 - Categorizing Data Sensitivity. In L. P. Taylor (Ed.), *FISMA Compliance Handbook (Second Edition)* (pp. 63-78). Boston: Syngress.

Taylor, R. G., & Brice, J., Jr. (2012). Fact or fiction? A study of managerial perceptions applied to an analysis of organizational security risk. *Journal of Organizational Culture, Communications and Conflict, 16*(1).

The Open Group. (2017). *Open Information Security Management Maturity Model (O-ISM3), Version 2.0*. Retrieved from Reading, United Kingdom:

Thompson, E. D., & Kaarst-Brown, M. L. (2005). Sensitive information: A review and research agenda. *Journal of the American Society for Information Science and Technology, 56*(3), 245-257. doi:10.1002/asi.20121

Tomhave, B. L. (2005). Alphabet Soup: Making sense of models, frameworks, and methodologies. In.

Vaishnavi, V., & Kuechler, W. (2004). Design Research in Information Systems. Retrieved from http://www.desrist.org/design-research-in-information-systems/

Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building an information system design theory for vigilant EIS. *Information Systems Research, 3*(1), 36-59.

Walls, J. G., Widmeyer, G. R., & El Sawy, O. A. (1992). Building Information System Design Theory for Vigilant EIS. *Information Systems Research, 3*(1), 36-59.

Walsham, G. (1993). *Interpreting Information Systems in Organizations*: John Wiley & Sons, Inc.

Walsham, G. (1995). The Emergence of Interpretivism in IS Research. *Information Systems Research, 6*(4), 376-394.

Walsham, G. (2006). Doing interpretive research. *European Journal of Information Systems, 15*(3), 320-330. doi:10.1057/palgreaves.ejis.3000589

Wikipedia. (2017, 19 October 2017). Classified information. Retrieved from https://en.wikipedia.org/wiki/Classified_information

Willison, R., & Warkentin, M. (2013). Beyond deterrence: an expanded view of employee computer abuse. *Mis Quarterly, 37*(1), 1-20.

Winkler, V. (2011). Chapter 3 - Security Concerns, Risk Issues, and Legal Aspects. In V. Winkler (Ed.), *Securing the Cloud* (pp. 55-88). Boston: Syngress.

Virtanen, T. (2001). Design Criteria to Classified Information Systems Numerically. In M. P. Dupuy, Pierre (Ed.), *Trusted Information* (Vol. 65, pp. 317-325): Springer US.

Wynekoop, J. L., & Russo, N. L. (1995). Systems development methodologies: unanswered questions. *Journal of Information Technology (Routledge, Ltd.), 10*(2), 65.

Åhlfeldt, R.-M., Andersén, A., Eriksson, N., Nohlberg, M., Bergström, E., & Fischer-Hübner, S. (2015). *Kompetensbehov och kompetensförsörjning inom informationssäkerhet från ett samhällsperspektiv*. Retrieved from

Åhlfeldt, R.-M., Spagnoletti, P., & Sindre, G. (2007). Improving the Information Security Model by using TFI. In H. Venter, M. Eloff, L. Labuschagne, J. Eloff, & R. Solms

(Eds.), *New Approaches for Security, Privacy and Trust in Complex Environments* (Vol. 232, pp. 73-84): Springer US.

PUBLICATIONS IN THE DISSERTATION SERIES

PUBLICATIONS IN THE DISSERTATION SERIES

1. Family name, Given name (Year) Title, Subject. Doctoral/Licentiate Dissertation, ISBN XXX
2. Family name, Given name (Year) Title, Subject. Doctoral/Licentiate Dissertation, ISBN XXX'

ERIK BERGSTRÖM A METHOD FOR INFORMATION CLASSIFICATION 2017

ERIK BERGSTRÖM

Add your text here

ISBN XXX-XX-XXXX-XX-X
Dissertation Series, No. Number (Year)

ERIK BERGSTRÖM A METHOD FOR INFORMATION CLASSIFICATION 2017

ERIK BERGSTRÖM

Add your text here

IN COLLABORATION WITH

ISBN XXX-XX-XXXX-XX-X
Dissertation Series, No. Number (Year)

ERIK BERGSTRÖM A METHOD FOR INFORMATION CLASSIFICATION 2017

ERIK BERGSTRÖM

Add your text here

IN COLLABORATION WITH

ISBN XXX-XX-XXXX-XX-X
Dissertation Series, No. Number (Year)

ERIK BERGSTRÖM A METHOD FOR INFORMATION CLASSIFICATION 2017

ERIK BERGSTRÖM

Add your text here

ISBN XXX-XX-XXXX-XX-X
Dissertation Series, No. Number (Year)