

# Bachelor Degree Project



UNIVERSITY  
OF SKÖVDE

## **Information Classification in Swedish Governmental Agencies**

Analysis of Classification Guidelines

Bachelor Degree Project in Computer Science  
G2E, 15 ECTS  
Spring Term 2015

Fredrik Anteryd

Supervisor: Erik Bergström  
Examiner: Rose-Mharie Åhlfeldt

## **Abstract**

Information classification deals with the handling of sensitive information, such as patient records and social security information. It is of utmost importance that this information is treated with caution in order to ensure its integrity and security. In Sweden, the Civil Contingencies Agency has established a set of guidelines for how governmental agencies should handle such information. However, there is a lack of research regarding how well these guidelines are followed as well as if the agencies have made accommodations of these guidelines of their own. This work presents the results from a survey sent to 245 governmental agencies in Sweden, investigating how information classification actually is performed today. The questionnaire was answered by 144 agencies and 54 agencies provided detailed documents of their classification process. The overall results show that the classification process is difficult, while those who provided documents proved to have good guidelines, but not always consistent with the existing recommendations.

**Keywords:** Information Security Management Systems, Information Classification, Classification Guidelines, ISO/IEC 27000, Governmental agencies

# Contents

- 1 Introduction** **4**
  
- 2 Background** **5**
  - 2.1 Information security management systems . . . . . 5
  - 2.2 Information security policy . . . . . 6
  - 2.3 Information classification . . . . . 7
    - 2.3.1 Guideline for classification . . . . . 8
  - 2.4 System security . . . . . 9
  - 2.5 Related work . . . . . 10
  
- 3 Problem description** **11**
  - 3.1 Research question . . . . . 12
  - 3.2 Delimitation . . . . . 12
  
- 4 Research method** **13**
  - 4.1 Research design . . . . . 13
  - 4.2 Literature review . . . . . 14
  - 4.3 Survey . . . . . 15
    - 4.3.1 Questionnaire . . . . . 16
  - 4.4 Validity and ethics . . . . . 17
  - 4.5 Alternative methods . . . . . 18
  
- 5 Results** **19**
  - 5.1 Overview . . . . . 19
  - 5.2 Quantitative results . . . . . 21
  - 5.3 Qualitative results . . . . . 23
    - 5.3.1 Who . . . . . 23
    - 5.3.2 When . . . . . 24
    - 5.3.3 What . . . . . 25
    - 5.3.4 How . . . . . 25
    - 5.3.5 Why . . . . . 26
  
- 6 Conclusion** **27**
  
- 7 Discussion** **28**
  - 7.1 Method . . . . . 28
  - 7.2 Results . . . . . 29
  - 7.3 Ethical aspects . . . . . 29
  - 7.4 Social aspects . . . . . 30
  - 7.5 Scientific aspects . . . . . 30
  
- 8 Future research** **30**
  
- References** **32**
  
- Appendix A Survey regarding information classification** **36**

# 1 Introduction

Working with information security is essential in our modern-day information technology (IT) society and is described as the "*preservation of confidentiality, integrity and availability of information*" by ISO/IEC (2014). An important part of information security is information security management systems (ISMS) which is a set of guidelines concerning information security (ISO/IEC, 2014). A vital part of ISMS is information asset management, to which information classification is crucial. Information assets can be persons with certain skills or knowledge, physical assets, services and intangibles which are valuable to an organization, which consequently means that they need protection. But in order to do so, the information assets must first and foremost be identified. Afterwards, issues such as ownership, responsibilities and guidelines for usage must be assigned. Thereafter, information can be classified according to their organizational value (ISO/IEC, 2013a).

According to a review done by the Swedish National Audit Office (2014) and a survey done by the Swedish Civil Contingencies Agency (2014), the information security in Swedish governmental agencies is inadequate. In the review by the Swedish National Audit Office (2014), both the National Defence Radio Establishment and the Swedish Security Service describe the existing protection for sensitive information as inferior. Existing flaws in the protection enable an attacker to take control over whole IT-environments and information regarding national security could be leaked (the Swedish National Audit Office, 2014). For a system administrator it is essential to know what information is important and how to protect it. But information cannot be secured by only implementing technological solutions such as firewalls and cryptography, the administrative security is important as well such as guidelines for usage of information. The information security policy is vital for protecting information within an organization to which information classification is a part of (ISO/IEC, 2013b).

Since the first of February 2010, Swedish governmental agencies have received new regulations regarding information security, and thus also new regulations for information classification. The governmental agencies are required to classify information with reference to requirements on confidentiality, integrity and availability, a model commonly known as the CIA-triad (MSBFS2009:10, 2009). These aspect are defined in ISO/IEC-27000:2014 as follows:

- **Confidentiality:** Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
- **Integrity:** Property of accuracy and completeness
- **Availability:** Property of being accessible and usable upon demand by an authorized entity

Information classification is problematic since only a limited number of recommendations for classification exist, and those that exist are often too generic to provide efficient support (Bayuk, 2010) and according to Baškarada (2009), it is problematic to develop a classification scheme.

In order to investigate the implementation of information classification in the governmental domain, a mixed method survey was used to collect both qualitative and quantitative data. By analysing existing classification guidelines, recommendations on how to handle issues with the classification process are hoped to be found. The results obtained can hopefully aid governmental agencies with their information classification process.

## 2 Background

This chapter provides an introduction to information security management systems (ISMS), with focus on information classification, its relation to the ISO 27000-series and the brief history of the ISO 27000-series. The chapter also explains some of the existing challenges and possibilities in the area.

### 2.1 Information security management systems

ISMS is a collection of guidelines used for information security management (ISO/IEC, 2013a). According to Coles-Kemp (2009), it is hard to define security management because of the relationship between the social and the material within information security. However, ISMS can be defined 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, 2013b). Not adhering to the ISMS, there is a risk that some aspects of information security are overlooked and, thus, that the implementation lacks the necessary security details needed which creates a gap between security controls (Coles-Kemp, 2009, Garcia, 2010). According to Humphreys (2008), there is also a need for organizations to be able to check the effectiveness of their ISMS in practice.

According to Oscarson and Karlsson (2009) and Humphreys (2008), a commonly used ISMS is the ISO 27000-series (ISO/IEC, 2014) which is well-known in the information security domain. The history of the ISO 27000-series is well-documented (Humphreys, 2011, Broderick, 2006, Garcia, 2010, Kokolakis & Lambrinouidakis, 2005, Humphreys, 2006), and dates back to the 90's with the development of BS7799 in the United Kingdom. The BS7799 standard consisted of two parts, BS7799-1 which was adopted as a standard in 1995 (Humphreys, 2011) and BS7799-2, which was adopted in 1999 (Garcia, 2010). BS7799-1 was about best practices for information security management and was later published by ISO/IEC as ISO/IEC 17799 "Code of practice for Information Security Management" (Kokolakis & Lambrinouidakis, 2005) in 2002 and thus replaced BS7799-1 (Garcia, 2010). The standard was later renamed and re-published in 2005 as ISO/IEC 27002:2005, which was further updated in 2013 to ISO/IEC 27002:2013. BS7799-2 described the implementation of ISMS and was published by ISO/IEC 2005 (Garcia, 2010) as ISO/IEC 27001:2005 "Information Security Management Systems – Requirements" (Kokolakis & Lambrinouidakis, 2005) which is considered the flagship of the ISO 27000-series (Humphreys, 2011). The ISO/IEC 27001:2005 was also updated in 2013 and published as ISO/IEC 27001:2013. Today the ISO 27000-series consists of more than 20 published standards and even more are under development.

In the ISO 27000-series, the information assets management of the ISMS systems is critical and key security aspects related to such management are confidentiality, integrity and availability, commonly known as the CIA-triad (ISO/IEC, 2013b). According to Greene (2005), protecting the CIA-triad is the same as protecting the organizations' information assets, and successful ISMS requires the support from the whole organization and sometimes, even support from external parties and stakeholders (ISO/IEC, 2013b). The Swedish governmental agencies are required to use ISO/IEC 27001 and ISO/IEC 27002 (Oscarson & Karlsson, 2009, MSBFS2009:10, 2009). All agencies are further required to focus on the CIA-triad aspects (Oscarson, 2009) and are also encouraged to implement optional aspects such as accountability

(MSBFS2009:10, 2009).

According to Coles-Kemp (2009), Garcia (2010), Humphreys (2011), in order to ensure the development and improvement of the management process, an approach based on the plan-do-check-act cycle (PDCA-cycle) is commonly used even though the most updated version of ISO/IEC 27001 (ISO/IEC27001:2013) does not explicitly mention it like previous versions (ISO/IEC, 2013a). Since the current ISO/IEC 27001 is still rather new, most of the research and recommendations have been done with the PDCA-cycle in mind. However, according to Siponen (2006), there is a lack of research regarding this development process and, it is not considered an academic pursuit by Coles-Kemp (2009).

Apart from the ISO 27000-series, other types of ISMS and standards exist, such as common criteria (CC) which is a combination of information technology security evaluation criteria (ITSEC), Canadian trusted computer product evaluation criteria (CTCPEC) and trusted computer system evaluation criteria (TCSEC). CC was developed by the governments of Canada, France, Germany, the Netherlands, the UK, and the US, and the first version was issued in 1994 (*Common Criteria History*, 2013). A number of nations also publish their own ISMS such as DoD information technology security certification and accreditation process (DITSCAP) and DoD information assurance certification and accreditation process (DIACAP) from the US, ISMS of Korea and IT Baseline Protection Manual from Germany (Jo, Kim, & Won, 2011).

Other standards related to ISMS are information technology service management (ITSM) such as control objectives for information and related technology (COBIT) and information technology infrastructure library (ITIL). COBIT is a framework created by information systems audit and control association (ISACA), which provides guidelines for the development and assessment of IT controls. COBIT has its focus on IT processes while ISO/IEC 27002 focuses on security controls (Lin, Cefaratti, & Wallace, 2012). According to Arora (2010), COBIT and ISO/IEC 27001 are overlapping and have similarities even though they are different in many aspects. According to Clinch (2009), ITIL is a framework which contains best practices for management of IT-services. ITIL no longer publishes security management due to the large content of international standards, instead ITIL can now be used together with other ISMS (Clinch, 2009).

## **2.2 Information security policy**

Information security policy is a large part of ISMS, which goal is "*[t]o provide management direction and support for information security in accordance with business requirements and relevant laws and regulations*" (ISO/IEC, 2013b). The information security policy should be defined by the highest level within an organization and should reflect the organization's approach for managing information security (ISO/IEC, 2013b, the Swedish Civil Contingencies Agency, 2014). Basically, the information security policy should ensure that everyone in the organization handles information in a secure way. However, organizations need to delegate responsibilities in order to ensure compliance with the information security policy (von Solms, 2005). Hagen, Albrechtsen, and Hovden (2008) argue that the information security policy is the foundation for a working security system, since it is linked to an organization's overall strategy and according to Hashimoto, Rosa, Filho, and Machado (2010), regardless of an organization's size, business or technology, information security should be addressed by an information security policy. However, since organizations are under constant change, the security plan needs to be

periodically reviewed and updated (Pfleeger & Pfleeger, 2006). While the information security policy state that information classification should be done, it does not provide any guidance on how it should be done (ISO/IEC, 2014).

## 2.3 Information classification

Information asset management is a central role of ISMS, in which information classification is a vital part. To begin the process of information classification, see Figure 1, information assets need to be identified by doing an inventory of all the information within the organization. These information assets can be persons with certain skills or knowledge, physical assets, services and intangibles like an organization's reputation. When assets have been identified, ownerships and responsibilities are assigned, as well as guidelines of their usage. Thereafter, the information assets should be classified according to their organizational value, or maybe labelled. Lastly the handling of information assets needs to be decided upon, for example access control and storage media (ISO/IEC, 2013a). The value of information may change over time. A previously secret document, now publicly available is no longer considered critical. The results of the classification should be updated in accordance with an eventual change of the information value (ISO/IEC, 2013b).



Figure 1: The information classification process: 1) Information identification, 2) assignment of ownerships, responsibilities and usage guidelines, 3) handling of information assets.

The standard classification scheme uses a hierarchical model with different categories. It is vital that organizations do not use too many classification categories due to the increase of complexity. When the complexity becomes higher the implementation becomes harder and uneconomic (ISO/IEC, 2013b). A typical organization may have three to five levels of classification. According to Axelrod, Bayuk, and Schutzer (2009), a common classification scheme is the one used by the US military. They used a hierarchical approach with three levels of classification: Top secret, secret and unclassified (Axelrod et al., 2009).

In Sweden, regulation for information classification can be found in MSBFS2009:10, where one part in the fourth paragraph is about information classification and translates to a governmental agency is required to *"classify its information with reference to requirements on confidentiality, integrity, and availability"*. In an existing recommendation published by the Swedish Civil Contingencies Agency, the classification scheme has four levels of consequence (from serious, via significant, moderate, to none or insignificant), for the aspects of confidentiality, integrity, and availability (Oscarson & Karlsson, 2009, Oscarson, 2009). Glynn (2011) presents a similar work but instead focuses on level of impact and level of classification instead of security aspect, see Figure 2.

Level of Classification	Levels of Impact
Top Secret	Exceptionally grave damage
Secret	Grave damage
Confidential	Damage
Restricted	Undesirable effects

Figure 2: Levels of classification.

### 2.3.1 Guideline for classification

Since information is important, a suitable level of protection is necessary (Al-Fedaghi, 2008, Axelrod et al., 2009, DuraiPandian & Chellappan, 2006, Feinberg, 2004, Fibikova & Müller, 2011, ISO/IEC, 2013b, Seifert & Relyea, 2004, the Swedish National Audit Office, 2014). To ensure adequate information security, classification guidelines are needed (Bergström & Åhlfeldt, 2014, Collette, 2006, Glynn, 2011, ISO/IEC, 2013b, Oscarson, 2009).

A good guideline should be reasonable, understandable and practicable (Verdon, 2006), and according to Fibikova and Müller (2011), ISO/IEC (2013b), Glynn (2011), Parker (1996), so should a classification scheme as well. The guideline should state what should be classified, this is referred to as the *what*. In both ISO/IEC 27002 and the Swedish recommendation, it is assumed that all information handled within an organization is classified (ISO/IEC, 2013b, Oscarson, 2009).

In ISO/IEC 27002:2013, examples for what a good classification guideline should answer exist. The first thing a guideline should do is stating the goal of classification, this is referred to as the *why*. This is defined as "*to ensure that information receives an appropriate level of protection in accordance with its importance to the organization*" (ISO/IEC, 2013b).

In order to ensure that information is classified, someone has to be responsible for the classification process. Within an organization, this task may be delegated to different key roles such as the information owner, system owner and similar roles even though ultimately, the organization executives is responsible (ISO/IEC, 2013b, Oscarson, 2009).

A guideline should state when the classification process should begin and, since information may change value (Al-Fedaghi, 2008, Axelrod et al., 2009, DuraiPandian & Chellappan, 2006, Glynn, 2011, ISO/IEC, 2013b, Oscarson, 2009, Virtanen, 2001) it also needs to state when information needs to be reclassified, this is referred to as the *when*. A classification scheme should include criteria for review, covering the information lifecycle (ISO/IEC, 2013b).

Lastly, the guideline should state how the information should be classified, this is referred to as the *how*. While several authors Baškarada (2009), Collette (2006), J. H. P. Eloff (1996), Feuerlicht and Grattan (1989), Fibikova and Müller (2011), Oscarson and Karlsson (2009), Parker (1996), Farn, Lin, and Lo (2008), recommend the use of classification scheme, only ISO/IEC 27002:2013 and the Swedish recommendation, explicitly state that a classification scheme should be used (ISO/IEC, 2013b, Oscarson, 2009). To secure that information is treated the same way within an organization, ISO/IEC 27002:2013 states that "*the scheme should be consistent across the whole organization so that everyone will classify information and related assets in the same way, have a common understanding of protection requirements and apply the appropriate protection*" (ISO/IEC, 2013b).

## 2.4 System security

According to Pfleeger and Pfleeger (2006), a system is only as strong as its weakest point, therefore all aspects of system security need to be considered. An attacker must have a method, an opportunity and a motive. If one of these is missing, no attack will occur. The method refers to an attacker's ability to perform the attack, such as his/her tools and knowledge. Opportunity refers to access and time-frame. Lastly, motive refers to an attacker's reasons for the attack – this can be both material and non-material (Pfleeger & Pfleeger, 2006).

Information assets are liable to both intentional and unintentional threats while processes, systems and people have inherent vulnerabilities (ISO/IEC, 2013b). Threats can come from both the inside and the outside of the organization. Internal changes, such as new business processes, or external changes, such as new regulations, might create new risks for information systems. With security controls information assets can be protected (ISO/IEC, 2013b). The ISO/IEC 27005:2011 contains numerous examples of threats, motivations, vulnerabilities and possible consequences (ISO/IEC, 2011).

The relationship between threats, controls and vulnerabilities is described by Pfleeger and Pfleeger (2006) as *"a threat can be blocked by control of a vulnerability"*. A scenario could be the following: An information asset, in this case a network connection, has a vulnerability: unprotected communications lines. A threat that exploits this vulnerability could be eavesdropping. According to Pfleeger and Pfleeger (2006), the following four kinds of threats exist:

- **Interception:** An unauthorized person gains access to an asset.
- **Interruption:** An unauthorized person makes an asset unavailable or unusable.
- **Modification:** An unauthorized person tampers with an asset.
- **Fabrication:** An unauthorized person creates false information.

A control is used as a protective measure (Pfleeger & Pfleeger, 2006), often referred to as security control (ISO/IEC, 2013b). For the previous scenario this could be securing the cabling (ISO/IEC, 2013b). ISO/IEC 27002 contains 14 security control clauses, from information security policies and supplier relationships to cryptography and access control. These clauses contain 35 main security control categories and 114 security controls. Each main security control category contains *"a control objective stating what is to be achieved"* and *"one or more controls that can be applied to achieve the control objective"* (ISO/IEC, 2013b).

In a review made by the Swedish National Audit Office (2014), both the National Defence Radio Establishment and the Swedish Security Service established that Swedish governmental agencies are lacking in information security. In the review, the National Defence Radio Establishment determines that the security controls most often do not correspond to the information that they are supposed to protect. Flaws discovered during their security assessments can lead to an attacker taking control over the IT-environment. In the same review, the Swedish Security Service determines that the inadequate security can lead to major consequences, since some of the information can be a threat to national security (the Swedish National Audit Office, 2014).

## 2.5 Related work

ISMS in general is an under-researched area (Siponen, 2006), and, according Bergström and Åhlfeldt (2014), Everett (2011), Oscarson and Karlsson (2009), research about information classification itself is very limited and not an academic pursuit (Fomin, Vries, & Barlette, 2008). However, several authors (Axelrod et al., 2009, Everett, 2011, Fibikova & Müller, 2011), point out that the process of information classification is not something new and that its necessity has been stated (Everett, 2011). Instead most research focuses on the later part of ISMS such as risk management (Everett, 2011). While information classification is an old practice from the military domain (Axelrod et al., 2009), it is still considered young in the private sector (Everett, 2011).

In 2014 the Swedish Civil Contingencies Agency made an extensive study of the Swedish governmental agencies' work with information security. The results from this study were sorted into different categories of information security, where each category represents a part of the fourth paragraph in the MSBFS2009:10. Further, some of the results were sorted in accordance to the size of the agencies (0-50, 51-500 and 501+). These sized-based results were only presented when the difference between the categories was deemed relevant (the Swedish Civil Contingencies Agency, 2014). The study shows that only 43% of the 227 agencies had decided upon an information classification scheme, that 24% of the agencies were still working on the development of such scheme and that 33% of the agencies did not have any scheme for handling information classification issues. When this result was further analysed it showed a significant difference between large agencies (501+ employees), medium-sized agencies (51-500) and small agencies (0-50). 57% of the large agencies, and 41% of the medium-sized agencies respectively, had decided upon a classification scheme whereas only 20% of the small agencies had decided upon such a scheme (the Swedish Civil Contingencies Agency, 2014). The study also shows that only 59% of the agencies knew who was/were responsible for information classification issues within their organization, as well as that only 41% of the agencies know when information is supposed to be classified in accordance to point of time or situation (the Swedish Civil Contingencies Agency, 2014).

According to Hilton (2009), information labelling is a commonly used method for information handling, but often these labels are not fully understood. Different organizations use different ways of classifying and labelling it. Hilton (2009) suggests the use of a labelling-scheme with 13 different icons from Creative Commons. Several authors (J. H. P. Eloff, 1996, Feuerlicht & Grattan, 1989, Parker, 1996, Farn et al., 2008), provide guidelines, frameworks and models for information classification while only Fibikova and Müller (2011) suggest alternative methods for information classification: one process-oriented approach and one application-oriented approach.

Several authors (Al-Fedaghi, 2008, DuraiPandian & Chellappan, 2006, Hayat, Reeve, Boutle, & Field, 2006, Virtanen, 2001), suggest methods for automation of classification using old information. There are also some studies mentioning issues with information classification (Bergström & Åhlfeldt, 2014), how to handle issues during the process (Collette, 2006) as well as tips for implementation (Glynn, 2011).

### 3 Problem description

Information security is essential in a modern-day society and access to reliable information in real-time is critical. Information is not only important but can also be sensitive, like patient journals (the Swedish National Audit Office, 2014). The security demands for information assets are getting higher due to bigger and more complex IT-architectures (Bechtsoudis & Sklavos, 2012). Many organizations relies on security certification based on different ISMS standards to protect their IT-environment, such as those published by ISO/IEC (Siponen & Willison, 2009). According to Mendyk-Krajewska and Mazur (2010), it is difficult to achieve and maintain high level system security due to rapidly increasing threats and new attack vectors caused by new technologies. To protect information assets, adequate security controls are needed (Pfleeger & Pfleeger, 2006). These security controls could be access restriction in computer systems, protecting valuable documents or encryption for network communication, protecting sensitive data (ISO/IEC, 2013b). In order to ensure that information has an appropriate level of protection, based on its value to the organization, information classification is needed (Al-Fedaghi, 2008, Fibikova & Müller, 2011, ISO/IEC, 2013b, Glynn, 2011, Axelrod et al., 2009).

While several authors (Axelrod et al., 2009, Everett, 2011, Fibikova & Müller, 2011, Glynn, 2011), highlight that information classification is not something new, the existing research about information classification is very poor and lack scientific verified implementations (Bergström & Åhlfeldt, 2014, Everett, 2011, Oscarson & Karlsson, 2009).

In Sweden, the governmental agencies are required to classify information following the ISO/IEC 27001 and ISO/IEC 27002 (Oscarson & Karlsson, 2009, MSBFS2009:10, 2009), which do not include a classification scheme (ISO/IEC, 2013b), instead the ISO/IEC 27002 only provides guidelines and Bayuk (2010) describes the general guidelines provided by standards as too generic for complex environments. There is a recommendation to use a classification scheme created by the Swedish Civil Contingencies Agency and the Swedish Standards Institute (Oscarson & Karlsson, 2009), but even though a recommendation exists there are still problems with the classification process and according to Baškarada (2009) and Parker (1997), it is generally problematic to develop a classification scheme. A study done by the Swedish Civil Contingencies Agency shows that the Swedish governmental agencies have inadequate information security (the Swedish Civil Contingencies Agency, 2014). Bergström and Åhlfeldt (2014) have identified numerous issues with information classification, divided into six categories. These categories consist of different management factors, human errors, policies, technology and external influences. According to Fibikova and Müller (2011), deciding on the size of information can be a problem: big pieces of information can lead to a general, inadequate classification while small pieces of information make the classification process unmanageable. The information lifecycle is also problematic, since information may change value over time, thus an organization need to address the issue of reclassification (Al-Fedaghi, 2008, Fibikova & Müller, 2011, Glynn, 2011, ISO/IEC, 2013b, Oscarson, 2009, Virtanen, 2001).

According to Åhlfeldt et al. (2015) and the Swedish National Audit Office (2014), the governmental agencies lack the mean to compare and evaluate their information security with each other. Several of the participants in the study by Åhlfeldt et al. (2015), highlight the fact that they do not know if their security level can be considered safe. According to Wrona and Hallingstad (2011), the fact that classification levels differ between organizations makes it hard to share and compare information.

While old information could be used for automatic classification of information, like suggested by DuraiPandian and Chellappan (2006), Hayat et al. (2006), Virtanen (2001), humans would still have to be a part of the process (Everett, 2011). This leads to human related issues and according to Booyesen and Eloff (1995), Everett (2011), Glynn (2011), Ku, Chang, and Yen (2009), Parker (1996), a common issue is subjective judgement. According to Parker (1996), the classification schemes can be too complex, while Puhakainen and Siponen (2010), Åhlfeldt et al. (2015), emphasize employees' lack of skills and Axelrod et al. (2009), the lack of guidance. This can lead to information being over- or under-classified (Axelrod et al., 2009). According to a review by the Swedish National Audit Office (2014), both the National Defence Radio Establishment and the Swedish Security Service consider information within governmental agencies as not well-protected, which should mean that the information is under-classified.

There is also problems within the organizations themselves. Coles-Kemp (2009) identifies the absence of a clearly defined "top" within organizations as well as the need to understand the patterns of power and its synergy with ISMS in organizations. Collette (2006) mentions the lack of authority for leaders of the information classification process while Janczewski and Xinli Shi (2002) and Hilton (2009), point out the need for support from the senior executives. Kajava, Anttila, Varonen, Savola, and Röning (2007) also mention the lack of commitment from senior executives. Everett (2011), Hilton (2009), Ku et al. (2009) mention the need for involvement within the organization to increase security awareness. In order to increase the security awareness organizations need to understand the "what", the "why" and the "how". Basically this comes down to: What information to protect, why the specific information? And how to protect the information (Hilton, 2009)? According to Humphreys (2008), organizations need to understand that they are ultimately responsible for information security. Organizations might also need a better control of information assets. Janczewski and Xinli Shi (2002) especially mention the need for clearly defined responsibilities and ownership. In general, information classification is considered problematic in organizations (Axelrod et al., 2009) which also includes governmental agencies (the Swedish Civil Contingencies Agency, 2014).

Due to the complexities of information classification, as described above, and the lack of research regarding information classification guidelines used by the Swedish governmental agencies, this work aims to investigate the existing information classification guidelines within the agencies and, to some extent, which problems that the agencies have encountered and how these problems have been solved.

### **3.1 Research question**

The main goal of this work is to answer the research question:

*Which kind of classification guidelines exists for information classification in Swedish governmental agencies?*

### **3.2 Delimitation**

The thesis project is delimited to the administrative authorities which constitute the largest group of Swedish governmental agencies (SCB, 2015). According to SCB (2015) there are 245 administrative authorities and only those fulfilling a certain set of requirements were selected

to the survey. These requirements were: They need to handle their own administration, they need to have at least one employee and they need to be affected by MSBFS2009:10. In the second paragraph in MSBFS2009:10 the following agencies were excluded: the Armed Forces, the Government Offices, the Swedish committees and to some extent missions abroad.

## **4 Research method**

This chapter presents the research methods applied in this thesis project: a literature review and a survey. The selected methods are described and motivated in relation to the research question. Further, the methods chosen are discussed in terms of their validity.

### **4.1 Research design**

Researchers can use a combination of methods to be able to analyse data with different views (Hartley, 2004) and according to Berndtsson, Hansson, Olsson, and Lundell (2008), reviewing literature is necessary to gain an understanding of an area. Creswell (2009) propose the use of an explorative mix-method approach to explore a broad research area, focusing on the qualitative findings, matching the research question of this thesis. According to Wohlin et al. (2012), using a survey is the most common way to collect qualitative or quantitative data. In order to reach out to a large number of respondents, a survey is considered a suitable method (Berndtsson et al., 2008). While interviews would be able to provide data regarding the research subject, it would limit the amount of data, since interviews by nature are made with fewer participants (Trost, 2010).

The research presented in this thesis has its roots in the lack of research on the application of information classification guidelines in Swedish governmental agencies and, in particular, how the guidelines can be improved to reflect the needs of their users. To investigate the state of the art of the handling of information classification issues at Swedish governmental agencies, an explorative study has been carried out. Due to the current sparse research conducted within the subject, an open-minded strategy toward the research subject was applied where focus was put on conducting a first pre-study to chart the current classification guidelines.

First, a literature review was conducted to investigate possible problems with information classification issues and their potential solutions. Based on this information, a survey was planned and a questionnaire distributed to all administrative authorities in Sweden. Finally, the data collected through the questionnaire as well as from the literature review was used to form the analysis and conclusions of the study.

To make sure that the investigations provide meaningful data, it is of utmost importance that appropriate research methods are chosen in relation to the research question. Thus, well-established strategies for the literature review and the survey have been chosen and followed during this thesis project. It is further important to choose relevant data analysis strategies to be able to extract valid conclusions from the data. The following sections describe these strategies and reflect upon their employment and an overview of the research design can be found in Figure 3.

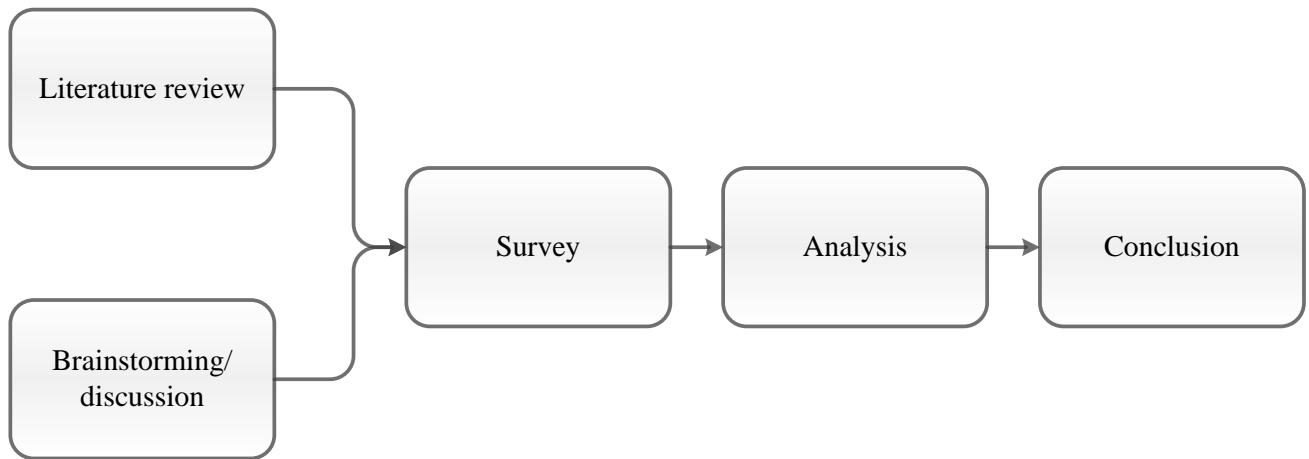


Figure 3: Model for research design.

## 4.2 Literature review

In order to investigate the state of the art of the research context, to design the survey and questionnaire as well as to analyse the survey results, continuous literature reviews have been conducted in relation to the research progression during the thesis project. According to Webster and Watson (2002), the search for relevant literature can be conducted in three steps:

1. Begin the literature search by selecting leading journals and conferences with good quality.
2. Proceed with going backwards and review the citations from the articles found in the first step.
3. Go forward and identify relevant articles that have been cited in the previous step.

This approach resulted in the acquisition of a large set of material that has been investigated, and key references within the research area have been identified. The literature search started with exploring the history and state of the art of the research on information classification and information security, of which a summary can be found in chapter 2. Keywords such as "*information security*", "*information classification*", "*data classification*" and "*security classification*" were used.

In relation to literature reviews, the question of "completeness" is most often prevalent, i.e. when has enough material been collected. According to Berndtsson et al. (2008), it is impossible to know how complete the collected information base is. However, the question should not be discarded due to its importance in terms of validity. To address this issue, the reader is provided with the strategy used, increasing the transparency of the process and, hopefully, increasing the reader's trust in the information provided.

### 4.3 Survey

As stated by Wohlin et al. (2012), the most common means of collecting qualitative or quantitative data are through interviews or questionnaires. To be able to answer the research question, i.e. *"Which kind of classification guidelines exists for information classification in Swedish governmental agencies"*, it was decided to distribute a questionnaire to those agencies. A questionnaire was selected as data collection method due to the possibility of reaching a larger set of respondents than if interviews had been conducted, thus increasing the possibility of answering the research question.

According to Wohlin et al. (2012) and Berndtsson et al. (2008), a survey is a method for exploring a phenomenon together with a large set of respondents who are requested to describe, compare or explain their knowledge, attitudes and behaviour regarding this particular phenomenon. The results from the survey can provide the researcher with descriptive and explanatory conclusions that can be generalized to the population from which the sample was taken (Wohlin et al., 2012). The advantage is that through very limited means, the researcher can collect answers from many respondents and thus quickly extract an overview of the issue of concern (Berndtsson et al., 2008). However, as with all research methods, there are downsides. For example, it is very difficult to investigate very complicated issues with the help of online surveys due to the lack of a direct two-way communication between the researcher and the participant. Moreover, the researcher cannot possibly know that it is the targeted person who actually answers the questions and, often, the participation rate is low (Berndtsson et al., 2008).

To delimit the scope of the possible downsides with the survey method, the questions used in the study were designed to be clear and short to avoid possible misinterpretations. The participants were prompted to contact the thesis author if they had any questions regarding the questions or the study as a whole (both the e-mail, address and phone number were provided to the participants). The number of questions (9) was also limited to better motivate the participants to actually answer them. As the research question covers a broad research area, a mixed method survey design was appropriated in order to capture both quantitative and qualitative data from the participants (Creswell, 2009). Within this survey setting, this approach was manifested in the inclusion of both free-text and "Yes/No" questions. A translated version of the questionnaire can be found in Appendix A and the motivation for each question can be found in section 4.3.1

Through the Swedish Statistical Database website (SCB, 2015), all existing governmental agencies in Sweden were found. The research conducted were limited to administrative agencies, the largest group of agencies in Sweden. In 2015, 245 agencies existed, and were contacted by email at the beginning of February 2015 where the purpose of the study and the handling of the data to be collected were explained, as well as the questions included. For example, the participants were informed that the answers would be handled anonymously and that the collected results could be included in future research papers. The participants were requested to hand in their answers before the 1st of April 2015. A gentle reminder to those who had not answered the questionnaire was sent by email on the 14th of April. Those who were interested in the survey results were prompted to contact the thesis author at the beginning of September of 2015 to be sent a summary of the collected results.

### 4.3.1 Questionnaire

According to Creswell (2009), the questionnaire should be related to the research question. By doing a literature review, literature supporting the questionnaire was identified. The literature was then later discussed during a brainstorming session with the supervisor of the thesis project, in order to formulate appropriate questions, suitable for the target audience.

In a previous survey about information security by the Swedish Civil Contingencies Agency, governmental agencies were categorised in three sizes (based on the number of employees): 0-50, 51-500 and 501+ (the Swedish Civil Contingencies Agency, 2014). To be able to compare the results with previous work, the following question was used:

*1. How many employees are working at the agency? (Select one alternative) 0-50, 51-500 or 501+.*

In ISO/IEC 27002:2013, it is recommended that the information owner is responsible for the information classification but the task may also be delegated to others (ISO/IEC, 2013b). In the recommendation published by the Swedish Civil Contingencies Agency, it is stated that the organization executives are ultimately responsible for information classification even though the task often is delegated to different key roles within the organization. Examples of these roles are: information, process or system owner and similar roles (Oscarson, 2009). To identify the delegation of who (if someone is responsible for information classification at the agency), the following question was used:

*2. Is it specified who is responsible for information classification at the agency?*

In MSBFS2009:10, it is specified that the agencies are required to classify their information. ISO/IEC 27002:2013 states that classification should be a part of an organization's processes (ISO/IEC, 2013b). The classification should also be updated when changes to value, sensitivity and criticality occur (Al-Fedaghi, 2008, Fibikova & Müller, 2011, Glynn, 2011, ISO/IEC, 2013b). If an organization does not know when to classify their information or when it should be reclassified, their guidelines would be defective and so their participation in the survey would no longer be necessary. In order to find out when information is classified and reclassified, the following question were used:

*3. Is it clarified when information shall be classified and when reclassification should take place? If the answer is Yes", please describe your reasoning. (If "No" thank you for your participation!)*

According to several authors (Baškarada, 2009, Collette, 2006, J. H. P. Eloff, 1996, Feuerlicht & Grattan, 1989, Fibikova & Müller, 2011, ISO/IEC, 2013b, Oscarson, 2009, Parker, 1996, Farn et al., 2008), it is recommended to use a classification scheme for information classification. In order to investigate the usage of classification schemes within the governmental agencies, the following question was used:

*4. Do you use a classification scheme for information classification? If not, have you commenced such a scheme implementation?*

A guideline should be reasonable, practicable and easy to use (Verdon, 2006), and according to Fibikova and Müller (2011) and Glynn (2011), so should a classification scheme as well. To identify the usability of the governmental agencies classification schemes, the following

question were used:

*5. Do you experience that it is easy or complicated to use your classification scheme? Please explain your answer if possible.*

In Sweden, the Swedish Civil Contingencies Agency has published a recommendation for information classification, containing a classification scheme (Oscarson, 2009). To investigate if the governmental agencies use this recommendation, the following question was used:

*6. Is your classification scheme based on the recommendation published by the Swedish Civil Contingencies Agency? If "Yes" have you made any modifications to it? If "No" what is your scheme based on?*

In order to be able to analyse the governmental agencies' classification guidelines, the following question was used:

*7. Would we be able to take part of your classification scheme and any documentation that explains how to use it? Please attach the scheme and any guidelines if possible.*

Each level of classification should be given a name appropriate for the classification context (ISO/IEC, 2013b). A typical organization may have between three to five levels of classification (Axelrod et al., 2009) and according to Glynn (2011), unclassified is not considered an official classification level. To investigate the number of classification levels used by the governmental agencies, the following question was used:

*8. How many levels of classification are you using?*

In the ISO 27000-series information security is focused around the CIA-triad ISO/IEC (2013b) and according to Pfleeger and Pfleeger (2006), the goal of security lies in the aspects of CIA. The Swedish governmental agencies are required to classify information with reference to requirements on confidentiality, integrity and availability, while other aspects are optional, such as traceability (MSBFS2009:10, 2009). To identify how the governmental agencies manage these aspects, the following question was used:

*9. Do you take confidentiality, integrity, availability and traceability into consideration or only some of them or do you use other aspects? Please describe which and your reasoning.*

#### **4.4 Validity and ethics**

According to Wohlin et al. (2012), the validity of a study refers to the trustworthiness of the results, meaning to which extent the results are true for the population of interest and not biased by the researcher's lack of objectivity. They further state that sometimes threats to validity have to be accepted, but that it is of utmost importance that the researcher acknowledges them and tries to minimize these threats, both when conducting the study and when analysing the results.

According to Wohlin et al. (2012), there are four different aspects of validity that a researcher should consider: construct validity, internal validity, external validity and reliability.

Construct validity implies that the researcher should take measures to make sure that the study really investigates or measures the research question. When conducting a survey, it is difficult, or impossible, to know how the participants interpret the questions and their understanding of

them. However, the participants were informed that they should contact the study responsible (i.e. the thesis author) if they had any questions regarding the study as a whole or the questions posed. Moreover, to avoid misunderstandings, the questions were formulated as clear and unambiguous as possible.

Internal validity is concerned with establishing relationships between variables. If the researcher does not know which factors affect the relationship that is being studied it might, in turn, affect the validity of the study (Wohlin et al., 2012). For example, if the participants in the study perceive the questionnaire as tedious, are afraid that their answers will affect them in some way or if some unanticipated event happens during the study that interrupts them, the internal validity of the study might be threatened. Due to the fact that the questionnaire was distributed online, the control over the internal validity of the study was limited. However, the questions were kept short, limited in number and were designed to be as unambiguous as possible to ensure some degree of internal validity.

External validity is about the possibility of generalizing from the study findings so that others might find the results interesting. Threats to this kind of validity are, for example, that the number of study participants is too limited and that the environment of the study is too specific to draw general conclusions from. In relation to the study presented in this thesis, a relatively large number of participants answered the same set of questions through the questionnaire distributed, thus guaranteeing some external validity. Moreover, as suggested by Lincoln and Guba (1985), the researcher should ensure that sufficient contextual information about the study is given to enable the reader to draw conclusions of his/her own regarding the similarities and differences between different studies, thus promoting external validity.

The fourth and last aspect of validity listed by Wohlin et al. (2012) is reliability. Reliability is concerned with providing the needed details regarding the study so that, would the study be repeated, in the same context, with the same method and with the same participants, similar results would be obtained (Wohlin et al., 2012). To ensure reliability, the process followed for the literature review has been documented, the questions posed in the questionnaire have been included (see Appendix A), the number of participants and where they were found have been provided, together with information such as the estimated length of the data collection sessions.

With regards to research ethics, the four ethical requirements listed by the Swedish Research Council (Vetenskapsrådet, 2002) have been adhered to when conducting the survey and when handling and analysing the results. The participants in the survey were informed of the study and the purpose of the research conducted. The instructions given to the participants further informed them that the data collected from the survey would not be used outside the current research context, as well as that the data collected would be handled anonymously.

## **4.5 Alternative methods**

As stated by Benbasat, Goldstein, and Mead (1987), each research method has advantages and disadvantages and it is not always evident how to choose the best strategy. Hartley (2004) argues that many researchers strive to use a combination of methods to carefully analyse the data from different views. The survey method, combined with continuous literature reviews, were deemed to constitute a good strategy for addressing the research question due to the possibility of grasping the state of the art of the research subject as well as the possibility of collecting

the knowledge and opinions of a large number of participants. However, it would have been interesting to triangulate the survey findings with interviews as well to extract more elaborative results. As previously stated, the number of questions included in the survey was limited in order to possibly increase the number of responses. During an interview setting, it would perhaps have been possible to ask additional questions, as well as to collect more profound opinions from the participants.

## **5 Results**

This chapter presents the results of the survey, starting with an overview of the governmental agencies followed by an overview of the quantitative data which are further divided into small (0-50 employees), medium-sized (51-500 employees) and large agencies (501+ employees). Further, the qualitative data is presented in a separate section. The chapter also presents an analysis of the survey findings.

### **5.1 Overview**

In Figure 4 all the Swedish administrative authorities contacted are divided into different categories. Of the 245 agencies contacted, only 144 agencies of those who responded to the survey fulfilled the requirements for participating in the survey in terms of the selection criteria, see Section 3.2. The other agencies' reasons for not participating are presented as well.

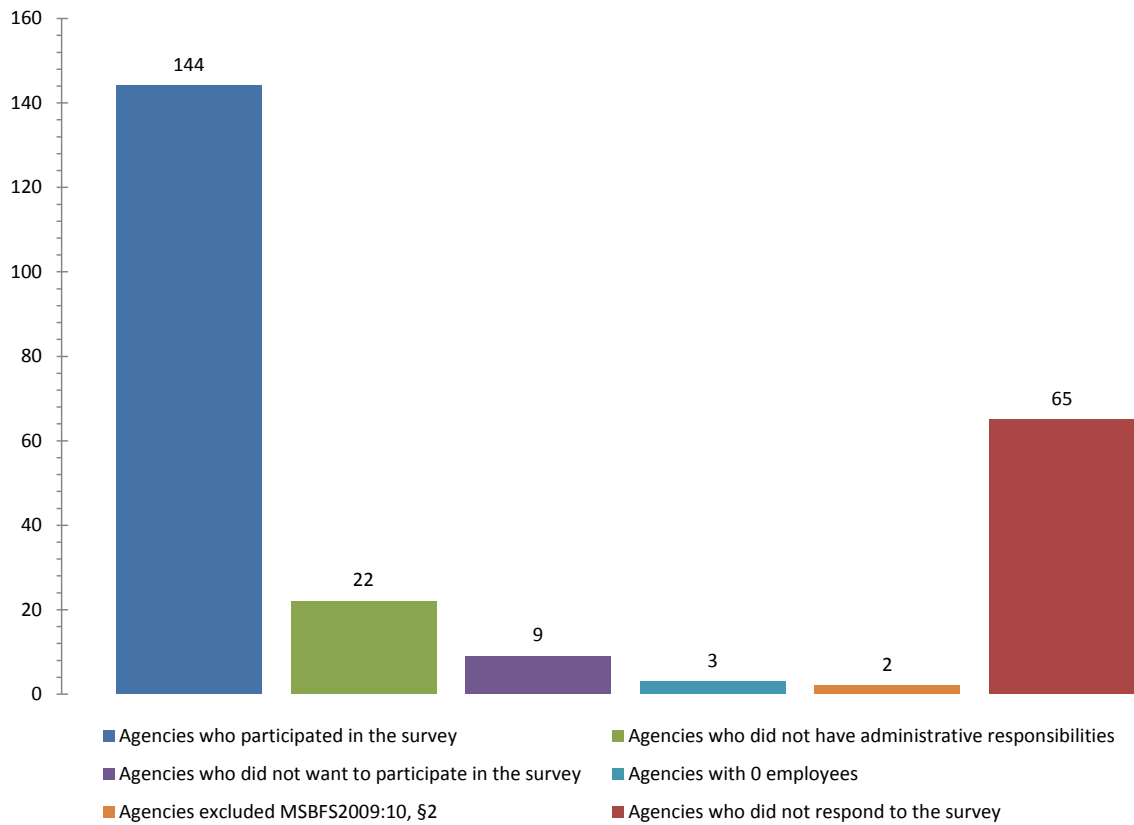


Figure 4: Swedish administrative authorities.

In Figure 5, the participating 144 agencies are divided into three size-based categories – small, medium-sized and large being 34 (24%), 65 (45%) and 45 (31%) respectively.

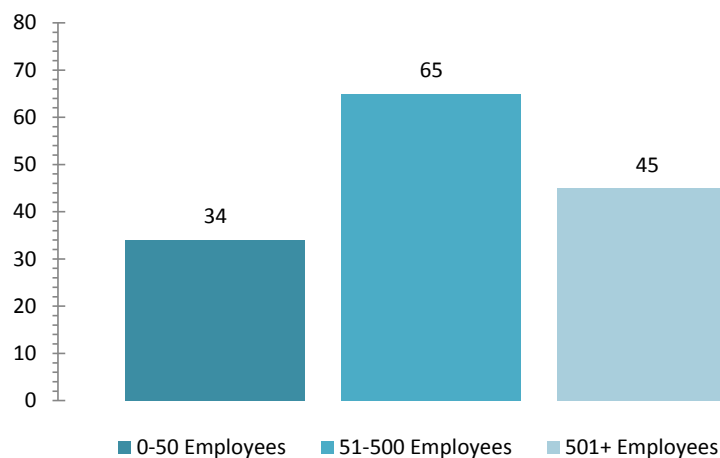


Figure 5: The number of small, medium-sized and large agencies.

## 5.2 Quantitative results

An overview of the "Yes/No" answers to question 2 (Q2) and question 3 (Q3) are presented in Figure 6 and Figure 7. These questions were 2) *"Is it specified who is responsible for information classification at the agency?"* and question 3) *"Is it clarified when information shall be classified and when reclassification should take place?"*. These results have been further analysed in accordance with the sizes of the agencies. A more qualitative analysis of the answers to these questions is presented in Section 5.3. Results from agencies who did not fulfill the requirements of the study were disregarded and are not presented.

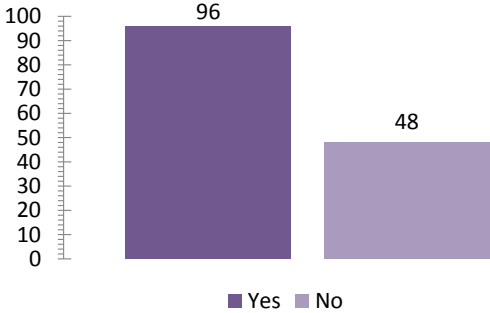


Figure 6: Q2 – Overview.

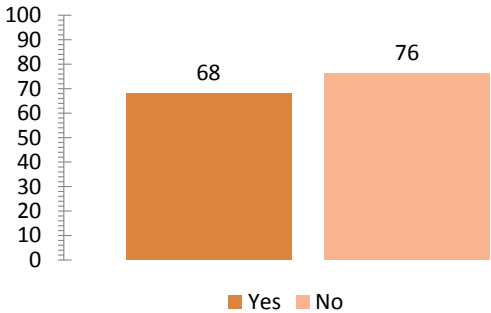


Figure 7: Q3 – Overview.

The results from question 2 and question 3 are further divided into sized-based categories. In Figure 8 and Figure 9 the results for the small agencies are presented.

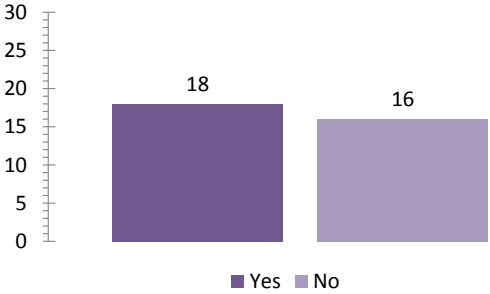


Figure 8: Q2 – Small agencies.

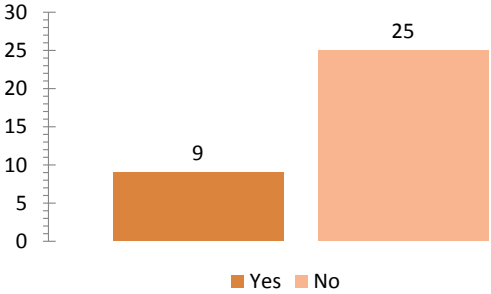


Figure 9: Q3 – Small agencies.

In Figure 10 and Figure 11 the results for the medium-sized agencies are presented.

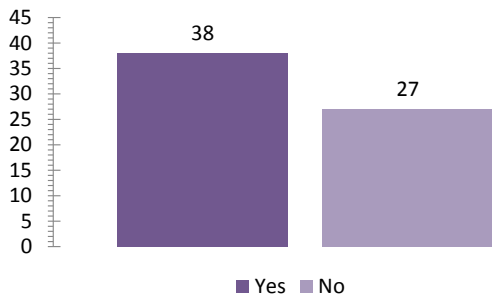


Figure 10: Q2 – Medium-sized agencies.

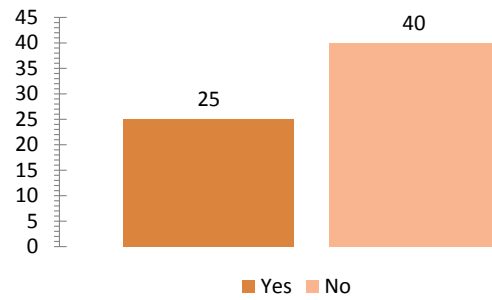


Figure 11: Q3 – Medium-sized agencies.

In Figure 12 and Figure 13 the results for the large agencies are presented.

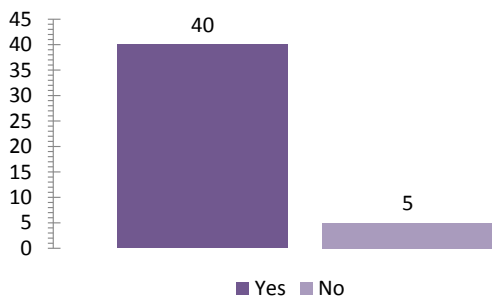


Figure 12: Q2 – Large agencies.

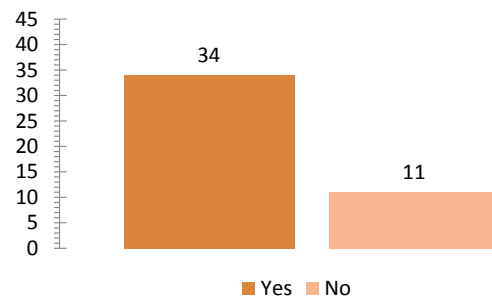


Figure 13: Q3 – Large agencies.

The results show that only 96 of the 144 agencies (67%) have at least one employee who is responsible for information classification. When this result is further analysed, the results can differ between agencies depending on their size. For small and medium-sized agencies the results were similar with 18 out of 34 (53%) and 38 out of 65 (58%) respectively. However, for large agencies the results were much higher, 40 out of 45 (89%) have at least one designated employee in charge of information classification. While the MSBFS2009:10 states that all agencies should classify their information, it might be difficult to actually confirm that the information at the agency has been classified when no one is responsible for the classification task. Ultimately, this task would fall on the agency’s executives, since they are responsible for the agency adhering to existing laws and regulation, this would make them accountable for the information classification as well, or the lack of.

The results further show that even fewer agencies have guidelines regarding when information classification and reclassification should be conducted. The results show that only 68 out of 144 (47%) have guidelines regarding the question. Much like the previous question, the results differ depending on size. Here, the results for the small and medium-sized agencies are still quite similar. With the small agencies having the lowest number with 9 out of 34 (26%) and the medium-sized agencies with 25 out of 65 (38%). However, the large agencies, similar with the previous question, have a higher result. Here, 34 out of 45 (76%) have a guideline for classification and reclassification.

The result may be a bit misleading, since it can be interpreted as that the agencies do not know how to classify information at all. This is most certainly not the case. Since the question handles both the initial classification and reclassification, agencies that perform the first initial classification but no reclassification would answer no. This could be one of the reasons for the high amount of "No" answers. Another possible reason could be that MSBFS2009:10 does not explicitly mention the need for reclassification, although, it specifies the use of the ISO 27000-series, which in turn describes the need for reclassification during the information life cycle.

## 5.3 Qualitative results

In this section qualitative data regarding the *who*, the *when*, the *what*, the *how*, and the *why* are presented, see section 2.3.1 for why these particular issues were selected. Answers to these questions have been identified by analysing questionnaire results: 76 documents consisting of 679 pages provided by 54 governmental agencies. These 54 agencies consisted of 7 small agencies, 17 medium-sized agencies and 30 large agencies.

### 5.3.1 Who

The results from the survey show that there are differences between agencies regarding who is responsible for the information classification. In general, the result show that either a specific role or every employee is responsible for the information handling. For example, one agency answered:

*"Every employee who creates or identifies new information is responsible for classifying the information."*

This statement illustrates that every employee has a responsibility for classifying information. However, other agencies follow a different approach, appointing for example an information or process owner as responsible for the classification process. Yet, despite such task delegation within the agencies, there are differences regarding, for example, the reappointment of the classification tasks. To illustrate this, one agency stated that:

*"Every information owner is responsible for classifying his/her information."*

This highlights the importance at this particular agency to appoint a specific role at the agency to deal with the information classification tasks. However, other agencies assign the classification responsibilities in a more hierarchical way, nominating the process owner as in charge of the classification tasks, who, in turn can delegate this responsibility further within the agency. This is illustrated by the following statement:

*"The process owner is the information owner for information that belongs to the process. The information ownership may be delegated. The department manager is the information owner for information not belonging to a process. The information owner is responsible for the [...] information classification."*

For information with shared ownership, e.g information used by multiply information owners stored in the same system, one agency stated that:

*"Systems containing information from more than one information owner, one information coordinator is appointed. The information coordinator is responsible for the classification of the combined information."*

One agency mentioned that, even though it is specified who is in charge of the information classification, it is questionable if this specific person is aware of this responsibility.

*"Every system owner is responsible for both classification and risk assessment of his/her information. But the question is if they are aware of it."*

The survey results described in the section above illustrate that there are differences regarding how governmental agencies handle their information classification tasks. Some appoint a specific role or employee to perform such tasks, whereas others delegate this responsibility in accordance with the process staff hierarchy. When analysing the survey results, no specific trend based on agency sized could be identified. Both approaches for handling the information were identified regardless of the size of the agencies.

Important to note is that the agencies that described their guidelines for handling information explicitly expressed a protocol for who should handle information classification at the agency, but more research is needed in order to investigate if such protocols are actually followed or not.

### **5.3.2 When**

Regarding when the information classification and reclassification should be performed, all agencies answered that they have such a scheme. However, the results differ when it comes to when reclassification should be further analysed, and here, two strategies were identified. The first mentions that reclassification should be performed when information has been changed, destroyed, published or in other ways modified:

*"Information should be classified when the information arrives at the agency or when information is created or in other ways produced. Reclassification may occur when, for example information is modified, becomes obsolete, have been requested or published."*

Secondly, the time aspect is highlighted, specifying that the information classification should be continuously reviewed.

*"Classification should be done when new information is created, for example during development of an IT-system or when documents are established [...]. ISMS define a classification as short-termed and because of that, information should be reclassified regularly."*

While the agencies cover the initial classification, i.e. the first time the information is used within the organization, many fail to cover the reclassification process. It is important to note for those who cover the reclassification process that, while change of information value is covered, agencies tend to miss changed requirements on the information itself as a reason for reclassification. Even if it is considered accounted for as information modification, they do not explicitly mention it. Another interesting finding is that, while time is one factor for reclassification, not all agencies have a defined time-space leading to the question: After how much time should the information be reclassified?

### 5.3.3 What

The agencies participating in the survey state that all information handled within the organization should be classified, regardless of size and form. This is illustrated by one agency's statement:

*"Information exists in every form. It can exist in writing, in a picture, in a photo or video, or be something you say. It does not matter if the information is working material, a draft or material meant for publication."*

While all agencies agreed that information can exist in many forms, the level of detail on what information is differ between the agencies which can be problematic. Although, if the employee is supposed to classify the information, he/she should already know what information is.

### 5.3.4 How

Regarding the subject of how to classify information, all the agencies explicitly stated the use of a classification scheme, with the use of supporting guidelines. By further analysing the classification guidelines, it was identified that information classification should be based on the CIA-triad, as illustrated:

*"Classifications should be done based on the aspects of confidentiality, integrity and availability."*

While all agencies specified that classification should be based on the CIA-triad, an extension exist, adding the aspect of traceability. While further investigating the aspect of traceability, two reason for not using it was identified:

*"We do not use the aspect of traceability. The reasoning for this is that it is not a part of the existing recommendation."*

The second reason that traceability is not considered an aspect of its own but rather something achieved by the CIA-triad, as explained by one agency:

*"We are not using traceability [...] it is include in the CIA-triad."*

The results from the survey, the agencies stated that their classification schemes were relatively easy to use and that the complexity lies in ambiguous requirements and complex systems, rather than using the scheme:

*"What they experience as complicated is understanding the requirements belonging to different levels of classification. They want to know what it means for their specific information or application."*

The agencies also mention the need for educated employees, as described by one agency:

*"The classification scheme is not complicated, but it is new for the employees and may be perceived as strange."*

Regarding levels of classification, three or four levels were identified as the most common, with a few exceptions where five levels of classification were used. Notably, the zero level, often know as "unclassified" was considered a level of its own by agencies specifying the usage of

four or five levels of classification, as illustrated by one agency:

*"We are using four levels of classification, 0-3."*

The agencies generally base their classification schemes on the recommendation published by the Swedish Civil Contingencies Agency. Interestingly, this would indicate that the agencies have rather new classification schemes, considering the fact that the recommendation was published 2009 (Oscarson, 2009).

Although, two exceptions exist. The first exception to this would be agencies cooperating with the Armed Forces, which have a recommendation based on their own regulations, FFS 2003:7. And the second, being agencies who have worked with classification schemes for a long time, this is illustrated by one agency's statement:

*"Our classification scheme has an unknown origin but has been used and improved during the last 15 years."*

While all the agencies provide guidelines for how to use the classification scheme, one agency specificity states that the classification should be done in workshops.

*"Information classification should be done i workshops under supervision of a local information security analysts."*

By doing the classification in a workshop, it might become easier to interpret requirements and increase the consistency to the classification process. Although, this may also require an increased commitment by the organization, allocation more resources and time.

### **5.3.5 Why**

Regarding why information classification should be conducted at the agencies, two statements clearly illustrate different viewpoints on the matter. The answer from one agency highlights the importance of classifying information due to laws and regulations, as well as from internal organizational documents:

*"Information classification is done by the agency in order to fulfil laws, regulations, internal and external requirements."*

However, the answer from another agency stresses the importance of handling such issues due to the value of the information itself:

*"Information classification is done in order to ensure that the information belonging to the agency is handled correctly, based on content and value."*

A combination of both viewpoints was also identified, mentioning both the need for properly protecting the information itself while still adhering to laws and requirements, as described by one agency:

*"Information classification is done to minimize the risk of deformation of sensitive information, intention and unintentional, not being available for authorized personnel or accessible for unauthorized personnel [...]. The classification is based on the requirements and laws of the organization."*

While stressing the importance of following laws, regulations and other requirements, is it enough for the agencies to acknowledge the importance of information classification? While it may be motivational for the agency as a whole, it may fail to motivate the individual employee.

## 6 Conclusion

In this thesis project, the purpose was to identify existing guidelines for information classification followed by Swedish governmental agencies. To do this, 245 governmental agencies were asked to participate in a survey.

The main goal of this work was to answer the research question: *"Which kind of classification guidelines exists for information classification in Swedish governmental agencies?"*

Overall, it seems that the Swedish governmental agencies struggle with information classification, with large agencies being an exception, from a quantitative perspective. Here, a high percentage knows when information shall be classified and who is responsible for doing so.

As described in section 2.3.1, a good classification guideline should be able to answer the aspects of *who, when, what, how* and *why*. The survey show that:

- Either a specific role or every employee should be responsible for the information classification and that the task can be delegated.
- Information should be classified when first encountered in the agency, then revised based certain criterion, such as modification or publication as well as being continuously reviewed.
- All information, no matter form or sized should be classified.
- Classification should be done with a classification scheme, taking the CIA-triad into consideration by educated employees. The scheme should use either three levels of classification, not including the unclassified level, or four levels, including the unclassified level. The classification could be done in workshop-session, providing that resources and time are available.
- Information classification should be done in order to protect information based upon its value and making sure that the agency fulfils laws, regulations, internal and external requirements.

The findings illustrate that, while not always consistent with the ISO-27000 series, good guidelines for information classification exists within the governmental agencies. Thus, answering the research question. The results provide valuable insight, specificity regarding who should be responsible for information classification and how to classify information. While the ISO/IEC 27002:2013 specify that the information owner should be responsible for information classification and that the task can be delegated, a more detailed explanation of how this task can be delegated was provided. For example, by letting every employee be responsible for classification, the understanding for information value could be increased. On the subject of how to classify information it is stated can classification schemes should be used. These schemes

focus on the CIA-triad, sometimes also considering the aspect of traceability. While guidelines of how to use the classification schemes are provided, it does not always cover on how to handle issues while using the scheme. Therefore, doing classification in workshop-sessions or have proper support available, would be recommended. This, on the other hand, could put an economic strain upon the agency.

## **7 Discussion**

In this chapter a discussion regarding different aspects of this thesis project will be presented, starting with a discussion regarding the method and results. Finally, a discussion regarding ethical, social and scientific aspects will be presented.

### **7.1 Method**

The main method used for this work was a survey. The main goal was to explore existing guidelines for information classification in Swedish governmental agencies and in order to reach out to as many as possible a questionnaire was sent via e-mail. The receiver of the e-mail at the different agencies could then forward the e-mail to the person in charge of the information security issues. Unfortunately, it is difficult to know whether the one responding to the e-mail actually was the one in charge of these issues at the agency.

Surveys can suffer from low response rates. To overcome this challenge, the questions posed in the survey were written so as to be easy to understand and to answer. Moreover, a reminder was sent to the potential participants, as proposed by Dillman, Smyth, and Christian (2008). Out of 245 agencies, 144 answered the survey. This relatively high participant rate is deemed to be enough for providing an overall picture of the existing guidelines presently used by the agencies, especially when the results obtained were consistent with the results from the survey conducted in 2014 by the Swedish Civil Contingencies Agency. However, only 54 out of 245 agencies contributed to the qualitative results by sharing their guidelines during this survey, marking the need for further investigations within the subject. According to Lazar, Feng, and Hochheiser (2010), open-ended questions that invite long, written responses are likely to go unanswered, thus to pose such open-ended questions during interviews could possibly enrich the qualitative results of this work.

Moreover, during interviews, the interviewer is able to pose follow-up questions and discuss the themes brought up at a deeper level than when using the survey method, which could further aid in the collection and analysis of the data collected. However, as with surveys, interviews have delimitations as well. An interview often takes a long time to prepare and to perform, and the number of participants is usually small.

Another challenge is to analyse and categorise the often large amounts of raw data, without biasing the results. However, according to Lazar et al. (2010), it is important to note that the results obtained from empirical studies are most likely biased due to the researcher's own opinions and experience. To minimize the effects of individual biases, joint analyses of the data collected were performed together with the thesis supervisor. The results were further analysed by comparing the results obtained with evidence found in relevant literature.

Important to note is that surveys, as well as interviews, involve data collection where the participants are forced to recall how they carry out their tasks, possibly distorting the data collected. However, due to the type of data handled by many of the agencies, real observations of the participants were deemed not to be suitable.

## **7.2 Results**

This study has focused on identifying information classification guidelines used within Swedish administrative governmental agencies. To get a deeper understanding of these guidelines, interviews could have been conducted with the agencies. However, it would be out of scope for this work and is suggested as future work.

This work, based on both qualitative and quantitative data, contributes with valuable insights of information classification within the governmental agencies, enabling future researchers to focus on the development of more specific guidelines, possibly providing the agencies with better means for handling their data. The work presented should be seen as a first step toward generating such guidelines.

The overall results show that information classification is problematic, consistent with previous work (Bergström & Åhlfeldt, 2014, the Swedish Civil Contingencies Agency, 2014). As stated by Bayuk (2010), existing standards are too generic to provide guidance, as shown by the various ways that the agencies handle their information classification issues, which are not always consistent with the ISO 27000-series.

However, the agencies' reasons for not following the guidelines provided by the ISO 27000-series were deemed to be valid. For example, letting every employee who handles information classify it could possibly lead to a general deeper understanding of the information value at the different agencies. This strategy might also be more efficient from an organisational point of view, where the information classification tasks are distributed amongst the personnel, thus not overwhelming a single employee or group of employees with such tasks. Yet, the risk might be that the classification conducted is less consistent than when a selected group of employees would classify all information. Regarding the aspect of how information should be classified, namely by following the classification schemes, one could argue that this needs further investigations since this work has not investigated how well the schemes actually covers the agencies' information handling requirements.

In summary, the study shows the importance of information classification from a system security perspective. Wrongly or unclassified information could lead to an inadequate implementation of security controls, allowing unauthorized users access to sensitive information. As such, the handling of information classification issues at the different agencies is of utmost importance and needs further investigations.

## **7.3 Ethical aspects**

It is important to emphasize that this work is not made to compare the different governmental agencies' classification guidelines with each other. The survey is done in order to get a collective overview of existing classification guidelines and identify good examples. Since the

agencies are required to answer the e-mail, based on the freedom of information legislation, their participation is not voluntarily, which can be an ethical dilemma. This might affect an agency's answer, making them more prompt to answer "No" in order to minimize their participation. An agency might also say that they classify information, due to it being a requirement. The work was conducted with regards to the ethical aspects mentioned in section 4.4.

## **7.4 Social aspects**

This survey has been done because information is important and needs a suitable level of protection. The Swedish governmental agencies are responsible for both critical and sensitive information that needs to be handled according to its value, which according to the Swedish National Audit Office (2014), is not the case. To be able to ensure that information is properly protected, information classification is needed. With the right classification, information security controls can be applied, thus proper information security is achieved. Information classification can also help an organization to identify which information that is sensitive and must be handled accordingly.

At present, the requirement is on the governmental agencies but tomorrow these requirements might be on municipalities or organizations in the private sector. In the social perspective this work can help the governmental agencies and other organizations with issues regarding information classification.

## **7.5 Scientific aspects**

This work focus on an area that have very limited research and the results might provide an insight, unique to the area. The overall results are consistent with previous research regarding information security in Swedish governmental agencies (the Swedish Civil Contingencies Agency, 2014, the Swedish National Audit Office, 2014). This survey also proves that Swedish governmental agencies struggle with information classification, consistent with the conclusion made by the Swedish Civil Contingencies Agency (2014) in their survey. By doing this survey, guidelines for classification were identified, proving that while developing classification guidelines based on general standards is difficult, it can be done.

## **8 Future research**

An interesting future work would be to conduct the same research but with a focus on governmental agencies in other countries or change domain to the private sector. The research could also be expanded to include all governmental agencies, regardless if they are required to classify information according to MSBFS2009:10 or not. Another interesting approach to investigate the area of information classification could be to let test subjects, belonging to the same or different organisation, classify the same information and compare the results.

Another possible angle would be to create new recommendations, more suitable for the governmental agencies. It would also be interesting to do a follow-up project, using interviews instead

of a questionnaire, to get more in-depth answers and be able to extract the participants' opinion regarding information classification.

## References

- Al-Fedaghi, S. (2008, Dec). On information lifecycle management. In *Asia-pacific services computing conference, 2008. apsc '08. ieee* (p. 335-342).
- Arora, V. (2010). *Comparing different information security standards: Cobit v s. iso 27001*. Retrieved 2015-06-10, from <https://qatar.cmu.edu/media/assets/CPUCIS2010-1.pdf>
- Axelrod, C., Bayuk, J., & Schutzer, D. (2009). *Enterprise information security and privacy*. Artech House.
- Baškarada, S. (2009). Analysis of data. In *Information quality management capability maturity model*. Vieweg+Teubner Verlag.
- Bayuk, J. L. (2010). The utility of security standards. In *Security technology (iccst), 2010 ieee international carnahan conference on* (p. 1-6).
- Bechtsoudis, A., & Sklavos, N. (2012, April). Aiming at higher network security through extensive penetration tests. *Latin America Transactions, IEEE (Revista IEEE America Latina)*, 10(3), 1752-1756.
- Benbasat, I., Goldstein, D. K., & Mead, M. (1987, September). The case research strategy in studies of information systems. *MIS Q.*, 11(3), 369–386.
- Bergström, E., & Åhlfeldt, R.-M. (2014). Information classification issues. In K. Bernsmed & S. Fischer-Hübner (Eds.), *Secure it systems* (p. 27-41). Springer International Publishing.
- Berndtsson, M., Hansson, J., Olsson, B., & Lundell, B. (2008). *Thesis Projects – A Guide for Students in Computer Science and Information Systems* (2nd ed.). Springer.
- Booyesen, H. A. S., & Eloff, J. H. P. (1995). Classification of objects for improved access control. *Computers & Security*, 14(3), 251-265.
- Broderick, J. S. (2006). Isms, security standards and security regulations. *Information Security Technical Report*, 11(1), 26 - 31.
- Clinch, J. (2009). Itil v3 and information security. *Best Management Practice*.
- Coles-Kemp, L. (2009). Information security management: An entangled research challenge. *Information Security Technical Report*, 14(4), 181 - 185. (Human Factors in Information Security)
- Collette, R. (2006). Overcoming obstacles to data classification. *Computer Economics Report (International Edition)*, 28(4), 8-11. (Computer Economics, USA.)
- Common criteria history*. (2013). Retrieved 2015-06-01, from [http://www.commoncriteriaportal.org/iccc/ICCC\\_arc/history.htm](http://www.commoncriteriaportal.org/iccc/ICCC_arc/history.htm)
- Creswell, J. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Thousand Oaks, California: SAGE Publications Inc.
- Dillman, D. A., Smyth, J. D., & Christian, L. M. (2008). Internet, mail, and mixed-mode surveys: The tailored design method.
- DuraiPandian, N., & Chellappan, C. (2006, 11-13 April 2006). *Dynamic information security level reclassification*. (2006 IFIP International Conference on Wireless and Optical Communications Networks. IEEE. 2006, 3 pp.. Piscataway, NJ, USA.)
- Everett, C. (2011). Building solid foundations: the case for data classification. *Computer Fraud & Security*, 2011(6), 5–8.
- Farn, K.-J., Lin, S.-K., & Lo, C.-C. (2008). A study on e-taiwan information system security classification and implementation. *Computer Standards & Interfaces*, 30(1–2), 1 - 7.
- Feinberg, L. E. (2004). Foia, federal information policy, and information availability in a post-9/11 world. *Government Information Quarterly*, 21(4), 439-460.
- 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.
- Fibikova, L., & Müller, R. (2011). A simplified approach for classifying applications. In N. Pohlmann, H. Reimer, & W. Schneider (Eds.), *Isse 2010 securing electronic business processes* (p. 39-49). Vieweg+Teubner.
- Fomin, V. V., Vries, H., & Barlette, Y. (2008). Iso/iec 27001 information systems security management standard: exploring the reasons for low adoption. In *Euromot 2008 conference, nice, france*.
- Garcia, J. J. B. (2010). *The information security management system according iso 27001 the value for services*. Van Haren Publishing. Retrieved 2015-05-10, from [http://www.vanharen.net/Player/eKnowledge/the\\_information\\_security\\_management\\_system\\_according\\_iso\\_27001\\_the\\_value\\_for\\_services.pdf](http://www.vanharen.net/Player/eKnowledge/the_information_security_management_system_according_iso_27001_the_value_for_services.pdf)
- Glynn, S. (2011). Getting to grips with data classification. *Database and Network Journal*, 2012(41), 8-9.
- Greene, S. (2005). *Security policies and procedures: Principles and practices (prentice hall security series)*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc.
- Hagen, J. M., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, 16(4), 377-397.
- Hartley, J. (2004). Case study research. In C. Cassell & G. Symon (Eds.), *Essential guide to qualitative methods in organizational research*. London: SAGE Publications Ltd.
- Hashimoto, G., Rosa, P., Filho, E., & Machado, J. (2010, Aug). A security framework to protect against social networks services threats. In *Systems and networks communications (icsnc), 2010 fifth international conference on* (p. 189-194).
- Hayat, Z., Reeve, J., Boutle, C., & Field, M. (2006). *Information security implications of autonomous systems*. IEEE Press.
- Hilton, J. (2009). Improving the secure management of personal data: Privacy on-line is important, but it's not easy. *Information Security Technical Report*, 14(3), 124-130.
- Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, 13(4), 247 - 255.
- Humphreys, E. (2011). Information security management system standards. *Datenschutz und Datensicherheit - DuD*, 35(1), 7-11.
- Humphreys, T. (2006). State-of-the-art information security management systems with iso/iec 27001: 2005. *ISO Management Systems*, 6, 1.
- ISO/IEC. (2011). *ISO/IEC 27005 information technology – security techniques – information security risk management*. ISO/IEC.
- ISO/IEC. (2013a). *ISO/IEC 27001 information technology – security techniques – information security management systems – requirements*. ISO/IEC.
- ISO/IEC. (2013b). *ISO/IEC 27002 information technology – security techniques – code of practice for information security controls*. ISO/IEC.
- ISO/IEC. (2014). *ISO/IEC 27000 information technology – security techniques – information security management systems – overview and vocabulary*. ISO/IEC.
- Janczewski, L., & Xinli Shi, F. (2002). Development of information security baselines for healthcare information systems in new zealand. *Computers & Security*, 21(2), 172-192.
- J. H. P. Eloff, S. T., R. Holbein. (1996). *Security classification for documents* (Vol. 15; Tech. Rep. No. 1). Elsevier Science Limited.
- Jo, H., Kim, S., & Won, D. (2011). Advanced information security management evaluation

- system. *KSII Transactions on Internet and Information Systems*, 5(6), 1192–1213.
- Kajava, J., Anttila, J., Varonen, R., Savola, R., & Röning, J. (2007). Senior executives commitment to information security – from motivation to responsibility. In Y.-m. L. H. Wang Yuping; Cheung (Ed.), *Computational intelligence and security* (Vol. 4456, p. 833-838). Springer Berlin Heidelberg.
- Kokolakis, S., & Lambrinouidakis, C. (2005). Ict security standards for healthcare applications. *Standardization for ICT Security*, 6(3), 47-54.
- 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.
- Lazar, J., Feng, J. H., & Hochheiser, H. (2010). *Research methods in human-computer interaction*. Wiley Publishing.
- Lin, H., Cefaratti, M., & Wallace, L. (2012). Enterprise risk management, cobit, and iso 27002: A conceptual analysis. *Internal Auditing*, 27(2), 3-12.
- Lincoln, Y., & Guba, E. (1985). *Naturalistic inquiry*. Newbury Park, California: SAGE Publications Inc.
- Mendyk-Krajewska, T., & Mazur, Z. (2010, May). Problem of network security threats. In *Human system interactions (hsi), 2010 3rd conference on* (p. 436-443).
- MSBFS2009:10. (2009). *Myndigheten för samhällsskydd och beredskaps författningssamling*. Myndigheten för samhällsskydd och beredskap. Retrieved 2014-12-10, from <https://www.msb.se/externdata/rs/94a3d208-2ac4-48a1-84f2-208268f5767e.pdf>
- Oscarson, P. (2009). *Modell för klassificering av information, version 1*. the Swedish Civil Contingencies Agency. Retrieved from <https://www.msb.se/RibData/Filer/pdf/25602.pdf>
- Oscarson, P., & Karlsson, F. (2009). A national model for information classification. In *Ais sigsec workshop on information security & privacy (wisp2009)*.
- Parker, D. B. (1996). The classification of information to protect it from loss. *Information Systems Security*, 5(2), 9-15. (Auerbach Publications, USA.)
- Parker, D. B. (1997). The strategic values of information security in business. *Computers & Security*, 16(7), 572-582.
- Pfleeger, C. P., & Pfleeger, S. L. (2006). *Security in computing (4th edition)*. Upper Saddle River, NJ, USA: Prentice Hall PTR.
- Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Q.*, 34(4), 757-778.
- SCB. (2015). *Scb statistical database*. Stockholm: Statistiska centralbyrån. Retrieved 2015-03-01, from <http://www.myndighetsregistret.scb.se/Myndighet.aspx>
- 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.
- Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Commun. ACM*, 49(8), 97–100.
- Siponen, M., & Willison, R. (2009, June). Information security management standards: Problems and solutions. *Inf. Manage.*, 46(5), 267–270.
- the Swedish Civil Contingencies Agency. (2014). *En bild av myndigheternas informationssäkerhetsarbete 2014*. Author. Retrieved 2014-12-10, from [https://www.msb.se/Upload/Nyheter\\_press/Pressmeddelanden/En%20bild%20av%20myndigheternas%20informations%C3%A4kerhetsarbete%202014\\_MSB740.pdf](https://www.msb.se/Upload/Nyheter_press/Pressmeddelanden/En%20bild%20av%20myndigheternas%20informations%C3%A4kerhetsarbete%202014_MSB740.pdf)
- the Swedish National Audit Office. (2014). Informationssäkerheten i den civila statsförvaltning-

- gen, rir2014:23.
- Trost, J. (2010). *Kvalitativa intervjuer* (4th ed.). Lund: Studentlitteratur.
- Verdon, D. (2006, July). Security policies and the software developer. *Security Privacy, IEEE*, 4(4), 42-49.
- Vetenskapsrådet. (2002). *Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning*. Stockholm: Author. Retrieved 2014-04-01, from <http://www.codex.vr.se/texts/HSFR.pdf>
- Virtanen, T. (2001). Design criteria to classified information systems numerically. In P. Dupuy Michel; Paradinas (Ed.), *Trusted information* (Vol. 65, p. 317-325). Springer US.
- von Solms, S. B. (2005). Information security governance – compliance management vs operational management. *Computers & Security*, 24(6), 443 - 447.
- Webster, J., & Watson, R. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, 26(2), 13–23.
- Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Experimentation in software engineering*. Springer (first edition by Kluwer in 2000).
- Wrona, K., & Hallingstad, G. (2011). Controlled information sharing in nato operations. In *2011-milcom 2011 military communications conference*.
- Åhlfeldt, R.-M., Andersén, A., Eriksson, N., Nohlberg, M., Bergström, E., & Fischer-Hübner, S. (2015). Kompetensbehov och kompetensförsörjning inom informationssäkerhet från ett samhällsperspektiv.

## **A Survey regarding information classification**

1. How many employees are working at the agency? (Select one alternative)  
0-50, 51-500 or 501+
2. Is it specified who is responsible for information classification at the agency?
3. Is it clarified when information shall be classified and when reclassification should take place? If the answer is "Yes", please describe your reasoning. (If "No" thank you for your participation!)
4. Do you use a classification scheme for information classification? If not, have you commenced such a scheme implementation?
5. Do you experience that it is easy or complicated to use your classification scheme? Please explain your answer if possible.
6. Is your classification scheme based on the recommendation published by the Swedish Civil Contingencies Agency? If "Yes" have you made any modifications to it? If "No" what is your scheme based on?
7. Would we be able to take part of your classification scheme and any documentation that explains how to use it? Please attach the scheme and any guidelines if possible.
8. How many levels of classification are you using?
9. Do you take confidentiality, integrity, availability and traceability into consideration or only some of them or do you use other aspects? Please describe which and your reasoning.