An information classification model for public sector organizations in Sweden: a case study of a Swedish municipality

Jan-Halvard Bergquist, Samantha Tinet and Shang Gao
Department of Informatics, Örebro University, Örebro, Sweden

Received 4 March 2021
Revised 15 June 2021
Accepted 7 July 2021

Abstract

Purpose – The purpose of this study is to create an information classification model that is tailored to suit the specific needs of public sector organizations in Sweden.

Design/methodology/approach – To address the purpose of this research, a case study in a Swedish municipality was conducted. Data was collected through a mixture of techniques such as literature, document and website review. Empirical data was collected through interviews with 11 employees working within 7 different sections of the municipality.

Findings – This study resulted in an information classification model that is tailored to the specific needs of Swedish municipalities. In addition, a set of steps for tailoring an information classification model to suit a specific public organization are recommended. The findings also indicate that for a successful information classification it is necessary to educate the employees about the basics of information security and classification and create an understandable and unified information security language.

Practical implications – This study also highlights that to have a tailored information classification model, it is imperative to understand the value of information and what kind of consequences a violation of established information security principles could have through the perspectives of the employees.

Originality/value – It is the first of its kind in tailoring an information classification model to the specific needs of a Swedish municipality. The model provided by this study can be used as a tool to facilitate a common ground for classifying information within all Swedish municipalities, thereby contributing the first step toward a Swedish municipal model for information classification.

Keywords Information classification, Information classification model, Information security, Information security principles, Swedish civil contingencies agency (MSB)

Paper type Research paper

1. Introduction

Information is considered to be the primary asset in organizations today, and the protection of these assets sets the foundation for information security (Oscarson, 2003). Failure to protect the information assets within public sector organizations could result in major economic consequences for society and what is more, cause social harm to human life (Halim

Information & Computer Security
Vol. 30 No. 2, 2022
pp. 153-172
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-03-2021-0032

and Yusof, 2019). Therefore, it is crucial to have a good protection for information assets in public organizations. Bergström *et al.* (2018) suggested that an information security management system (ISMS) needs to be implemented to protect organizations' information assets in a correct and systematic way.

A central and integral part of an ISMS is the classification of information based on its value through the perspective of the information security principles, namely, confidentiality, integrity and availability (CIA) (Bergström *et al.*, 2018). Many information security professionals consider information classification to be the foundation of any information security activity (Everett, 2011; Ma *et al.*, 2008). ISO 27002 standard describes the objective of information classification as "to ensure that information receives an appropriate level of protection in accordance with its importance to the organization" (ISO/IEC 27002, 2017, p. 15). In accordance with the ISO/IEC 27000 standard series, asset management has a major role to play in the formation of an ISMS (ISO/IEC 27002, 2017). As part of asset management, information classification also serves as the major input to the risk analysis process, which is a requirement according to the ISO 27000 standard series (ISO/IEC 27000, 2017; Ozkan and Karabacak, 2010; Oscarson and Karlsson, 2009). Information classification is one essential element for the success of risk analysis and management in organizations (Everett, 2011).

Despite information classification being an essential and in many cases a compulsory practice for many organizations within the public sector (Ozkan and Karabacak, 2010), many organizations struggle with the implementation of information classification (Ghernaouti *et al.*, 2011). A survey conducted by the UK Department of Culture showed that 54% of organizations do not address information classification in their information security policies (Button *et al.*, 2016). Furthermore, an individual's subjective judgment on information classification can lead to inconsistent results of classification. The same type of information might be classified differently by two individuals, as they might have different subjective perceptions on information (Booysen and Eloff, 1995; Eloff *et al.*, 1996).

Information classification is in general a globally understudied area, especially when it comes to how information classification is practiced in organizations (Bergström and Åhlfeldt, 2014), as well as the structure and formulation of information classification models (Oscarson and Karlsson, 2009). What is more, a majority of research within the area of information classification is from the perspective of technological automated systems (Na *et al.*, 2019; Tijan, 2009). Furthermore, only a few studies (Bergström and Åhlfeldt, 2014) address the problem of modifying the information classification model to a specific organization. Therefore, it is crucial to further explore information classification issues, particularly the underlying issues that exist in the information classification process and the solutions to address these issues, in public sector organizations in developed countries.

In this study, Sweden has been selected as the representative country in the context of developed countries. According to the Global Cybersecurity Index, Sweden is one of the countries with a high cybersecurity commitment (ITU-D, 2018). To address the need of information classification from various organizations in Sweden, the Swedish civil contingencies agency (MSB) provided an information classification model (MSB, 2020) on the basis of the research by Oscarson and Karlsson (2009) in 2018. According to the survey results from Bergström *et al.* (2016), about 75% of organizations within the Swedish public sector use the MSB model and of those, about 77% have done the modification to the model. Furthermore, according to the findings from Bergström *et al.* (2018), many Swedish public sector organizations struggle with the implementation of information classification due to a lack of standardized instructions for implementation of information classification or a lack

of elaborated instructions for implementation of information classification. The evidence above highlights the need for the MSB model to be tailored to the organization's specific needs. In addition, MSB in their ISMS guidelines instructs that the model has to be tailored to the specific organization (MSB, 2020).

To address the identified gap, this study aims to tailor an information classification model to suit the specific needs of a public sector organization in Sweden. A case study at one Swedish municipality is conducted in this study. The MSB information classification model is used as a base for creating the tailored model, as it is used by many organizations in the Swedish public sector, and according to MSB's information security regulations, all organizations in the Swedish public sector are recommended to classify their information using their model (Bergström *et al.*, 2016). Accordingly, the research question of this study is as follows:

RQ. How should the MSB information classification model be tailored to suit Swedish municipalities?

The rest of the paper is organized as follows. Section 2 describes the theoretical background of the study's research area, as well as forming the foundation for the case study and the collection of the empirical data. Section 3 illustrates the research method. The result and analysis of the empirical data is presented in Section 4. Section 5 discussed the results. Finally, Section 6 presents the main conclusions of this paper and points out some future research directions.

2. Theoretical background

This section provides a theoretical basis and explanatory approach of the case study, which is based on the analysis of literature, website and document review.

2.1 Information classification

Information classification is a practice that has been recommended in several ISMS standards [e.g. ISO/IEC 27000, Control Objectives for Information and Related Technologies]. In addition, information classification is a mandatory activity for government agencies in many countries (e.g. UK and Sweden). Classifying information in a proper way can lead to advantages such as deciding the right level of protection that is needed to safeguard information (Agrawal, 2017; Bergström *et al.*, 2016; Peltier, 1998), which can result in an efficient allocation of resources (Peltier, 1998). A further advantage is that it ensures that information receives an appropriate level of protection in accordance with its importance to the organization through the CIA principles (ISO/IEC 27002, 2017). What is more, during the information classification process, organizations can identify the specific laws and regulations that certain types of information need to follow and thereby avoid the risk of non-compliance (Agrawal, 2017).

2.2 Information classifications models

One of the tools that are used in the information classification process is an information classification model (Bergström *et al.*, 2016). An information classification model often contains different evaluation levels aimed at one or more information security principles, e.g. CIA (Bergström *et al.*, 2016). Bergström *et al.* (2016) found that most countries focused primarily on the principle of confidentiality in their information classification model and policy. The other two principles of integrity and availability are considered to be concepts

that are more difficult to understand by the employees, as well as being the responsibility of the information technology (IT) department (Bergström *et al.*, 2016).

2.2.1 MSB information classification model in Sweden. Most information classification models in Sweden are based on the national model provided by MSB. One aspect that is highlighted by MSB in their model is the need to tailor the model to the organization's context and characteristics (MSB, 2018a).

MSB's model uses four consequence levels for the three different information security principles of CIA (Table 1 in the next page). The four consequence levels are "none or insignificant," "moderate," "significant" and "serious" (Bergström *et al.*, 2016; MSB, 2018a). According to MSB, when applying the model in the organization, each information security principle has to be classified separately, as a specific asset may have different consequence levels for each of the CIA principles (Bergström *et al.*, 2016; MSB, 2018a). MSB also emphasizes that the use of the consequence level "none or insignificant" is expected to be rare for the integrity and availability principles (Bergström *et al.*, 2016; MSB, 2018a).

Furthermore, MSB explains that consequences caused by lack of confidentiality, integrity or availability may be due to different categories of events, which MSB calls consequence categories (MSB, 2018a). Examples of such categories according to MSB (2018a) are:

- Financial loss (causes such as lower revenues, increased costs, damage to assets).
- Negative impact on or interruption in operational activities of the organization.
- Violation/non-compliance with legal requirements.
- Damaged brand/decreased confidence.
- Damage to other organizations/surrounding communities.
- Personal injury.
- Environmental damage.

MSB further explains that the consequence categories above should be seen as an example and not a complete list and that organizations should identify consequence categories that are relevant to their organization (MSB, 2018a).

2.3 The setting of this study: municipality X in Sweden

This case study focuses on the information classification process at a Swedish municipality.

2.3.1 Current information classification status in municipality X. Municipality X is the selected case for this study. Municipality X is one of the 290 municipalities in Sweden with a population of about 153,000 inhabitants. The different sections at municipality X operate in many different areas, therefore, knowing the specific operating areas at municipality X is crucial to answer the research question, as the goal is to create a tailored information classification model that suits all the areas that the municipality operates in. This led to the first aspect that needed to be investigated to create a tailored model:

- *Aspect A:* Identifying the organizational structure and the different operating areas within municipality X.

These operating areas are presented in Table 2. The table also provides a description together with some examples of the responsibilities that the municipality has within each operating area.

2.3.2 Current information classification process. Municipality X has adopted an information classification model that is based on MSB's model for information classification

Security aspect/level of consequence	Confidentiality	Integrity	Availability
Serious	Information where the loss of confidentiality means seriously/catastrophically negative impact on the organization and its assets, other organizations or individuals	Information where the loss of integrity means seriously/catastrophically negative impact on the organization and its assets, other organizations or individuals	Information where the loss of availability means seriously/catastrophically negative impact on the organization and its assets, other organizations or individuals
Significant	Information where loss of confidentiality means a significant negative impact on the organization and its assets, other organizations or individuals	Information where loss of integrity means a significant negative impact on the organization and its assets, other organizations or individuals	Information where loss of availability means a significant negative impact on the organization and its assets, other organizations or individuals
Moderate	Information where loss of confidentiality means moderate negative impact on the organization and its assets, other organizations or individuals	Information where loss of integrity means moderate negative impact on the organization and its assets, other organizations or individuals	Information where loss of availability means moderate negative impact on the organization and its assets, other organizations or individuals
None or insignificant	Information without requirements regarding confidentiality or where loss of confidentiality means none or insignificant negative impact on the organization and its assets, other organizations or individuals	Information without requirements regarding integrity or where loss of integrity means none or insignificant negative impact on the organization and its assets, other organizations or individuals	Information without requirements regarding availability or where loss of availability means none or insignificant negative impact on the organization and its assets, other organizations or individuals

Table 1.
MSB's national information classification model (Oscarson and Karlsson, 2009; MSB, 2018a)

Table 2.
Municipality X operating areas

Operations area	Description of the operating area	Examples of the operating area
Physical planning and construction	This operational area refers to physical planning, which is about how to use land and water areas, where buildings and roads should be located, as well as their design and the construction development, which is regulated through the planning and building act (PBL)	– Construction plans and construction issues – Land Survey and cartography – Building permit
Environmental and societal protection	This operational area refers to all the activities at the municipality that are about the protection of the environment and society as a whole in accordance with the environmental code	– Environmental and health protection – Order and safety – Rescue services
Infrastructure	This operating area contains activities that include water, sewer, fiber network, public transport and "traffic maintenance"	– Water and sewage – Waste management – Maintenance of streets and parks – Public transport – Fiber network
Business, work and integration	This operating area includes activities that contribute to a functioning business sector and a functioning labor market, as well as everything relating to the integration of individuals into society	– Labor market and employment – Promotion of business and development – Integration
Education	This operating area includes any activity that is related to education as defined in the Swedish School Act	– Preschool – Elementary education – Secondary education – Adult education
Culture, leisure and tourism	This operating area contains any activity that is related to culture, art, tourism and leisure activities such as swimming school, bicycle trails and fishing	– Library – Promotion of tourism – Exhibiting art – Management of historical archives – Management of physical heritage – Operation of sports and leisure facilities – Schools for culture- and technology education
Social care and support	This operating area includes all the activities related to social care and support to the elderly, the functional impaired, children, adolescents and families, as well as financial support. This area also includes activities related to addiction support	– Income support – Elderly care – Support and care for functional and mental impairment – Support for children and adolescents – Addiction care and support – Home care services
Special societal support	This operating area includes activities that are related to supervision of legal guardianship and trustee, as well as civil ceremonies such as funerals and weddings. This area also includes other activities that are related to legal- and economic advise, as well as consumer support	– Legal guardian and trustee – Legal guardian and trustee supervision – Civil ceremonies – Support to associations – Consumer support – Economic advise – Legal advise

with some minor modifications. The current information classification model has three columns representing the three aspects of CIA and three rows for levels of protection – no protection (0), normal protection (1) and high protection (2), as seen in Figure 1.

2.3.3 Current information classification issues. According to the chief information security officer (CISO) at municipality X, information currently is classified based on the available protection measures rather than its value and sensitivity. In addition, the CISO also stated that the classification of information is conducted by the IT department at the municipality and people working with information are not included in the classification process. This way of conducting information classification can lead to inaccurate classification, which, in turn, can lead to over or under the protection of information assets and result in inadequate protection or waste of resources (Bergström and Åhlfeldt, 2014; Peltier, 1998).

As described in Section 2.2.1, MSB is requiring organizations to classify information based on the consequence categories for each of the CIA principles (MSB, 2018a). However, the current information classification model at municipality X does not take consequence categories into consideration, and therefore, it is still general despite the modifications that have been made. Based on a recommendation from MSB (MSB, 2018b), it is important that municipality X incorporates the relevant consequence categories into their information classification model and choosing an adequate number of necessary consequence levels. Based on this, Aspects B–D needed to be investigated to answer the research question and create a tailored information classification model for municipality X:

- *Aspect B:* Identify the relevant consequence categories for municipality X that should be incorporated in the tailored model.
- *Aspect C:* Identify how many consequences levels that are suitable for each of the identified consequence categories.
- *Aspect D:* Formulate the consequence levels for each of the information security principles in an appropriate way for municipality X.

Protection level	Confidentiality	Integrity	Availability
2 High protection demands	**Confidential** information that in case of unauthorized access may have serious consequenses for municipality X, external actors or individuals.	Information that in case of inaccuracy or incompleteness can cause serious consequenses for municipality X, external actors or individuals.	Information that if not avaliable can cause serious consequenses for municipality X, external actors or individuals.
1 Normal protection demands	**Internal** information that in case of unauthorized access may have moderate negative consequenses for municipality X, external actors or individuals.	Information that in case of inaccuracy or incomplete-ness can cause moderate negative consequenses for municipality X, external actors or individuals.	Information that if not avaliable can cause moderate negative consequenses for municipality X, external actors or individuals.
0 *No protection demands	**Public** information that may be freely distributed within and outside of municipality X.	* Information is always required to be accurate and avaliable.	

Figure 1.
Municipality X information classification model

3. Method

To investigate the aspects mentioned in Section 2.3.3, a case study (Yin, 2014) was used in this research. An interpretive approach is used, as it aims to understand people in their natural settings and in their own words (Oates, 2006). An interpretive case study uses data collection and analysis methods that are qualitative in nature (May, 2011). Case study as the research strategy was selected for this study, as it is widely used within information security research and when investigating organizations in the public sector (Agrawal, 2017; Ali *et al.*, 2020; Hedström *et al.*, 2011; Evans *et al.*, 2019).

3.1 Case selection

The choice of municipality X as the studied case was in accordance with Oates's (2006), a convenience selection, as this study is based on a project that was presented to the researchers by municipality X on how MSB's information classification model should be tailored to suit their specific needs. What is more, municipality X is a good representative of all Swedish municipalities, as they handle the same type of information and have to abide by the same laws and regulations.

3.1.1 Selection of respondents. To find employees who worked at different operating areas, relevant committees and boards at the municipality were contacted in mid-February of 2020. The interview invitation email that was sent to the committees and boards started with an introduction of the researchers and the purpose of the study, as well as what the interview questions are about. As a result, 11 employees from 7 sections participated in this study. Table 3 shows the list of all the interviewees together with their titles, which committee, board or department they belong to and the operating area they represent, as well as the interviewee code.

Table 3.
An overview of the interviewees

Administration/ committee/board/ department	Operating area	Title of the interviewee	Interviewee code
Urban planning office	Physical planning and construction, as well as infrastructure	Geographical information system engineer	I1
		Geographical information system strategist	I2
		Administrative coordinator (information manager)	I3
Social welfare	Social care and support	Committee secretary	I4
Human resources (HR) department	Support department. Not included as an operational area	Head of HR	I5
Children and education committee	Education	Planner	I6
Economy department	Support department. Not included as an operational area	Purchaser	I7
		System economist	I8
Social efforts	Social care and support	Development strategist	I9
Environmental office committee	Environmental and societal protection	Head of administration	I10
		Registrar and administrator (information security coordinator)	I11

3.2 Data collection

Semi-structured interviews have been used as the primary data source of this study. Semi-structured interviews generate qualitative data, as it allows interviewees to talk about the subject matter in their own words and from their own perspective, as well as introduce issues that they believe are relevant to the subject (May, 2011; Oates, 2006).

The interviews were planned to be conducted face to face at the interviewee's place of work. However, due to the Covid-19 pandemic, the interviews were conducted through Microsoft Teams instead. A preparational document containing questions and related information were emailed a minimum of two weeks before the interview for the interviewees to prepare for the interviews. Each interview started with the interviewers introducing themselves and explaining the purpose of the study and the interview, as well as how important and valuable the interviewees' contribution was to the study. The interviewees have also been informed that the results would be reported anonymously. The interviews were audio-recorded and later transcribed. Before recording the interviews, interviewee's permission was obtained.

3.3 Data analysis

The collected data from the interviews were presented in Section 4. Textual data analysis method (Oates, 2006) was used to analyze the qualitative data in a structured manner. The first step was to transcribe all the interview data. Second, relevant data was identified and segmented into three segment themes: Irrelevant segments, general descriptive information segments needed to describe the research context and segments relevant to the research question (Oates, 2006). The third step was to focus on the segment of data that was deemed to be relevant to the research question in the previous step by identifying patterns from the data within the following themes, namely, consequence categories, consequence levels and consequence category formulations.

4. Results

In this section, the result and analysis of Aspects B–D of the proposed research question based on the empirical data collected from the interviews are presented.

4.1 Aspect B: Relevant consequence categories

4.1.1 Result of consequence categories. The consequence categories that are relevant for the municipality that should be incorporated in the tailored model are Economy, Business, Individual, Trust, Legal and Environment:

- 11 out of 11 interviewees stated that violation against the CIA principles when handling information could have consequences for the Economy category.
- 10 out of 11 (91%) stated that violation against the CIA principles when handling information could have consequences for the Business and Individual categories.
- 9 out of 11 (82%) stated that violation against the CIA principles when handling information could have consequences for the Trust category.
- 6 out of 11 (55%) stated that violation against the CIA principles when handling information could have consequences for the Legal category.
- 3 out of 11 (27%) stated that violation against the CIA principles when handling information could have consequences for the Environment category.

4.1.2 Analysis of consequence categories. In the tailored model the MSB consequence categories are incorporated as following:

- Financial loss (causes such as lower revenues, increased costs and damage to assets) is represented by *Economy*.
- Negative impact on or interruption in the operational activities of the organization is represented by *Business*.
- Personal injury is represented by *Individual*.
- Damaged brand/decreased confidence is represented by *Trust*.
- Violation/non-compliance with legal requirements is represented by *Legal*.
- Environmental damage is represented by Environment. Although Environment as its own category was deemed to be necessary only by a few interviewees, however, most other interviewees indicated the need for Environment as its own category, as handling information in a way that violates against CIA principles could lead to devastating environmental consequences, and therefore, must be considered when classifying information. Some examples of such environmental consequences as stated by I2, is that *incorrect information could increase the consequences of a forest fire* and as stated by I10, *incorrect information could lead to leakage of pollutants that could damage the environment indefinitely*.
- The MSB consequence category: Damage to other organizations/society. This category is represented in the tailored model by incorporating the "society" perspective into the categories Individual, Business, Economy, Trust and Environment and the "other organizations" perspective into the category External actors. This is because of how broad and ambiguous other organizations/societies can be as its own category.

When asking the interviewees about the adequacy of the consequence categories presented to them during the interviews, most of the interviewees confirmed that the consequence categories are relevant and adequately cover most of the potential consequences that a violation against CIA would have for the municipality. For instance, I4 stated that *I think these are quite good, the ones you have listed*. Then, I9 indicated that *I think they actually cover most things*.

Additionally, interviewees highlighted that the municipality is a big and complex organization that has vast and diverse interaction and cooperation with other organizations and municipalities:

> But a municipality is a very, very large and complex organism that does very, very many different things and in almost all the parts it is about support for municipal members or companies. It provides services and social services, school, elderly care, infrastructure, etc. As a support, lubricant in the society. For our part, we do the municipality's business and then you suddenly mix private actors in a different way. (I7)

Therefore, it became evident that there is a need to incorporate the external perspective in the tailored model. The external perspective is when the violation of information security principles caused by the municipality affects external actors such as companies, other municipalities and authorities. This was highlighted by I9 "[. . .] not just the municipality but actually the region, [. . .] or other municipalities." This shows that an incorrect handling of information by municipality X could negatively affect the business of other municipalities. Furthermore, I4 stated that "[. . .] it will be a financial consequence for

external companies working together with the municipality." To address this, the external perspective was added to the model as its own category by the name of External actors.

4.2 Aspect C: Number of consequence levels

4.2.1 Result of consequence levels. When interviewees were asked about how many consequence levels they believed are necessary for information classification, 2 out of 11 stated that 5 levels are necessary. In total, 1 out of 11 stated 3 to 5 levels, 1 stated 4 to 5 levels and 1 stated 3 levels. In total, 6 out of 11 interviewees had no comments or opinions about how many levels are necessary.

4.2.2 Analysis of consequence levels. The tailored model has the following three consequence levels:

- Level 1. Minor (Normal protection demand).
- Level 2. Considerable (Extended protection demand).
- Level 3. Serious (High protection demand).

The number of consequence levels was one of the questions that most interviewees had difficulty answering and more than half of the interviewees had no comments or opinions about it. The answers from the rest of the interviewees ranged from 3 to 5 levels. The choice of having three consequence levels in the model despite some of the interviewees preferring 4 or 5, was because according to MSB, adding more levels can increase the complexity of the classification process and it may lead to increased costs without improving information security (MSB, 2018a). The tailored model has three consequence levels as opposed to the four levels that the MSB information classification model has. This is because in the tailored model the level 0 has been removed. The reason for this change is that according to municipality X's guidelines for information classification, information is always required to be accurate (integrity) and available (availability) (Ander, 2020). However, information can have a level 0 for confidentiality but still need to be accurate and available. This could be addressed in the instructions instead of the model and thereby reducing the amount of unnecessary information in the model. What is more, most of the interviewees stated that the lowest level of consequence should not be no or zero consequence.

Furthermore, I3 indicated that:

> I think it is important that you have an equality for all areas if you are to classify this, so that you do not take in a way, this one has five, this one has three and this one has eight. Then it becomes difficult for us who will do the job of finding homogeneity in the whole.

Therefore, the tailored model has the same number of consequence levels for all the consequence areas.

4.3 Aspect D: Formulation of the consequence levels

4.3.1 Result of the consequence levels formulation. The formulation of the consequence levels for each of the information security principles and consequence categories based on the interviews are presented in Tables 4 to 10.

4.3.2 Analysis of the consequence levels formulation.

4.3.2.1 Business. The formulation of the consequence category of Business in the tailored model has two different perspectives. The need for two different perspectives was evident from the two distinct formulations that the interviewees provided during the interviews. One perspective is related to the severity of the consequence that violation against the

Category: business	
Minor (normal protection demand) Level 1	Information where loss of confidentiality/integrity/availability leads to minor or limited negative impact on the ability of the business to achieve its goals or primary tasks. Can be counted/considered in the amount of extra work/loss of working hours Information where loss of confidentiality/integrity/availability has a negative impact on a (small) sector/limited part of the municipality in its ability to achieve its goals or fulfil its primary tasks
Considerable (extended protection demands) Level 2	Information where loss of confidentiality/integrity/availability lead to considerable negative impact on the ability of the business to achieve its goals or primary tasks. Can be counted/considered in the amount of extra work/loss of working hours Information where loss of confidentiality/integrity/availability has a negative impact on several sectors/parts of the municipality in its ability to achieve its goals or fulfil its primary tasks
Serious (high protection demands) Level 3	Information where loss of confidentiality/integrity/availability leads to serious negative impact on the ability of the business to achieve its goals or primary tasks. Can be counted/considered in the amount of extra work/loss of working hours Information where loss of confidentiality/integrity/availability has a negative impact on many sectors/a majority of the municipality in its ability to achieve its goals or fulfil its primary tasks

Table 4.
Formulation of the consequence levels for category business

Category: trust	
Minor (normal protection demand) Level 1	Information where loss of confidentiality/integrity/availability leads to minor or limited damage to the trust in the business/municipality Information where loss of confidentiality/integrity/availability leads to a few to several individuals and/or a few organizations lose confidence in the municipality. Organizations can include companies, parts of the municipality, other municipalities, regions, etc
Considerable (extended protection demands) Level 2	Information where loss of confidentiality/integrity/availability leads to considerable damage to the trust in the business/municipality Information where loss of confidentiality/integrity/availability leads to many individuals and/or several organizations lose confidence in the municipality. Organizations can include companies, parts of the municipality, other municipalities, regions, etc
Serious (high protection demands) Level 3	Information where loss of confidentiality/integrity/availability leads to serious damage to the trust in the business/municipality Information where loss of confidentiality/integrity/availability leads to a large to very large number of individuals and/or many organizations lose confidence in the municipality. Organizations can include companies, parts of the municipality, other municipalities, regions, etc

Table 5.
Formulation of the consequence levels for category trust

information security principles can have for the municipality. The other perspective is about how many sections of the municipality are affected by the consequence.

4.3.2.2 Trust. The Trust category also has two different formulations. The first perspective is about the severity of loss of trust and the other perspective is about how many individuals or organizations that lose trust in the municipality due to violation against the CIA principles. It was evident based on the interviews that the municipality needs to have cooperation with many other organizations to provide services.

Category: economy	
Minor (normal protection demand) Level 1	Information where loss of confidentiality/integrity/availability leads to minor or limited economic damage for the business. Examples of economic damage could be reduced revenues, increased costs and damage to assets
Considerable (extended protection demand) Level 2	Information where loss of confidentiality/integrity/availability leads to economic damages of up to 5% of the budget. Examples of economic damage could be reduced revenues, increased costs and damage to assets Information where loss of confidentiality/integrity/availability leads to considerable economic damage for the business. Examples of economic damage could be reduced revenues, increased costs and damage to assets Information where loss of confidentiality/integrity/availability leads to economic damages of 5% to 15% of the budget. Examples of economic damage could be reduced revenues, increased costs and damage to assets
Serious (high protection demand) Level 3	Information where loss of confidentiality/integrity/availability leads to serious economic damage for the business. Examples of economic damage could be reduced revenues, increased costs and damage to assets Information where loss of confidentiality/integrity/availability leads to economic damages of over 15% of the budget. Examples of economic damages could be reduced revenues, increased costs and damage to assets

Table 6. Formulation of the consequence levels for category economy

Category: individual	
Minor (normal protection demand) Level 1	Information where loss of confidentiality/integrity/availability has a minor or limited negative impact on the individual/employee's physical and/or mental health (minor damage that can heal within a foreseeable time) and/or violation of rights
Considerable (extended protection demand) Level 2	Information where loss of confidentiality/integrity/availability has a considerable negative impact on the physical and/or mental health of the individual/employee (serious, non-life-threatening or permanent injury) and/or violation of rights
Serious (high protection demand) Level 3	Information where loss of confidentiality/integrity/availability has a serious adverse effect on the physical and/or mental health of the individual/employee (life threatening, permanent or fatal injury) and/or violation of rights

Table 7. Formulation of the consequence levels for category individual

Category: legal	
Minor (normal protection demand) Level 1	Information where loss of confidentiality/integrity/availability leads to a minor infringement/non-compliance with legal requirements such as getting a complaint and/or low fines
Considerable (extended protection demand) Level 2	Information where loss of confidentiality/integrity/availability leads to a considerable violation/non-compliance with legal requirements such as multiple complaints and/or moderate fines
Serious (high protection demand) Level 3	Information where loss of confidentiality/integrity/availability leads to a serious violation/non-compliance with legal requirements such as conviction and/or high fines

Table 8. Formulation of the consequence levels for category legal

4.3.2.3 Economy. This category is also formulated in two perspectives. The first perspective is about the severity of the consequence that the economic damage can have for the municipality. The second perspective is using the percentage of budget as a way to measure the economic damage. Most interviewees agreed that measuring economic consequences in the percentage of the budget was appropriate. Two quotes that illustrate the preference of percentage as a measurement for an economic consequence are: "[. . .] I would like to say the percentage of the municipality's economy. The whole Swedish krona can be difficult" (I5) and "it is definitely a percentage there" (I9).

4.3.2.4 Individual. Based on the analysis of the interviews it was evident that an individual can be both individuals in society and the employees working at the municipality. Therefore, it was important to incorporate both categories of individuals in the formulation.

4.3.2.5 Legal. The formulation of the Legal category is about the severity of a non-compliance that can lead to legal fines, as most of the interviewees viewed fines as the direct consequence of a legal non-compliance. Both legal fines and complaints were added as examples of legal consequences in the formulation, as those were deemed suitable by most of the interviewees making it more useful for the municipality as a whole.

4.3.2.6 Environment. The formulation of the category Environment is based on the severity of the damage on the environment. In the formulation examples of environmental damages have been provided to ensure that the consequences are related to damage to the environment and not the individuals, as there were indications that some interviewees related environmental damage to damage toward individuals, which is not the primary consequence in this category.

4.3.2.7 External actors. The External actors category is formulated in two perspectives. The first perspective is about the severity of the damage that violation of CIA caused by the municipality can have for external actors. The second perspective is about the number of external actors that are affected. In both formulations, examples of damages to external actors are provided. These examples are from a trust, economy and business perspective.

5. Discussion

The theoretical contributions, outcomes and benefits and limitations of the study are discussed in this section.

5.1 Theoretical contribution

The findings of this study provide several interesting theoretical contributions. This study confirms that employees need the education to conduct an information classification. There

Table 9.
Formulation of the consequence levels for category environment

Category: environment	
Minor (normal protection demand) Level 1	Information where loss of confidentiality/integrity/availability leads to minor damage to the environment. Such as pollution of soil or water, groundwater, damage to buildings or establishments, etc. Establishments can be parks, building sites, sports arenas, water plants, garbage sites etc
Considerable (extended protection demand) Level 2	Information where loss of confidentiality/integrity/availability leads to considerable damage to the environment. Such as pollution of soil or water, groundwater, damage to buildings or establishments, etc. Establishments can be parks, building sites, sports arenas, water plants, garbage sites etc
Serious (high protection demand) Level 3	Information where loss of confidentiality/integrity/availability leads to serious harm to the environment. Such as pollution of soil or water, groundwater, damage to buildings or establishments, etc. Establishments can be parks, building sites, sports arenas, water plants, garbage sites etc

Category: external actors	
Minor (normal protection demand) Level 1	Information where loss of confidentiality/integrity/availability leads to a minor damage to external actors (companies, other municipalities, regions, other authorities). Damage to external actors can be a loss of trust in them, negative impact in their ability to achieve their goals or fulfil their primary tasks, as well as economic damage such as reduced revenue, increased costs and damage to assets
	Information where loss of confidentiality/integrity/availability leads to damage toward one or a few external actors (companies, other municipalities, regions, other authorities). Damage to external actors can be a loss of trust in them, negative impact in their ability to achieve their goals or fulfil their primary tasks, as well as economic damage such as reduced revenue, increased costs and damage to assets
Considerable (extended protection demand) Level 2	Information where loss of confidentiality/integrity/availability leads to considerable damage to external actors (companies, other municipalities, regions, other authorities). Damage to external actors can be a loss of trust in them, negative impact in their ability to achieve their goals or fulfil their primary tasks, as well as economic damage such as reduced revenue, increased costs and damage to assets
	Information where loss of confidentiality/integrity/availability leads to damage toward several external actors (companies, other municipalities, regions, other authorities). Damage to external actors can be a loss of trust in them, negative impact in their ability to achieve their goals or fulfil their primary tasks, as well as economic damage such as reduced revenue, increased costs and damage to assets
Serious (high protection demand) Level 3	Information where loss of confidentiality/integrity/availability leads to a serious damage to external actors (companies, other municipalities, regions, other authorities). Damage to external actors can be a loss of trust in them, negative impact in their ability to achieve their goals or fulfil their primary tasks, as well as economic damage such as reduced revenue, increased costs and damage to assets
	Information where loss of confidentiality/integrity/availability leads to damage toward many external actors (companies, other municipalities, regions, other authorities). Damage to external actors can be a loss of trust in them, negative impact in their ability to achieve their goals or fulfil their primary tasks, as well as economic damage such as reduced revenue, increased costs and damage to assets

Table 10.
Formulation of consequence level for category external actors

was a general lack of understanding about one of the most important aspects of information security, the information security principles, which can point to the fact that information security awareness should be raised through education and awareness programs. This issue was also highlighted by I3 that:

> If we are to get through information classification, it is important that there is guidance available. [. . .] people need to be educated and that there is good method support available.

This is in line with a study conducted in public organizations in Greece where the findings showed that the level of employee information security awareness is low and needs to be raised (Loukis and Spinellis, 2001). Furthermore, other previous studies also confirm the lack of information security awareness among employees (Chan and Mubarak, 2012; Mataracioglu and Ozkan, 2011; Khando *et al.*, 2021) and highlight the fact that the human factor is one of the most common reasons for security breaches in organizations due to the employees' lack of information security awareness (Soomro *et al.*, 2016; Spears and Barki, 2010; Parsons *et al.*, 2014).

Another finding that confirms the need for education is that employees at the studied municipality had difficulties identifying the type of information that they work with. One of the first steps of conducting information classification is to identify information assets and its value for the organization (Oscarson and Karlsson, 2009) and failing to do so is deemed to be one of the factors for inadequate protection levels within organizations (Adesemowo *et al.*, 2016). This is in line with the findings of a literature study, which showed that one of the elements of information security awareness is that employees understand the value of the information they handle and that it can be achieved through education (Nel and Drevin, 2019).

Furthermore, the findings of this study highlight the necessity for the usage of a unified information security language within the organization. This necessity was also addressed by I10 in the following quote:

> I think that these different concepts and vocabularies, such as these principles, [. . .] and I think that this common use of language is very important that we establish within the municipality, so that we can communicate with each other.

Having a unified language that is used by everyone in an organization helps create a shared vocabulary that makes communication easier and helps create a better understanding of the shared goals of the organization (Tamjidyamcholo *et al.*, 2013).

Additionally, I9 indicated that:

> [. . .] understandability is an important aspect of availability in their work since the individuals they provide services for might have disabilities that require specific aids such as image support and sign interpreter in order to understand the information communicated to them by the municipality.

This raised the question of adding understandability as an aspect of the information security principle of Availability. Within the information security field, understandability has been studied from the perspective of understanding and compliance with information security policies (Alkhurayyif and Weir, 2017; Nel and Drevin, 2019), but not from the perspective of being an aspect of availability. In an organization such as the municipality where communication of information to the public is one of the most important tasks, whether the communicated information is understood by the receiver of that information, is directly related to the availability of that information. One can argue that if information that is supposed to be communicated is not understood then it has not been made available. One example that highlights this fact is that despite the efforts of the Swedish authorities to communicate crucial information to the public during the early stages of the Covid-19 pandemic, the information was not understood by people with disabilities such as hearing disabilities and people who do not understand Swedish, which could have resulted in the increase of infection in society (Hrf Stockholm län, 2020).

5.2 Outcomes and benefits

As discussed in Section 2.3.3, the information classification model currently used at the studied municipality is based on MSB's model with only minor modifications, and therefore, does not address the information classification issues that the municipality is experiencing. This study has addressed these issues by creating an information classification model that is tailored toward the municipality. The main contribution of this study is the provided information classification model for the studied municipality and all Swedish municipalities. This is because all Swedish municipalities operate in similar areas, handle similar types of

information and must abide by the same laws and regulations. The provided model can be viewed as the first step toward a Swedish municipal model for information classification.

The provided model will help the municipalities with the implementation of their information classification process. This will allow employees who work within the different operating areas of the municipalities to be part of the information classification process and thereby classify the information that they handle in their daily work, based on the value that the information has for the specific area that the employees work in. A further benefit of employees being part of the information classification process is that it can make them aware of how sensitive some information they work with is and how important it is to protect it (Tankard, 2015). This can ultimately lead to a more mature information security culture in an organization (Nel and Drevin, 2019).

According to Oscarson and Karlsson (2009), when many organizations share information, there is a need for an agreement on a common level of protection and the first step is to agree on a common ground for valuing and classifying information. Furthermore, Oscarson and Karlsson (2009) state that to enable such a common ground, there is a need for a uniform tool for information classification. The model provided by this study can be used as a communication tool for facilitating a common ground in the business negotiation process between municipalities and other organizations. Furthermore, having a common municipal information classification model eases the communication between municipalities and information will be classified on the same basis in all municipalities.

Moreover, while conducting this study it became evident that the following set of steps was necessary to tailor an information classification model to suit a specific organization:

(1) Investigate the organizational structure, goals and visions to have an understanding about the organizational values and the different areas that the organization operates in.

(2) Investigate relevant information security documents such as policy and guidelines to understand how information classification is supposed to be conducted according to the specific organization's policies and regulations.

(3) Interviewing relevant employees that have responsibility for or have a close insight into the handling of information in each part of the organization.

(4) The tailored model should be based on:

(5) The national information classification model forms the baseline for the model and the consequence categories.

(6) The organizational structure and the identified operating areas determine the relevant consequence categories to be incorporated within the model.

(7) The interview data establish the baseline for the formulation of the consequence categories and levels.

To make the model easier to use and understand (Oscarson and Karlsson, 2009), this study suggests that the model design should be divided into the identified consequence categories. Having all the consequence categories in one single model would make the model too big and less user friendly (MSB, 2018a). Furthermore, this division makes the participants in the information classification process focus on one category at a time and decrease the risk of overlooking some categories. Additionally, according to the CISO at municipality X the division by the consequence categories create a good foundation for making the information classification process digitally interactive. The final models for each category are written in Swedish and are available upon request.

The set of steps for how to tailor an information classification model to a specific organization that this study provides can be used by any organization in Sweden and other Scandinavian countries. Furthermore, other organizations outside of Scandinavia could use this set of steps as a guideline while taking into consideration the cultural and organizational differences.

5.3 Limitations

We are also aware of some limitations of this study. First, the representatives of some operating areas (i.e. leisure, culture and tourism and special societal support) of municipality X support were not able to take part in an interview due to time constraints and possibly because of the current Covid-19 situation. Second, there are some other information security principles (e.g. traceability, understandability) could have been further investigated. Last but not least, all the interviewees in this study were conducted in one municipality from Sweden. The generalizability of the results to other Swedish municipalities needs to be further explored.

6. Conclusions

This study aimed to tailor an information classification model to the specific needs of a Swedish municipality. A case study in a Swedish municipality was carried out. This study resulted in an information classification model that is tailored to suit the specific needs of Swedish municipalities. In addition, a set of steps for tailoring an information classification model to suit a special public organization were recommended. The findings also indicate that for a successful information classification it is necessary to educate the employees about the basics of information security and classification and create an understandable and unified information security language.

It also exists some opportunities for future research. First, a further study could expand this study to investigate the need for traceability as another information security principle in the tailored information classification model. Second, the usability of the created information classification model can be tested in other Swedish municipalities.

References

Adesemowo, A.K., von Solms, R. and Botha, R.A. (2016), "Safeguarding information as an asset: do we need a redefinition in the knowledge economy and beyond?", *SA Journal of Information Management*, Vol. 18 No. 1, pp. 1-12.

Agrawal, V. (2017), "A framework for the information classification in ISO 27005 standard", *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*.

Ali, O., Shrestha, A., Chatfield, A. and Murray, P. (2020), "Assessing information security risks in the cloud: a case study of Australian local government authorities", *Government Information Quarterly*, Vol. 37 No. 1.

Alkhurayyif, Y. and Weir, G.R.S. (2017), "Readability as a basis for information security policy assessment", *Proceedings – 2017 7th International Conference on Emerging Security Technologies, EST 2017, 8090409*, pp. 114-121.

Ander, T. (2020), *Rutin – Informationsklassning [Routine - Information classification]* (Ks 63/2020). X: X municipality.

Bergström, E. and Åhlfeldt, R.M. (2014), "Information classification issues", in Bernsmed, K., Fischer-Hübner, S. (Eds), *Secure IT Systems. NordSec 2014. Lecture Notes in Computer Science, 8788*, Springer, Cham, pp. 27-41.

Bergström, E., Åhlfeldt, R.M. and Anteryd, F. (2016), *Informationsklassificering Och Säkerhetsåtgärder [Information Classification and Security Measures]*, Högskolan i Skövde, Skövde.

Bergström, E., Anteryd, F. and Åhlfeldt, R.M. (2018), "Information classification policies: an exploratory investigation", *Proceedings of the Annual Information Institute Conference*.

Booysen, H.A.S. and Eloff, J.H.P. (1995), "Classification of objects for improved access control", *Computers and Security*, Vol. 14 No. 3, pp. 251-265.

Button, M., Wang, V., Klahr, R., Amili, S. and Shah, J. (2016), "Cyber Breaches Survey 2016", Ipsos MORI, London, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/521465/Cyber_Security_Breaches_Survey_2016_main_report_FINAL.pdf (accessed 11 February 2020)

Chan, H. and Mubarak, S. (2012), "Significance of information security awareness in the higher education sector", *International Journal of Computer Applications*, Vol. 60 No. 10.

Eloff, J.H.P., Holbein, R. and Teufel, S. (1996), "Security classification for documents", *Computers and Security*, Vol. 15 No. 1, pp. 55-71.

Evans, M., He, Y., Maglaras, L., Yevseyeva, I. and Janicke, H. (2019), "Evaluating information security core human error causes (is-CHEC) technique in public sector and comparison with the private sector", *International Journal of Medical Informatics*, Vol. 127, pp. 109-119.

Everett, C. (2011), "Building solid foundations: the case for data classification", *Computer Fraud and Security*, Vol. 2011 No. 6, pp. 5-8.

Ghernaouti, S., Simms, D. and Tashi, I. (2011), "Protecting information in a connected world: a question of security and of confidence in security", *2011 International Conference on Network-Based Information Systems, NBiS 2011*, pp. 208-212.

Halim, H. and Yusof, M.M. (2019), "Framework for digital data access control from internal threat in the public sector", *International Journal of Advanced Computer Science and Applications*, Vol. 10 No. 8, pp. 61-67.

Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J.P. (2011), "Value conflicts for information security management", *The Journal of Strategic Information Systems*, Vol. 20 No. 4, pp. 373-384.

HRF Stockholm län (2020), "This is how covid-19 affects HRF and people with hearing loss", available at: https://hrf.se/stockholmslan/om-oss/sa-paverkar-covid-19-hrf-och-personer-med-horselskada/ (accessed 13 May 2020)

ISO/IEC 27000 (2017), *Information technology – Security techniques – Information security management systems – Overview and vocabulary* (ISO/IEC 27000:2016).

ISO/IEC 27002 (2017), *Information technology – Security techniques – Code of practice for information security controls* (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015).

ITU-D (2018), "Global cybersecurity index 2018. (GCI 2018)", available at: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Khando, K., Gao, S., Islam, S.M. and Salman, A. (2021), "Enhancing employees information security awareness in private and public organisations: a systematic literature review", *Computers and Security*, Vol. 106, p. 102267.

Loukis, E. and Spinellis, D. (2001), "Information systems security in the Greek public sector", *Information Management and Computer Security*, Vol. 9 No. 1, pp. 21-31.

Ma, Q., Johnston, A.C. and Pearson, J.M. (2008), "Information security management objectives and practices: a parsimonious framework", *Information Management and Computer Security*, Vol. 16 No. 3, pp. 251-270.

Mataracioglu, T. and Ozkan, S. (2011), "User awareness measurement through social engineering", *arXiv preprint arXiv:1108.2149*.

May, T. (2011), *Social Research Issues, Methods and Process*, 4th ed., McGraw Hill, Maidenhead.

MSB [Swedish Civil Contingencies Agency] (2018a), "Klassningsmodell [Classification model]", available at: www.informationssakerhet.se/metodstodet/utforma/#klassningsmodell (accessed 22 February 2020)

MSB [Swedish Civil Contingencies Agency] (2018b), "Utformning av matrisen – antal kolumner och rader [Layout of the matrix – number of columns and rows]", available at: www.informationssakerhet.se/metodstodet/utforma/#utformning-av-matrisen-%E2%80%93-antal-kolumner-och-rader (accessed 13 February 2020)

MSB [Swedish Civil Contingencies Agency] (2020), "Informationssäkerhet.se [Information security]", available at: www.informationssakerhet.se/ (accessed 3 February 2020)

Na, O., Park, L.W., Yu, H., Kim, Y. and Chang, H. (2019), "The rating model of corporate information for economic security activities", *Security Journal*, Vol. 32 No. 4, pp. 435-456.

Nel, F. and Drevin, L. (2019), "Key elements of an information security culture in organisations", *Information and Computer Security*, Vol. 27 No. 2, pp. 146-164.

Oates, B.J. (2006), *Researching Information Systems and Computing*, SAGE Publications, London.

Oscarson, P. (2003), "Information security fundamentals: graphical conceptualisations for understanding", in Irvine, C. and Armstrong, H. (Eds), *Security Education and Critical Infrastructures. IFIP, 125*, Springer, New York, NY, pp. 95-107.

Oscarson, P. and Karlsson, F. (2009), "A national model for information classification", *AIS SIGSEC Workshop on Information Security and Privacy (WISP 2009)*, *Phoenix, AZ, USA*.

Ozkan, S. and Karabacak, B. (2010), "Collaborative risk method for information security management practices: a case context within Turkey", *International Journal of Information Management*, Vol. 30 No. 6, pp. 567-572.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)", *Computers and Security*, Vol. 42, pp. 165-176.

Peltier, T.R. (1998), "Information classification", *Information Systems Security*, Vol. 7 No. 3, pp. 31-43.

Soomro, Z.A., Shah, M.H. and Ahmed, J. (2016), "Information security management needs more holistic approach: a literature review", *International Journal of Information Management*, Vol. 36 No. 2, pp. 215-225.

Spears, J.L. and Barki, H. (2010), "User participation in information systems security risk management", *MIS Quarterly*, Vol. 34 No. 3, pp. 503-522.

Tamjidyamcholo, A., Bin Baba, M.S., Tamjid, H. and Gholipour, R. (2013), "Information security – Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language", *Computers and Education*, Vol. 68, pp. 223-232.

Tankard, C. (2015), "Data classification - The foundation of information security", *Network Security*, Vol. 2015 No. 5, pp. 8-11.

Tijan, E. (2009), "Data classification and information lifecycle management in port community systems", *Pomorstvo*, Vol. 23 No. 2, pp. 557-568.

Yin, R. (2014), *Case Study Research: Design and Methods*, 5th ed., Sage Publications, Thousand Oaks, CA.

Corresponding author
Shang Gao can be contacted at: shang.gao@oru.se