# Controlled Information Security

## Results and conclusions from the research project

JONAS HALLBERG, MARGARETHA ERIKSSON,
HELENA GRANLUND, STEWART KOWALSKI,
KRISTOFFER LUNDHOLM, YNGVE MONFELT,
SOFIE PILEMALM, TOVE WÄTTERSTAM,
LOUISE YNGSTRÖM

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
Box 1165
SE-581 11 Linköping

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

www.foi.se

FOI-R--3187--SE
ISSN 1650-1942

Base Data Report
March 2011

**Information Systems**

Jonas Hallberg, Margaretha Eriksson[1],
Helena Granlund, Stewart Kowalski[1],
Kristoffer Lundholm, Yngve Monfelt[1],
Sofie Pilemalm, Tove Wätterstam[1],
Louise Yngström[1]

# Controlled Information Security

Results and conclusions from the research project

[1] Stockholm University, DSV

| | |
|---|---|
| Titel | Controlled information security: Resultat och slutsatser från forskningsprojektet |
| Title | Controlled Information Security: Results and conclusions from the research project |
| Rapportnr/Report no | FOI-R--3187--SE |
| Rapporttyp<br>Report Type | Underlagsrapport<br>Base Data Report |
| Månad/Month | Mars/March |
| Utgivningsår/Year | 2011 |
| Antal sidor/Pages | 42 p |
| ISSN | ISSN 1650-1942 |
| Kund/Customer | Myndigheten för samhällsskydd och beredskap, MSB |
| 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

## Sammanfattning

Inom den offentliga sektorn har flera åtgärder vidtagits för att förbättra informationssäkerheten. Exempelvis har Myndigheten för Samhällsskydd och Beredskap (MSB), med syfte att uppnå en bättre styrning av arbetet med informationssäkerhet, föreskrivit att ledningssystem för informationssäkerhet (LIS) ska inrättas vid Svenska myndigheter. Riksrevisionen fann dock inom ramen för en studie av elva myndigheter att ingen av dessa kunde anses uppnå lämpliga nivåer av informationssäkerhet.

För att skapa bättre förutsättningar för effektivt informationssäkerhetsarbete inrättade MSB ett forskningsprogram inom informationssäkerhet. Inom ramen för detta program har projektet COntrolled INformation Security (COINS) genomförts. I denna rapport presenteras de resultat som producerades under genomförandet av COINS.

Nyckelord: Informationssäkerhet, metrik, ISO/IEC 27001, ISO/IEC 27004

## Summary

The Swedish public sector has taken a number of steps to improve the information security. For instance, the Swedish Civil Contingencies Agency has prescribed the implementation of information security managements systems. Still, in a study covering eleven government agencies, the Swedish National Audit Office found that none of the assessed agencies were considered to have adequate levels of information security.

In order to address the needs of understanding, learning, and managing information security, the Swedish Civil Contingencies Agency started an information security research program. Within this program the COntrolled INformation Security (COINS) research project was established. The COINS project aims at providing knowledge, methods, and tools to support the improvement of the information security abilities in organizations, with a focus on Swedish government agencies. In this report, the results produced within the COINS project are presented.

Keywords: Information security, metric, ISO/IEC 27001, ISO/IEC 27004

# Contents

# 1 Introduction

The ever increasing importance of the information handled by organizations renders information security an important aspect to consider. Adequately deployed information systems provide the means to increase the potential as well as the effectiveness and efficiency of our business processes. However, the extensive use of Information Technology (IT) also comes with related problems caused by the abstract nature of the systems and the lack of physical control over the data. This is mainly due to the possibilities to, for example, swiftly and covertly copy data, access systems remotely, and transfer permissions. Thus, in order to enable efficient use of information systems, it is vital to ensure the necessary information security qualities of these systems.

The Swedish public sector has taken a number of steps to address the information security. For instance, the Swedish Civil Contingencies Agency has prescribed the implementation of information security managements systems (ISMS) in coherence with the standard ISO/IEC 27001 (Hedström, 2009; ISO/IEC, 2005). The standard specifies requirements that can be adopted by organizations in order to uphold an adequate level of security. However, in a study covering eleven government agencies, The Swedish National Audit Office found that none of the assessed agencies were considered to have reached adequate levels of information security (Riksrevisionen, Swedish National Audit Office, 2007).

In order to address the needs of understanding, learning, and managing information security, the Swedish Civil Contingencies Agency started an information security research program. Within this program the COntrolled INformation Security (COINS) research project was established. The COINS project aims at providing knowledge, methods, and tools to support the improvement of the information security abilities in organizations, with a focus on Swedish government agencies. A central question for the project is how information security issues are communicated within the organizations. The project is carried out in a number of steps which embrace:

1. Design modeling techniques and metrics for the communication of information security issues in organizations
2. Collect data from a Swedish government agency
3. Use the modeling techniques to model the communication of information security at the agency
4. Apply metrics on the data in order to assess the information security at the agency
5. Design information security metrics for a specific agency using a participatory design approach

6. Apply the metrics at the agency and produce the related reports
7. Develop a framework for inter-organizational comparison of the maturity of information security and metrics programs
8. Produce a roadmap for future research in the area

This report summarizes the results from the COINS project.

## 1.1 Problem Formulation

The central research questions for the COINS project are:

- How can the use of models and modeling techniques support investigations on and visualize the communication of information security issues in organizations?
- Are metrics a viable tool for assessing the information security in organizations and how should metrics in this case be beneficially applied?
- How can inter-organizational comparisons of information security be performed?

## 1.2 Contributions

The main contributions of the COINS project are listed below. All of these items are further described in Chapter 3. Here, references to the original COINS reports describing the results are provided.

- **Modeling techniques for the communication of information security issues**. During the COINS project five different modeling techniques have been designed. These modeling techniques support the analysis of organizational communication of information security issues, each with emphasis on different aspects (Yngström et al., 2009a; Lundholm & Hallberg, 2009). Further details are provided in the form of an enclosure (Yngström et al., 2009b). A summary of the modeling techniques is provided in (Hallberg et al., 2010).
- **Information security metrics based on textual analysis and the classification of statements**. These information security metrics are based on textual data describing the information security effort of organizations and supports the analysis of its focus. There are two main approaches starting from raw text (Yngström et al., 2009a) and statements extracted from the text (Lundholm & Hallberg, 2009) respectively. Summaries of both approaches are provided in (Hallberg et al., 2010).

- **A quantitative analysis of information security communication**. Based on the designed modeling techniques models have been developed for a government agency. Thereafter the designed metrics were applied to these models. (Yngström et al., 2009a; Lundholm & Hallberg, 2009)
- **A qualitative analysis of information security communication**. Based on the textual descriptions of the studied agency, originating from documentation and interviews respectively, qualitative analyses have been performed. (Yngström et al., 2009a; Hallberg et al., 2010)
- **A method for the design of information security metrics**. A study has been performed in order to evaluate a method for the design and use of information security metrics based on the standard ISO/IEC 27004 (ISO/IEC, 2009b; Lundholm et al., 2011).
- **A framework for inter-organizational comparison of information security and metrics programs**. To enable the comparison of different organizations regarding their information security capabilities and its instrumentation, a framework based on the controls specified in the standard ISO/IEC 27001 (ISO/IEC, 2005) and the information security maturity model presented by the National Institute for Standards and Technology (NIST) (Chew et al., 2008) has been developed. (Granlund et al., 2011)
- **A roadmap for the future research in the area**. A structured description of the research issues that need to be addressed in order to enhance the capabilities in the area has been presented. (Yngström et al., 2011)

# 2 Background

This chapter includes relevant background to the work presented in this report. The following sections present the subjects of information security and trust, information security metrics, the study context, the standards ISO/IEC 27001 and ISO/IEC 27004, and the used terminology. These sections are based on or equivalent to those included in other reports produced within the COINS project.

## 2.1 Information Security and Trust

A prevalent view of the subject of information security is that the problems have not yet been solved simply because the technical expertise is not yet refined enough. In this view we only have to trust the development of more advanced technical tools and the whole problem will eventually go away. This view is however waning and a more realistic (though regrettably more complex) view is gaining ground: The problems of information security depend on far more than just the technical aspects. They also include, for instance, education and understanding (Yngström, 1996), economics (Anderson, 2001), and psychology (Schneier, 2008).

With such relatively complex pictures of what information security entails, it becomes clear that upholding required security of information is a complex issue. The information age has brought about increasing investment and dependence in information systems, yet questions of how far we can trust that information, remain to the larger extent unanswered. If we should continue to put our trust in societies that are increasingly reliant upon information technology, methodological means of dealing with the complexity involved are surely a necessity.

The knowledge and assumptions about information security result in perceptions of the information security of organizations. These images affect the trust and actions of several actors, such as, staff, organizational units, other organizations, the public, and regulatory agencies (Figure 1). However, there are many relations not easily understood; this is what the research started with the COINS project ultimately aims to reveal.

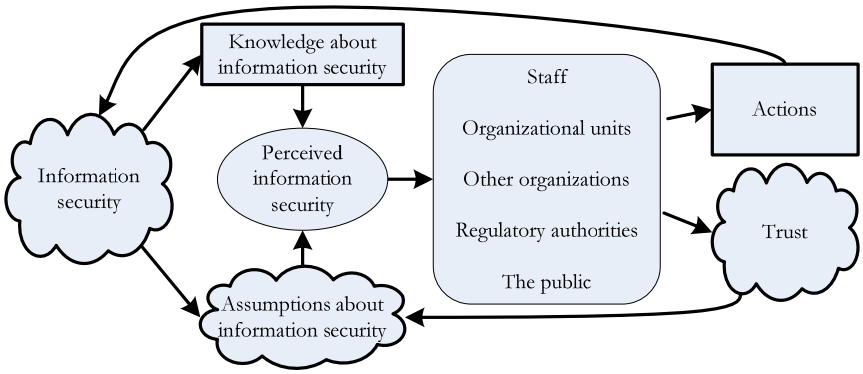


Figure 1: Relations between the concepts of information security, knowledge and assumptions about information security, perceived information security, actors, and their actions affecting and trust in information security

## 2.2 Information Security Metrics

The purpose of security assessments is to produce knowledge about relevant security characteristics of systems. The results used to reach this knowledge can be straightforward, like a binary yes/no, or complicated, like color-coded system and organization maps or vectors with real numbers. In order to be useful, the results have to correspond to the needs for security assessment, which are found in other system related processes, e.g. systems development and risk management.

Security metrics are central to security assessment (ACSA, 2002; Geer et al., 2003). According to the definition by Hallberg et al. (2004): “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”. Thus, if security values correspond to security metrics, they will be possible to interpret. However, the formulation of viable security metrics is challenging and usually left out during the design of security assessment methods.

As part of the COINS project, a thorough analysis of the current state of the area of information security metrics has been performed (Barabanov, 2011).

## 2.3 Study Context

The studies presented in this report were undertaken at one of the largest government agencies in Sweden. The agency uses and maintains comprehensive, centralized data registers. The agency has a close link to the Swedish government

and is the central supervisor and coordinator of the local agencies of their branch, with a mission to support and rationalize their activities. The selected agency may also, by direction of the government, direct and supervise different activities at the national level.

## 2.4 The Standard ISO/IEC 27001

The standard ISO/IEC 27001 (ISO/IEC, 2005) presents a normative method to create, implement and operate an Information Security Management System (ISMS). The standard in addition prescribes an adequate set of information security goals, which if properly fulfilled, provide confidence for the information security of the organization.

According to the ISO/IEC 27001 standard, a number of actions must be taken when an ISMS is to be implemented. Examples of actions are to define an information security policy, to conduct a risk assessment, to prioritize among identified risks, and to approach the risks in an intentional and controlled manner.

The ISO/IEC 27001 prescribes a set of 133 information security controls for an ISMS. These controls should either be implemented as part of or excluded from the ISMS. Exclusion of a control requires a thorough justification. Further, the impact of the controls should be measured regularly to ensure that they are in line with the organizations goals and that these goals are fulfilled. A description of how to perform these measurements is not included in the ISO/IEC 27001. This is instead described in the supplementing standard ISO/IEC 27004.

## 2.5 The Standard ISO/IEC 27004

In addition to presenting the standard, this section introduces several terms that are central to this report as well as how these terms relate to each other.

The ISO/IEC 27004 standard concerns the creation and use of an information security measurement program. To create such a program, metrics (called measurement constructs in the ISO/IEC 27004) are designed for the controls included in the ISMS of the organization. Even though it is assumed in the ISO/IEC 27004 that there is an implemented ISMS, as described in the ISO/IEC 27001, there is nothing stopping an organization from using the method described in the ISO/IEC 27004 for the design of metrics measuring other aspects of information security, defined by the organization, as well.

The process of designing a metric according to the ISO/IEC 27004 is shown in Figure 2. The process is performed for each metric that is to be designed. If the control to be measured is too extensive for one metric, several metrics may need to be designed.

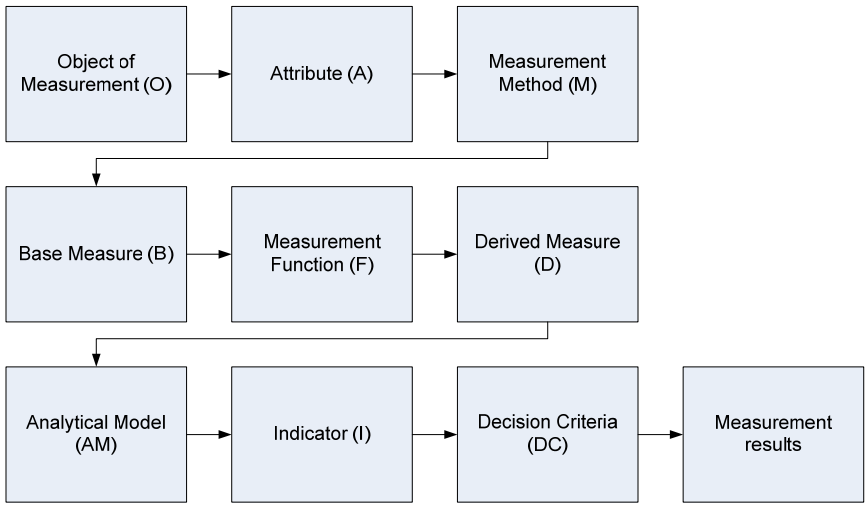


Figure 2: The steps in the design of measurement constructs as described in the ISO/IEC 27004

In short the method starts by identifying *objects of measurement*, i.e. where the measurement data can be gathered. A set of *attributes*, describing what data is to be extracted from these objects, is defined. The *measurement method* states how the data collection should be performed and the results from this data collection are called *base measures*.

The base measures can then be combined using *measurement functions* which aggregate data. The result from such an aggregation is called a *derived measure*. An *analytical model*, using the derived measures and/or some base measures, further aggregates the data so it can be related to some reference values. This aggregation produces an *indicator* which is then compared to the reference values defined in the *decision criteria*. Finally, the comparison of the reference values and the actual values yields the *measurement results*.

## 2.6 Terminology

In this section, the terminology central to the COINS project is presented. Although some of the terms are discussed earlier in this chapter, a digested version of their description is included here for completeness. Following the name, within parentheses, the used shorter forms of the terms are listed.

**Control**. In this context, controls signify means to manage risk. That is, the information security is supported by a number of controls, whose implementation address social and technical aspects of information security. The standard

ISO/IEC 27001 (ISO/IEC, 2005) includes 133 controls to be considered when establishing an **information security management system** (ISMS).

**Information security**. Information security relates to information assets and the ability to uphold security-related characteristics, such as confidentiality, integrity, and availability (Gollmann, 2006; ISO/IEC, 2009a). 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 security assessment** (security assessment). Information security assessments are performed in order to establish how well a system meets specific security criteria. The aim of an IT security assessment is to produce knowledge, which can, for example, be used to improve the security levels of the assessed system. Although perfect security should be the goal, it cannot be achieved. By increasing the knowledge of the assessed system, security assessments improve the validity of the corresponding actors' perception of the information security. Although security assessments cannot guarantee any level of security, they can provide a basis for confidence in the assessed system (Bishop, 2003). Thus, the trust in the system may be increased.

**Information security communication**. Communication in the cybernetic sense means control; to be in control is to communicate (Beer, 1981). Thus, information security communication is in the COINS project treated as communication to be in control of information security issues.

**Information security management system** (ISMS). According to ISO/IEC (2009a) "An ISMS (Information Security Management System) provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets to achieve business objectives based upon a risk assessment and the organization's risk acceptance levels designed to effectively treat and manage risks." Note that an ISMS includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

**Information security metric** (security 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.

**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 (Encyclopædia Britannica, 2011).

**Statement of applicability** (SoA). A SoA specifies the **controls** to be included in an ISMS (ISO/IEC, 2009a). The standard ISO/IEC 27001 constitutes an adequate basis for the specification of a SoA. However, additional controls should be included whenever necessary.

# 3 Results

This chapter presents an overview of the results from the COINS project. For more detailed descriptions of the results, see the corresponding reports.

## 3.1 Modeling the Communication of Information Security

In order to capture the communication of information security issues within organizations, a framework and four models have been designed. The reason for designing several different approaches is the need to focus on different aspects of the communication depending on the context. The results adhere to the principles of cybernetics (Beer, 1981), including variety engineering and recursion, in order to provide adaptation and learning. The system in focus is a generalized Information Security Management System (ISMS) for an organization.

The results consist of: the 14-layer framework, the 3-level organizational model, the cube model, a reference model based on the normative security objectives in appendix A of the standard ISO/IEC 27001, and the entity-action model. These results are presented in the following sections.

### 3.1.1 The 14-layer Framework

The 14-layer framework (Yngström et al., 2009a; Hallberg et al., 2010) was designed to clarify and emphasis the existence of 14 layers in the communication of information security. The framework includes seven social and seven technical layers. The seven social layers are SWOT, cultural, ethical, legal, managerial, organizational, and adaption. The seven technical layers are those included in the Open Systems Interconnection model (OSI model) (ISO/IEC, 1994), that is, application, presentation coding, session, transport, network, link, and physical medium. Further, the framework builds on previously published work considering five of the social layers of communication (Kowalski, 1994; Langefors, 1968; Falkenberg et al., 1998). Novel in the 14-layer framework are the SWOT and adaption layers. The SWOT layer was added since every system has to be viewed in relation to its environment, starting with a risk analysis. The adaption layer was added to represent the interpretation of data in the technical layers as information in the social layers and the transformation of information in the social layers to data in the technical layers.

### 3.1.2 The 3-level Organizational Model

An important characteristic of information security communication is the relation between different decision levels in the corresponding organizations. The 3-level

organizational model (Yngström et al., 2009a; Hallberg et al., 2010) is based on the assumption that an enterprise has three main decision levels: the strategic, the tactic, and the operational level. From this a generalized recursive model of the three decision levels was created. The model includes aspects regarding:

- inter- and intra-level communication in the organization,
- the distinction between the communication of strategic issues, peer-to-peer communication, and physical signals.
- relations between parts of enterprises, that is executive, quality of service, enterprise communication architecture, and data communication technology, and
- recursiveness of the model, that is, the ability to capture several levels of abstraction.

### 3.1.3 The Cube Model

The cube model was created to provide a compact, yet comprehensive picture of the information security work in an organization. The first revision of the cube model has the three dimensions Decisions, Rules, and Communication. The Decisions dimension represents the life cycle stages for any system, modeled as the stages *Policy*, *Manage and control*, and *Implement and maintain*. The Rules dimension represents the *Environment*, the *Social layers* (SWOT, cultural, ethical, legal, managerial, organizational, and adaption), and the *Technical layers* (application, presentation coding, session, transport, network, link, and physical medium). In the cube model, the seven social and the seven technical layers are merged into the social and technical aspects, respectively. The Communications dimension represents the three decision levels in an enterprise, that is, the *Strategic*, *Tactic*, and *Operational* decision levels.

In the second revision of the cube model (Lundholm & Hallberg, 2009), the naming of the dimensions was changed to the actual values of the dimensions, that is,

- *Environment, Social, Technical* to represent what is communicated,
- *Strategic, Tactical, Operational* to represent to what decision level in the organization the communication belongs, and
- *Plan, Operate, Control* to represent where in the life cycle of the organization's information security program the communication take place.

For the third dimension, that is, plan, operate, and control, this involved a renaming of the values to represent the life cycle stages of an information security program.

The method for construction of cube models representing organizations starts from statements describing the information security work performed in the organization. Each statement is classified by assigning a triplet of values representing the three dimensions. Consequently, the statements are mapped the 27 sub-cubes which together form the cube (Figure 3).

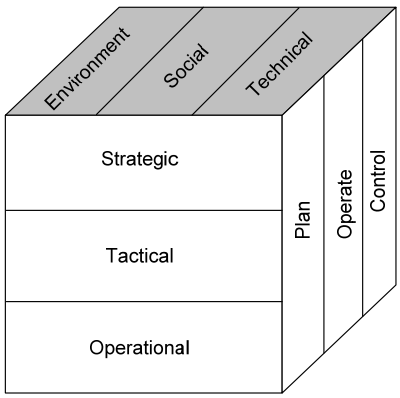


Figure 3: The cube with its layers

### 3.1.4 The Reference model

To be able to compare the emphasis of different artifacts relating to security (such as, policies, instructions, and communication) on the various aspects of information security, a reference model has been created. The reference model is based on the normative security objectives in appendix A of the standard ISO/IEC 27001 and a terminology. The terminology is based on established security standards (CC, 2006; ISO/IEC, 2005; ISO/IEC/JTC 1/SC 7, 2007; ISO/IEC, 1994; ITU, 1994; Swedish Emergency Management Agency, 2006; SIS, 2007; 2003) and frameworks (IT Governance Institute, n.d.; COSO, 2004; The Federal Facilities Council, 2001; Oxford University Press, 2004) as well as the FRISCO report (Falkenberg et al., 1998), which provides control perspectives on information systems in general. The resulting terminology includes 229 terms. (Yngström et al., 2009a; 2009b)

To model the emphasis of an artifact, such as the documentation of information security work, on different aspects of information security involves the following steps. Firstly, the artifact has to be described in textual form. Secondly, the information security-relevant statements included in the text have to be extracted. Thirdly, the statements are classified as belonging to one of the eleven normative objectives, labeled A5 to A15, included the standard. Thus, eleven sets of statements labeled A5 to A15 are formed. Fourthly, the number of occurrences of the 229 terms included in the terminology are counted for each of the statements

and accumulated for all statements belonging to the same set. Finally, the fraction of occurrences is computed for each of the eleven sets of statements.

### 3.1.5 The Entity-Action Model

The objective of the entity-action models is to visualize the communication between entities in the modeled organization. The entity-action model is based on the 3-layer organizational model. To ease the modeling it has been simplified and do not distinguish between different types of communication, the different parts of entities in an enterprise, and recursion.

An entity-action model consists of a table and a graph and is based on statements extracted from textual descriptions of the organization to be modeled. Each statement constitutes one action in the model. The involved entities are identified from the statements. An interaction is an action that involves two entities where one entity is the sender and one entity is the receiver and thus an interacting entity is an entity participating in an interaction.

Each entity is represented by a row in the table with references to the actions where the entity is sender, receiver, or indirectly referenced. The graph includes the entities being part of the indentified interactions. Further, the graphs are divided in such a way that the entities belonging to the strategic, tactical, and operational levels are depicted at the top, in the middle, and at the bottom of the graph respectively.

## 3.2 Information Security Metrics based on Organizational Models

In this section, a set of information security metrics is presented. These metrics are based on the cube, reference, and entity-action models presented in the previous section.

### 3.2.1 Metrics Based on the Cube Model

The metrics based on the cube model (Section 3.1.3) are intended to support the identification of gaps in the information security work of an organization. Two sets of metrics are specified, based on observations of single models and the comparisons of models respectively.

The metrics computed from single models involve the distribution of statements over clusters of the sub-cubes in the model. The used clusters are the elementary 27 sub-cubes, the 27 possible blocks of three sub-cubes, and the nine possible slices (with 3 by 3 sub-cubes) of the cube.

The metrics computed by comparing different cube models can be used to compare the relative focus of the models. This is supported by diagrams including plots of the relative distribution of statements in different cube models or direct comparisons achieved by plotting the difference of the relative values for two models. These two mean of comparison can be used for the three different types of sub-cube clusters considered by the metrics computed for single models.

### 3.2.2 Metrics Based on the Reference Model

The metrics based on the reference model supports the comparison of artifacts considering their focus on different information security aspects. In principle, the comparisons can involve any textual descriptions of artifacts. However, the presented metrics are based on the comparison with the normative standard ISO/IEC 27001 (ISO/IEC, 2005).

For each control in each section, labeled A5 to A15, in Appendix A of the standard, the number of occurrences of 229 selected security related terms was recorded. Based on this data the fraction of occurrences was computed for each of the sections A5 to A15 (Figure 4).

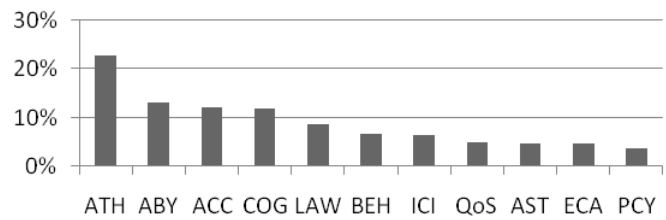


Figure 4: The fraction of occurrences of the 229 security-related terms for each of the sections A5 to A15 in Appendix A of the standard ISO/IEC 27001.

To analyze an artifact, such as documentation of the information security work performed in an organization, statements are classified as belonging to one of eleven sets representing the sections A5 to A15 in Appendix A of the standard. Thereafter the number of occurrences of the 229 terms is counted for each of the statements and accumulated for all statements classified as belonging to the same set, that is, A5 to A15. Finally, the fraction of occurrences is computed for each of the eleven sets of statements. The resulting distribution over the sets A5 to A15 was compared to the distribution for the appendix A of the standard. (Yngström et al., 2009a)

### 3.2.3 Metrics Based on the Entity-Action Model

The metrics based on the entity-action model are divided into two sets supporting the analysis of a single model and the comparison of different models respectively. The metrics for model analysis involve measurements and computations related to the size of the model and interaction patterns. In Table 1, the proposed measurements and computations are listed.

Table 1: The measurements and computations proposed as support for the analysis of entity-action models

| Measurements and computations |
|---|
| Entities |
| Interacting entities |
| Interactions |
| Actions |
| Assigned actions |
| Interactions between layers |
| Interactions within layers |
| Interactions with external entities |
| Internal interactions with undefined entities |
| Percent of entities with at least one interaction |
| Percent of actions that are assigned |

The metrics for model comparison involve the same measurements and computations related to the size of the model and interaction patterns as used for the analysis of single models. To support comparison the results for multiple models can be plotted in common diagrams. (Lundholm & Hallberg, 2009)

## 3.3 Quantitative Analysis of Information Security Communication

During the project, the designed models and the corresponding metrics have been used to analyze data collected from the studied agency. In this section, a selection of the results is presented for each of the cube, reference, and entity-action models.

### 3.3.1 The Cube Models

The cube models can be presented as histograms in two or three dimensions. In either case, there are 27 bars, corresponding to the sub-cubes of the model, showing the relative focus of the input data on the area represented by that particular sub-cube. Using three dimensional histograms, the 27 bars are ordered as to reflect the location of the corresponding parts of the cube (Lundholm & Hallberg, 2009). An example of the cube model, using the standard ISO/IEC 27001 as the data source, is depicted in Figure 5.

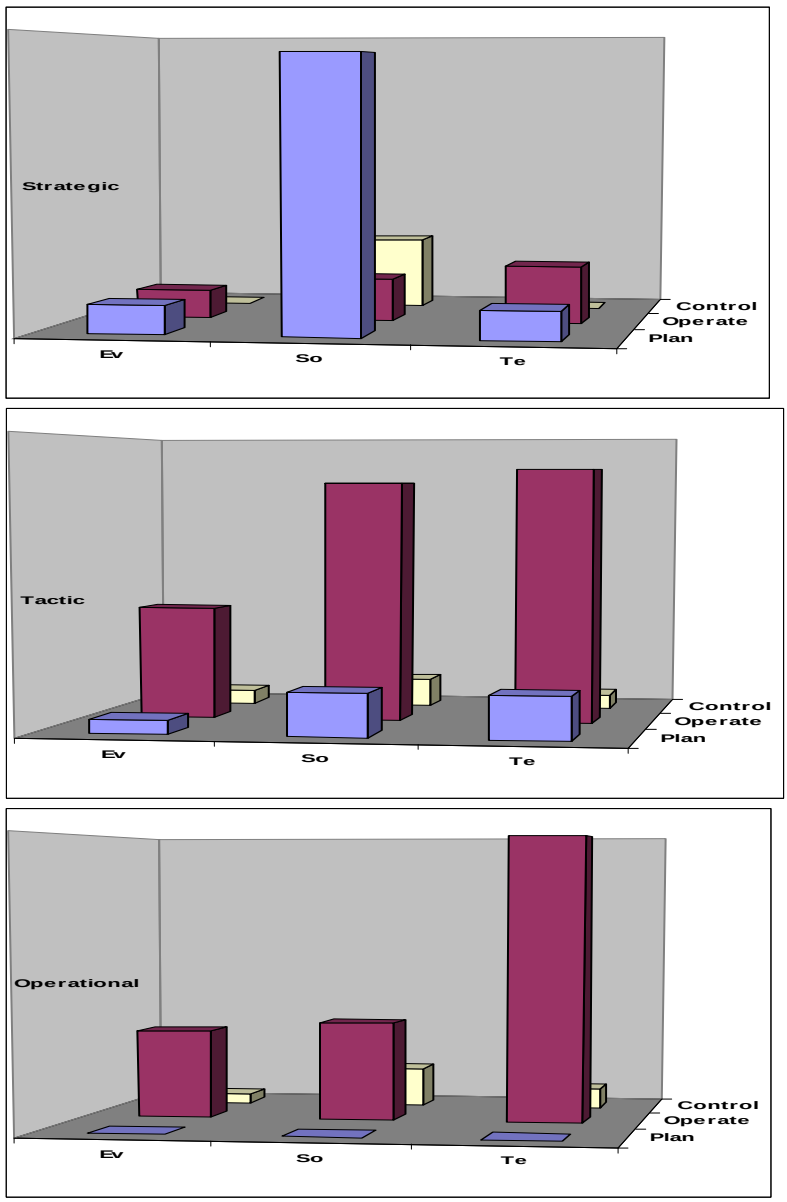


Figure 5: Three dimensional histograms representing the distribution of statements extracted from the ISO/IEC 27001 appendix A

An example of a metric computed for the Appendix A of the standard ISO/IEC 27001 is shown in Figure 6. Each color in the figure represents nine clusters of sub-cubes (each represented by one bar), where each cluster consists of three

sub-cubes. Each bar is labeled with the two dimensions that are fixed and an asterisk representing the dimension that varies. The top row of labels indicates the lifecycle phase, while the middle row indicates the decision level and the bottom row indicates the type of communication.

Each bar in the graph shows the fraction of the statements that was classified as belonging to the corresponding cluster. Since each bar shows a percent value for that cluster and each color in the figure is a separate set of clusters, the sum of the bars for each color is 100 %.

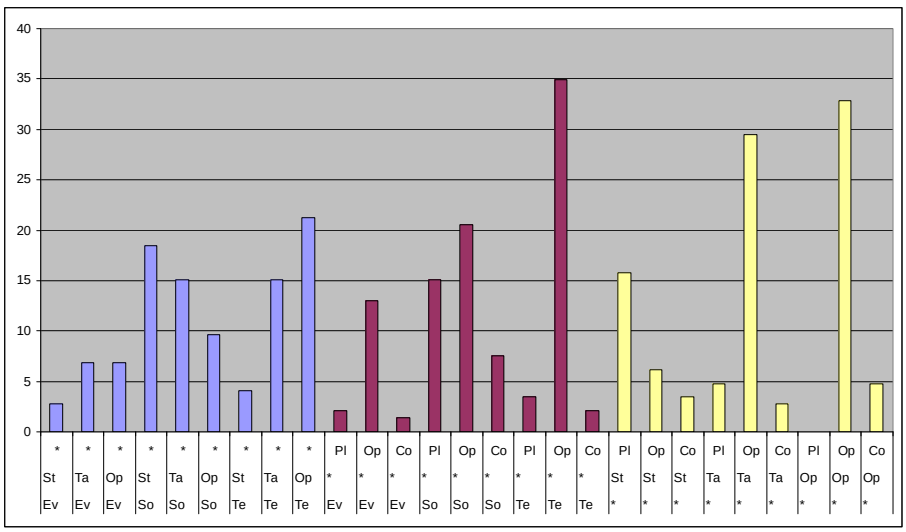


Figure 6: Graph showing the distribution of the controls specified in Appendix A of the standard ISO/IEC 27001 over the rectangular blocks (with three sub-cubes) from the cube

### 3.3.2 The Reference Model

The results from the computations on textual data considering a collection of documents relating to information security work and interviews with personnel at the studied agency respectively are presented in Figure 7 and Figure 8. As specified by the metric (Section 3.2.2), the results for the documents and interviews respectively are compared to the result from the analysis of Appendix A of the ISO/IEC 27001.

To support the interpretation of figures below, the understanding of norms/acronyms according to the standard is (including the consecutive numbering as applied in Appendix A of the standard):

Authorization (ATH) for ECA, A10
Accessibility (ACC), A11
Availability (ABY), A12

Account (ICI), A13
Account (QoS), A14
Account (LAW), A15
Policy (PCY), A5
Organization (ECA), A6
Asset (AST), A7
Cognition (COG), A8
Behaviour (BEH), A9

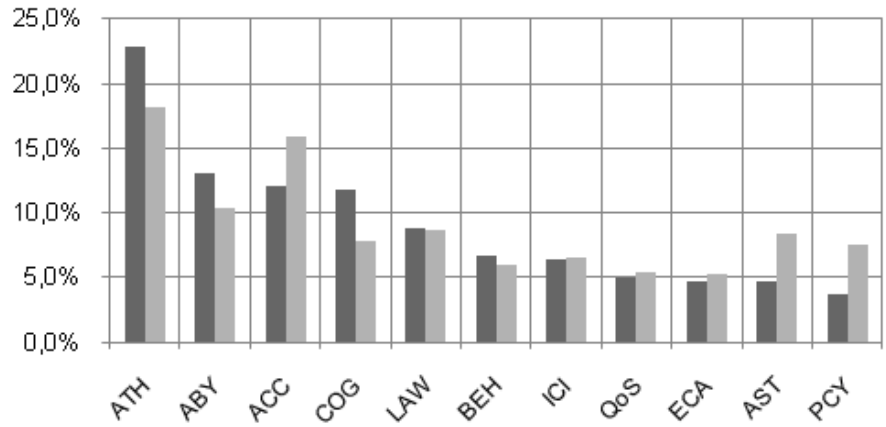


Figure 7: Relative occurrences of the terms in Appendix A of the ISO/IEC 27001 (dark grey) and the agency documents (light grey)

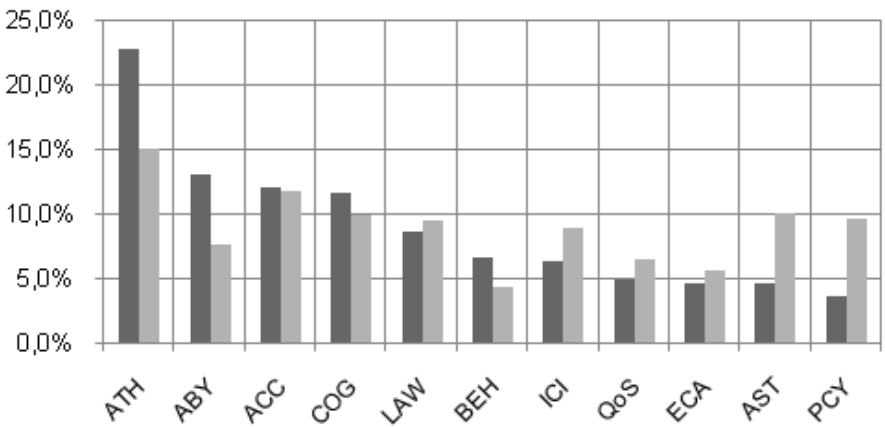


Figure 8: Relative occurrences of the terms in Appendix A of the ISO/IEC 27001 (dark grey) and the interviews with agency personnel (light grey)

### 3.3.3 The Entity-Action Models

Using entity-action models, models for Appendix A of the ISO/IEC 27001, the studied documents, and the interview responses, have been designed. As an example, a simplified version of the graph part of the model resulting from the document study is presented in Figure 9. The edges indicate the direction of the primary data flow.

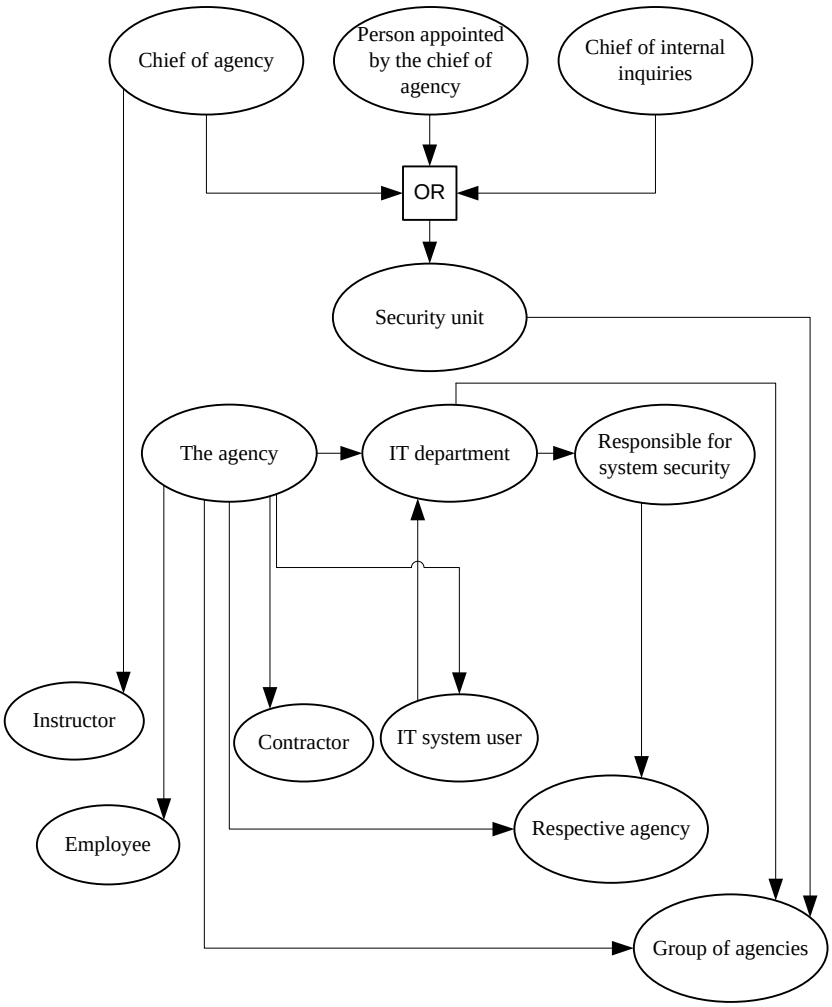


Figure 9: A simplified version of the graph part of the entity-action diagram for the statements extracted during the document study

Examples of measurements and computations for the entity-action model illustrated in Figure 9 are included in Table 2. Since, the number of entities is

larger than the number of interacting entities, there are entities not included in the graph part of the model. The number of actions indicates the size of the relevant parts of the underlying data. An assigned action is an action that is connected to at least one entity, either as sender or as receiver (or both). Since there are internal interactions with undefined entities, there are also interactions not included in the graph. The layers mentioned in connection with the interactions are the three decision levels: strategic, tactical, and operational. External entities are those that are not part of the studied organization, for example contractors, whereas undefined entities are those that are internal to the organization but can not be assigned to a decision level, for example employees or the agency.

Table 2: Measurements and computations for the entity-action model created from the agency documents

| Measurements and computations | Result |
|---|---|
| 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% |

## 3.4 Qualitative Analysis of Information Security Communication

In order to capture the qualitative aspects of information security communication within a government agency a longitudinal case study was performed. A case study is a common way of performing a qualitative inquiry with an explorative, descriptive or explanatory character. The foundation of a case is a phenomenon, such as an individual, a setting, an incident, an organization, or a system. Case studies are suitable when the investigator has little control over events, and when the focus is on a contemporary phenomenon within a real life context (Yin,

1994). Interviews and document studies are often used in case studies, as complementary data sources (Travers, 2001).

### 3.4.1 Design, Data collection and Analysis

The methodology chosen for this exploratory case study, where the object of study is the information security posture of a government agency, was a series of three sets of semi-structured interviews and an initial document review. The empirical data collected focused on values, practices, and communication structures of the information security. The study embraces the entire project time, 2008 to 2011. The document study and the first set of interviews where performed according to the predicted design. For the second and third interview set, however, the preferred order was disturbed with regards to participating respondents during the three years period (Table 3).

Table 3: The performed document reviews and interviews

| Year | Document review | Interview set | | | Interview guide |
|---|---|---|---|---|---|
| | | Exe-0 | Exe-1 | Exe-2 | |
| 2008 | 5 official documents | A | B | C | Exploratory |
| 2010 | | A | | C and D | 8 categories |
| 2011 | | D and E | | | 8 categories, organization change and experience on metrics |

The review of five available policy documents, in 2008, was assumed to illustrate the agency's normative views on information security, i.e. what employees had to relate to. In the document analysis all information security statements were extracted and sorted into 8 categories. Each category was provided with a short summary describing the interpretative meaning of the category (Pilemalm et al., 2010).

In the first set of interviews, in 2008, three respondents, A, B and C, representing three different organizational levels were interviewed. A represented the upper managerial executive level denoted as Exe-0. B represented the agency middle managerial level, Exe-1. C represented the operative level, Exe-2. The agency's top managerial level was not interviewed. In the interview analysis all information security statements were extracted, sorted and interpreted within the same 8 categories as the document statements (Pilemalm et al., 2010).

In the second set of interviews three respondents, A, C and D, were interviewed. A had an unchanged position at the agency. C just left the agency and was replaced by D at operative level. In the third set of interviews two respondents, D and E, were interviewed. Recently before the third set of interviews a major change in the agency's information security organization was performed. Respondent A at Exe-0 level left the agency. Two respondents, D and E, both former Exe-2 representatives, changed position to Exe-0 and was interviewed. B continuously, through out the period, had the same position, but was unable to be interviewed due to heavy work load at second and last occasion.

Comparative analyses of the different perspectives of Exe-0, Exe-1, and Exe-2, and of interview and document review results, were performed. The aim was to perceive a picture of the correspondence between the official/ideal (Exe-0), the established (Exe-1), and the real/operative (Exe-2) views on information security to the normative view as found in the documents analysis.

### 3.4.2 Comparative Analysis 2008, Summary

The comparative analysis is built around the themes: Document analysis, interview analysis, systems development, and future improvements.

The document analysis showed that the policy documents had a narrow interpretation of information security relating almost exclusively to technology. There were few guidelines for daily operative activities (1) and no assignment of responsibility to different organizational roles (2). Information security was not a part of organizational development or clearly integrated in its information systems. In conclusion, there was a clear lack of normative guidance concerning information security at the agency.

The interview analysis showed that the perception of information security is vague, narrow and technology oriented on all managerial levels (3). There was a low transparency between levels in that the lower organizational levels were not aware of the little available security training and information (4), of existing policies and regulations (5) and only the Exe-0 knew about structures for communication and feedback. There was a hierarchical organizational structure with little influence from operative personnel over information security issues, and no direct communication from top to bottom organizational level (6). Information security did not affect other decisions at the agency, no meetings where specifically devoted to security issues and there where no sufficient routines for handling new employees. There was also no common information security terminology available. In summary, no common view on information security between managerial levels existed (7).

During the agency systems development insufficient integration of information security aspects occurred, inherent system errors that violated high quality information security was reported and there were no back-up routines for one of

the most critical systems of the agency (8). The consequences appeared although the agency spent resources on transparent technical solutions rather than on education of the personnel.

Future improvements of information security should include strategies and planning (9), information and education, continuous feedback, follow-ups and communication with personnel, and a uniform information security terminology. However, equally important is a clarification of who has what roles and responsibilities, a reconsideration of the organizational structures and a revision of the division of labor (10). Decentralization, a lower transparency of organizational levels and a bottom-up approach, where different actors are allowed to identify their most pressing information security problems and suggest how to work on them, is recommended. An organizational integration where information security builds on daily routines and is rooted at the operative level before they are put into practice seems necessary.

Future improvements regarding information systems, information security aspects need to be clearly integrated in future systems development. Again development of the systems should be based on the participation of the personnel (users) in the development process and information security should reflect their recurrent routines and problems.

### 3.4.3 Longitudinal Analysis 2010 and 2011, Summary

The longitudinal analysis handles the information security issues chronological as they appear in the thematic comparative analysis.

1. The official documents lack of normative guidance has been enforced by a set of operational guidelines. The guidelines where immediately sought after and appreciated by employees in all managerial levels, not only the operational (2010). The guidelines are now objects of renewal (2011).
2. No operative changes was made to the assignment of responsibility to different organizational roles, only minor adjustments, such as assigning responsibility for updating intranet information (2010). The recent major change of the information security organization though has impact on responsibility allocation. Roles have become clear and streamlined, with the objective to highlight the information security within the organization (2011).
3. The bias towards technological security still existed but had to some extent given way to administrative information security (2010). There seems to be a conscious acceptance of technological security as dominant due to the agency's business area, and the ratio between technology and administrative information security is perceived as satisfactory (2011). This could be an

indication that the change in the ratio from 2008-2010 was enough to produce equilibrium.

4. All managers at the agency had participated in an information security education (2010). The education is extended to all employees during fall 2011 (2011). Leading to that the vague view of IS that existed 2008 in the managerial levels is replaced by a more stable, common view that is possible to address by all levels in the organization.

5. The poor ability to express the sense of policies and regulations remained (2010). After the reorganization it was clearly improved, policies and regulations were known and understood (2011).

6. The rigid communications structure from 2008 showed in 2010 no positive change (2010). In 2011, after the organizational change a difference could be detected. The structure was changed with an advantage for a bottom up communication. The responsibility for the incident management, the means for operational personnel to communicate problems and errors, was moved from Exe-2 level to Exe- 0 level and thereby altering the ability to communicate from top to bottom to the better (2011). The structure for recurrent meetings devoted to information security has not been improved (2011). The clear statements from 2008 and 2010 on little attention from top management is in 2011 altered to a perceived positive interest from top management (2011).

7. The vague view of information security started to alter due to the common information security education for managers at the agency and the issuing of guidelines (2010). The extended education, clarification of responsibilities and understood toll gates at system development efforts have changed the vague view to a clearer, joint vision where the technological bias is accepted without administrative information security being reduced (2011).

8. When developing new systems information security was addressed. This however was only clear to the Exe-0 level. Respondents on the Exe-1 and Exe-2 levels had little information in the matter and found the grade of information security attention in the develop process rely on capabilities of the individual members of different projects. The agency is responsible for the development and administration of systems for subordinate agencies. There was uncertainty whether the real end users, that is, the operational personnel in the sub agencies, were involved or not in the development of their own information security architecture. Also, there still existed an IS risk with inherent errors in legacy systems that continuously were updated (2010). All development of new systems now has two definite, well known toll gates where information security is considered. However, the problem with involving end users still remains (2011).

9. To implement an ISMS with structured strategies and planning and systematic work processes was an ambition in 2008. The task was not accomplished due to resources allocated to systems development, rather than to ISMS development. The ambition still remained (2010). After the reorganization the conditions for actually implementing an ISMS seems good. The top management pays attention to and is positive about information security matters. Roles and tasks have been streamlined. There have been roles created for implementing a plan-do-check-act based ISMS. The work is delayed as resources are allocated for accreditation tasks (2011).
10. The reconsideration of the organizational structures and a revision of the division of labour that seemed inevitable 2008 started between second and third set of interviews. The conditions for success are good, see 9.

## 3.5 Design of Information Security Metrics

The international standard for the development and use of an information security management system (ISMS), ISO/IEC 27001, has been available since 2005. This standard mandates that measurements of the processes for managing an organizations information security should be performed in order to demonstrate how well they are working. A method for how to develop these measurements was published 2009 in the standard ISO/IEC 27004.

In order to investigate the capacity of the method presented in the standard ISO/IEC 27004, a case study was performed at a Swedish government agency (Lundholm et al., 2011). The aim of the study was to design and implement metrics using an augmented method of the one described in the standard ISO/IEC 27004. The augmentation to the method is the inclusion of a participatory design approach to the creation of the metrics. The standard provides a template for the specification of metrics, whereas the augmentation is essential in order to extract the information needed from the agency in order to be able to design the metrics.

The first step in the design of metrics was to *identify the controls* for which to design metrics. The identification of controls included a needs analysis based on the document review and first set of interviews described in 3.4.1. The needs analysis resulted in a structure of 42 relevant security characteristics. The 42 security characteristics were mapped to the controls in the standard ISO/IEC 27001, resulting in the identification of 25 controls. The identified controls were prioritized in cooperation with a security specialist at the studied agency resulting in the selection of five controls for which metrics was to be designed within the case study.

The next step was to *design metrics* for the controls. The guiding principle for the case study was that metrics design and use should be feasible to perform with limited resources and still provide value to the agency. The participatory design

was implemented as two sets of interviews with security personnel, whose responsibilities correspond to the security areas of the controls. The first set of interviews established areas of interest for measurement as well as possible data sources for performing measurements. The data from these interviews were formalized and suggestions on how to continue were prepared. These suggestions were presented, discussed and subsequently modified during the second set of interviews.

The final step was *measurement using the metrics*. Once the metrics was completed, they were sent back to the respondent who performed the measurements defined in the metrics.

From the study it was concluded that design of a metrics program for an organization with an immature information security program should probably be performed by first identifying areas of interest for measurement. Next, the metrics program should be initiated by gathering data that is readily available and slowly expand the metrics program to measurements requiring data that is more difficult to collect. Expansion of the metrics program in this way may require development of new processes for collection of data. A vital point is that the presence of metrics programs supports the efforts to make the ISMS more mature and, thereby, improves the availability of data to be measured.

## 3.6 Framework for Inter-Organizational Comparison of Information Security Capabilities

In order to support the effort of Swedish government agencies to address information security in accordance with the established standards for ISMS, a framework for inter-organizational comparisons of information security capabilities has been presented (Granlund et al., 2011). The framework provides means to assess the maturity of the information security metrics program that is supposed to be part of the ISMS.

Applying the framework will provide illustrations of the maturity of the metrics program as well as the overall results of the implemented information security metrics. The framework includes three phases (Figure 10). In the first phase, the information security program and the associated metrics program are measured in terms of their extent as related to the 133 controls specified in the standard ISO/IEC 27001 (ISO/IEC, 2005). In the second phase, the maturity of the metrics in the metrics program is measured by classifying the metrics according to the maturity model presented by the National Institute for Standards and Technology (NIST) (Chew et al., 2008). This classification of a metric is related to the maturity of the process for collecting security related data. In the third phase, the

task fulfillment is measured in terms of the specified metrics being satisfactorily or insufficiently fulfilled for each of the maturity levels.

These results can be used for the comparisons of organizations as well as the basis for discussions and exchange of knowledge related to ISMS and information security metrics programs. It is foreseen that the application of the framework among Swedish government agencies would increase the ability of regulatory authorities to assess the ISMSs of agencies as well as the inter- and intra-organizational learning related to information security.

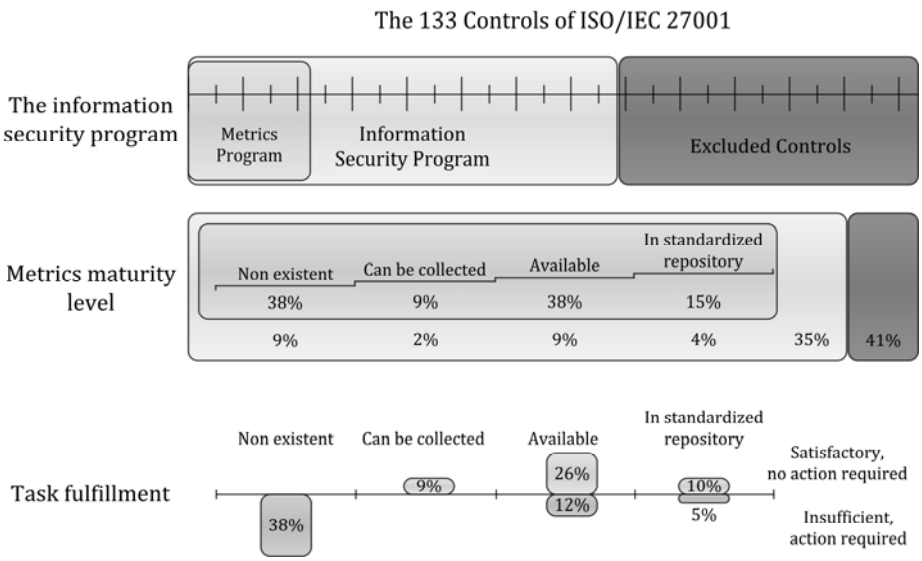


Figure 10: The concluding illustration of the three phases in the framework

## 3.7 Roadmap for Future Research

Prior to discuss future research within the area of information security metrics a comprehensive State of the Art report was produced (Barabanov, 2011). In summary, the report concludes that considerable progress has been made in recent years even though the research area, in certain respects, still can be said to be in its infancy. Due to the two standards ISO/IEC 27004 (ISO/IEC, 2009b) and NIST SP 800-55 (Chew et al., 2008), the terminology and common understanding of certain related concepts is stabilizing, even though there is still a lack of consensus on such matters as a common classification scheme and universal basic sets of measures. Also, the two standards may be said to be complementary where NIST SP 800-55 better describes the long term, strategic perspective including factoring in the maturity and capabilities of organizations security programs whereas ISO/IEC 27004 gives more detailed guidance on

operational aspects of security measurement and is generally more formalized. However, it is not expected that they together provide comprehensive guidance on all relevant issues.

Apart from these standardization efforts and related work on automation tools such as the Security Content Automation Protocol (SCAP) (Quinn et al., 2009), efforts are presently being made to measure the effectiveness of an entire ISMS, as opposed to individual controls, by means of attack surface and attack graph based metrics. Open issues still remain; one such also studied by COINS through the top-down approach as used in the first phase 2008-2010 is how to translate lower-layer metrics into higher-layer ones and to further research and investigate how different approaches may provide adequate and “good enough” measurements (Barabanov, 2011). Other open issues are the appropriateness of specific data formats of measurements and how to relate measurements – including standardization of processes and measurements – to the constant changes in the environment (Yngström et al., 2011).

## 3.8 List of Publications

The COINS project has resulted in the reports and articles listed below.

### 3.8.1 Reports

COINS Report #1: Modelling the Communication of Information Security Issues. DSV Report series 09-008A. (Yngström et al., 2009a)

Enclosures to COINS Report #1. DSV Report series 09-008B. (Yngström et al., 2009b)

Information security metrics based on organizational models. Base Data Report. FOI-R--2812--SE. (Lundholm & Hallberg, 2009)

Controlled Information Security: How to recognise and improve organisational information security status, FOI Memo 3102. (Hallberg et al., 2010)

Relevant information security characteristics: Based on needs for information security assessment. FOI-R--3188--SE. (Lundholm & Hallberg, 2011)

Information Security Metrics: State of the Art. DSV Report series 11-007. (Barabanov, 2011)

Information Security Assessment. A Roadmap for Research. DSV Report series 11-008. (Yngström et al., 2011)

Summary Report COINS project Open Seminar on Metrics. DSV Report series 11-009. (Kowalski et al., 2011)

Design and Use of Information Security Metrics: Application of the ISO/IEC 27004 standard. Scientific Report. FOI-R--3189--SE. (Lundholm et al., 2011)

A Framework for Inter-Organizational Comparisons of Information Security Capabilities. Methodology Report. FOI-R--3186--SE. (Granlund et al., 2011)

Controlled Information Security: Results and conclusions from the research project. Base Data Report. This report.

### 3.8.2 Articles

Datafel om våra pengar blir aldrig upptäckta. Debattartikel i Dagens Nyheter. (Yngström & Mähring, 2008)

The 14 layered framework for including social and organisational aspects in security management, Proceedings of the South African Information Security Multi-Conference (SAISMC) 2010. (Monfelt et al., 2010)

Information Security as a Pre-requisite for E-government Services – developing the organizations and the information systems. Proceedings of the 6th International Conference on e-Government. (Pilemalm et al., 2010)

Information Mechanism Adaptation to Social Communication. Proceedings of the 50th Annual IACIS International Conference. (Monfelt, 2010)

Observations on Practical Information Security Issues and Life Cycle Management in IT Systems. Presented at the Security Conference – Europe 2010 – Discourses in Security, Assurance and Privacy. To be published in the Journal of Information System Security.

The 14 Layered Framework for Including Social and Organisational Aspects in Security Management. Accepted for publication in the Journal of Information Management and Computer Security.

Modelling Static and Dynamic Aspects of Security: A Socio-Technical View on Information Security Metrics. International Symposium on Models and Modeling Methodologies in Science and Engineering (MMMse 2011) in the 2nd International Multi-Conference on Complexity, Informatics, and Cybernetics (IMCIC 2011). (Kowalski & Barabanov, 2011)

Knowledge Management throughout Controlled Information Security. Accepted for publication at IIIS 2011, July 19-22, 2011 Orlando, Florida

Coherent Control of Information Security (COINS). Accepted for publication at Technology Innovation and Industrial management 2011 28-30 June, Oulu, Finland

On the Information Security Posture in an Government Agency - a Longitudinal Study 2008-2011. Submitted to conference.

A Case Study in Security Mental Models at Swedish Government Agency. Submitted to conference

Information Security Metrics: Research Directions. Submitted to conference

Protection of Social Entities' Dependability. Submitted to conference

Condition Audit and Dependability Protection is Communication Security. Submitted to conference

# 4 Discussion

The main objectives of the COINS project has been (1) to use models and modeling techniques to explore and visualize the communication of information security issues in organizations, (2) to investigate how metrics can be beneficially applied as tool for assessing the information security in organizations, and (3) to find a means for inter-organizational comparisons of information security between organizations. In order to achieve the main objectives, the research team has had a comprehensive approach trying to capture the research area from as many perspectives as possible including social as well as technical aspects of information security.

To explore and visualize the communication of information security issues in organizations, five different modeling techniques were designed during the COINS project. The *14-layer Framework* tries to capture all aspects of the communication within an organization. The framework is comprehensive, but abstract and thus not straightforward to grasp. The *3-level organizational model* makes an assumption on enterprises having three main decision levels, the strategic, the tactical, and the operational. These levels are found in most of the work within the project. The *Cube model*, the *Reference model* and the *Entity-Action* model was further used as a basis for design of information security metrics. These modeling techniques and the accompanying metrics support the analysis of organizational communication of information security issues with emphasis on different aspects and, thus, the first objective of the COINS project is also supported by these modeling techniques.

To investigate how metrics can be beneficially applied as tool for assessing the information security in organizations, several information security metrics have been developed. One set of information security metrics are based on textual data describing the information security effort of organizations and supports the corresponding analysis. Furthermore, a study has been performed in order to evaluate a method for the design and use of information security metrics based on the standard ISO/IEC 27004 and the use of participatory design. The second objective of the COINS project is thoroughly addressed by these metrics.

To find a means for comparisons of information security between organizations, a framework for inter-organizational comparison of information security and metrics programs has been developed. The framework is based on the controls specified in the standard ISO/IEC 27001 (ISO/IEC, 2005) and the information security maturity model presented by the National Institute for Standards and Technology (NIST) (Chew et al., 2008). Thus, by supporting the inter-organizational comparisons of information security, the third objective of the COINS project has been achieved.

The results of the COINS project support the understanding of how information security issues are communicated within organizations, the modeling of information security communication, the assessment of information security programs, and inter-organizational comparison of information security. Thus, the information security programs of government agencies, and other organizations, may benefit from the results of the COINS project. However, there is a need for more studies to be performed in order to strengthen the information security abilities of organizations. These studies should address issues, such as, information security assessment, risk analysis, the utility of proposed frameworks and standards, and human as well as organizational learning considering information security.

# 5 References

ACSA (eds.) (2002). *Proc. Workshop on Information Security System Scoring and Ranking*. [Online]. Applied Computer Security Associates. Available from: http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf.

Anderson, R. (2001). Why information security is hard - an economic perspective. In: *Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual*. 2001, pp. 358-365.

Barabanov, Rostyslav (2011). *Information Security Metrics: State of the Art*. Kista, Sweden: Department of Computer and Systems Sciences, DSV, Stockholm University and the Royal Institute of Technology.

Beer, Stafford (1981). *Brain of the Firm*. 2nd Ed. John Wiley & Sons.

Bishop, M. (2003). *Computer Security - Art and Science*. Addison-Wesley.

CC (2006). *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Information. Version 3.1 Revision 1*.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A. & Robinson, W. (2008). *Performance Measurement Guide for Information Security*. [Online]. National Institute of Standards and Technology. Available from: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

COSO (2004). *Enterprise Risk Management — Integrated Framewor. Executive Summary*. [Online]. Committee of Sponsoring Organizations of the Treadway Commission. Available from: http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf. [Accessed 6 October 2008].

Encyclopædia Britannica (2011). Information system. *Encyclopædia Britannica Online*. [Online]. Available from: http://www.britannica.com/EBchecked/topic/287895/information-system.

Falkenberg, E., Hesse, Wolfgang, Lindgreen, Paul, Nilsson, Björn, Oei, Han, Rolland, Colette, Stamper, Roland, Van Assche, Frans, Verrijn-Stuart, Alexander & Voss, Klaus (1998). *A Framework of Information System Concepts: The FRISCO Report*. [Online]. Leiden, The Netherlands: International Federation for Information Processing, IFIP. Available from: http://www.mathematik.uni-marburg.de/~hesse/papers/fri-full.pdf. [Accessed 26 September 2008].

Geer, D., Hoo, K. S. & Jaquith, A. (2003). *Information Security: Why the Future Belongs to the Quants*.

Gollmann, Dieter (2006). *Computer security*. 2nd Ed. Chichester: Wiley.

Granlund, Helena, Lundholm, Kristoffer, Hallberg, Jonas & Eriksson, Margaretha (2011). *A Framework for Inter-Organizational Comparisons of Information*

*Security Capabilities*. Linköping, Sweden: Swedish Defence Research Agency, FOI.

Hallberg, J., Hunstad, A., Bond, A., Peterson, M. & Påhlsson, N. (2004). *System IT security assessment*. Swedish Defence Research Agency, FOI.

Hallberg, Jonas, Pilemalm, Sofie, Lundholm, Kristoffer, Yngström, Louise, Monfelt, Yngve & Davidson, Alan (2010). *Controlled information security: How to recognize and improve organizational information security status*. Linköping, Sweden: Swedish Defence Research Agency, FOI.

Hedström, Key (2009). *Myndigheten för samhällsskydd och beredskaps föreskrifter om statliga myndigheters informationssäkerhet (MSBFS 2009:10)*. Myndigheten för samhällsskydd och beredskap (Swedish Civil Contingencies Agency).

ISO/IEC (2009a). *ISO/IEC 27000:2009 – Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

ISO/IEC (2005). *ISO/IEC 27001:2005 - Information technology -- Security techniques -- Information security management systems -- Requirements*.

ISO/IEC (2009b). *ISO/IEC 27004:2009 Information technology — Security techniques ― Information security management — Measurement*.

ISO/IEC (1994). *ISO/IEC 7498-1 -- Information technology -- Open Systems Interconnection -- Basic Reference Model: The basic model*. [Online]. Available from: http://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip. [Accessed 10 March 2011].

ISO/IEC/JTC 1/SC 7 (2007). *ISO/IEC 15288:2002, Systems engineering - System life cycle processes*. Multiple. Distributed through American National Standards Institute (ANSI).

IT Governance Institute (n.d.). *COBIT 4.1*. [Online]. Available from: www.itgi.org. [Accessed 27 September 2008].

ITU (1994). *ITU-T Recommendation E.800: Terms and definitions related to quality of service and network performance including dependability*. [Online]. Available from: http://www.itu.int/rec/T-REC-E.800-199408-S/en. [Accessed 1 October 2008].

Kowalski, Stewart (1994). *IT insecurity : a multi-disciplinary inquiry*. [Online]. Doctoral Thesis SU/KTH Department of Computer and Systems Sciences. Report Series No. 94-004. ISSN 1101-8526. ISRN SU-KTH/DSV/R–94/4–SE. Available from: http://www.kb.se/soka/kataloger/regina/?func=find-b&find_code=WRD&request=IT%2BInsecurity&x=0&y=0. [Accessed 28 September 2009].

Kowalski, Stewart & Barabanov, Rostyslav (2011). Modelling Static and Dynamic Aspects of Security: A Socio-Technical View on Information Security Metrics. In: *Proceedings of International Symposium on Models and Modeling Methodologies in Science and Engineering (MMMse 2011) in the 2nd International Multi-Conference on Complexity, Informatics, and Cybernetics (IMCIC 2011)*. 27 March 2011, Orlando, USA.

Kowalski, Stewart, Barabanov, Rostyslav & Yngström, Louise (2011). *Summary Report COINS project Open Seminar on Metrics*. Kista, Sweden: Department of Computer and Systems Sciences, DSV, Stockholm University and the Royal Institute of Technology.

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

Lundholm, Kristoffer & Hallberg, Jonas (2009). *Information security metrics based on organizational models*. Linköping, Sweden: Swedish Defence Research Agency, FOI.

Lundholm, Kristoffer & Hallberg, Jonas (2011). *Relevant information security characteristics: Based on needs for information security assessment*. Linköping, Sweden: Swedish Defence Research Agency, FOI.

Lundholm, Kristoffer, Hallberg, Jonas & Granlund, Helena (2011). *Design and Use of Information Security Metrics: Application of the ISO/IEC 27004 standard*. Linköping, Sweden: Swedish Defence Research Agency, FOI.

Monfelt, Yngve (2010). Information mechanism adaptation to social communication. In: *Issues in Information Systems, Volume XI, No. 2*. [Online]. 6 October 2010, Las Vegas, Nevada, pp. 138-144. Available from: http://iacis.org/iis/2010_iis/Table%20of%20Contents%20No2_files/138-144_LV2010_1492.pdf. [Accessed 27 March 2011].

Monfelt, Yngve, Pilemalm, Sofie, Hallberg, Jonas & Yngström, Louise (2010). The 14 layered framework for including social and organisational aspects in security management. In: *Proceedings of the South African Information Security Multi-Conference (SAISMC 2010)*. 17 May 2010, Port Elizabeth, South Africa.

Oxford University Press (2004). *Concise Oxford English Dictionary*. 11th Ed. Oxford University Press.

Pilemalm, Sofie, Lundholm, Kristoffer, Hallberg, Jonas & Yngström, Louise (2010). Information Security as a Pre-requisite for E-government Services – developing the organizations and the information systems. In: *Proceedings of the 6th International Conference on e-Government*. 30 September 2010, Cape Town, South Africa, pp. 82-90.

Quinn, S., Waltermire, D., Johnson, C., Scarfone, K. & Baghart, J. (2009). *The technical specification for the security content automation protocol, Version 1.0*.

[Online]. Gaithersburg, MD: National Institute of Standards and Technology. Available from: http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf.

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

Schneier, Bruce (2008). *The Psychology of Security, Crypto-Gram Newsletter*. [Online]. 2008. Available from: http://www.schneier.com/essay-155.html. [Accessed 30 March 2011].

SIS (2003). *Information security management systems: specification with guidance for use. SS 627799-2, 2nd ed*.

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

Swedish Emergency Management Agency, Sema (2006). *Basic level for information security (BITS) SEMA recommends 2006:1*.

The Federal Facilities Council (2001). *Sustainable Federal Facilities:A Guide to Integrating Value Engineering, Life-Cycle Costing, and Sustainable Development*. Washington, D.C. The National Academies Press.

Travers, Max (2001). *Qualitative Research through Case Studies*. 1st Ed. Sage Publications Ltd.

Yin, R (1994). *Case study research: Design and methods*. 2nd Ed. Beverly Hills, CA: Sage Publishing.

Yngström, Louise (1996). *A systemic-holistic approach to academic programmes in IT security*. Report series - Department of Computer & Systems Sciences, 1101-8526 ; 96:21. Stockholm: Univ.

Yngström, Louise, Hallberg, Jonas, Monfelt, Yngve, Eriksson, Margaretha, Pilemalm, Sofie, Davidson, Alan & Moradian, Esmiralda (2009a). *COINS Report #1: Modelling the Communication of Information Security Issues*. Kista, Sweden: Department of Computer and Systems Sciences, DSV, Stockholm University and the Royal Institute of Technology.

Yngström, Louise, Hallberg, Jonas, Monfelt, Yngve, Eriksson, Margaretha, Pilemalm, Sofie, Davidson, Alan & Moradian, Esmiralda (2009b). *Enclosure to COINS Report #1: Modelling the Communication of Information Security Issues*. Kista, Sweden: Department of Computer and Systems Sciences, DSV, Stockholm University and the Royal Institute of Technology.

Yngström, Louise, Kowalski, Stewart & Barabanov, Rostyslav (2011). *Information Security Assessment. A Roadmap for Research*. Kista, Sweden: Department of Computer and Systems Sciences, DSV, Stockholm University and the Royal Institute of Technology.

Yngström, Louise & Mähring, Magnus (2008). *Datafel om våra pengar blir aldrig upptäcktaa. Debattartikel i Dagens Nyheter*. 22 December.