Information security metrics based on organizational models

JONAS HALLBERG, KRISTOFFER LUNDHOLM

FOI, Swedish Defence Research Agency, is a mainly assignment-funded agency under the Ministry of Defence. The core activities are research, method and technology development, as well as studies conducted in the interests of Swedish defence and the safety and security of society. The organisation employs approximately 1000 personnel of whom about 800 are scientists. This makes FOI Sweden's largest research institute. FOI gives its customers access to leading-edge expertise in a large number of fields such as security policy studies, defence and security related analyses, the assessment of various types of threat, systems for control and management of crises, protection against and management of hazardous substances, IT security and the potential offered by new sensors.

FOI
Swedish Defence Research Agency
Information Systems
P.O. Box 1165
SE-581 11 Linköping

Phone: +46 13 37 80 00
Fax: +46 13 37 81 00

www.foi.se

FOI-R--2823--SE
ISSN 1650-1942

Base data Report
September 2009

Information Systems

Jonas Hallberg, Kristoffer Lundholm

Information security metrics based on organizational models

Titel	Informationssäkerhetsmetriker baserade på organisationsmodeller
Title	Information security metrics based on organizatic models
Rapportnr/Report no	FOI-R--2823--SE
Rapporttyp Report Type	Underlagsrapport
Månad/Month	September
Utgivningsår/Year	2009
Antal sidor/Pages	72 p
ISSN	ISSN 1650-1942
Kund/Customer	Myndigheten för samhällsskydd och beredskap
Kompetenskloss	26 IT-säkerhet
Extra kompetenskloss	
Projektnr/Project no	B7110
Godkänd av/Approved by	Hans Frennberg

FOI, Totalförsvarets Forskningsinstitut
Avdelningen för Informationssystem
Box 1165
581 11 Linköping

FOI, Swedish Defence Research Agency
Information Systems
Box 1165
SE-581 11 Linköping

Summary

It has proved to be difficult for organizations, including government agencies, to reach adequate information security levels, as illustrated by a report from the Swedish national audit office published in 2007 (RiR, Swedish National Audit Office 2007). The COntrolled INformation Security (COINS) research project, of which this report is an intermediate result, aims to support Swedish government agencies in reaching higher levels of information security.

The report studies a Swedish agency by creating two different types of models. The input to these models was taken partly from the agency's intended information security program, as described by documents, and partly from the agency's security work, captured through interviews with security personnel. For the sake of comparison, the same two types of models were also created from the controls listed in the standard ISO/IEC 27001 appendix A.

The models show that many interactions within the agency involve entities which are very broadly defined, e.g. "agency personnel". With entities like this in the organizational model it is hard to assign responsibilities for actions connected to these interactions.

The models also show that the relative focus of the agency's intentions corresponds well with the relative focus of the ISO standard while the relative focus for the actual work differs from both the standard and the intentions. This difference is, however, believed to stem from the focus of the questions asked in the interviews rather than inconsistencies between the procedures and the actual work.

Keywords:

Information security, Information system, Organizational model, Security metric

Content

1 Introduction

It has proved to be difficult for organizations, including government agencies, to reach adequate information security levels (RiR, Swedish National Audit Office 2007). This is because the actual security levels of organization are unknown. Commonly, there are not even qualified assumptions regarding the information security levels. Thus, it is important to distinguish between perceived and actual information security (Oscarson 2007). All too often, there is a divide between the perceived and actual level of information security, a divide that has to be diminished.

This report is an intermediate result of the research project Controlled Information Security, COINS, which is funded by the Swedish Civil Contingencies Agency (MSB). The purpose of COINS is to support government agencies in their work to reach adequate levels of information security and to be able to communicate this to relevant parties, such as other agencies and the general public. The purpose of this report is to illustrate how the modeling of security-related data and use of security metrics can be used to illustrate the status of the security work in governmental agencies.

1.1 Motivation

There is much data to be collected from governmental agencies regarding their information security. In the COINS project, the focus is on how information security issues are communicated within these organizations. Information security data can be collected from many different domains, such as human factors, organization, technology, and system operation. Because of all the relevant data powerful methods for analysis are necessary, else the data will not support, only obstruct, the relevant decision processes.

The studies performed within the COINS project have resulted in data related to the communication of security issues within a governmental agency. In order to illustrate the results, this data has been modeled using innovative techniques (Yngström et al. 2009). These models constitute a foundation for the development of security metrics supporting security-related decision processes.

1.2 Problem formulation

The main problem considered in this report is how to support the analysis of the information security of an organization based on data sets of the kind that have been collected within the COINS project. For this purpose a set of information security metrics have to be defined. In order to formulate these metrics, supporting models of the organization have to be derived. These models are

based on the modeling techniques devised within the COINS project (Yngström et al. 2009).

Thus far, the data collection from interviews within the COINS project has been focused on the communication of information security issues while the data collection from documents encompasses all received documents. An important aspect is how this data can be augmented with additional data describing the information security qualities of the studied agency.

The problem formulation is captured by the following questions.

- What models can be created based on the available data and models in order to illustrate the information security level of the studied organization?
- What metrics can be formulated to support the analysis of the information security of the studied organization?

1.3 Contributions

This report presents two different types of models for the following instances of organizations for information security.

- The normative standard of information security management systems ISO/IEC 27001. These models are based on appendix A of the standard.
- The, by the management, decided organization for information security. These models are based on documents regarding information security collected from the studied agency.
- The organization of information security as detected at the agency. These models are based on the transcripts of interviews with security personnel at the studied agency.

The first type of model is the cube, presented in (Yngström et al. 2009, sec.4.4), and the second type is meant to show between what entities communication takes place. The second type of model is based on the modeling technique showing the three decision levels of an organization (Yngström et al. 2009, sec.4.2).

Finally, a number of security metrics which will support the analysis based on the introduced models are identified. Thus, the questions formulated in the problem formulation are addressed by the results presented in this report.

1.4 Report layout

Chapter 1 contains the introduction to the report

Chapter 2 provides background needed to understand the report, including a summary of the modeling techniques described in (Yngström et al. 2009).

Chapter 3 presents the modeling techniques that will be used to create the models presented in chapter 5 and 6.

Chapter 4 presents the metrics used in this report

Chapter 5 contains the cube models for ISO/IEC 27001 appendix A, the statements from the agency documents, and the statements from the interviews with agency security personnel as well as the metrics introduced in chapter 4 and their interpretation.

Chapter 6 contains the entity-action models for ISO/IEC 27001 appendix A, the statements from the agency documents, and the statements from the interviews with agency security personnel as well as the metrics introduced in chapter 4 and their interpretation.

Chapter 7 presents the discussion of the results as well as possible future paths.

2 Background

The background of this work is presented through a list of relevant terminology and related work.

2.1 Terminology

In Table 1 terms used in this report are explained. The descriptions of the terms should not be considered universally applicable, but constitute a setting for the work presented in this report.

Table 1: Terms related to information security metrics relevant for this report.

Term	Description
Information security	Information security relates to information assets and the ability to uphold security-related characteristics, such as confidentiality, integrity, and availability (SIS 2007). Consequently, information is a vast area including administrative as well as technical security issues. Contrary to IT security, information security includes issues related to information processing not connected to information (IT) systems, such as transmission by speech or paper documents.
Information system	Information systems collect, process, store and distribute information. The term has a general meaning, but is most often used for computer based information systems. The definition includes the technical equipment of a system as well as its human activities and routines (http://www.ne.se/jsp/search/article.jsp?i_art_id=211494).
ISO/IEC 27001 appendix A	Appendix to the security standard containing the controls from ISO/IEC 27002. In this report ISO/IEC 27001 appendix A will be referred to as the standard.
Metric	The purpose of information security metrics is to support the measurement and computation of security values characterizing the information security posture of entities. Studied entities can be, for example, organizations, humans, and routines. There are many interpretations of the term security metrics. Here the following definition is adopted. A security metric contains three main parts: a magnitude, a scale and an interpretation. The security values of systems are measured according to a specified magnitude and related to a scale. The interpretation prescribes the meaning of obtained security values. (Hallberg et al, 2004) The presence of magnitude and scale means there should be values that can be measured or computed. Moreover, the interpretation of the values, in the context of information security posture, should be possible. However, to achieve measurability and computability on one hand and interpretability on the other hand has proved to be difficult.

Term	Description
Model	The purpose of models is to describe something. This something can be tangible, as houses or computer systems, or abstract such as human emotions. Models are used to enable the analysis of the modeled thing. Thus, adequate models need to capture the characteristics relevant to the analysis. Meta-models are modeling models.
Modeling technique	Modeling techniques support the modeling, that is, the process resulting in models. A meta-model may support a modeling technique.

2.2 Related work

The area of information security metrics has recently received considerable attention. This is manifested by the works of Herrmann (2007), Jaquith (2007), Chew et al (2008), and others. Still, it has not been stated to what extent the use of information security metrics can provide relevant and valid knowledge of the security level for the studied organization. Thus, the COINS project aims at studying the context of security metrics programs at governmental agencies. For this purpose, a combination of system theory and cybernetics is utilized (Beer 1981; Gigch 1974; Shannon 1998; Langefors 1968; Ashby 1956; P. P. Schoderbek et al. 1990).

2.2.1 The model report

The model report (Yngström et al. 2009) predates this report and was also produced within the COINS project. The model report contains a number of generic models that capture different aspects of communication between entities. Two of these models, the cube model and the three decision levels model, constitute the foundation for the models in this report. The model report also contains some of the data used to populate the models created in this report. The original models from the model report, and the data used are discussed below. The description of how the cube model was modified is found in chapter 5 and the description of how the three decision levels model was modified is found in chapter 6.

2.2.1.1 Three decision levels model

An enterprise is assumed to have three decision levels; the strategic, the tactic, and the operational. The concept of the generalized model of the three decision levels is shown in Figure 1. The generalized model is recursive, meaning that each of the circles could be an enterprise or all of the circles could be fit into one circle of a larger enterprise (Yngström et al. 2009, sec.4.2). The circles represent the generalized decision motivator which will not be further discussed here since it is not used in the modified model presented in this report. In Figure 1, the

dotted lines represent peer-to-peer communication, the solid lines represent physical signals, and the arrows represent the communication of strategic issues.

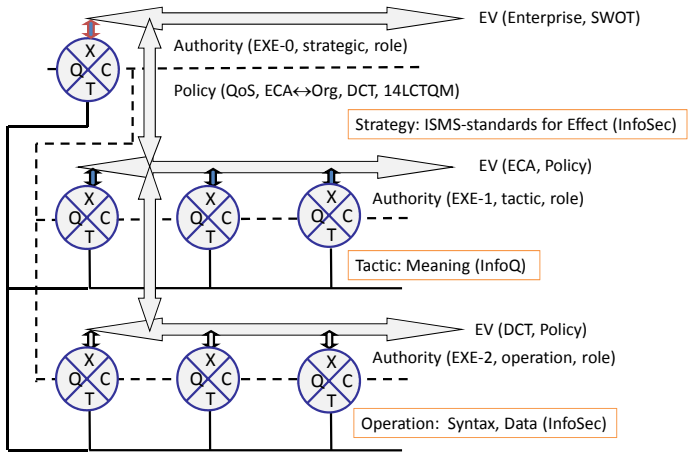

Figure 1: Generic model showing three decision levels. (Yngström et al. 2009, sec.4.2)

2.2.1.2 Cube model

The cube model was introduced in (Yngström et al. 2009, sec.4.4) as a way of providing a compact, yet comprehensive picture of the information security work of an enterprise.

The cube, Figure 2, has axes representing decisions, communications, and rules. The decisions axis represents the life cycle stages for any system. The rules axis represents the environment, the seven social layers (SWOT, cultural, ethical, legal, managerial, organizational, and adaption), and the seven technical layers (application, presentation coding, session, transport, network, link, and physical medium) (Yngström et al. 2009, sec.4.1). In the cube model, the seven social and the seven technical layers are merged into the social and technical aspects, respectively. The communications axis represents the three decision levels in an enterprise as described above.

In this report, data concerning information security is inserted into the cube. Once all available data has been inserted a picture emerges of the organizations security efforts. The data inserted into the cube comes from statements. These statements are either extracted from documents and interviews from the studied agency, as explained below, or consisting of the security controls from the standard. The statements are allocated to one of the sub cubes by classification. How the classification is done is presented in section 3.1.1 of this report.

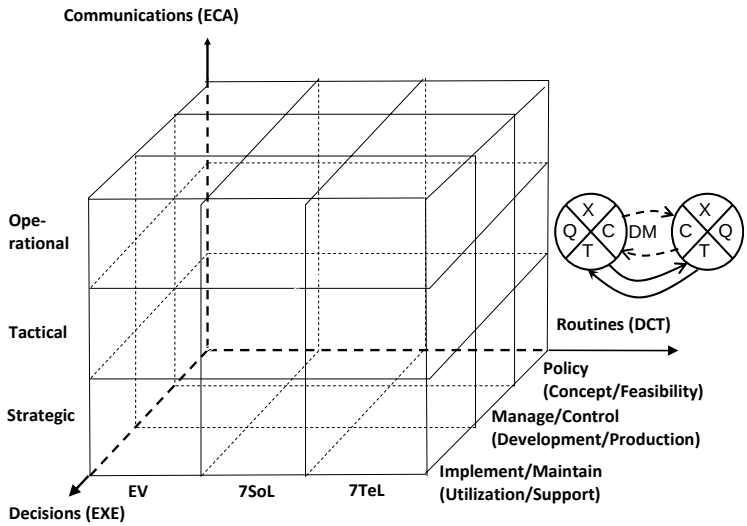

Figure 2: The cube as presented in the models report. (Yngström et al. 2009, sec.4.4)

2.2.1.3 Agency documentation and interviews

In the model report (Yngström et al. 2009, chap.6), the result of an analysis of documents is presented. The studied documents regard the security work at the agency. The presented results consist of 93 identified statements. Since the report deals with the communication of security issues, each identified statement is analyzed from a communications perspective. Thus, for 72 of the statements the sender or receiver has been identified. The data used to create the model of the agency documents presented in this report comes from the statements in the model report.

The result from the analysis of the interviews is included in appendix C. There were three persons interviewed and the interviews had a focus on the communication of information security. The analysis presents the 93 statements, where a sender or receiver could be identified for 60 statements.

3 Modeling techniques

This chapter outlines how the models presented in later chapters were created.

3.1 Classification using the cube

A summary of the cube modeling technique was given in the background chapter. For a more detailed description see (Yngström et al. 2009, sec.4.4). The cube modeling technique will here be used to create models of the studied organization's documents and the answers from interviews with security personnel as well as the standard. Thus, there are models of the norm, the decided structure, and the agency's security work.

Classification will be performed on statements. In the case of the standard, these statements are the controls that can be found in the standard. For the agency the statements are those described in section 2.2.1.3 of the background.

Each type of input data (standard, documents, and interviews) will be displayed as a bar graph with one bar for each of the 27 sub cubes showing the relative distribution of how the statements have been classified for each of the 27 sub cubes in the cube modeling technique.

3.1.1 Description of the classification process

The classification of statements according to the cube takes into account the communication expressed in these statements. For statements that explicitly describe some form of communication, the methods below can be used directly. For statements that do not have this explicit description, an analysis is performed in order to identify what kind of communication needs to be present for the statement to be fulfilled. The result of the analysis is used to classify the statement.

Statements that are produced from documents or interviews should be possible to classify to one single value for each dimension. If this is not true then the statement should be rewritten as several statements so that this property holds.

Statements from standards or other sources that can not be modified before classification is performed may be classified as belonging to more than one value for each dimension.

Before the classification is performed, the scope of the communicating entities should be defined. This is because it should be possible to determine what should be considered external to the scope and thus part of the environment and what is considered as belonging to the scope.

3.1.1.1 Environment, Social, Technical

This dimension concerns *what* is communicated. Classification of statements in this dimension is done by following the three step algorithm below.

1. If the communication identified in a statement concerns any external entity or interaction with an external entity, the statement should be classified as “environment”.
2. For the remaining statements, if the communication identified in a statement concerns technical maters the statement should be classified as “technical”. Statements concerning the interaction with information systems are classified as *technical* when the interaction is part of the maintenance of the information system. When the interaction is related to the use of the information system, the statement is classified as *social*.
3. The remaining statements should be classified as “social”.

3.1.1.2 Strategic, Tactic, Operational

This dimension concerns to what level in the organization the communication belongs.

- Statements considering how to carry out work tasks that directly affect information security or that support the tactical or strategic level by providing data describing current information security level should be classified as “operational”.
- Statements concerning how to fulfill established goals and decide what actions are needed to achieve them as well as distribution of information security tasks should be classified as “tactical”.
- Statements concerning creation of goals and policies as well as decisions contributing to increasing the organization’s overall information security should be classified as “strategic”.

3.1.1.3 Plan, Operate, Control

This dimension considers where in the life cycle of the organization’s information security program the communication take place. Classification should be performed by considering what phase of the life cycle the communication identified in the statement is most likely to occur.

- Communication about the development of policies, routines or procedures, or the creation of plans should be classified as “plan”.
- Communication about using policies, routines or procedures, or about performing actions according to already developed plans should be classified

as “operate” (note the special case of controlling something according to a policy, routine or procedure which should be classified as “control” in stead of “operate”).
- Communication about checking up on, controlling or evaluating should be classified as “control”.

3.2 Entity-action models

The objective of the entity-action models is to visualize the communication between entities by showing what entities in the modeled organization that interact with each other.

Each model consists of a table and a graph. The table includes the entities explicitly stated in the underlying data and references to where the entities are mentioned. In the graphs, the nodes represent the entities and the connections between the nodes represent interaction. Only those entities involved in interactions where both the sender and the receiver have been specified are included in the graphs. The direction of the interaction is indicated by an arrow. On each such arrow is listed a set of numbers that refers to the statements describing the interaction.

The graphs are divided in such a way that entities belonging to the strategic level are depicted at the top of the graph, entities belonging to the tactic level are depicted in the middle of the graph and entities belonging to the operational level are depicted at the bottom of the graph. The entities that are considered external to the organization or undefined have been placed as to minimize the number of intersections of the interactions.

4 Metrics

This chapter presents a set of metrics supporting the analysis of the security level of the governmental agencies, and organizations in general. Firstly, metrics computed from single models are introduced. Secondly, metrics based on data from several models are specified.

4.1 Metrics based on model observations

To support the characterization of the introduced models metrics are introduced for the cube as well as the entity-action models.

4.1.1 Metrics for the cube model

4.1.1.1 Cumulative sum of classifications over the 27 sub cubes

A metric connected to this graph will measure the least amount of sub cubes that are required for the cumulative sum of statements included in these sub cubes to be larger than a certain fraction of the total number of statements. For example, what is the smallest number of sub cubes that contains 80% of the statements? The value of this metric will show how concentrated the classification is. A high value means that the classification is spread more evenly over the sub cubes while a low value indicates that a few sub cubes are dominating the data set.

Another metric connected to this graph will measure the number of sub cubes without any classified statements. The value of this metric represents the number of the 27 areas represented by the sub cubes that are not addressed in the underlying data for the model.

In order to visualize the metrics from the two paragraphs above, a graph should be created displaying the cumulative sum of the value from the sub cubes, starting from the largest value. From this graph it will also be possible to find the most significant sub cube which is a useful metric for later analysis.

4.1.1.2 Graph with 9 rectangular blocks for each dimension

This metric shows the number of statements classified within each rectangular block of three sub cubes. A rectangular block is defined by fixing the values for two of the dimensions in the cube and varying the third. Doing this will remove the dependence on one of the dimensions. From this it is interesting to extract the most significant rectangular block as well as the least significant rectangular block (can be more than one).

4.1.1.3 Graph with 3 slices of the cube

This metric shows the three graphs for each cube model where each color represents one set of slices of the cube. A slice is created by fixing one of the dimensions and varying the other two. This removes the dependence on two of the variables showing only the dependence on one dimension at the time. From this it is interesting to extract which value is the most significant for each slice.

4.1.2 Metrics for the entity-action models

4.1.2.1 Size of the model

Measurements of the size of a model are useful as an indicator of how much information it can be considered to contain. The size of the model is indicated by the following metrics:

- The number of entities in the model.
- The percentage of entities with at least one interaction. This metric indicates how many percent of the entities that could be tied to an interaction. A low value means that many entities are part of half defined interactions (interactions where only one part of the communication is defined) or were indirectly referenced as the subject of an interaction.

In order to calculate these metrics the following needs to be extracted from the models.

- The number of entities in the model.
- The number of interacting entities in the model (entities with at least one interaction).
- The number of interactions in the model. This is measured by counting the number of actions that has both a sender and a receiver.
- The number of actions in the model. This is defined as the number of statements or controls that was used in the creation of the model.
- The number of assigned actions in the model. This is defined as the number of actions with a sender or receiver (or both).

4.1.2.2 Interaction patterns

Measurements of interactions give information about how communication flows within the modeled organization and is measured by the following metrics:

- The percentage of interactions between layers
- The percentage of interactions inside layer

- The percentage of interactions from inside the organization to external parties. This interaction can be from either defined or undefined entities.
- The percentage of internal interactions involving at least one undefined entity. This value contains all interactions within the organization where at least one of the interacting entities is unknown.

In order to calculate these metrics the following needs to be extracted from the models.

- The number of interactions between layers
- The number of interactions inside layers
- The number of interactions from inside the organization to external parties. This includes all interactions where one entity is external to the organization.
- The number of internal interactions involving at least one unknown entity.

4.2 Metrics based on model comparisons

4.2.1 Metrics for the cube model

4.2.1.1 Comparison of the relative focus

This metric compares the relative focus of the cube models. The metric is calculated by subtracting the relative value for one sub cube in one model with the value from the same sub cube for another model. The result from this subtraction is the percentage point difference between the relative focus for the models. The metric will illustrate how the priority expressed by the modeled aspects of the organization differs.

4.2.1.2 Graph with 9 rectangular blocks for each dimension

This metric is a graph with the metrics graphs from all the models to be compared in the same figure. From this compound metric it is possible to make comparisons between the different metrics for each of the models, where the comparison is independent of one of the three dimensions of the cube.

4.2.1.3 Graph with 3 slices of the cube

This metric is a graph with the metrics graphs from all the models to be compared in the same figure. From this metric it is possible to compare the metrics for each of the models looking at just one dimension at a time.

4.2.1.4 Relative difference between models

In order to see where the focus for the models differ the most, a metric with the difference between the relative focus for two models is plotted. This metric is constructed by subtracting the values from the 27 sub cubes for one model from another model. A large positive or negative value in this graph represents a big difference in the relative focus of the models. Note that the metric consist of the difference between two normalized data sets, which necessitates the sum of all the values in this metric to be zero.

4.2.2 Metrics for the entity-action models

Comparisons of the size of the model are done by comparing the values of the metrics concerning the size of a single model. This is best done by plotting the number of entities, number of interactions and number of actions for each model in the same graph.

Comparisons of interaction patterns are also best displayed by plotting the individual values of the models to be compared in the same graph.

5 Cube models, metrics, and interpretations

In this chapter the controls of the standard, statements extracted from the agency documentation, and statements extracted from the interviews are modeled. Each model is enhanced with computations of the relevant metrics and their interpretation. Finally, the computations of metrics based on model comparisons and their interpretation is presented.

The differences between the original model, presented in the model report (Yngström et al. 2009, sec.4.4), and the one used in this report are:

- the removal of the axes names, since they do not add any information
- the change of the values of the life cycle axis to plan, operate, and control representing the life cycle stages of an information security program.

The cube model will in this chapter be represented as graphs. When the cube is to be represented as a graph, each sub cube is represented by a triplet representing what layer from each of the three dimensions it came from. A graph of the model will thus contain 27 bars, one for each of the sub cubes. The layers of the cube are shown in Figure 3.

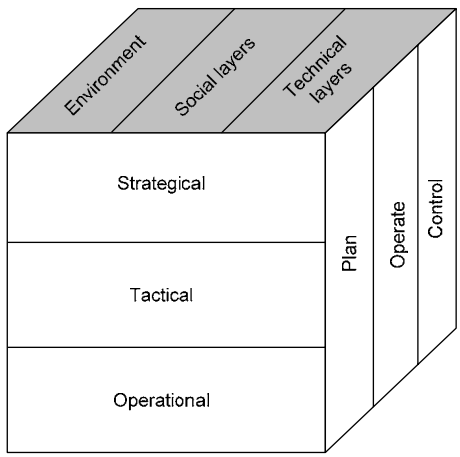

Figure 3: The cube with its layers

Note that all graphs in this chapter contain the relative distribution of values for each model meaning that a high value in one place necessitates a low value somewhere else. The graphs do not show the magnitudes of the absolute values

for the underlying data sets. The reason for using relative values is so that the models should be possible to compare with each other.

In this chapter there will be several references to the different dimensions of the cube and to facilitate the reading a short form for describing a sub cube or block a short form is introduced. To illustrate this short form, consider a sub cube connected to the planning phase of an information security program, concerning strategic work towards the environment, this sub cube will have the short form: (Pl,St,Ev). In this parenthesis the first abbreviation represents what phase in the life cycle for the information security program the sub cube is taken from, where possible values are “Pl” for plan “Op” for operate and “Co” for control. The second abbreviation represents the decision level of the sub cube, where possible values are “St” for strategic, “Ta” for tactic and “Op” for operational work. The last abbreviation represents what is communicated and possible values are “Ev” for environment, “So” for social and “Te” for technical.

The short form also allows for the representation of a rectangular block in the cube. A block is represented by having a wild card in the short form, e.g. (Op,*,Te) which translates to communication about technical maters in the operate phase of the information security program.

5.1 The norm, ISO/IEC 27001 appendix A

5.1.1 The model

It is the organization described by the standard that was considered when the classification of the control objectives was performed. This assumes an organization constructed according to the standard that is supposed to work according to the controls described in the standard.

Classification was performed for each control of the standard according to the description in 3.1. A full list of how each statement was classified is included in appendix A of this report.

The cube model of the standard is shown in Figure 4. When the model was created through the classification of controls in the standard, several of the controls were classified as belonging to more than one sub cube. This is in accordance with the classification guidelines presented in section 3.1.1.

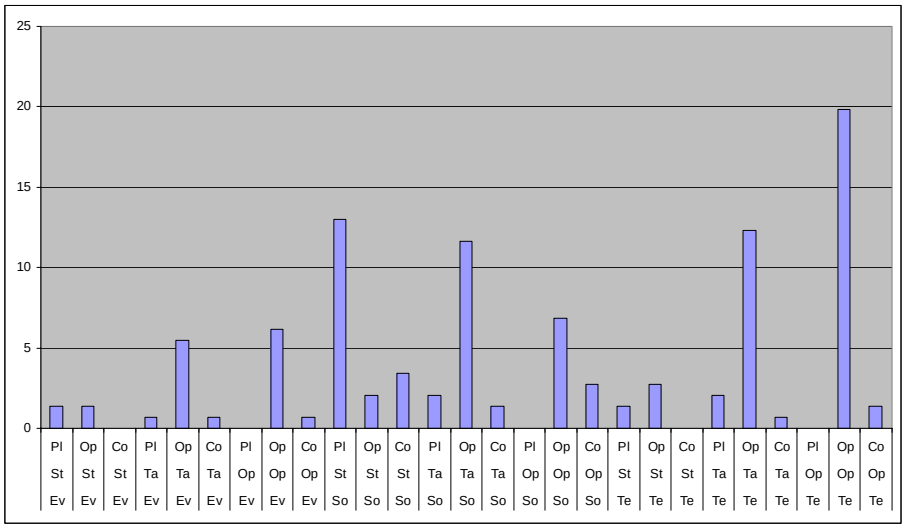

Figure 4 Relative frequency of each sub cube for ISO/IEC 27001 appendix A

5.1.2 The metrics

In Figure 5 the result of ordering the sub cubes according to the number of contained controls is depicted, as described in section 4.1.1.1. The most significant sub cube is the one connected to the operate phase's operative information security work concerning technical aspects (Op,Op,Te). A little over 80% of the classified controls can be covered by 9 sub cubes. The figure also shows that 5 sub cubes are empty.

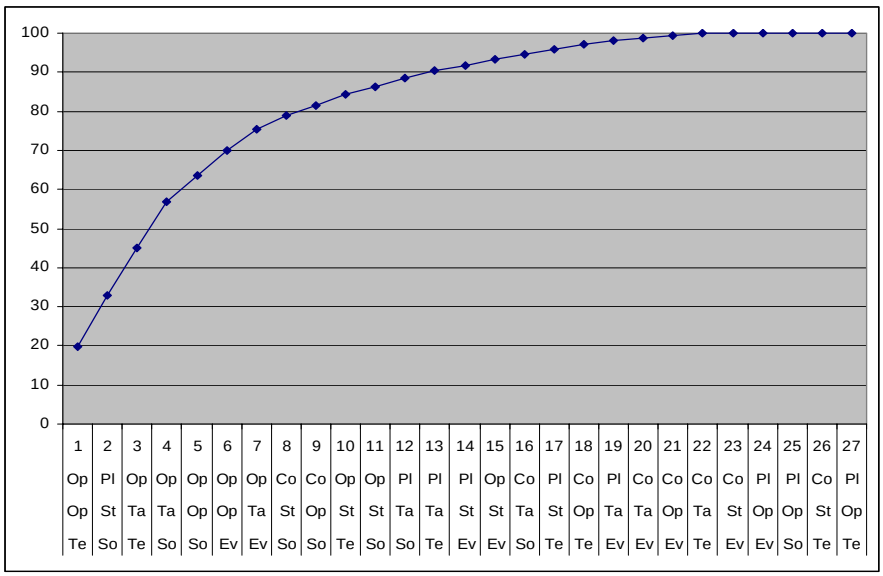

Figure 5: Cumulative percentage of classification of controls in ISO/IEC appendix A for the 27 sub cubes.

The following metrics are all using Figure 6

- The most significant block from the cube where the phase in the life cycle of the information security program is not fixed is the block connected to operational information security work concerning technical aspects (*,Op,Te). The least significant block is the one connected to strategic information security work concerning environmental aspects (*,St,Ev).
- The most significant block from the cube where the decision level is not fixed is the block connected to the operate phase of the information security program concerning technical aspects (Op,*,Te) and the least significant is the block connected to the control phase of the information security program concerning environmental aspects (Co,*,Ev).
- The most significant block from the cube where the content type of the communication is not fixed is the block connected to the operate phase of the information security program concerning operative work (Op,Op,*) and the least significant block is connected to the planning phase of the information security program concerning operative work (Pl,Op,*).

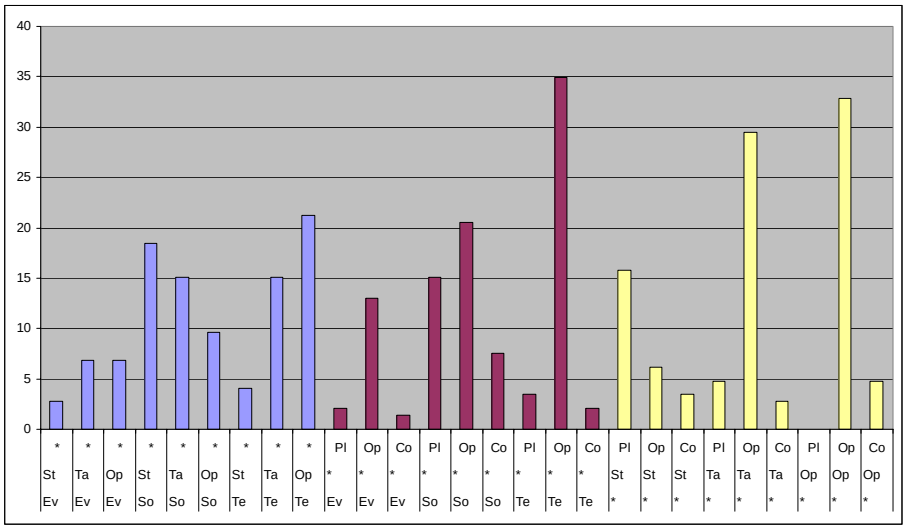

Figure 6: Relative frequency for each rectangular block in the cube for ISO/IEC 27001 appendix A.

The following metrics are all using Figure 7:

- The most significant slice when only considering the life cycle stage of the information security program is the operate phase (Op).
- The most significant slice when only considering the decision level is a tie between tactical (Ta) and operational (Op).
- The most significant slice when only considering the content of the communication is that concerning social aspects (So).

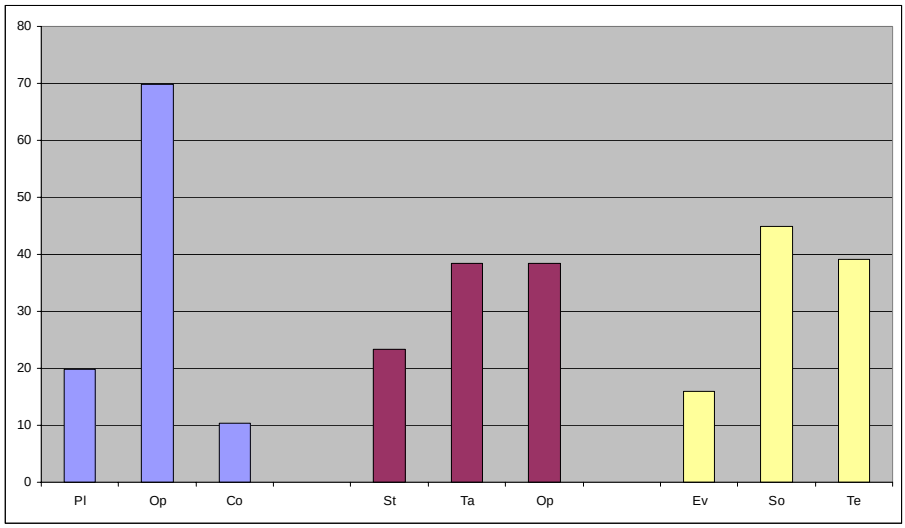

Figure 7: Relative frequency of each slice of the cube for ISO/IEC 27001 appendix A.

5.1.3 Interpretations

The graph with the cumulative percentage of the 27 sub cubes shows that the controls of the standard are rather spread out over the sub cubes with about 80% of the controls concentrated to 9 sub cubes and the remaining 20% found in 13 sub cubes which leaves 5 sub cubes empty.

When interpreting the results from what the most significant cube/block/slice is for appendix A it is quite clear that a majority of the controls are connected to the operate phase of the information security programs life cycle.

When the content of the communication is not considered a very plausible pattern emerges. The three most significant blocks from the cube are those connected to Operational work in the operate phase (Op,Op,*), Tactic work in the operate phase (Op,Ta,*) and strategic work in the planning phase (Pl,St,*).

5.2 Agency intentions, based on studied documents

5.2.1 The model

In order to classify the agency documents using the guidelines, a set of statements to perform the classification on had to be extracted. The extraction of statements from the documents was described in the background.

A table of how each statement was classified is included in appendix A of this report.

The cube model of the agency's intentions as described by documents is shown in Figure 8. In this model each statement was mapped to exactly one sub cube, as demanded by the classification guidelines.

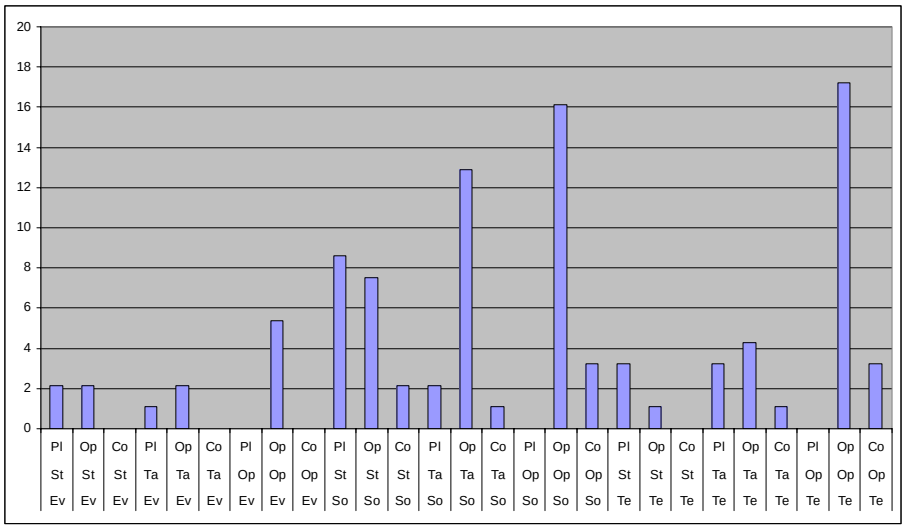

Figure 8: Relative frequency of each sub cube for agency documentation.

5.2.2 The metrics

In Figure 9 the result of ordering the sub cubes according to the number of contained controls is depicted, as described in section 4.1.1.1. The most significant sub cube is the one connected to the operate phase's operative information security work that concerning technical aspects (Op,Op,Te). A little over 80% of the classified controls can be covered by 10 sub cubes. The figure also shows that 7 sub cubes are empty.

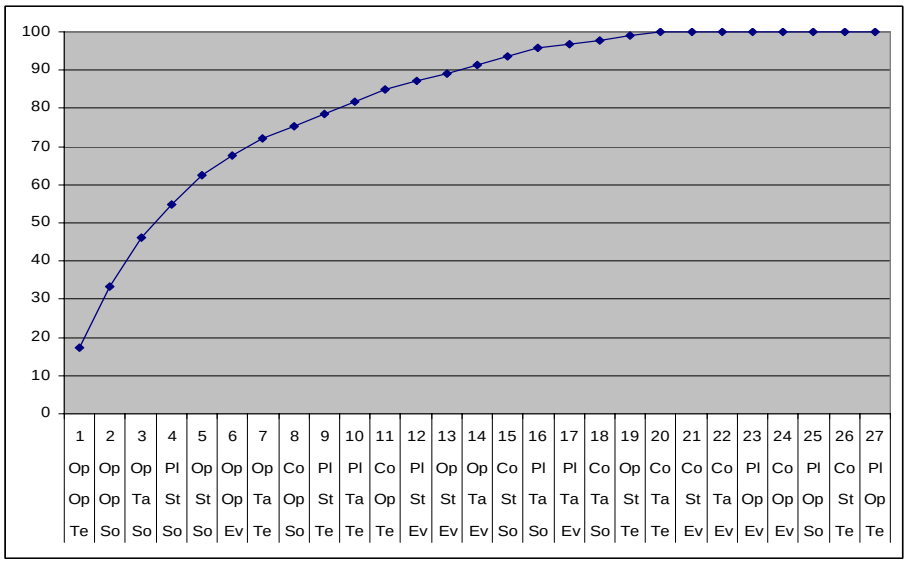

Figure 9: Cumulative percentage of classification of statements from agency intentions for the 27 sub cubes.

The following metrics are all using Figure 10:

- The most significant block from the cube where the phase in the life cycle of the information security program is not fixed is the block connected to operational information security work concerning technical aspects (*,Op,Te). The least significant block is the one connected to tactic information security work concerning environmental aspects (*,Ta,Ev).
- The most significant block from the cube where the decision level is not fixed is the block connected to the operate phase of the information security program concerning social aspects (Op,*,So) and the least significant is the block connected to the control phase of the information security program concerning environmental aspects (Co,*,Ev).
- The most significant block from the cube where the content type of the communication is not fixed is the block connected to the operate phase of the information security program concerning operative work (Op,Op,*) and the least significant block is connected to the planning phase of the information security program concerning operative work (Pl,Op,*).

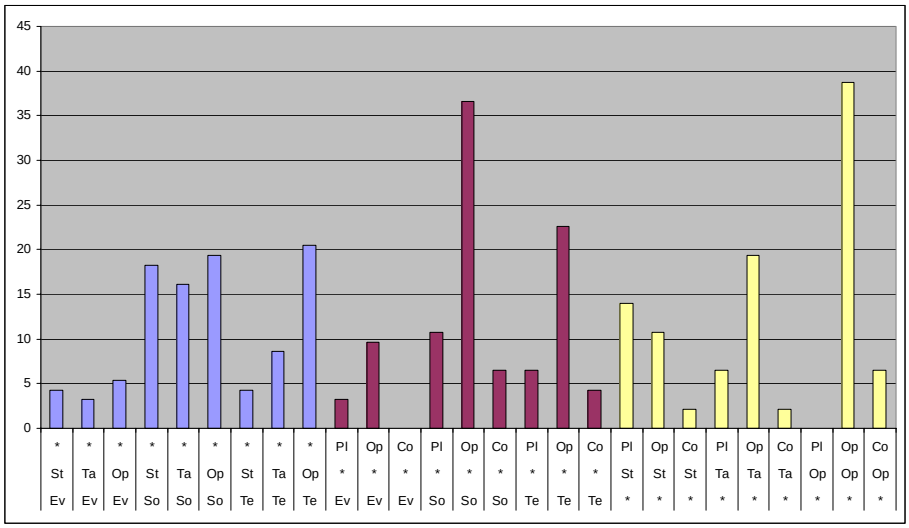

Figure 10: Relative frequency for each rectangular block in the cube for agency documentation.

The following metrics are all using Figure 11:

- The most significant slice when only considering the life cycle stage of the information security program is the operate phase (Op).
- The most significant slice when only considering the decision level is the operational (Op).
- The most significant slice when only considering the content of the communication is that concerning social aspects (So).

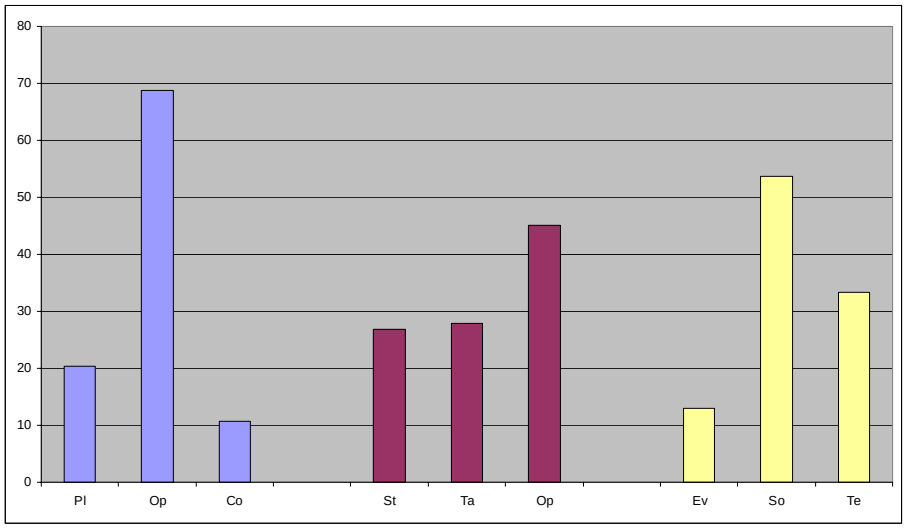

Figure 11: Relative frequency of each slice of the cube for agency documentation.

5.2.3 Interpretations

The graph with the cumulative percentage of the 27 sub cubes shows that the statements from the agency documents are rather spread out over the sub cubes with about 80% of the controls concentrated to 10 sub cubes and the remaining 20% found in 10 sub cubes which leaves 7 sub cubes empty.

Concerning the agency's intentions the metrics shows that the operative phase of the information security programs life cycle is the most important. It also shows that the operative work is the most significant.

When the content of the communication is not considered a very plausible pattern emerges. The three most significant blocks from the cube are those connected to Operational work in the operate phase (Op,Op,*), Tactic work in the operate phase (Op,Ta,*) and strategic work in the planning phase (Pl,St,*).

5.3 Agency work, based on interviews

5.3.1 The model

The model of the interviews with security personnel at the studied agency is based on the statements as described in the background. The summary of the interviews was written by those who performed the interviews so there should be minimal loss of accuracy.

The interviews were performed with the intent of studying communication of information security at the agency and even though the questions asked are very general there is a noticeable bias towards communication. This bias should be considered when analysis based on the model is performed.

The cube model of communication of information security issues at the agency is shown in Figure 12. Most of the statements extracted from the interviews were mapped to one sub cube in accordance with the guidelines described in chapter 3.1.1. The statements that were not mapped are negated statements e.g. “No common view on information security”. These statements were not included when classification was performed since they do not express actual work but rather describes lack of it. It should also be noted that unlike the model of the standard and the agency’s documents, this model of the security work is less likely to give a completely accurate picture. The model is based on the answers to the questions that were asked during the interviews and thus the model contains more uncertainty than those created from documents or from the standard.

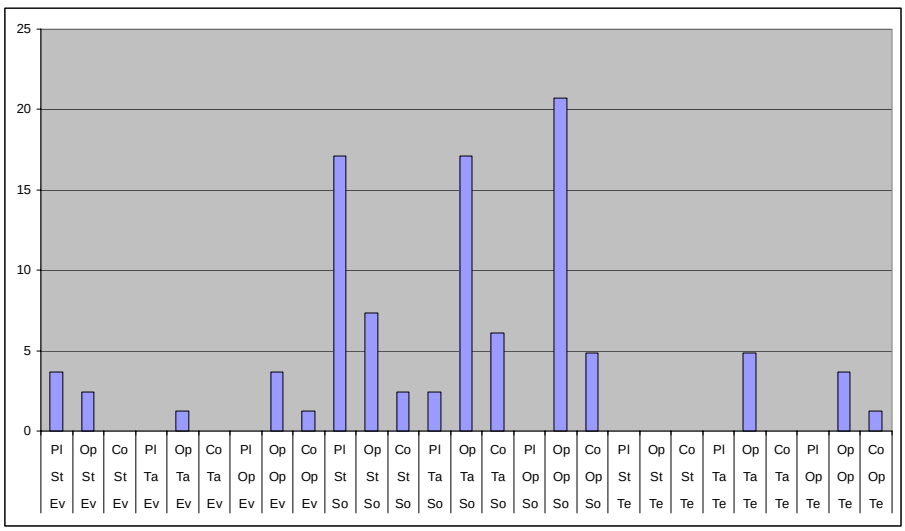

Figure 12: Relative frequency of each sub cube for interviews with agency personnel.

5.3.2 The metrics

In Figure 13 the result of ordering the sub cubes according to the number of contained controls is depicted, as described in section 4.1.1.1. The most significant sub cube is the one connected to the operate phase's operative information security work that concerns social aspects (Op,Op,So). A little over 80% of the classified controls can be covered by 8 sub cubes. The figure also shows that 11 sub cubes are empty.

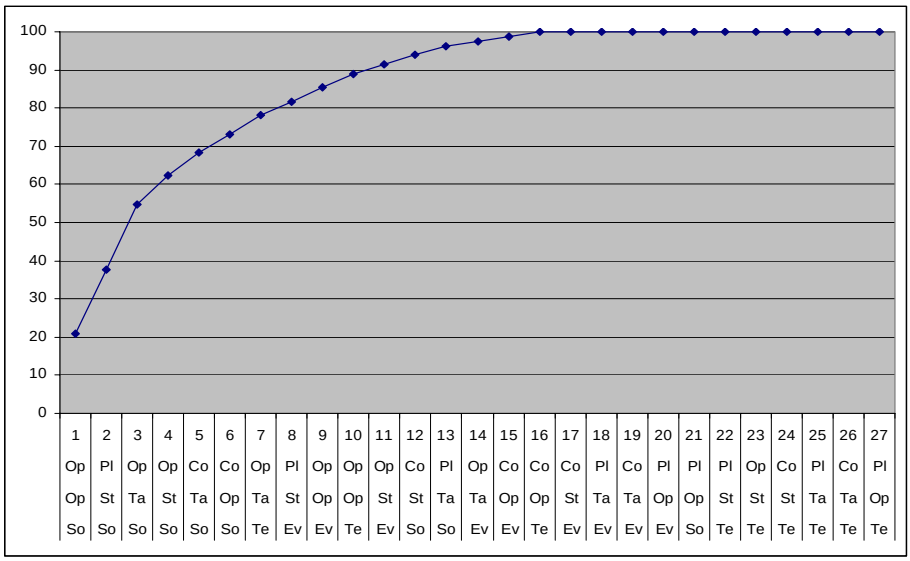

Figure 13: Cumulative percentage of classification of statements from agency work for the 27 sub cubes.

The following metrics are all using Figure 14:

- The most significant block from the cube where the phase in the life cycle of the information security program is not fixed is the block connected to strategic information security work concerning social aspects (*,St,So). The least significant block is the one connected to strategic information security work concerning technical aspects (*,St,Te).
- The most significant block from the cube where the decision level is not fixed is the block connected to the operate phase of the information security program concerning social aspects (Op,*,So) and the least significant is the block connected to the planning phase of the information security program concerning technical aspects (Pl,*,Te).
- The most significant block from the cube where the content type of the communication is not fixed is the block connected to the operate phase of the

information security program concerning operative work (Op,Op,*) and the least significant block is connected to the planning phase of the information security program concerning operative work (Pl,Op,*).

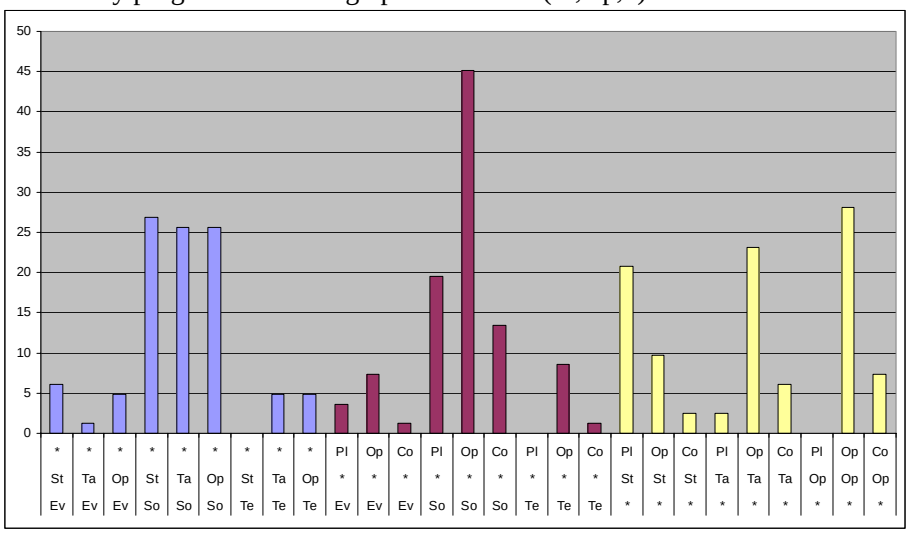

Figure 14: Relative frequency for each rectangular block in the cube for interviews with agency personnel.

The following metrics are all using Figure 15:

- The most significant slice when only considering the life cycle stage of the information security program is the operate phase (Op).
- The most significant slice when only considering the decision level is the operational (Op).
- The most significant slice when only considering the content of the communication is that concerning social aspects (So).

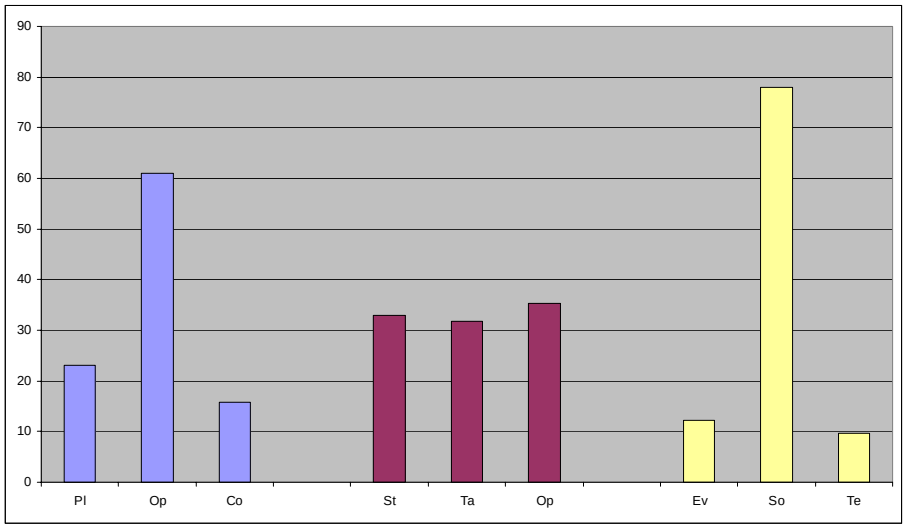

Figure 15: Relative frequency of each slice of the cube for interviews with agency personnel.

5.3.3 Interpretation

The graph with the cumulative percentage of the 27 sub cubes shows that the statements from the interviews are quite concentrated with about 80% of the controls concentrated to 8 sub cubes and the remaining 20% found in 8 sub cubes which leaves 11 sub cubes empty.

Since the interviews that the models and thus the metrics are based on were focusing on communication of information security it is not surprising to see that social aspects are completely dominating the data set when included.

When social aspects are not considered a very plausible pattern emerges. The three most significant blocks from the cube are those connected to Operational work in the operate phase (Op,Op,*), Tactic work in the operate phase (Op,Ta,*) and strategic work in the planning phase (Pl,St,*).

5.4 Comparison of the cube graphs

This section contains comparisons of the three models presented in previous sections. When performing analysis of the comparisons the following should be taken into consideration.

Due to the uncertainty and slight bias that cannot be avoided in the model of the agency work, any inconsistencies found when comparing this model with the others should be considered an area worth further investigation and not as an indication of actual inconsistencies in the security work.

5.4.1 Comparison graphs

This comparison can be used to identify differences between the models. In Figure 16 the three graphs representing the models from the previous chapters are merged into one graph. In the following section, metrics for comparison of the models are presented.

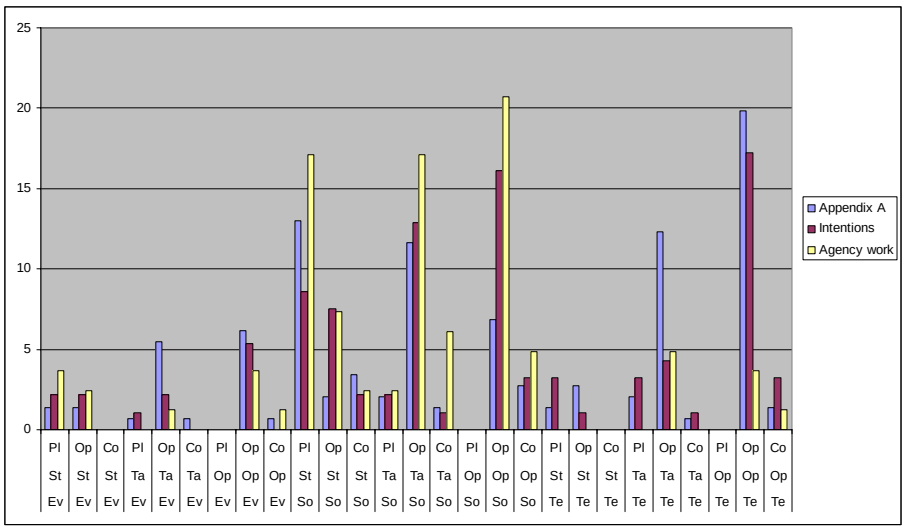

Figure 16: Comparison of norm, motives and agency work for each sub cube.

5.4.2 Comparison metrics

In Figure 17, Figure 18 and Figure 19 the results from applying the metric introduced in section 4.2.1.1 are presented.

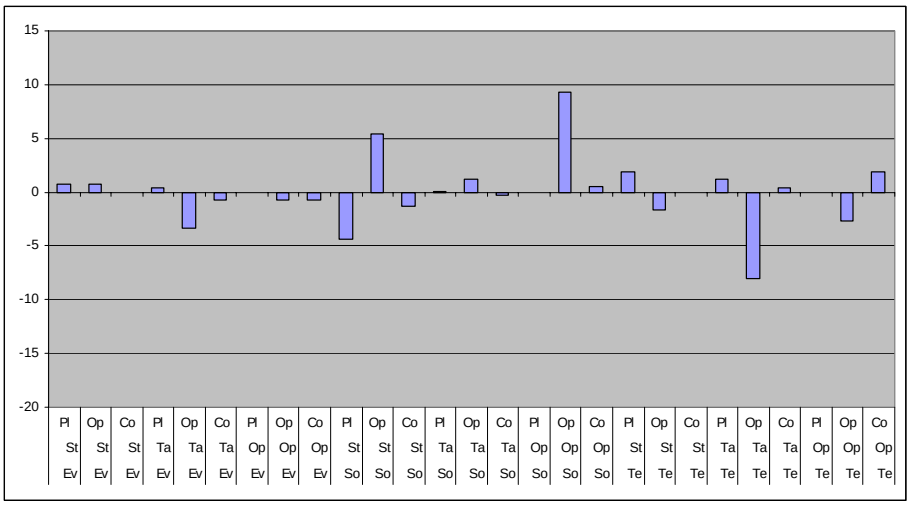

Figure 17: Appendix A percentage points subtracted from intentions percentage points.

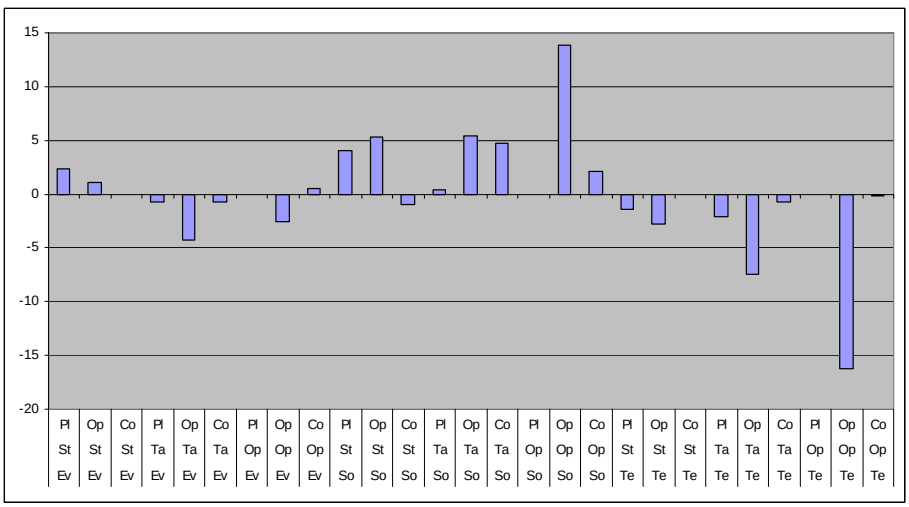

Figure 18: Appendix A percentage points subtracted from agency work percentage points.

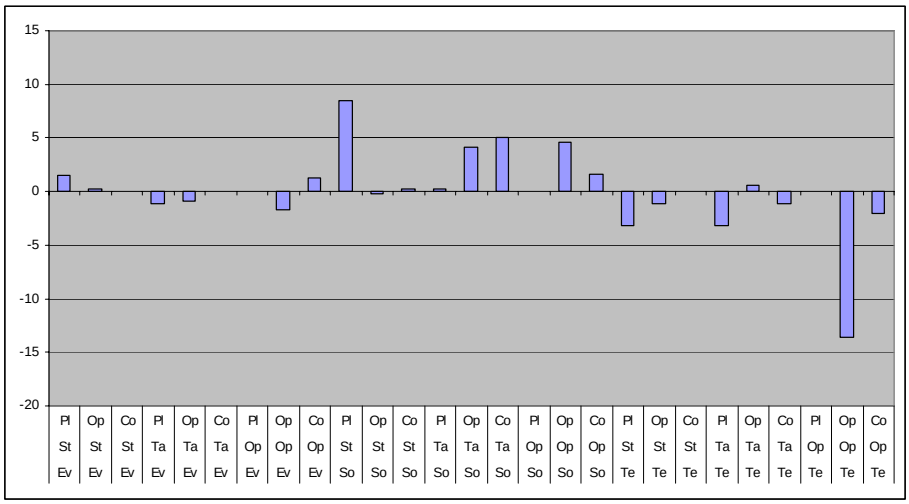

Figure 19: Intentions percentage points subtracted from agency work percentage points.

In Figure 20 the metric with nine rectangular blocks is shown for each of the three models previously presented in this chapter.

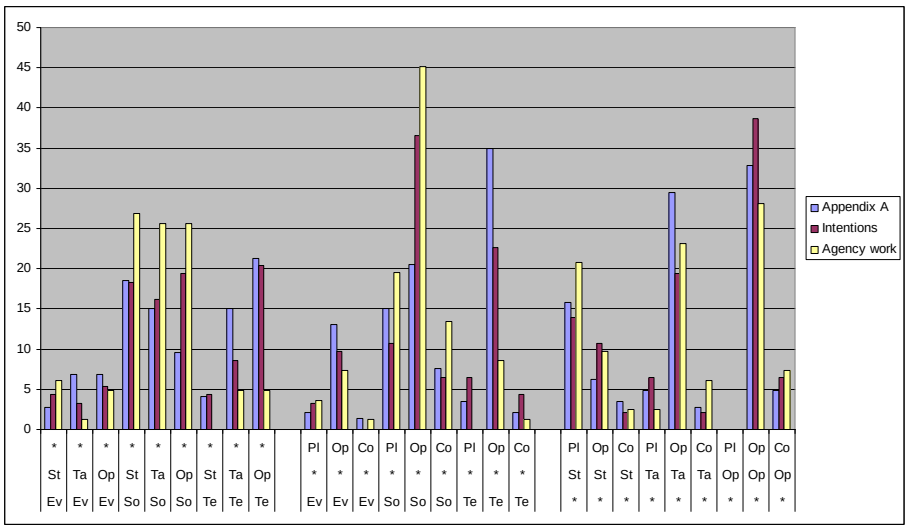

Figure 20: Comparison of norm, motives and agency work for each rectangular block.

In Figure 21 the metric with three slices of the cube is shown for each on the three models previously presented in this chapter.

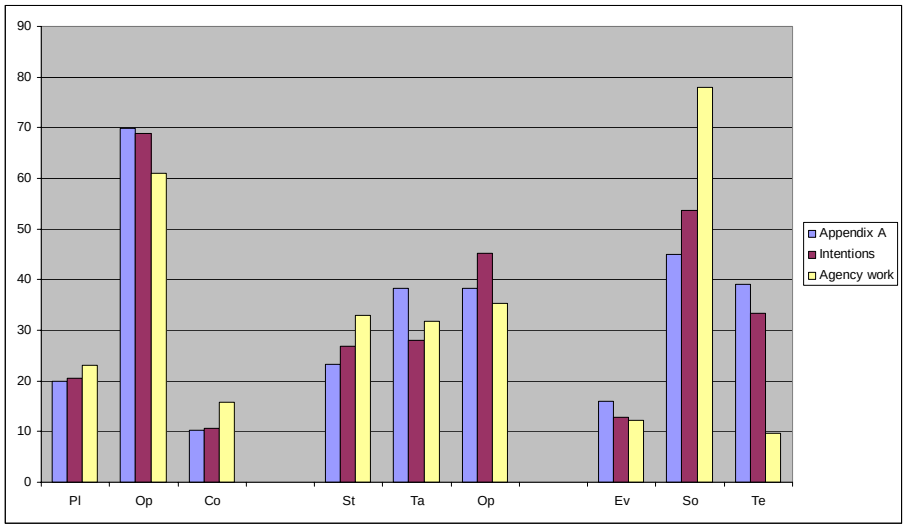

Figure 21: Comparison of the norm, motives and agency work for each dimension in the cube.

5.4.3 Interpretation

As can be seen in Figure 21, the focus of the documents corresponds rather well with the focus set out in the standard. The same can be said for the agency work with the exception of the huge imbalance in social aspects compared to technical aspects. A major factor for this imbalance is the emphasis of the interviews on the communication of information security issues, i.e. social aspects. The difference between social aspects and technical aspects is not that significant in the standard while it is rather significant for the documents.

Also note in Figure 21 that work in the operate phase of the information security program contains 60-70% of the classified statements for all three models.

As can be seen in Figure 21 there is a large focus on the operative phase for all three data sources. However, as illustrated by fig Figure 20 there is a large difference in the distribution between the technical and social aspects of this phase (see (Op,*,So) and (Op,*,Te)). This indicates that focus is shifted from technical to social aspects when going from the standard, via the documents, to the interviews.

Note in Figure 20 that the block for Pl/Op is empty. Statements that could be classified into this block would be concerning for example the actual work performed when documenting developed procedures. This level of detail is not described in the used data sets, which is why this block is empty. Furthermore,

there is a low focus on control of information security work where an external party is involved (Co,*,Ev).

From Figure 17 the pair of opposite focuses found in (Pl,St,So) and (Op,St,So) indicates that the agency intentions concentrate more on the operate phase than the planning phase for strategic work with social aspects. The agency intentions focus more on operative work with social aspects during the operate phase which is compensated by a low focus on tactical work with technical aspects compared to the standard.

The trend of focusing on operative work with social aspects over tactical work with technical aspects is found also in Figure 18. The figure also confirms that the social aspects are dominant in the interviews which most likely are why the technical work in the operative phase has such relatively low focus.

Figure 19 manifests the large focus on social aspects found in the interviews and the correspondingly low focus on technical aspects. This is further emphasized by the largest differences found in (Pl,St,So) and (Op,Op,Te).

6 Entity-action models

In this report, the three decision level model (section 2.2.1.1) was modified by making all types of interaction equal and allowing entities that cannot be defined as belonging to one of the decision levels. Making all interactions equal transforms the model by removing the use of the generalized decision motivator, effectively giving each entity only a single interface for incoming and outgoing communication. Allowing undefined entities is necessary since all the data sources used in modeling contain entities that cannot be mapped to any of the three levels prescribed by the original modeling technique. Thus, the models can capture the ambiguities of the collected data or the modeled organizations.

6.1 The norm, ISO/IEC 27001 appendix A

6.1.1 The model

The entity-action models based on the controls specified in the standard is limited to the entities explicitly specified in the descriptions of the controls. Thus, the model is generic and can be used as a reference for the models of actual organizations, functioning as a baseline for the presence of entities and the action associated with these entities. The numbers in the model are the identifiers of the objectives in the standard.

Table 1: The entities stated in Appendix A of ISO/IEC 27001, preceded by their organizational level, and the related controls categorized as sender, receiver, or indirect depending on the role of the entity in the control specification.

Level	**Entity**	**Related controls**		
		Sender	Receiver	Indirect
Strategic	Management	5.1.1, 6.1.1, 8.2.1, 11.2.4, 15.2.1	13.1.1, 13.2.1	
Tactic	Information asset owner		7.1.2	
	Information security co-ordinator	6.1.2		
Operative	Authorized personnel			9.1.2
	Independent reviewer of security management	6.1.8		

	Person			13.2.3
	Support personnel			11.6.1
	System administrator/operator			10.10.4
	Users	11.3.2	10.1.1, 11.3.1, 15.1.5	11.2.1, 11.4.1, 11.4.2, 11.4.6, 11.5.2, 11.6.1
External	Candidates for employment			8.1.2
	Contractors	8.1.3, 8.3.2, 13.1.2	8.2.1, 8.2.2, 8.2.3	8.1.1, 8.1.2, 8.3.3
	Customer			6.2.2
	External parties		10.8.2	6.2.1
	Other organization			13.2.3
	Relevant authorities			6.1.6
	Special interest groups, Specialist security forums, and professional associations			6.1.7
	Third party users	8.1.3, 8.3.2, 13.1.2	6.2.3, 8.2.1, 8.2.2, 8.2.3	8.1.1, 8.1.2, 8.3.3, 10.2.1, 10.2.2
	Unauthorized persons			9.1.6
Undefined	Employees	8.1.3, 8.3.2, 13.1.2	5.1.1, 8.2.1, 8.2.2, 8.2.3	8.1.1, 8.3.3
	Information system		10.10.6	10.3.2, 10.8.5, 15.1.1, 15.2.2, 15.3.1
	The organization	10.8.2, 12.5.5	8.1.3	15.1.1

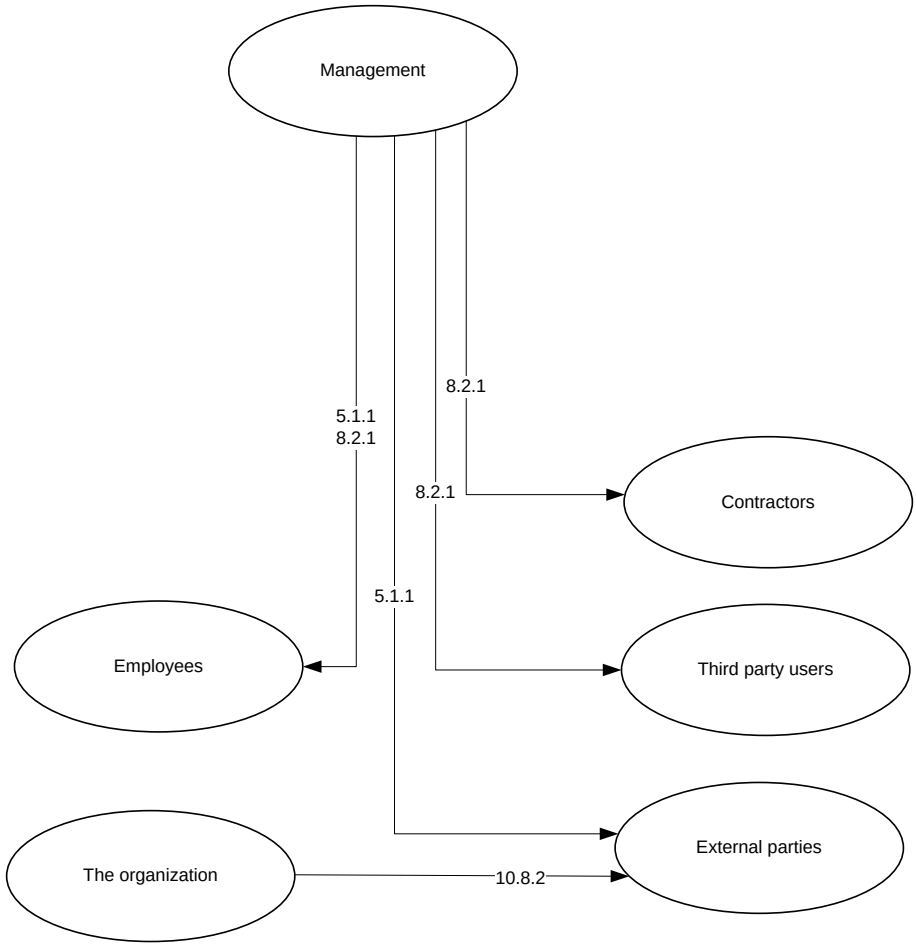

Figure 22: The entities with communication relations specified in Appendix A of ISO/IEC 27001.

6.1.2 The metrics

Some of the metrics from section 4.1.2 with percentage values are presented with all the other models' values in graphs that can be found in the comparative section (6.4.1) of this chapter.

Table 2: Metrics and data for the model of the standard.

Measurement	**Value**
Entities	21
Interacting entities	6
Interactions	6
Actions	133
Assigned actions	32
Interactions between layers	0
Interactions within layers	0
Interactions with external entities	4
Internal interactions with undefined entities	2
Percent of entities with at least one interaction	29%
Percent of actions that are assigned	24%

6.1.3 Interpretation

The model of the standard contains only the entities explicitly stated in the controls of the standard. The number of interacting entities in the model is very low meaning that there are not many information flows defined in the standard. Most of the defined interactions concerns external parties. The rest concerns interaction with internal undefined entities.

The percent of entities involved in interactions is only 29%. Consequently, the standard, to a large extent, does not define the necessary interactions. Further, the low percent of assigned actions, 24%, indicates that for the majority of the actions, no explicit responsibility has been allocated.

6.2 Agency intentions, based on the studied documents

6.2.1 The model

The model of the agency documents is assumed to show how the agency intends their information security program to operate including what communication should take place for it to work.

The model was created from the statements presented in (Yngström et al. 2009, chap.6) and shows the entities that were identified as well as how they are meant to interact with each other.

Table 3: The entities stated in the statements extracted from the agency documents (Yngström et al. 2009, chap.6), preceded by their organizational level, and the related statements categorized as sender or receiver depending on the role of the entity in the statement (none of the entities are indirectly referenced in the statements).

Level	**Entity**	**Related statements**		
		Sender	Receiver	Indirect
Strategic	Chief of agency	2.1, 2.2		
	Chief of agency (or person appointed by the chief of agency)	1.2, 2.3, 3.29		
	Chief of internal inquiries	3.29		
Tactic	Responsible for system security	1.24, 3.1, 3.2, 3.3, 3.5, 3.9, 3.11, 3.20, 3.28, 3.32	4.6	
	Responsible for development or procurement of or substantial changes to IT system	3.7		
	Responsible for security	3.8		
	IT department	1.12, 3.4, 3.12, 3.13, 3.16, 3.17, 3.18, 3.19, 3.22, 3.23,	1.39, 3.26, 4.1	

		3.33, 4.6		
	Development and strategy unit	3.34		
	Security unit	3.6, 3.14, 3.21, 3.30, 3.31	3.29	
Operative	IT system user	3.25, 3.26, 3.27, 4.1	1.1, 1.8, 1.25, 1.32	
	Employee	3.15	1.26, 1.31, 4.2, 4.3	
	Instructor		2.2	
External	Group of agencies		1.3, 1.5, 1.6, 1.49, 3.21, 3.23	
	Contractor	3.15	1.29, 1.31, 4.4	
Undefined	The agency	1.3, 1.4, 1.5, 1.6, 1.9, 1.10, 1.13, 1.23, 1.25, 1.26, 1.27, 1.28, 1.29, 1.31, 1.36, 1.37, 1.39, 1.47, 1.48, 1.49, 3.24, 4.2, 4.3, 4.4		
	IT system	3.10		
	Respective agancy	4.7	1.10, 3.1, 4.6	

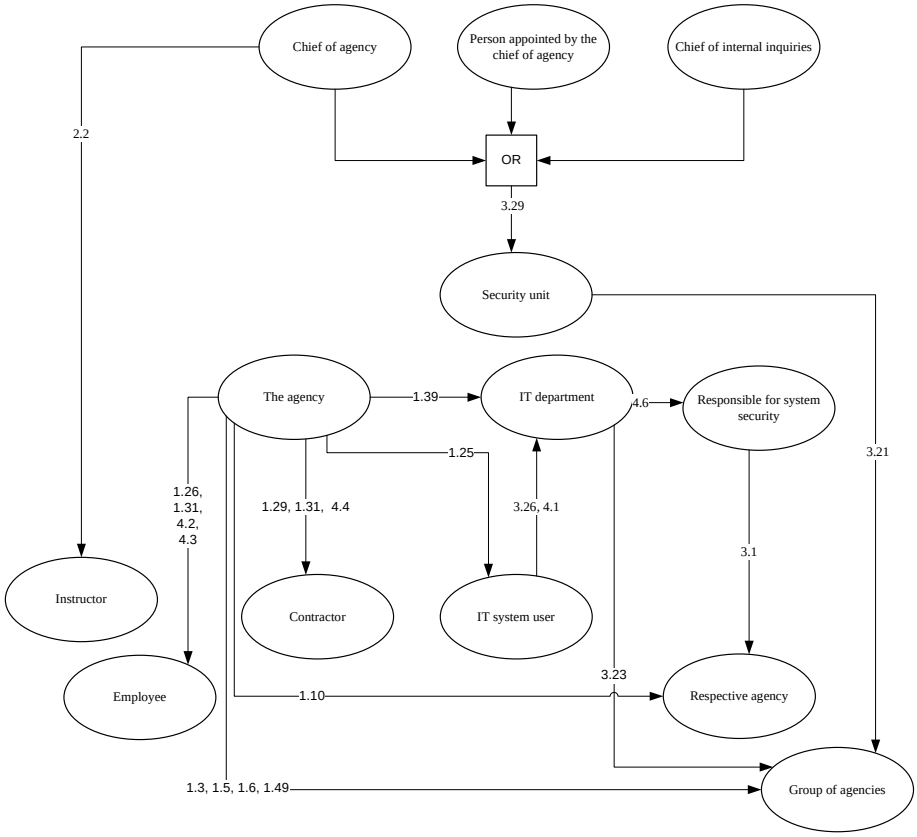

Figure 23: The entities with communication relations specified in the statements extracted from the agency documents (Yngström et al. 2009, chap.6).

6.2.2 The metrics

Some of the metrics from section 4.1.2 with percentage values are presented with all the other models values in graphs that can be found in the comparison section (6.4.1) of this chapter.

Table 4: Metrics and data for the model of the agency intentions.

Measurement	Value
Entities	17
Interacting entities	13
Interactions	22
Actions	93
Assigned actions	72
Interactions between layers	4
Interactions within layers	1
Interactions with external entities	9
Internal interactions with undefined entities	8
Average number of interactions per interacting entity	1.7
Percent of entities with at least one interaction	76%
Percent of actions that are assigned	77%

6.2.3 Interpretation

The model of the agency documents has a high ratio of entities that are part of at least one interaction (76%). Even though the model contains a good amount of interactions the majority of them are connected to external or undefined entities. There are actually only five interactions that can be considered to fully define communication within the agency.

The percent of actions that are assigned is high for this model, 77%, meaning that for most of them, responsibility has been explicitly allocated.

6.3 Agency work, based on interviews

6.3.1 The model

The model of the interviews was created from the statements presented in Appendix C. As with the cube model presented in chapter 3.1, negated

statements have been excluded in the creation of this model. The model should not be considered to give a complete picture of the work at the agency since it is based on a non exhaustive set of interview questions. It should also be noted that there is a slight bias towards communication in the answers.

The entities in the model are fewer than those identified in the interviews. This is because the interviewed persons call some entities by slightly different names and these entities have been unified into one entity. A map of how the entities from the statements were merged into the entities found in the model is included in appendix B.

Table 5: The entities stated in the statements extracted from the interviews, preceded by their organizational level, and the related statements categorized as sender or receiver depending on the role of the entity in the statement (none of the entities are indirectly referenced in the statements).

Level	**Entity**	**Related statements**		
		Sender	Receiver	Indirect
Strategic	Chief of agency		2.7	2.6
	Highest level manager	6.13	6.7, 6.12	
	Security manager			2.12
	Security representatives	2.7		
	Security unit 1	1.3, 2.2, 2.3, 2.8, 2.9, 2.10, 3.1, 3.6, 6.1, 6.8, 7.1, 7.9, 7.10		2.12
	Security unit 2	1.4, 2.4, 2.5, 6.3, 6.4, 6.5		2.12
	Upper level manager	1.6, 2.11, 3.3, 6.7	7.5, 7.13	
Tactic	Administration management	4.1		
	Lawyer	2., 6.8, 8.3		
	Middle level manager	2., 6.7, 6.9, 6.10, 6.11, 6.19	5.4, 5.5, 6.8, 7.10	
Operative	Administrative personnel		5.1	

	Administrator of systems at the agency		2.1	
	Disciplinary boards			2.13
	IT system user		4.1, 5.6	
	Operative personnel	1.5, 6.19, 7.7, 7.8	3.1, 5.3, 7.10	
	Subordinates		6.9	
	System developer	2.1		
	System owner	6.8		
External	Agency outside the group of agencies		7.14	
	Consult	2.1		
	Other agencies operative personnel		3.3	
	Other agency	6.14	1.4, 2.4, 2.5, 7.7, 7.8	
	Security representatives of other agencies		6.3, 6.4, 6.5, 6.18	
Undefined	Agency personnel	4.4, 6.12, 6.15	1.7, 2.10, 4.3, 6.1, 6.2, 6.10, 6.11	1.8, 1.9, 4.5, 6.13
	The agency	1.7, 1.12, 1.13, 7.6	1.3, 2.2, 2.3, 7.7, 7.8, 7.9, 7.11, 7.12, 8.3	8.1,8.2

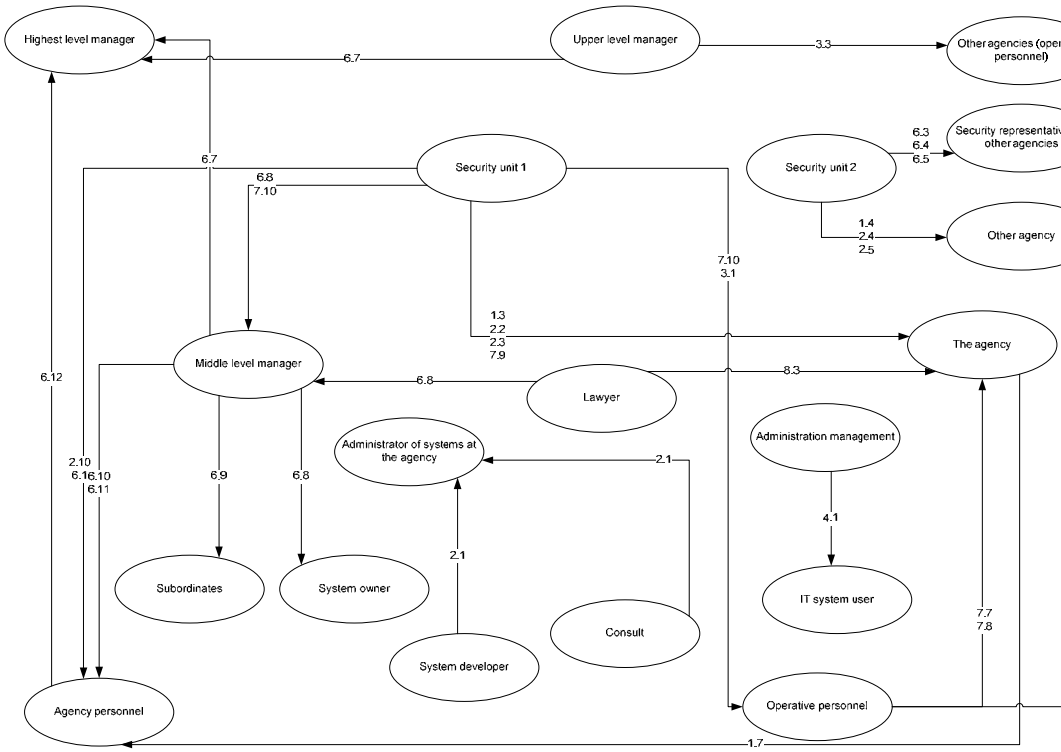

Figure 24: The entities with communication relations specified in the statements extracted from the interviews.

6.3.2 The metrics

Some of the metrics from section 4.1.2 with percentage values are presented with all the other models values in graphs that can be found in the comparison section (6.4.1) of this chapter.

Table 6: Metrics and data for the model of the agency work.

Measurement	Value
Entities	25
Interacting entities	19
Interactions	34
Actions	82
Assigned actions	60
Interactions between layers	8
Interactions within layers	3
Interactions with external entities	10
Internal interactions with undefined entities	13
Percent of entities with at least one interaction	76%
Percent of actions that are assigned	73%

6.3.3 Interpretation

This model has a high ratio of entities with at least one interaction but a majority of these concern external or undefined parties. It is worth noting that even though this model is created from interviews, references to communication with “the agency” or “agency personnel” is the most common.

The percentage of entities involved in interactions is 76%. Consequently, the interviews have a high level of defined interactions. However the model can probably be improved significantly if extended with further data from additional interviews. The percent of assigned actions, 73%, would be higher if statements concerning needs were not included in the actions. See chapter 7 for further development of this.

6.4 Comparing entity-action models

6.4.1 Comparing metrics

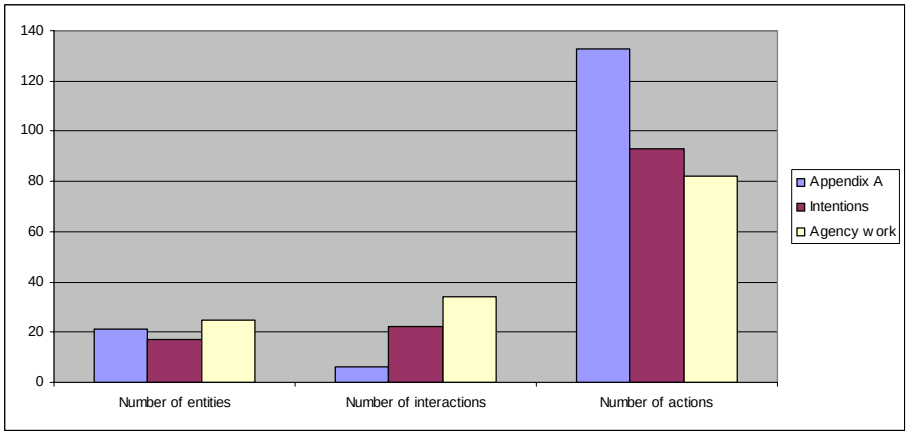

Figure 25: Number of entities, interactions and actions for the three models

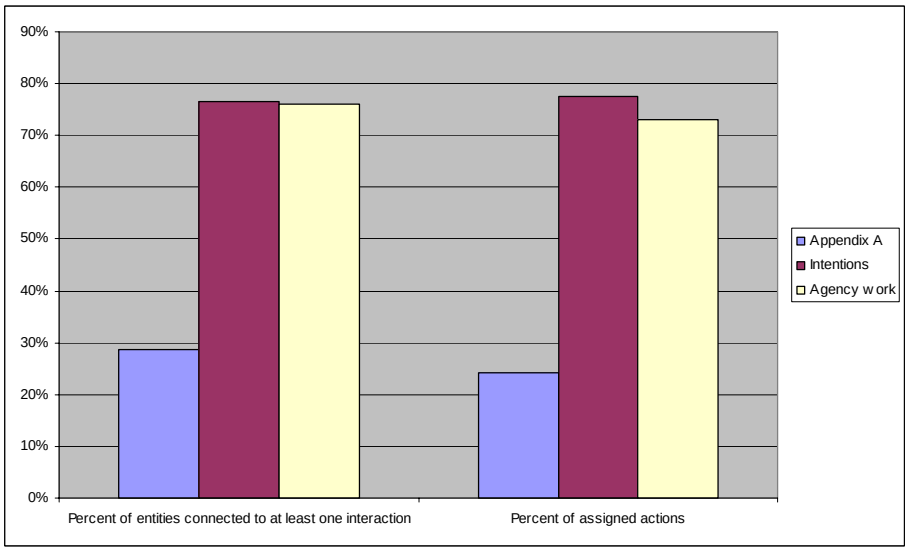

Figure 26: Percent of entities with at least one interaction and assigned actions

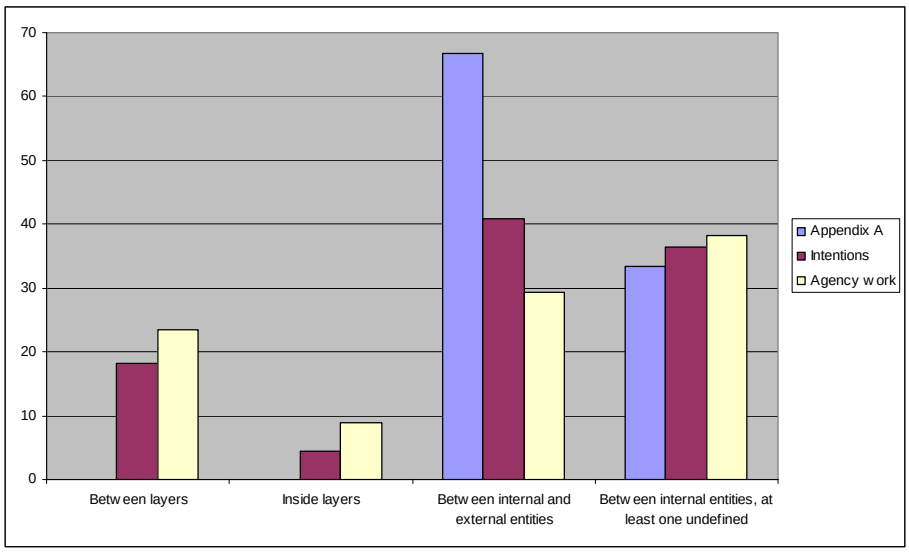

Figure 27: Percent of interactions with a specific property for appendix A, agency intentions and agency work.

6.4.2 Interpretation

Comparing the models, Figure 25, the number of entities is fairly similar. The number of actions is larger in the model of the standard than in the models of the agency. However this difference could be reduced by further modeling of the agency. The number of interactions is larger for the models of the agency. This reflects the generic nature of the standard. Considering the low number of interactions it is no surprise that the standard also has a low percentage of entities with at least one interaction. This is indicated by Figure 26 which also shows that the percent of assigned actions is considerably lower for the standard than the agency models.

The type of interaction found in the models, shown in Figure 27 indicates that for both the model of the agency intentions and the interviews, there is a large fraction of interactions with undefined entities. This indicates a need for further modeling and possibly better definitions in the agency documents. The values for the standard are included for the sake of completeness. Since the standard only has six interactions, the percentage distribution of the type of interaction can not really be compared to the values from the other models.

7 Discussion

7.1 Cube models

Building the cube models provides situational pictures regarding the prioritization considering the work with different aspects of information security. The purpose of the models is to present relative values for how the information security aspects corresponding to each sub cube is prioritized. The reason relative values are used is so that models can be compared with each other, even though they are created from different sized data sets. Thus the problems related to the intrinsic difficulties to provide absolute values for the levels of information security are avoided. Consequently, the absolute level of the effort considering information security within an organization cannot be judged based on the models. This is not a weakness in the modeling but rather a consequence of the modeling technique. It is possible to classify two completely different data sets and still get the exact same distribution, both in relative and absolute numbers. An example of this would be taking the standard and for each control create a new statement that would fall into the same phase of the life cycle, the same decision level and the same communication content. This would create a model identical to the standard but that in reality would differ in every statement.

However, one situation where the absolute value can be interesting in these models is those sub cubes with no values. Whenever a sub cube is empty this indicates a lack of emphasis of the corresponding aspects of information security. This lack could be either intentional, i.e. an accepted risk, or unintentional. There is also a possibility that the zero value originates from a flaw in the model. At the moment the authors are not aware of any such flaws but further development of the modeling technique might reveal such flaws.

The models show strong emphasis on social aspects. This may seem contradictory to the belief that technical issues often are the focus of information security work. One explanation for this is that the model considers where the end points for a communication are. If the endpoint is a technical system, e.g. maintenance or configuration of information system, the corresponding statement will be classified as technical. If the endpoint is a human, e.g. talking to a coworker, sending an e-mail or publishing an article on the intranet, the corresponding statement will be classified as social. Moreover the focus of the modeling has been the communication of information security issues rather than the actual performance of information security work. Thus the emphasis of the studied documents and the interviews is more on the social aspects then the technical aspects. Possibly further studies considering the more detailed aspects of information security would increase the emphasis on the technical aspects.

7.2 Entity-action models

From the entity-action models it is possible to get an overview picture of all entities that are interacting with each other. In the current models the entity labels are extracted directly from the analyzed statements. Some merging of similar labels has been performed for the interviews where two different labels were obviously describing the same entity. However no cross-model unification of labels has been performed. This results in non standardized naming of the entities, the role represented by an entity labeling in one model does not necessarily correspond to the same role in another model even though the same label might occur. Thus models can be difficult to compare. Further development of the modeling technique could potentially solve this problem by either creating a standardized set of entity definitions or developing a method for comparing two entities to establish similarities.

In the entity-action models being based on the tree decision levels model, all entities should be assigned to the strategic, tactic or operative levels or if the entity is external to the organization, assigned to the environment. Thus ideally there should be no entities classified as undefined. The reason for having undefined entities in the model comes from the use of too general definitions of actors in the underlying data. Examples of this are “agency personnel” or just “the agency”. The judgment of what entities should be undefined was a subjective decision taken by the authors. The basis for this decision was if an entity could be classified as belonging to one of the three decision levels. To illustrate this, consider “security unit” which is rather well defined with all members on the same decision level, while “the agency” includes employees from every level. This is why “security unit” is defined and “the agency” is undefined.

When the model of the standard was created the authors were quite surprised to see how few fully defined interactions there were. This can be explained by the fact that the standard has a wide scope and should be applicable to vastly different kinds of organizations. There were also a lot more controls that only contained indirectly referenced entities meaning that they described communication about an entity without stating the sender or receiver in this communication. The model can likely be improved and extended by incorporating additional information found in the international standard ISO/IEC 27002 (ISO/IEC 2005).

The models of the agency documents and the interviews with agency personnel are based on the data presented in (Yngström et al. 2009) they should be considered as a starting point for further discussions. As with the model of the standard, most of the internal interactions involve at least one undefined entity. This reflects the need to improve the underlying data. In some cases it also

highlights the need to more clearly specify the roles for organization of information security work.

The set of statements used when the models were created includes different kinds of statements, some of which do not describe the actual situation. Statements concerning unfulfilled needs do not describe any kind of communication and will therefore not be included in the model. The statement will however be counted when statistics for the models are generated which explains the lower value for assigned actions found in section 6.3.3. The authors have thought of a solution for this which is presented in the future work section.

7.3 Future work

7.3.1 Statement categories

To be able to extract only the relevant statements from the underlying data, a set of statement categories should be defined. Doing this will enable users of the modeling techniques to only use relevant statements in the creation of models and also to create models for each category. Suggested categories are: current state, future state, needs, unfulfilled needs, and identified problems.

7.3.2 From standard to agency specific model

In order to characterize the information security processes of organizations, a method for producing a model of the organization will be designed. The purpose is to start from the standard and generate an agency specific model encompassing hopefully all the controls in the standard. The method starts from the model of the standard described in section 6.1.1 and will contain the following steps:

1. Identify the entities from the standard in the organization and check if these entities perform the tasks set out in the associated controls.
2. Map additional controls in the standard to the identified entities.
3. Identify additional entities associated with the assigned controls. This requires further analysis of the controls based on the number and nature of entities connected to them.
4. If there are any controls left to assign, go back to step 2.

8 References

Ashby, R., 1956. *An Introduction to Cypernetics*, Chapman & Hall Ltd.

Beer, S., 1981. *Brain of the Firm* 2nd ed., John Wiley & Sons.

Chew, E. et al., 2008. *Performance Measurement Guide for Information Security*, National Institute of Standards and Technology. Available at: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

Gigch, J.P., 1974. *Applied General Systems Theory*, Joanna Cotler Books.

Herrmann, D., 2007. *Complete guide to security and privacy metrics: measuring regulatory compliance, operational resilience, and ROI*, Auerbach Publications.

ISO/IEC, 2005. *ISO/IEC 27002:2005 - Information technology -- Security techniques -- Code of practice for information security management*,

Jaquith, A., 2007. *Security metrics: replacing fear, uncertainty, and doubt*, Addison-Wesley.

Langefors, B., 1968. *Introduktion till informationsbehandling*, Berlingska Boktryckeriet.

Oscarson, P., 2007. *Actual and perceived information systems security*. Department of Management and Engineering, Linköping University.

RiR, Swedish National Audit Office, 2007. *Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen*,

Schoderbek, P.P., Schoderbek, C.G. & Kefalas, A.G., 1990. *Management Systems: Conceptual Considerations* 4th ed., Richard D Irwin.

Shannon, C.E., 1998. *The Mathematical Theory of Communication*, Urbana: University of Illinois Press.

SIS, 2007. *SIS HB 550: Terminologi för informationssäkerhet, utgåva 3*, SIS Förlag.

Yngström, L. et al., 2009. *COINS Report #1: Controlled Information Security*, Kista, Sweden: Department of Computer and Systems Sciences, DSV, Stockholm University and the Royal Institute of Technology.

Appendix A: Statement classifications

ISO/IEC 27001 appendix A

Control			Ev/So/Te	St/Ta/Op	Pl/Op/Co
5	1	1	So	St	Pl
5	1	2	So	St	Co
6	1	1	So	St	Op
6	1	2	So	Ta	Op
6	1	3	So	Ta	Op
6	1	4	So	St	Pl
6	1	5	So	St	Pl/Co
6	1	6	Ev	St	Op
6	1	7	Ev	St	Pl
6	1	8	So	Op	Co
6	2	1	Ev	Ta	Op
6	2	2	Ev	Op	Op
6	2	3	Ev	Ta	Op
7	1	1	Te	Op	Op
7	1	2	So	St	Pl
7	1	3	So	St	Pl
7	2	1	Te	Op	Op
7	2	2	So	St	Pl
8	1	1	Ev/So	St	Pl
8	1	2	So	Op	Op
8	1	3	So	Op	Op
8	2	1	Ev/So	St	Op
8	2	2	Ev/So	Op	Op
8	2	3	So	Ta	Op
8	3	1	So	Ta	Op
8	3	2	Ev/So	Op	Op
8	3	3	Ev/So	Op	Op
9	1	1	Te	Ta	Op
9	1	2	Te	Ta	Op
9	1	3	Te	Ta	Op
9	1	4	Ev	Ta	Pl/Op
9	1	5	So	St	Pl
9	1	6	Ev	Op	Op
9	2	1	Ev	Ta	Op
9	2	2	Ev	Ta	Op
9	2	3	Ev	Ta	Op
9	2	4	Te	Op	Op
9	2	5	Ev	Op	Op
9	2	6	Te	Ta	Op
9	2	7	So	Ta	Op
10	1	1	So	Ta	Op
10	1	2	So	St	Op
10	1	3	So	St	Pl
10	1	4	Te	Ta	Op
10	2	1	Te	Ta	Co
10	2	2	Ev	Ta	Co
10	2	3	So	St	Pl
10	3	1	So	St	Pl/Co
10	3	2	Te	Ta	Pl
10	4	1	So/Te	Ta	Op
10	4	2	Te	Op	Op
10	5	1	Te	Op	Op
10	6	1	Te	Op	Op
10	6	2	Te	St	Pl

Control			Ev/So/Te	St/Ta/Op	Pl/Op/Co
10	7	1	Te	Ta	Op
10	7	2	Te	Op	Op
10	7	3	So	Ta	Pl
10	7	4	Te	Ta	Op
10	8	1	So	St	Op
10	8	2	Ev	Ta	Op
10	8	3	Ev	Op	Op
10	8	4	Te	Ta	Op
10	8	5	So	St	Pl
10	9	1	Te	Ta	Op
10	9	2	Te	Op	Op
10	9	3	Ev	Op	Op
10	10	1	Te	Op	Op/Co
10	10	2	So	Ta	Op/Co
10	10	3	Te	Op	Op
10	10	4	Te	Op	Op
10	10	5	Te	Op	Op/Co
10	10	6	Te	Op	Op
11	1	1	So	St	Pl
11	2	1	So	Ta	Op
11	2	2	So	Ta	Op
11	2	3	Te	Ta	Op
11	2	4	So	St	Co
11	3	1	Te	Op	Op
11	3	2	Te	Op	Op
11	3	3	So	Op	Op
11	4	1	So	Ta	Op
11	4	2	Te	Op	Op
11	4	3	Te	Ta	Op
11	4	4	Te	Op	Op
11	4	5	Te	Ta	Op
11	4	6	Ev	Ta	Op
11	4	7	Te	Ta	Op
11	5	1	Te	Ta	Op
11	5	2	Te	Ta	Op
11	5	3	Te	Op	Op
11	5	4	Te	Op	Op
11	5	5	Te	Op	Op
11	5	6	Te	Op	Op
11	6	1	So	Ta	Op
11	6	2	Te	Op	Op
11	7	1	So	Ta	Op
11	7	2	So	St	Pl
12	1	1	So	St	Pl
12	2	1	Te	Op	Op
12	2	2	Te	Op	Op
12	2	3	Te	Ta	Pl
12	2	4	Te	Op	Op
12	3	1	So	St	Pl/Op
12	3	2	Te	Ta	Op
12	4	1	So	Ta	Op
12	4	2	Te	Op	Op
12	4	3	So	Ta	Op
12	5	1	So	Ta	Pl
12	5	2	Te	Op	Co
12	5	3	Te	Op	Op
12	5	4	So	Ta	Pl
12	5	5	Ev	Op	Co
12	6	1	So	Ta	Op
13	1	1	So	Op	Op
13	1	2	Ev/Te	Op	Op

Control			Ev/So/Te	St/Ta/Op	Pl/Op/Co
13	2	1	So	St	Pl
13	2	2	So	Op	Op
13	2	3	So	Op	Co
14	1	1	So	St	Pl/Op
14	1	2	So	St	Pl
14	1	3	Te	Ta	Pl
14	1	4	So	St	Op
14	1	5	So	Ta	Co
15	1	1	So	St	Co
15	1	2	So	Ta	Op
15	1	3	So	Op	Op
15	1	4	Te	Ta	Op
15	1	5	Te	Op	Op
15	1	6	Te	Op	Op
15	2	1	So	Op	Co
15	2	2	So	Op	Co
15	3	1	Te	St	Pl
15	3	2	So	Op	Op

Statements from chapter 6

Statement	Ev/So/Te	St/Ta/Op	Pl/Op/Co
1.1	So	Ta	Op
1.2	So	St	Pl
1.3	So	St	Pl
1.4	So	St	Pl
1.5	So	St	Op
1.6	So	Ta	Op
1.7	So	Ta	Op
1.8	So	Ta	Op
1.9	So	St	Pl
1.10	Ev	St	Pl
1.11	Te	Op	Op
1.12	Ev	Ta	Pl
1.13	Te	Ta	Pl
1.14	Te	Ta	Op
1.15	Te	Op	Op
1.16	Te	Op	Op
1.17	Te	Op	Co
1.18	Te	Op	Co
1.19	Te	Op	Co
1.20	Te	Op	Op
1.21	Te	Ta	Pl
1.22	So	St	Op
1.23	Te	Op	Op
1.24	So	Op	Op
1.25	So	Ta	Op
1.26	So	Op	Op
1.27	Ev	St	Pl
1.28	So	Ta	Op
1.29	Ev	St	Op
1.30	Ev	St	Op
1.31	So	St	Op
1.32	So	Op	Op
1.33	Te	Op	Op
1.34	Te	Op	Op
1.35	Te	St	Pl
1.36	So	Ta	Op

Statement	Ev/So/Te	St/Ta/Op	Pl/Op/Co
1.37	Te	Op	Op
1.38	Te	Op	Op
1.39	Ev	Op	Op
1.40	Ev	Op	Op
1.41	Ev	Ta	Op
1.42	Te	St	Pl
1.43	So	Ta	Op
1.44	So	Ta	Op
1.45	Te	Op	Op
1.46	Ev	Ta	Op
1.47	So	St	Pl
1.48	So	Op	Co
1.48	So	Op	Co
1.49	Te	Ta	Co
2.1	So	St	Op
2.2	So	St	Op
2.3	So	St	Op
3.1	So	St	Pl
3.2	So	Ta	Op
3.3	So	Op	Op
3.4	Te	Op	Op
3.5	So	Ta	Op
3.6	So	Op	Op
3.7	So	St	Op
3.8	So	Op	Op
3.9	Te	Op	Op
3.10	Te	Op	Op
3.11	Te	Ta	Op
3.12	So	Op	Co
3.13	So	Ta	Op
3.14	So	St	Co
3.15	Ev	Op	Op
3.16	Te	Ta	Op
3.17	Te	Ta	Pl
3.18	So	Ta	Pl
3.19	So	Op	Op
3.20	Te	Op	Op
3.21	Te	Ta	Op
3.22	Te	Op	Op
3.23	Te	St	Pl
3.24	Ev	Op	Op
3.25	So	Op	Op
3.26	So	Op	Op
3.27	So	Op	Op
3.28	So	Ta	Co
3.29	So	St	Co
3.30	So	Op	Op
3.31	Te	St	Op
3.32	So	Ta	Pl
3.33	So	St	Pl
3.34	So	St	Pl
4.1	So	Op	Op
4.2	So	Op	Op
4.3	So	Op	Op
4.4	Ev	Op	Op
4.6	Te	Op	Op
4.7	So	Op	Op

Statements from chapter 7

Statement	Ev/So/Te	St/Ta/Op	Pl/Op/Co
1.3	So	St	Pl
1.4	So	St	Pl
1.5	So	Op	Co
1.6	So	St	Co
1.7	So	Ta	Op
1.8	So	Op	Op
1.9	So	Ta	Op
1.10	So	St	Pl
1.12	So	St	Co
1.13	So	St	Op
2.	So	St	Pl
2.1	So	Op	Op
2.2	So	St	Op
2.3	So	St	Pl
2.4	Ev	St	Op
2.5	Ev	St	Pl
2.6	So	St	Op
2.7	So	Op	Op
2.8	So	Ta	Op
2.9	So	St	Pl
2.10	So	Ta	Op
2.11	So	St	Pl
2.12	So	St	Op
2.13	So	Op	Op
3.1	So	Op	Op
3.3	Ev	Op	Op
3.4	So	Op	Op
3.5	Te	Ta	Op
3.6	So	Op	Op
4.1	Te	Op	Op
4.2	Te	Ta	Op
4.3	Te	Op	Op
4.4	So	Ta	Op
4.5	So	Op	Op
4.6	So	Ta	Op
5.1	So	Op	Op
5.2	So	Ta	Co
5.3	So	Op	Op
5.4	So	Ta	Pl
5.5	So	Op	Op
5.6	Te	Ta	Op
5.7	So	Ta	Pl
5.8	So	Ta	Co
5.9	So	Ta	Co
5.12	So	Op	Co
5.13	So	St	Pl
5.14	Te	Op	Co
5.15	So	Ta	Co
5.16	Te	Op	Op
6.1	So	Op	Op
6.2	So	Ta	Op
6.3	Ev	Op	Op
6.4	Ev	Op	Op
6.5	Ev	St	Pl
6.7	So	Ta	Op
6.8	So	Op	Op
6.9	So	Op	Op
6.10	So	Op	Op
6.11	So	Ta	Op

Statement	Ev/So/Te	St/Ta/Op	Pl/Op/Co
6.12	So	Op	Op
6.13	So	Ta	Op
6.14	Ev	Op	Co
6.15	So	Op	Co
6.18	Ev	Ta	Op
6.19	So	Op	Co
7.1	Te	Ta	Op
7.4	So	Ta	Co
7.5	So	Op	Op
7.6	So	St	Pl
7.7	So	St	Pl
7.8	So	Ta	Op
7.9	So	Ta	Op
7.10	So	Ta	Op
7.11	So	St	Op
7.12	So	St	Op
7.13	So	Ta	Op
7.14	Ev	St	Op
7.15	So	St	Pl
7.16	Ev	St	Pl
8.1	So	St	Pl
8.2	So	St	Pl
8.3	So	St	Pl

Appendix B: Statement entities to model entities

This appendix will present a map of how the entities from the interview statements were merged and changed into the entities found in the model of the agency work. The left column of Table 7 lists the entities found in the interview statements while the right side lists the corresponding entities that were used in the model. Entities marked with a '*' were split into several entities since they were too aggregated.

Table 7: Map of interview entities to modeled entities

Entities before	Entities after
Administration management	Administration management
Administrative personnel	Administrative personnel
Administrator of systems at the authority	Administrator of systems at the agency
Agencies outside the group of agencies	Agencies outside the group of agencies
Chief of authority	Chief of agency
Consultants	Consult
Disciplinary boards	Disciplinary boards
Employee	Agency personnel
Employees	
Individual	
Personnel	
Group of authorities	The agency, Other agency
Highest management	Highest level manager
Highest managerial level	
IT system user	IT system user
IT system users	
Lawyer	Lawyer
Managerial level*	Middle level manager
Middle managers	
Middle level manager	
Middle managerial level	
Resp 1	
Security specialist (resp. 1)	
Operative level	Operative personnel
Operative personnel	
Resp. 3	
Other authority	Other agency
Other agencies	
Other authorities (operative personnel)	Other agencies operative personnel
Security representatives	Security representatives
Security representatives at other agencies	Security representatives of other agencies
Security representatives of other authorities	

Entities before	Entities after
Security unit 1	Security unit 1
Security unit*	
Security unit 2	Security unit 2
Security unit*	
Security manager	Security manager
Subordinates	Subordinates
System developers	System developers
System owner	System owner
The authority	The agency
Upper managerial level	Upper level manager
Resp 2	
Upper-level management	
Managerial level*	Upper level manager, Middle level manager

Appendix C: Statements extracted from interviews with agency personnel

This appendix presents the statements extracted from the interview material presented in (Yngström et al. 2009, chap.7). The statements were created at the same time as the model report but were later merged with the results from further analysis. Statements marked with gray are those that were removed when models from the statements were created.

ID	Actor	Task/artifact	Sender/receiver	Ref.
1.1	The authority	No common view on information security	N/A	1, 3
1.2	The authority	No common information security methodology	N/A	1
1.3	Security unit 1	Strategic information security for the authority	The authority	2
1.4	Security unit 2	Strategic information security towards other authorities	Group of authorities	2
1.5	Operative level	Information security associated with technology	N/A	2
1.6	Upper managerial level	Negative attitude towards information security	N/A	3
1.7	Employees	The policies and regulations direct the work within the authority	N/A	?
1.8		Internal investigations	Employee	1
1.9	Employee	Use information responsibly (there are no regulations for that)	N/A	2
1.10		Specific detailed goals	N/A	1
1.11		No overall, comprehensive goals	N/A	1
1.12	The authority	Verification of long-term overall goals	N/A	2
1.13	The authority	Risk management	N/A	2
2.	Security specialist (resp. 1), lawyer	Information security policies for the use and administration of information systems	N/A	1
2.1	Administrator of systems at the authority	Supervises and responds to questions form the system developers and consultants	N/A	1
2.2	Security unit 1	Responsible for the information security rules and regulations at the authority	The authority	2
2.3	Security unit 1	Revising internal regulations regarding information security	The authority	2
2.4	Security unit 2	Responsible for the information security rules and regulations at the authority	Other authority	2
2.5	Security unit 2	Revising internal regulations regarding information security	Other authority	2
2.6	Chief of authority	Overall responsibility for the security at the authority	N/A	2
2.7	Security representatives	Support chief of authority in their information security work, as defined in the authority regulations	N/A	2
2.8	Security unit	Create efficient management of information	N/A	2

ID	Actor	Task/artifact	Sender/receiver	Ref.
		security with the support of a command and control systems		
2.9	Security unit	Establish an efficient risk handling process	N/A	2
2.10	Security unit	Training of personnel to increase their safety	N/A	2
2.11	Upper managerial level	Develop guidelines, policies and handbooks for information security	N/A	2, 3
2.12	Security unit and the security manager	Responsible for information security work	N/A	3
2.13	Disciplinary boards	Handle serious cases of violation of the authority regulations and rules	N/A	3
3.1	Security unit	Training in information security thinking	Operative personnel	1, 2
3.2	Operative personnel	Lack of understanding for information security	N/A	1, 2
3.3	Resp 2	Training in information security	Other authorities (operative personnel)	3
3.4	N/A	Work on course development	N/A	3
3.5	N/A	Intranet-based support for information security work at high-level of abstraction	N/A	3
3.6	Security unit	Advice on information security issues	N/A	3
4.1	Administration management	Granting access rights	IT system user	1
4.2	N/A	Assign security levels to systems	N/A	1
4.3	Individual	Access control for paper-based information	N/A	2
4.4	Individual	Classification of paper-based information	N/A	2
4.5	Individual	Protect their personal information	N/A	3
4.6	N/A	Identify and classify critical systems	N/A	2
5.1	N/A	Improved security training for administrative personnel, especially substitutes	Administrative personnel	1
5.2	N/A	More information, more structure, more "missioning" and more tools are needed	N/A	3
5.3	N/A	Regular meetings with operative personnel	N/A	3
5.4	Middle managers	Increase the knowledge and competence needed to take responsibility for the security related work	N/A	3
5.5	N/A	Training of and information to	Middle managers	3
5.6	N/A	Knowledge of the security levels of the different systems	IT system users	1
5.7	N/A	Routines for authorization should be strengthened	N/A	1
5.8	N/A	Documentation on who has what access right	N/A	1
5.9	N/A	Documentation on who has sufficient information security training	N/A	1
5.10	N/A	Lack of policies and guidance	N/A	1
5.11	N/A	Lack of knowledge about existing policies and guidance	N/A	2
5.12	N/A	Misuse of data	N/A	2

ID	Actor	Task/artifact	Sender/receiver	Ref.
5.13	N/A	More efficient process for new policies	N/A	1, 3
5.14	N/A	Difficult to test systems with personal data	N/A	1
5.15	N/A	Security check performed after employment	N/A	1
5.16	N/A	Detection of information system malfunction	N/A	1
6.1	Security unit	Informing newcomers about basic security issues	Employee	1
6.2	N/A	Information meetings may regard security issues	Employee	1
6.3	Security unit	Inform the security representatives of other authorities about new strategies and result	Security representatives of other authorities	2
6.4	Security unit	Receive feedback from the security representatives of other authorities	Security representatives of other authorities	2
6.5	Security unit	Define information security related goals	Security representatives of other authorities	2
6.6	Managerial level	The hierarchical structure is a hindrance to effective direct communication from managerial to operative level (and the other way round)	Operative level	2
6.7	Managerial level	Anchor new information, basic data, suggestions and documentation at the highest management	highest management	2
6.8	Resp 1	Acquire security information about a specific issue, when needs arise, by phone, e-mail or face-to-face	System owner, the security unit, lawyer	1
6.9	Resp 1	Direct communication is the most common way for her to transfer security-related information to her subordinates.	subordinates	1
6.10	Personnel	Acquire security information about a specific issue, often by e-mail (more seldom they use the regulations, laws et c available)	Resp 1	1
6.11	Middle managerial level	The Intranet, internal mails and yearly conferences are used to communicate information security issues to the operative level	Personnel	3
6.12	Personnel	Ask for help on security issues	Highest managerial level	3
6.13	Highest managerial level	Order assistance with information security issues to personnel	N/A	3
6.14	N/A	Informal feedback on new policies and regulations from other agencies	other agencies	1
6.15	N/A	Informal feedback on new policies and regulations from authority personnel	personnel	1
6.16	N/A	No formal feedback on information security matters	N/A	1
6.17	N/A	Informal requests to grant access rights	N/A	1
6.18	N/A	Two conferences are held each year to inform about recent security related activities	Security representatives	2

ID	Actor	Task/artifact	Sender/receiver	Ref.
		and goals	at other agencies	
6.19	N/A	Feedback before final decisions on information security issues are taken	Middle level manager, operative level	3
7.1	Security unit	Responsible for scrutinizing new systems and information security issues at the authority	N/A	1
7.2	N/A	No uniform and overview information on all information security matters the personnel at the authority need to care about, at one and the same time and place	N/A	1
7.3	N/A	No systematic process for measuring and evaluation information security activities at the authority	N/A	2
7.4	N/A	Activities are measured against the internal regulations	N/A	2
7.5	N/A	Report perceived deficiencies and suggestions on remedies	Upper-level management	2
7.6	N/A	Implement long-term plan on the PDCA-method providing new tools for controlling and measuring large amounts of information	The authority	2
7.7	Resp. 3	Perform risk analyses based on a general method including estimations of probabilities and consequences of risks	Group of authorities	3
7.8	Resp. 3	Provide education, tools, and templates for self risk analyses	Group of authorities	3
7.9	Security unit	Integrate information security in the processes performed at the authority	The authority	2
7.10	Security unit	Provide support and resources for dealing with information security related matters	Middle managerial level, Operative level	2
7.11	N/A	Integrate control as a positive quality-increasing support in the organization	N/A	3
7.12	N/A	Increase organizational learning by learning from mistakes	N/A	3
7.13	N/A	Increase upper-level awareness by illustrative quantitative information security data	Upper-level management	3
7.14	N/A	Work on sharing information regarding information security with agencies outside the group of agencies	N/A	2
7.15	N/A	There is a need for a common view to protect the information through the whole chain of authorities	N/A	2
7.16	N/A	Collaboration between authorities regarding information exchange and classification	N/A	3
8.1	The authority	Need for common information security terminology	The authority	2
8.2	The authority	Need to adopt the terminology of SS-ISO/IEC 27000	The authority	3
8.3	Lawyer	Common definitions of concepts contained in the regulations	The authority	N/A