Relevant information security characteristics

Based on needs for information security assessment

KRISTOFFER LUNDHOLM, JONAS HALLBERG

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--3188--SE
ISSN 1650-1942

Base data report
March 2011

Information Systems

Kristoffer Lundholm, Jonas Hallberg

Relevant information security characteristics

Based on needs for information security assessment

Titel	Relevanta informationssäkerhetsegenskaper: baserade på behov avseende värdering av informationssäkerhet
Title	Relevant information security characteristics: Based on needs for information security assessment
Rapportnr/Report no	FOI-R--3188--SE
Rapporttyp Report Type	Base data report
Månad/Month	Månad/Month
Utgivningsår/Year	2011
Antal sidor/Pages	34 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

Det finns ett allmänt behov av att kunna värdera informationssäkerhet. Att ta fram mer specifika behov kräver dock noggrann analys. Dessutom behöver så kallade metrikprogram vilka motsvarar de identifierade behoven tas fram. En viktig del av detta är att avgöra vad som i sammanhanget avses med informationssäkerhet. Att bestämma vilka säkerhetsrelevanta egenskaperna som behöver värderas är ett sätt att åstadkomma detta.

I denna rapport presenteras en struktur med behov avseende värdering av informationssäkerhet. Strukturen bygger på en analys av utsagor som erhållits via intervjuer och dokumentanalys vid en myndighet. Utgående ifrån behovsstrukturen formas även en struktur av relevanta informationssäkerhetsegenskaper. Dessa egenskaper kan nyttjas som en grund för uppbyggnaden av ett metrikprogram.

Nyckelord: Informationssäkerhet, behov, värdering, metrik

Summary

There is a need to be able to comprehend the status of the information security. To transform this general need into more specific needs require careful analysis. Moreover, when needs have been detected security metrics schemes have to be designed to satisfy these needs. A central issue is to define what information security include. To decide the information security characteristics corresponding to the identified security assessment needs is a possible approach to define information security in the current context.

In this report, a structure of information security assessment needs is presented. The structure is built through an analysis of statements extracted from interviews with personnel and documentation from an agency. Based on the structure of needs, a structure of relevant information security characteristics is formed. These information security characteristics can be used as a basis for the design of an information security metrics scheme.

Keywords: Information security, need, assessment, metric

Innehållsförteckning

1 Introduction

Information security is an important quality of all organizations. Depending on the tasks and focus of different organizations, the needs relating to information security varies, but they always exist in some form. In the context of Swedish government agencies, a lack of control over the information security of the agencies has been detected (RiR, Swedish National Audit Office, 2007).

1.1 Motivation

Besides the need of organizations to reach adequate levels of information security, expressed as combinations of organizational/administrative and technical security, the capability to demonstrate and communicate the adequacy of their information security is vital. Thus, it is essential to be able to understand how information security issues are effectively and efficiently communicated. Since information security is an abstract property, there may be substantial differences between the perceived and actual information security of organizations (Oscarson, 2007). The limited resources highlight the need to ensure efficient use of resources for achieving information security.

Thus, there are needs to achieve, communicate, understand, and manage information security. All these needs are supported by the ability to capture the information security levels of organizations. There is a strong relation between information security levels and the communication of information security. On one hand, the specification of information security levels provides essential information about the issue to be communicated. On the other hand, the actual communication processes are vital properties of organizations to be studied when establishing information security levels.

1.2 Problem formulation

The purpose of security assessment is to provide knowledge that is essential for other processes, such as information security management. Thus, the needs for knowledge motivating the actual security assessments have to be established. Thereafter, a security assessment process satisfying these needs has to be developed.

The work described in this report is part of the research project COINS (COntrolled INformation Security) and focusing on the information security qualities of government agencies. The main research question of the COINS project is what effects security assessments have on the communication of information security issues in the assessed organizations. Thus, the main issue addressed in this report is the identification of needs for security metrics schemes

and associated relevant information security characteristics. In order to enable the design of security metrics schemes addressing these high-level needs, the following issues are addressed.

- What are the needs for security assessment at the studied agency?
- What are the relevant information security characteristics to be studied in order to satisfy the identified needs?

1.3 Method

The detection of relevant information security characteristics is supported by the following activities, which correspond to the initial two activities of the process model for security assessment (Section 2.3). The needs analysis (activity 1 to 3 below) is based on the corresponding part of the *Quality-driven process for requirements elicitation* (Hallberg et al., 2005).

1. Statements relating to information security assessment are extracted from the available data. In this study, the formulation of the statements presented in the documentation of the analyses on information security communication and the design of metrics based on information security communication (Yngström et al., 2009) is used.
2. The identified relevant statements are transformed into a set of needs. Since some statements can be directly transformed into relevant information security characteristics a set of such statements is created.
3. A hierarchical structure of needs is built from the set of identified needs.
4. The identified security assessment needs are used to define a set of relevant information security characteristics. This set is augmented by the relevant information security characteristics extracted during the second activity.
5. A hierarchical structure is built from the set of relevant information security characteristics.

1.4 Contributions

The main contributions described in this report are:

- A structure of security assessment needs identified from documents and interviews related to the studied agency. The security assessment needs are categorized in order to form a tree-like structure with a single top-level need, 6 intermediate nodes, and 29 leaves.
- Based on the structured set of security assessment needs, a set of relevant information security characteristics is identified. Providing quantitative

values for these high-level characteristics will provide answers corresponding to the identified security assessment needs.

1.5 Layout

In Chapter 2, relevant background for the work described in this report is presented. In Chapter 3, the result of the needs analysis is presented. In Chapter 4, the structure of relevant information security characteristics is included. In Chapter 5, finally, the results and their future use are discussed.

2 Background

In this chapter, relevant background is presented. The following sections include the general ideas behind this work, security assessment terminology, and description of a model for security assessment processes.

2.1 Controlled information security

The project COINS (COntrolled INformation Security) aims at providing support for the vital tasks of understanding, learning, and managing information security. With the overall goals to
1) reach adequate levels of information security and
2) demonstrate and communicate the adequacy of the information security, it is essential to understand how information security issues are communicated and, thus, controlled.

Figure 1 illustrates the relations between several central concepts within information security. The actual information security results in knowledge about and perception of information security. Knowledge and assumptions affect the perception and, thereby, the action of relevant actors, such as the staff of an organization, and their trust in information security. Closing the loop the behavior of actors affects the information security. Moreover, the achieved trust affects the assumptions regarding information security.

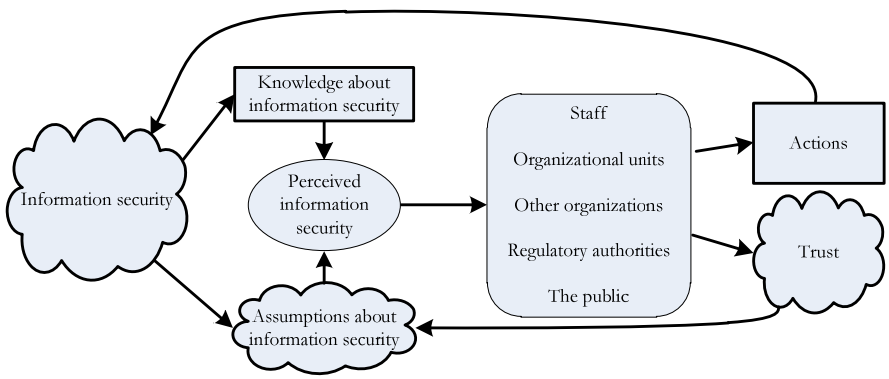

Figure 1: Relations between the concepts of information security, knowledge and perception of information security, actors, and their actions affecting and trust in information security.

The ability to assess information security, which is the topic of this report, influences the knowledge about as well as the perception of information security. Together with other topics studied within the framework of the COINS project,

such as the communication of information security issues, information security assessment will increase the possibilities to reach adequate levels of information security and to communicate the security posture to relevant actors.

2.2 Security assessment terminology

This section introduces central parts of the terminology used in this report. The words marked in italic in the text are explained in another sub-section of this section.

2.2.1 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 security 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 computer-based information systems (IT systems), such as transmission by speech or paper documents.

2.2.2 Information 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.

2.2.3 Need

Needs describe activities or resources that are required to be able to perform tasks or reach goals. Needs can be conscious or unconscious, real or imagined, and satisfied or unsatisfied. Outspoken needs are often related to implicit requirement for action or change.

2.2.4 Information security metric

Information security metrics (usually referred to as security metrics) are defined by the three properties magnitude, scale and interpretation. The *security values* of

systems are measured according to a specified magnitude and related to a scale (Hallberg et al., 2007a). The interpretation transforms acquired data into information for the users of the security assessment. In other words, “a measure is an operation for assigning a number to something. A metric is our interpretation of the assigned number” . Moreover, there is a distinction between metrics where the security values are obtained through measurement of the system to be assessed and metrics where the security values are computed from other security values. These types of metrics are referred to as measurement and computed metrics respectively.

2.2.5 Information security value

The values used to specify the security posture of information systems are called information security values (or just security values). The meaning of security values is prescribed by the corresponding *security metric*.

2.3 Security assessment process model

Security is assessed when, for example, a password is selected and, explicitly or implicitly, judged to provide adequate security; or to support the procurement and commissioning of IT systems or components, such as administrative support systems and firewalls. All security assessments are based on six sub-tasks, although in most ad hoc style assessments, these sub-tasks are not necessarily explicitly performed (Hallberg et al., 2007b). To address the problem of most security assessment processes being performed without much regard to which steps are necessary or which steps are actually performed Hallberg et al presented a model for security assessment processes. The process model includes the six activities illustrated in Figure 2.

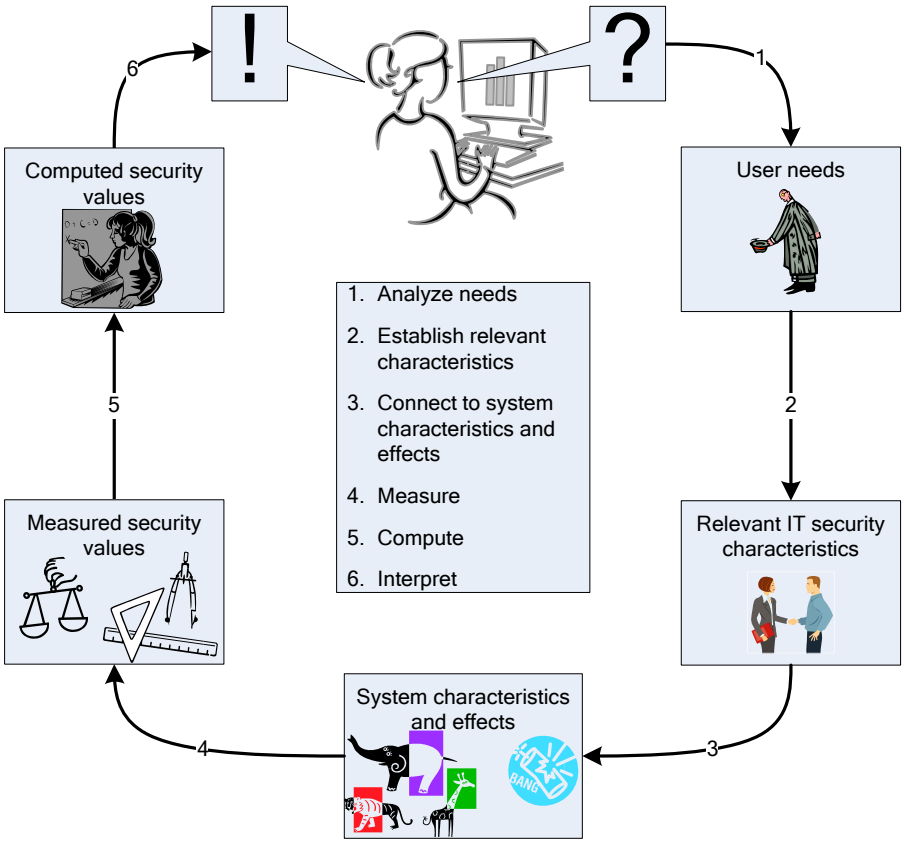

Figure 2: The process model for security assessment.

The first activity in the security assessment process consist of needs analyses. Security assessment cannot be justified purely on its on merits. Contrary, all security assessment has to be motivated by identified users. For successful security assessments, the needs of the identified users have to be identified, documented, and agreed on.

The second activity concerns the establishment of relevant security characteristics. To support the user, it is essential to define the characteristics of the systems and organizations, whose assessment will fulfill the needs of the user. Thus, when the assessments have been performed there should be a set of security values corresponding to the relevant security characteristics. This activity is essential in order to remove the problems associated with the lack of common and, considering security assessment, useful definitions of information security.

The third activity involves the connection of measurable security characteristics to the relevant security characteristics. Unfortunately, relevant security characteristics may not be directly measurable. In those cases, the other system characteristics have to be measured and the resulting values aggregated into a security value for the relevant security characteristics. This corresponds to the difference between measurement and computed security metrics (section 2.2.4).

The fourth activity deals with the measurement of the specified measurable security characteristics. During this activity the actual data collection is performed.

The fifth activity is the computation of security values. The security values that are not directly measurable have to be computed based on the data collected during the previous activity.

Finally, the sixth activity concerns the interpretation of the produced security values. The interpretation mainly concerns the security values corresponding to the relevant security characteristics, although other security values may be considered in order to support the understanding of the security posture.

3 Result of needs analysis

In this chapter, an analysis of the data retrieved from the studied organization is presented. The analysis is based on the data retrieved from the studied authority, through interviews with personnel involved in the information security work and agency documentation of information security procedures. This data was also used for the analyses of information security communication and the design of metrics based on information security communication (Hallberg et al., 2010). The main purpose of the analysis is to identify the needs of the specific organization considering information security assessment. These needs are in the following chapter used to define a set of relevant information security characteristics, which can serve as a basis for the formulation of information security metrics for the organization.

The needs analysis is performed in three steps. Firstly, the relevant statements contained in the data collected from the agency are identified. Secondly, the identified statements are transformed into a set of needs. Thirdly, the set of needs is transformed into a hierarchical structure with the most general need at the top and the most specific needs at the bottom. The identified statements and the structure of needs are listed in Section 3.1 and 3.2 respectively.

Some of the identified statements can be directly mapped into relevant information security characteristics. Consequently, these characteristics have not resulted in any needs but are directly reused in the following chapter describing the relevant information security characteristics.

3.1 Relevant statements

In this section, a subset of the statements identified during the study on information security communication values and structures is presented (Hallberg et al., 2010). The subset consists of those statements relevant considering security assessment.

3.1.1 Relevant statements extracted from the documents

The following relevant statements were identified from the studied documents.

1. IT system users should obey the rules
2. The chief of authority is responsible for the information security
3. The authority is responsible for the information security policy document
4. The authority directs the development of methods and tools for information security

5. The authority should review the information security work
6. For each IT system the following should be documented: The system and its operation, Performed tests, Use and maintenance, Contingency plans, Permission for the operation, Decision on the extent and use of logs, Decided exceptions, Inspection of system security
7. IT system users should employ responsible use of IT resources for other purposes than demanded by work tasks
8. Before processing in computer systems information should be assigned classification levels
9. The IT department certifies business providing maintenance services for IT equipment
10. The authority stipulates routines for updates of protection against malware
11. Backups of essential information and software should be maintained and verified
12. Backups should be safely stored
13. Log every access to IT systems with data requiring special protection (classified)
14. Log and generate alert on user activities that may be considered an intrusion or violation of access rights
15. Keep logs for IT system for five years, if not otherwise is specified
16. Decide the frequency of log inspection, what should be analyzed, and who is responsible for the inspection of logs.
17. Maintain plan for training in protection of security
18. The authority should assure that backups can be restored
19. The responsible for system security should perform analysis of security requirements demanded by systems considered for procurement, use, development, or alteration; including description of security targets and requirements, proposed log policy, and statement from the security unit and IT department
20. The authority should train employees in information security
21. The authority should perform risk analysis to identify necessary security procedures
22. The authority should ensure the presence of specialist competence responsible for the coordination of the information security work at the authority

23. Areas with IT systems enabling access to sensitive data shall be under constant surveillance or protected by physical access control
24. Data medium with sensitive data shall be under constant surveillance or protected by physical access control
25. IT systems used by several authorities or a large numbers of users shall be adequately located and protected in areas with physical access control
26. The authority should decide on security routines when IT systems enabling access to sensitive data is brought outside areas with physical access control
27. Encryption shall be used when sensitive data is transmitted through radio, tele, or data communication outside the realm of the authority
28. IT equipment should, if possible, use approved functions for malware detection
29. Authorization to IT systems requires suitability from a security perspective, adequate knowledge, and need to use
30. If authorized person does not fulfill requirements on suitability from a security perspective, adequate knowledge, and need to use an IT system, the authorization should be withdrawn
31. Strong authentication is required for IT systems processing sensitive data and with more than five users
32. The authority should perform an annual documented control for the information security at the authority
33. The authority should perform an annual audit of the access rights for the IT systems. The inventory should be kept available
34. The responsible for multi-authority system security should supply foundation for accreditation decisions for the respective authorities
35. The responsible for system security should coordinate the security work realated to the system
36. The responsible for system security should assure compliance with security-related business requirements
37. IT department should monitor and protect the computer network
38. The responsible for system security should grant permission for the operation of information systems
39. Security department and IT department should approve the security of IT systems

40. The responsible for development or procurement of or substantial changes to IT system should assure fulfillment of security requirements
41. The responsible for system security should ensure the enforcement of access control in IT system
42. The responsible for system security should assure information security classification is performed to information to be processed in computer systems
43. Security unit should decide on inquiries into serious incidents, faults, or weaknesses that affect, or may affect, several authorities
44. Employees or contractors with adequate competence should supervise service provider lacking authorization for IT systems or area if sensitive information can be accessed
45. The IT department should decide the required security functions for IT equipment to be connected to the common network
46. The IT department should keep an updated documentation of the common IT infrastructure at the authority
47. Security unit should approve equipment and functions for encryption for use at the authorities
48. The IT department should approve and maintain functions for malware detection for IT equipment connected to the common network
49. The IT department should maintain routines for malware detection for IT equipment not connected to the common network at the authorities
50. IT system users should keep access credentials personal
51. IT system users should report loss of access credentials to the IT department
52. IT system users should change exposed passwords
53. The responsible for system security should ensure that there are tools for the analysis of logs
54. Security unit should approve software for use in IT systems connected to the common network
55. IT system users should report incidents, faults, and flaws that may affect the information security to the IT department
56. The authority should regularly inform employees about information security
57. The authority should inform employees about the information security regulations of the authority

58. The authority should inform contractors about the information security regulations of the authority
59. The IT department should inform about discovered security incidents, faults, and weaknesses to the responsible for system security

3.1.2 Relevant statements extracted from the interviews

The following relevant statements were identified from the performed interviews.

1. No common view on information security at the authority
2. Information security associated with technology at operative level
3. Negative attitude towards information security at upper managerial level
4. The policies and regulations direct the work within the authority for employees
5. Employees should use information responsibly (no regulations exist)
6. The chief of authority has the overall responsibility for the security at the authority
7. The security unit creates efficient management of information security with the support of a command and control system
8. The security unit establishes an efficient risk handling process
9. The security unit performs training of personnel to increase their safety
10. The security unit performs training in information security thinking
11. Operative personnel lacks understanding for information security
12. Intranet-based support for information security work at high-level of abstraction
13. The security unit gives advice on information security issues
14. The administration management grants access rights to IT system users
15. The responsibility for access control for paper-based information resides with each individual
16. The responsibility for classification of paper-based information resides with each individual
17. There is a need to identify and classify critical systems
18. There is a need for improved security training for administrative personnel, especially substitutes
19. There is a need for more meetings with operative personnel

20. Middle level managers need increased knowledge and competence in order to take responsibility for the security related work
21. There is a need to strengthen the routines for authorization
22. There is a need for documentation on who has what access rights
23. There is a need for documentation on who has sufficient security training
24. Existing policies and guidance need to be more widely known
25. There is a perceived problem that personal data in registers are misused out of curiosity or for personal reasons
26. There is a need for more efficient processes for new policies
27. The security unit informs newcomers about basic security issues
28. The security unit defines information security related goals
29. The hierarchical structure is a hindrance to effective direct communication from managerial to operative level (and the other way round)
30. The intranet, internal mails and yearly conferences are used to communicate information security issues to the operative level
31. No formal feedback on information security matters
32. Informal requests to grant access rights
33. The security unit is responsible for scrutinizing new systems and information security issues at the authority
34. 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
35. Implement long-term plan on the PDCA[1]-method providing new tools for controlling and measuring large amounts of information
36. Integrate information security in the processes performed at the authority
37. The security unit provides support and resources, for dealing with information security related maters, to the middle managerial level and to the operative level
38. Increase organizational learning by learning from mistakes
39. There is a need for a common information security terminology
40. There is a need to adopt the terminology of ISO/IEC 27000

[1] Plan–do–check–act

41. Lawyers determine the interpretation of common definitions of concepts contained in the regulations

3.2 Assessment needs

Based on the identified relevant statements, a set of assessment needs are derived. For each need resulting from one or more relevant statements, references to the source relevant statements (D*n* or I*n* for documents and interviews respectively) are provided. The 100 statements resulted in a set of 34 needs.

Thereafter, the needs were organized into a structure where the more specific needs have been placed below more general needs. This resulted in the single top-level need

> *Need to know that the level of information security at the agency is adequate (D2, D32, I6).*

The underlying needs are placed in 6 sub-trees consisting of 6, 5, 1, 14, 8, and 1 needs respectively. Two of the needs at level 2 (N2 and N5) appeared during the process of constructing the hierarchical structure as abstraction of the underlying needs. Thus, the number of identified needs totals 36 and the hierarchical structure contains 1, 6, 21, and 8 needs at level 1, 2, 3, and 4 respectively. The 6 sub-trees are presented below.

N1: How efficient is the management of information security? (I7, I29, I30)

- N1.1: How well implemented is the command and control system for information security (I7, I19, I35)
- N1.2: How efficient is the process for deciding new policies? (D3, I26)
- N1.3: What will the effects on the information security be when a specific information security goal is achieved? (I28)
- N1.4: To what extent is information security addressed in the processes at the authority? (I36)
- N1.5: How well is knowledge from mistakes integrated into existing routines? (I38)

N2: What is the security awareness of the personnel?

- N2.1: Do the employees work in accordance with established policies and routines? (I4)
- N2.2: Do employees use information responsibly even though no regulations exist? (D7, I5, I25)

N2.3: What is the current information security competence of the personnel? (D17, D20, D22, D56, D57, D58, I9, I10, I11, I18, I20, I23, I27)

N2.4: Are the security routines for paper based information followed? (I15, I16)

N3: Is the physical surveillance and access control adequate? (D23, D24, D25, D26, D44)

N4: How effective is the information security work? (D5)

N4.1: How available is the support regarding security issues provided by the security unit? (I13, I37)

N4.2: What is the usability of the information security-related information on the intranet? (I12, I30, I34)

N4.3: How effective are the methods and tools for information security? (D4)

N4.4: How efficient is the risk handling system? (D21, I8)

N4.4.1: What information security routines or functions are required to prevent specific incidents? (I33)

N4.5: How effective is the information security work for IT systems? (D35)

N4.5.1: How effective is the incident handling? (D43, I31)

N4.5.2: Are there routines for when and how encryption should be used? (D27, D47)

N4.5.3: How effective is the management of access rights? (D29, D30, D33, D41, I14, I21, I22, I32)

N4.5.4: Are the responsible for system security made aware of discovered security incidents, faults, and weaknesses? (D59)

N4.5.5: Are the backup routines adequate? (D11, D12, D18)

N4.5.6: Are the routines for log handling adequate? (D13, D14, D15, D16, D53)

N4.5.7: Are the routines for update of protection against malware adequate? (D10, D28, D48, D49)

N5: What is the security level of IT systems and infrastructure?

N5.1: Is the security posture of the IT infrastructure adequate? (D37, D46)

N5.2: What is the security level of new systems? (I33)

N5.3: Is the software affecting the security posture of the IT-infrastructure? (D54)

N5.4: Are the mechanisms for authentication of IT system users adequate? (D31)

N5.5: Are the IT security requirements covering all relevant aspects? (D19, D40, D45)

N5.6: Do businesses providing maintenance services for IT systems fulfill applicable security requirements? (D9)

N5.7: Do IT systems fulfill accreditation requirements? (D34, D36, D38, D39)

N6: There is a need to indentify and classify critical systems (I17)

4 Relevant information security characteristics

This chapter presents the relevant information security characteristics that were extracted from the statements and needs presented in Chapter 3. To a large extent the characteristics are direct transformations of the identified needs. However, some characteristics originate directly from the relevant statements presented in Section 3.1.The characteristics are presented as a structure, which corresponds to the structure of needs presented in Section 3.2. The top-level characteristic is *Adequate information security* (Figure 3), which corresponds directly to the most general need that was identified in Section 3.2.

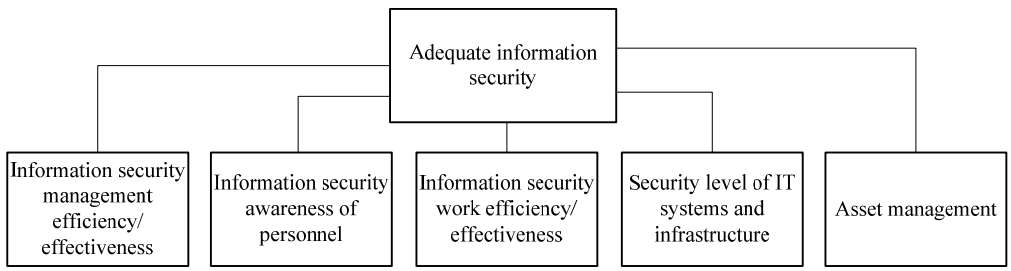

Figure 3: The single top-level and the five level 2 characteristics of the presented structure of relevant information security characteristics.

The structure includes 42 characteristics. 7 of the characteristics originate directly from the relevant statements, while 35 are transformed needs. Below the 5 second-level characteristics there are 23 characteristics at level 3, 9 characteristics at level 4, and 4 characteristics at level 5. For each identified characteristic there will be a short text that will clarify both the scope of that characteristic as well as describing the connection with the characteristic one level up in the hierarchy.

4.1 Information security management efficiency/effectiveness

Efficient processes resulting in the desired effects require efficient and effective management. Therefore efficient and effective information security management is essential for the information security level of organizations.

4.1.1 Policy development efficiency

This characteristic concerns both efficient development of new policies but primarily how quickly existing policies are adjusted and updated to reflect internal or external changes. The information security policy should outline the management's ambition about information security which means that keeping the policy current and up to date constitutes the foundation for efficient management.

4.1.2 Security-relevant mistakes considered when updating routines

This characteristic concerns the agency's ability to utilize experience gained from mistakes when updating information security routines. Adequate level of feedback into the security routines are a basis for efficient information security management as well as an indication of efficient information security management.

4.1.3 Implementation level of the information security management system

This characteristic concerns the agency's development and implementation of an information security management system (ISMS). The purpose of an ISMS is to increase the efficiency of the information security management at the agency.

4.1.4 Security awareness in processes

This characteristic concerns the agency's current consideration of information security in its processes. The inclusion of information security in the processes as a default will increase security thinking in the organization and thus lessen the effort of managers responsible for the information security of these processes.

4.1.5 Impact of security goal fulfillment on information security

This characteristic concerns the agency's ability to evaluate the effects of fulfilling an information security goal as well as planning for what should be done once a goal is fulfilled. Knowing the effects of fulfilling security goals supports manager's prioritization of the security work aiming at fulfilling the goals. Plans for further action when a goal is achieved provide continuity in the information security work.

4.2 Information security awareness of personnel

The behavior of the personnel will dictate the success of the information security effort at the agency. Security enhancing behavior requires security awareness. Achieving security awareness requires education of personnel as well as their understanding of the underlying reasons for security controls, rules and regulations.

4.2.1 Responsible use of access to sensitive resources

This characteristic concerns how responsible the agency personnel are with their access to systems that handle personal data. Responsible means that the employees only use this access for business related purposes and not for personal gain or out of curiosity. Understanding of why this distinction has to be made is connected to the security awareness of the personnel.

4.2.2 Employee compliance with policies and routines

If the information security program is to be successful those affected by it, the employees, should uphold security by complying with existing policies and routines. How well employees know of and are abiding by the security rules will dictate the success or failure of the agency's security program. Since security awareness results in employee understanding the importance of security policies and routines compliance should be an effect of awareness.

4.2.2.1 Compliance with routines for paper based information (I15, I16)

This characteristic concerns, in addition to papers, all those media except computer based ones on which sensitive information is stored. In order for the security work to be effective it needs to be clear how to handle documents containing sensitive information.

4.2.2.2 IT-system users obey the rules (D1)

This characteristic relates to the importance of the compliance to rules specified for the IT systems of the individuals authorized to use the IT systems of the organization. Considering information security, this is a vital aspect of the overall compliance with policies and routines.

4.2.2.2.1 IT-system users keep access credentials personal (D50)

To be able to limit the access to the IT systems it is imperative that users do not share access credentials. This is a central part of the security policy for IT systems.

4.2.2.2.2 IT-system users report loss of access credential to the IT department (D51)

Whenever access credentials have been revealed, this has to be reported to the IT department. This is a central part of the security policy for IT systems.

4.2.2.2.3 IT-system users change exposed passwords (D52)

If passwords may have been revealed they have to be replaced. This is a central part of the security policy for IT systems.

4.2.2.2.4 IT-system users report incidents, faults, and flaws that may affect the information security to the IT department (D55)

The involvement of users in detecting security breaches is essential to the information security level of the organization. This is a central part of the security policy for IT systems.

4.2.3 Information security competence of personnel

The employee's competence regarding information security is fundamental for their security awareness. In order to avoid the mistakes that occur due to employees having to use systems they do not have training for, recording who has what competence will support managers planning of training. The needed competence varies with the work tasks, organizations, and support systems (tools)

4.2.4 Common view on information security at the authority

In order for the agency to achieve the necessary awareness, all parts of the agency needs to have the same view and the same definitions when communicating about information security. A common view on information security includes issues such as security terminology and goals. A common view of what information security means and what needs to be achieved will facilitate the communication and management of information security.

4.3 Information security work efficiency/effectiveness

The limited resources available for information security work necessitate their efficient and effective use in order to achieve adequate information security.

4.3.1 Availability of support provided by the security unit

For those employees that primarily do not work with information security, having someone to ask about what the correct procedure is or what should be considered in the current situation would make their work proceed more smoothly. The security unit of an agency can provide this kind of support and the concern for this characteristic is how available this help is to other employees.

4.3.2 Usability of the intranet in addressing information security issues

The intranet should provide a straight forward and reliable link from the security managers to the employees of the agency. Having answers to frequently asked questions readily available on the intranet will save time for those seeking the information as well as the security unit that would otherwise have been engaged in answering the questions. If these statements are to be true the information on the intranet must be useful to those seeking the information.

4.3.3 Information security tool effectiveness

The effectiveness of information security work can be enhanced by tools, mainly implemented in software. Thus the effectiveness of tools is essential. Such tools could for example support the administration of access rights.

4.3.4 Risk handling system efficiency

To be efficient, the prioritization of information security work tasks should be based on appropriate risk management. Risk management includes threat, vulnerability and risk analysis as well as prioritization of privacy, protection and responsibility measures

4.3.5 IT system security work efficiency/effectiveness

The security of IT systems is an abstract, emerging property of these systems depending on organizational and human factors as well as technical routines. Thus the effectiveness of IT systems security work is differently judged, but still

essential due to the increasing importance of IT systems for the business of most organizations.

4.3.5.1 Incident handling effectiveness

Handling incidents usually involves finding the source of the incident, stopping whatever has happened from continuing, and ensuring that it will not happen again. Since security never will be complete, incidents will occur and have to be handled. The effectiveness considered in this control is that of how fast this can be done and how much effort it is for the agency to handle an issue.

4.3.5.2 Implementation level of encryption routines

This control concerns when and how encryption is used at the agency. Routines for what information should be protected with encryption and how encryption should be applied to this information will facilitate appropriate use of encryption.

4.3.5.3 Access rights management efficiency/effectiveness

This characteristic concerns if the currently implemented access control for IT systems is provided with proper access rights and how much effort the access rights management requires.

4.3.5.4 Security-relevant issues reported to affected system security-responsible

This characteristic concerns how much and how fast information about issues that might affect a system is communicated to the person responsible for that system. This is vital to be able to respond adequately to security incidents as well as pro-actively remove vulnerabilities potentially leading to security incidents.

4.3.5.5 Adequacy of the backup routines

This characteristic concerns to which extent the data that the agency needs to have backups for that is actually covered by the backup routine. Adequate backups are necessary for the recovery from security incidents causing data loss.

4.3.5.6 Adequacy of the log handling routines

This characteristic concerns weather the agency has concluded what should be logged as well as who is responsible for checking the logs for signs of malicious activity or other issues that might be found. In relation to effectiveness this control concerns how many issues that are discovered early due to analyzing logs.

4.3.5.7 Adequacy of the routines for updating the malware protection

Malware protection is mostly about installing security patches for known vulnerabilities and having the anti-virus software up to date. The characteristic concerns the completeness of the routines for updating malware protection i.e. how many of the agency's computers that are covered by the update routines.

4.4 Security level of IT systems and infrastructure

The increasing importance of IT systems and infrastructure for the business of most organizations results in the corresponding security levels of IT systems and infrastructure becoming more central for the level of information security. The security level of information systems depends on several factors including organizational, human, and technological.

4.4.1 Strength of the physical access control

This characteristic concerns how well the physical access control i.e. restriction of access to areas handling or storing sensitive information as well as these areas resilience to natural disasters. This is connected to the security level of the infrastructure by increasing the effort to compromise the infrastructure and by increasing the traceability of found issues.

4.4.2 Software impact on the IT security level

This characteristic concerns how new software or updates to existing software affects the security of the IT systems connected to the common network.

4.4.3 Accreditation level of IT systems

This control concerns how many of the organizations information systems that have a documented accreditation decision. Complete accreditation is connected to the security level of IT systems by ensuring that systems at least fulfill the specified security requirements.

4.4.4 Strength of user authentication in IT systems

This characteristic concerns the completeness of the procedures and policies for user access to information systems as well as the usability and level of implementation for these procedures and policies.

4.4.5 IT system documentation

This characteristic was identified directly from the statements from the documentation and concerns that various aspects have been documented for each IT system.

4.4.6 Completeness of IT security requirements

The agency should have a set of security requirements on its IT systems and IT infrastructure. These characteristics concern if the requirements cover all the areas that are relevant to the agency.

4.4.7 Third party compliance to security requirements

This characteristic concerns the agency's policies and procedures for ensuring that all third parties that are allowed any form of access to the agency's information systems comply with all the requirements. It also concerns the agency's procedures for informing third parties about these requirements.

4.5 Asset management

In order to achieve adequate information security, it is essential to know what needs to be secured. Asset management provides information on what needs to be protected considering information and systems as well as security characterizations, e.g. confidentiality, integrity, and availability.

4.5.1 The agency has identified and classified all critical systems

Each agency needs to know what systems are critical for maintaining the service the agency is providing. These systems should be identified and documented so that there is no doubt about which systems are considered critical. The document should also contain a classification of each system so that the documentation can be used to check what service each critical system provides as well as what kind of information that system handles.

4.5.2 All information has been classified

This characteristic concerns if the agency has classified all the information that is handled. This should be done so that agency personnel know how to handle the information and what systems the information may be used in.

5 Discussion

Since governmental agencies in Sweden are supposed to adhere to the ISO/IEC 27001, there are demands for information security assessment (ISO/IEC, 2005). Ideally, this should be a momentum paving the way for adequate information security metrics schemes and improved control over the information security levels at the agencies. To achieve this it is essential to build the metrics based on the needs of each agency. In this report, an effort to identify such needs has been presented. Moreover, the needs have been mapped into relevant information security characteristics. These characteristics describe the knowledge required to satisfy the information security assessment needs in the organization.

By designing a security metrics schemes providing security values corresponding to these characteristics the agency will acquire relevant knowledge on the status of the information security in the organization. Compliance with ISO/IEC 27001 requires the implementation of the associated standard for security measurement ISO/IEC 27004 (ISO/IEC, 2009). The structure of relevant information security characteristics included in this report can serve as a basis for the selection of controls to be monitored according to ISO/IEC 27004.

The next step towards a security metrics scheme is to acquire feedback on the identified information security characteristics from the agency security personnel. Based on this feedback an adequate set of controls from the ISO/IEC 27001 standard can be selected and the design of the corresponding metrics can begin.

6 References

(n.d.). *Risk Measure and Risk Metric*. [Online]. Available from: http://www.riskglossary.com/link/risk_metric_and_risk_measure.htm. [Accessed 17 March 2009].

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

Hallberg, J., Bengtsson, J. & Andersson, R. (2007a). *Refinement and realization of security assessment methods*. Swedish Defence Research Agency, FOI.

Hallberg, J., Hunstad, A. & Hallberg, N. (2007b). *Handbok för IT-säkerhetsvärdering (in Swedish)*. [Online]. Linköping, Sweden: Swedish Defence Research Agency, FOI. Available from: http://foi.se/upload/10960/FOI_Memo_2099.PDF.

Hallberg, J., Pilemalm, S., Lundholm, K., Yngström, L., Monfelt, Y. & Davidson, A. (2010). *Controlled information security: How to recognize and improve organizational information security status*. Linköping, Sweden: Swedish Defence Research Agency, FOI.

Hallberg, N., Andersson, R. & Westerdahl, L. (2005). *Quality-driven process for requirements elicitation: the case of architecture driving requirements*. Linköping, Sweden: Swedish Defence Research Agency, FOI.

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

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

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*.

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

Yngström, L., Hallberg, J., Monfelt, Y., Eriksson, M., Pilemalm, S., Davidson, A. & Moradian, E. (2009). *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.