The TSAR procedure

Test of Security Assessment Relevance and validity

JOHAN BENGTSSON, JONAS HALLBERG, AMUND HUNSTAD, JACOB LÖFVENBERG

FOI-R--2624--SE
ISSN 1650-1942

Scientific report
December 2008

Information Systems

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

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

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

www.foi.se

Johan Bengtsson, Jonas Hallberg,
Amund Hunstad, Jacob Löfvenberg

The TSAR procedure

Test of Security Assessment Relevance and validity

Titel	TSAR-proceduren – Test av relevans och validitet avseende säkerhetsvärdering
Title	The TSAR procedure – Test of Security Assessment Relevance and validity
Rapportnr/Report no	FOI-R--2624--SE
Rapporttyp Report Type	Vetenskaplig rapport Scientific report
Månad/Month	12
Utgivningsår/Year	2008
Antal sidor/Pages	75 p
ISSN	1650-1942
Kund/Customer	Försvarsmakten / Swedish Armed Forces
Forskningsområde Programme area	7. Ledning med MSI 7. C4I
Delområde Subcategory	71 Ledning 71 Command, Control, Communications, Computers, Intelligence
Projektnr/Project no	E7046
Godkänd av/Approved by	Martin Rantzer

FOI, Totalförsvarets Forskningsinstitut	FOI, Swedish Defence Research Agency
Avdelningen för Informationssystem	Information Systems
Box 1165	Box 1165
581 11 Linköping	SE-581 11 Linköping

Sammanfattning

I dagsläget finns en uppsjö av olika säkerhetsvärderingsmetoder. Säkerhetsvärderingsmetoderna skiljer sig bland annat åt genom att ha olika angreppssätt, investeringskostnader med mera. För att underlätta valet av värderingsmetod behövs ett formaliserat sätt att utvärdera säkerhetsvärderingsmetoder.

I denna rapport presenteras testproceduren TSAR som används för att utvärdera säkerhetsvärderingsmetoder och på så sätt underlätta valet av en säkerhetsvärderingsmetod. TSAR-proceduren beskriver till vilken grad en säkerhetsvärderingsmetod uppfyller de generella kvaliteterna *relevans* och *validitet*. På så sätt fås ett testresultat som visar om en säkerhetsvärderingsmetod tillhandahåller de efterfrågade värderingsresultaten, samtidigt som det visar om säkerhetsvärderingsmetoden är lämplig för den aktuella klassen av informationssystem. För att kunna beräkna en uppfyllandegrad för de identifierade kvaliteterna tillhandahålls även en uppsättning egenskaper för var och en av dem.

Nyckelord: Säkerhetsvärdering, relevans, validitet

Summary

Nowadays there exist a great number of different security assessment methods. Different security assessment methods have, for example, different approaches to how to perform security assessments at the same time as the cost of performing an assessment can vary widely. In order to facilitate the choice of security assessment method, a formalized way of evaluating security assessment methods is needed.

This report presents the testing procedure TSAR, which is used to evaluate security assessment methods and thereby facilitates the process of choosing a method. The TSAR procedure describes to what degree a security assessment method fulfills the general qualities *relevance* and *validity*. Thus, test results indicate whether a security assessment method provides the needed security assessment results as well as if the method is appropriate for the type of information system in question. To be able to calculate the identified qualities' degree of fulfillment, a set of characteristics is also provided for each one of the qualities.

Keywords: Security assessment, relevance, validity

Contents

1 Introduction

The omnipresence of information systems, and our dependency on them, stresses the need to be able to discuss their security. One way of doing this is to define a numerical metric reflecting the security of the system under consideration. A variety of security assessment methods and tools strive to produce such security values for information systems.

1.1 Motivation

Considering the large number of methods specified for – as well as the abundance of not specified, but still used, ad hoc approaches to – security assessment, the complexity of information systems and the wide range of different reasons for security assessments, users are facing difficult decisions regarding the selection of, and investment in, security assessment methods. Thus, to facilitate the choice of assessment methods a formalized way of evaluating security assessment methods, that is, a testing procedure, would be of considerable value. The purpose of the testing procedure is to describe to what degree security assessment methods fulfill important general qualities, and thereby facilitate in choosing between different assessment methods.

1.2 Problem formulation

To be able to characterize the key qualities of security assessment methods, test procedures have to be defined. This involves finding solutions to several questions, among which are the following.

- What are the key qualities of security assessment methods to characterize?
- How can the identified key qualities be quantified?
- What characteristics of the security assessment methods can be used to decide the values of the identified key qualities?
- How can, with reasonable effort, the testing of security assessment methods be performed?

1.3 Contributions

The results presented in this report contribute to the area of security assessment by providing:

- The Test of Security Assessment Relevance and validity (TSAR) procedure that simplifies the analysis and comparison of security assessment methods. The TSAR procedure uses the qualities relevance and validity to characterize security assessment methods, and specifies how to compute relevance and validity values for tested security assessment methods. Thus the first, second, and fourth question of the problem formulation (section 1.2) are addressed.
- The TSAR tables that provide lists of characteristics for the two identified qualities relevance and validity. The TSAR tables, consequently, address the third question specified in the problem formulation (section 1.2).

1.4 Report layout

Chapter 2 presents a background and the terminology used in the report. In Chapter 3, a general description of the testing procedure is presented. Chapter 4 presents the details of the testing procedure. Chapter 5 presents an overview of the TSAR tables. Finally, Chapter 6 presents the observations and conclusions made.

2 Background

In this chapter, terminology for the area of security assessment is presented. The use of the relevance and validity qualities for characterizing security assessment methods is discussed. Finally, the context of security assessment method and testing procedures is illustrated.

2.1 Security assessment terminology

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. (Encyclopedia Britannica, 2008)

IT security assessments
IT security assessments are performed in order to establish how well an IT system meets specific security characteristics. The aim of an IT security assessment is to produce knowledge, which can be used in order to improve the security levels of the assessed system. Performing IT security assessments can give insights into the security posture of systems and provide a basis for confidence in the assessed systems even though it cannot guarantee any level of security (Bishop 2003).

Security assessment
In this report, the term *security assessment* is used in the meaning of IT security assessment.

Security assessment method
Security assessment methods support processes assessing the security of a system.

Security assessment tool
Tools are implementations of methods. Security assessment tools are used to produce the results of the security assessment methods. Tools can be anything from tailor-made software to spreadsheets in Excel.

However, the distinction between methods and tools is not always apparent. Thus, in this report, the term *method* is used in a more wide sense, covering both what formally is methods as well as tools.

System
A system consists of cooperating entities working together with a common purpose.

2.2 Relevance and validity

Information quality can in general, as illustrated by Figure 1, be described as depending on two fundamental qualities (SIS, 2007):

Relevance: Correspondence between the users' information needs and the available data.
Validity: Correspondence between the registered data and the reality.

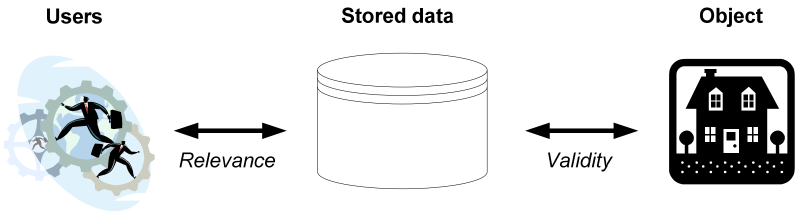

Figure 1: Relevance and validity as measures of information quality (SIS, 2007).

In the specific context of the described testing procedure, two measures of quality, as illustrated in Figure 2, are defined. The selection of these qualities is based on the users' need for increased knowledge of the security qualities of information systems. This stipulates the need for information presenting a valid picture of the assessed systems.

Relevance measures the degree of correspondence between a specific security assessment method and the user's needs of security assessment. It describes to what degree a specific user's security assessment needs are met by the tested security assessment method. The testing procedure models the specific user's needs as weights for a number of relevance characteristics of the specific assessment method. Values from measurements of the specific security assessment method are multiplied with their corresponding weights and the products are added, yielding the relevance value of the security assessment method for this user.

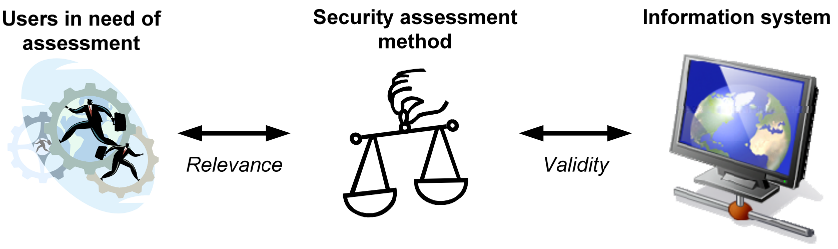

Figure 2: Relevance and validity as measures of information quality related to the testing procedure.

Validity measures the degree of correspondence between the output of a specific security assessment method and the information system to be assessed. It describes to what degree the correct measurements of the information system to be assessed are correctly performed and reported. The testing procedure models the validity requirements as weights for a number of validity characteristics of the specific assessment method. Values from measurements of the specific security assessment method are then multiplied with their corresponding weights and the products are added, yielding the validity value of the security assessment method.

2.3 Context of security assessment methods and testing procedures

Figure 3 illustrates the relations between an information system, a security assessment method and a testing procedure. Two feedback loops are illustrated in order to illuminate how a security assessment method and a testing procedure relate to each other.

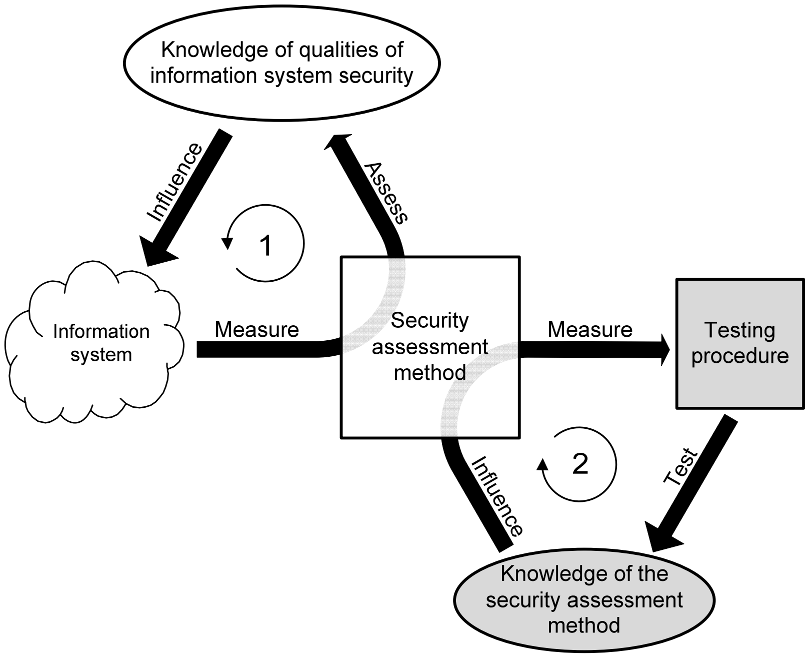
Knowledge of qualities of information system security
Influence
Assess
1
Information system
Measure
Security assessment method
Measure
Testing procedure
2
Influence
Test
Knowledge of the security assessment method

Figure 3: The relation between the testing procedure, security assessment methods, and information systems.

The first loop describes the feedback loop for assessing the security of an information system. The loop starts with a system assessor preparing the input to the assessment method by making measurements on the system. The input is used by the security assessment method in order to perform the assessment. The result of the security assessment is knowledge of qualities of the information system security, which is used by an information system user, administrator, designer etc. in order to influence the system.

The second loop describes the feedback loop for testing a security assessment method. In the first step of the loop, a test supervisor makes measurements on a security assessment method. The measurements are used as input to a testing procedure which is used by the test supervisor to test the security assessment method. The result of the test is knowledge of the security assessment method, which is used by a system assessor, method designer etc. in order to influence the security assessment method.

The testing procedure is used to measure the qualities of methods for security assessment and thus increase the knowledge about the security assessment methods. The output from the testing procedure is measures of relevance and validity for the tested security assessment methods.

3 A general description of the testing procedure

This chapter provides an abstract description of our model for how testing is done. The description is more general than the specific testing procedure introduced in Chapter 4. We believe that this may give an understanding of what the testing procedure really “means”, and the mechanics of how and why it works.

3.1 Modeling the assessment method

Every assessment method has a huge number of properties, or characteristics. Not all of them are relevant to study and not all of them are of value in a given situation. The properties that have the potential to be relevant will be called attributes. With this definition, characteristics that are not attributes are considered irrelevant in the context of testing a specific security assessment method.

Attributes are thus properties that may be relevant to the testing procedure. For every attribute and security assessment method there is, at least in principle, a value describing the magnitude of the attribute for the assessment method to be tested. This means that an assessment method can be described using the values of every attribute. The values are represented by real numbers in the range [0, 1], even in cases when the attribute only allows for a finite number of values. In such cases the discrete attribute values will be encoded as real values in such a way that a higher value corresponds to a better security assessment method. By imposing an order on the attributes (any order will do) we can describe the assessment method as a real vector with elements in [0, 1].

In most cases we will not use all characteristics, but a subset of them. This means that the dimension of the attribute value vector will be less than the number of characteristics, possibly forsaking some information in the process. The attribute values must be measured as correctly as possible, yielding an approximation of the true attribute value vector. In practice, there will be two such attribute value vectors, one for each of the qualities relevance and validity. Together these two approximations constitute the model of the assessment method that will be used in the testing procedure.

In the left part of Figure 4 an overview of this procedure is shown. The object to be modeled contains a number of characteristics, denoted by squares. Some of these are attributes, shown as arrows, symbolizing the measuring, from the characteristics to the attribute value vector. The right part of the figure is related to the next section.

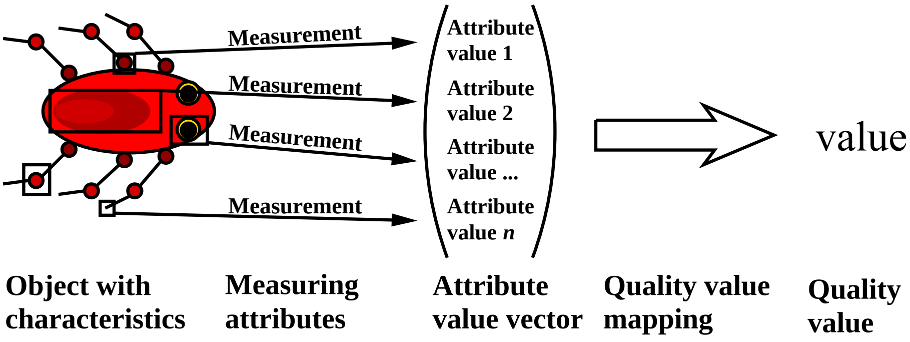

Figure 4: Overview over attribute measuring and quality value mapping.

3.2 Mapping the model to a quality value

The attribute value vector is used as input to a mapping defined by the corresponding requirements, that is, either the user’s needs or statically defined validity requirements. The mapping will take the multi-dimensional vector as input and output a single quality value in the range [0, 1]. Depending on how this mapping is defined it could be a quite complex expression. It is reasonable that it should be continuous in most variables. However, even though we have chosen to represent every variable as a real value in the range [0, 1], some values may be fundamentally discrete in nature, so that only a finite number of values are possible. In these cases, large discrete steps in quality value are possible also from small absolute changes in input variables.

Figure 5 shows a surface plot of a hypothetical mapping to a quality value from a model with two attribute values. The mapping is rather complex, in that it contains several local maxima and the global maximum is not obtained when the attribute values are simultaneously maximized. A more common behavior will be that the quality value will be non-decreasing with increasing variable values.

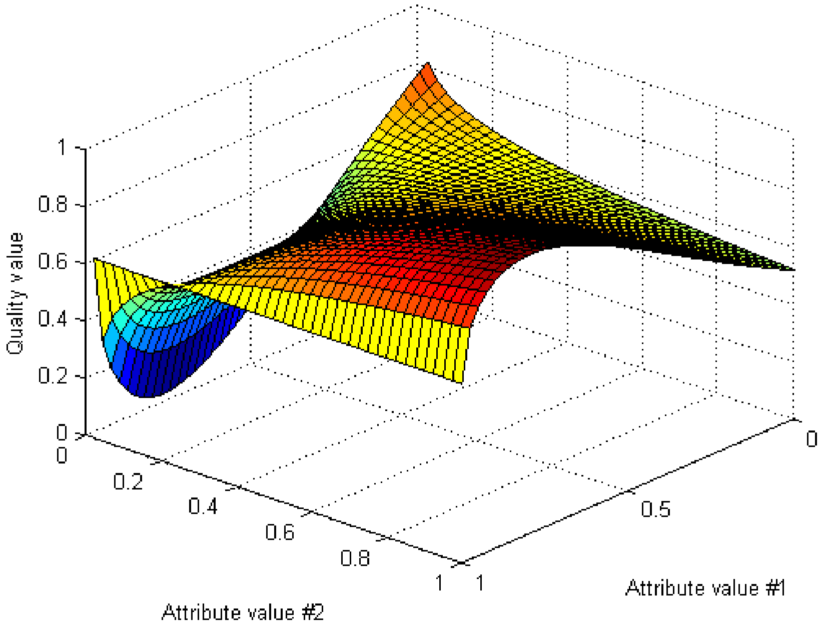

Figure 5: A hypothetical mapping from a model with two attribute values to a quality value.

The right part of Figure 4 shows the mapping procedure. The attribute value vector is used as input to a mapping that yields the quality value. What is not shown in Figure 4 is how the mapping is defined. Whatever requirements there are on the security assessment method, they are modeled by choosing a quality mapping such that desirable properties improve the quality value. This will be explained in the following section.

3.3 Overview of the TSAR procedure

To perform a test using the testing procedure, a security assessment method needs to be decided upon along with a set of user needs. The aim of the testing procedure is to evaluate the security assessment method in terms of relevance and validity, yielding numerical values for these qualities.

In order to evaluate these qualities, the security assessment method needs to be modeled. The modeling is done by measuring a number of attributes of the assessment method, as described in Section 3.1. The attributes are chosen among the characteristics in the TSAR tables, which are further described in Chapter 5 and in Appendix A. The characteristics in the TSAR tables are of two kinds, corresponding to the qualities relevance and validity. The attribute measurements constitute the model of the assessment method and are used for producing a value representing the fulfillment of the qualities, as illustrated in Figure 6.

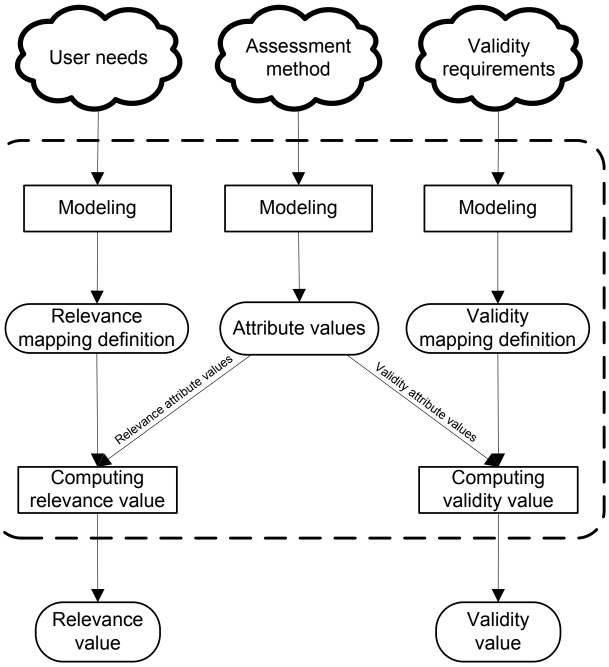

Figure 6: An overview of the testing procedure. Clouds represent input, boxes represent activities and the rounded boxes represent results.

The relevance of an assessment method indicates how well it matches the needs of the user. The needs of the user are modeled by assigning weights to the attributes according to their importance, something which is described in Section 4.1. The validity requirements are modeled in the same way, with the difference being that this weight assigning is done only once, when defining the testing procedure. The weights of the validity attributes are included in Appendix B. Since the user needs can vary from test to test, choosing the relevance attribute weights will have to be done for each separate test.

4 The TSAR procedure

This chapter describes the TSAR procedure by adding details to the general description presented in Chapter 3.

4.1 Quality mapping definitions

The attributes to be examined when testing a security assessment method will in general be of different importance. To capture this difference of importance, the attributes can be weighted based on their relative importance. In the next two subsections, two different mappings are defined. Both will use a simple convex combination of the attribute values, that is, a computation of the inner product of the attribute value vector and a weight vector of non-negative weights that add up to 1. In this way, the mapping becomes non-decreasing in all of its variables and results in a quality value in the range [0, 1]. The difference between the two mappings to be proposed is how the weight vector is chosen. Of course it is possible to use other methods for choosing the weight vector, or for defining a more general quality value mapping.

In the case of computing the relevance quality value, choosing the weights is the way the testing procedure is adapted to different users. This means that the weight vector is the model of the user's unique needs.

4.1.1 Type I – AHP weighting of attributes

The first method for defining the weight vectors is to use the mechanisms for criteria weighting in the Analytical Hierarchy Process[1], AHP (Saaty, 1994). AHP is suggested due to its ability to support decision making in scenarios where decision criteria are related in a complex way. AHP also takes advantage of the human capability to perform pair-wise comparisons of alternatives and state how much more or less important a certain criterion is compared to another criterion.

The characteristics in the TSAR tables are grouped into different categories within each set of characteristics, which results in a structured view of what area each characteristic regards. Out of the two sets of characteristics the applicable characteristics, that is the attributes, are chosen. The relevance-related attribute set will differ between tests, since it should reflect the needs of different users in different situations. Therefore the weighting of the relevance attributes using

[1] A brief summary of AHP and its advantages using selection of a new car as an illustrative example: http://www.boku.ac.at/mi/ahp/ahptutorial.pdf

AHP will have to be performed for each test. The validity attributes and their respective weights are statically defined in the testing procedure. Therefore it is not necessary to re-weight these attributes as long as the TSAR tables have not been altered.

The weighting of the attributes starts with the weighting of the leaves of each category. The weight of each leaf is calculated by performing pair-wise comparisons of all leaves within the same category. When the leaves have been weighted, all the categories are pair-wise compared in order to get the weight of each category. The overall weight of each attribute can then be calculated by multiplying the weight of the attribute with the weight of its categories. The weight of all attributes in a category always sums up to 1. Hence the sum of the overall weights for all attributes also sums up to 1. Thereby the importance of a specific attribute can be compared to the importance of any other attribute, regardless of what category it belongs to.

Example

The following example uses AHP for weighting the attributes. Category A consists of the attributes A1, A2 and A3. Category B consists of the attributes B1, B2 and B3. The attributes in category A are pair-wise compared in order to get their relative importance. Then the same thing is done for category B. All leaves now have a weight which shows the relative importance compared to the other attributes in the same category. In order to be able to compare the weights of attributes from different categories, the categories have to be weighted. Therefore the importance of category A is compared to category B, which results in their relative importance. The results are shown in Table 1. By multiplying the weight of a specific attribute with the weight of its category, the overall weight of that specific attribute is achieved. The overall weight of attribute A1 would be $0.6 \cdot 0.4 = 0.24$, while the overall weight of attribute B1 would be $0.4 \cdot 0.5 = 0.20$. Thereby it is possible to find that attribute A1 is of greater importance than attribute B1.

Table 1: Example of weights. W is the weight and OW is the overall weight.

	W	OW
Category A	**0.6**	
Attribute A1	0.4	0.24
Attribute A2	0.3	0.18
Attribute A3	0.3	0.18
Category B	**0.4**	
Attribute B1	0.5	0.20
Attribute B2	0.2	0.08
Attribute B3	0.3	0.12

4.1.2 Type II – Simple weighting of attributes

The second proposed method for finding the weight vectors can be seen as a simplification of the AHP weighting method. Since there are so many elements in the testing procedure that are approximate, subjective and incomplete, it may be unnecessarily scrupulous to perform the AHP weighting procedure, yielding such extremely exact weights. Instead we propose the following procedure:

Remove from the set of characteristics all those that are not relevant for the user in question. These will not be further considered. The remaining characteristics are referred to as attributes.

Divide the attributes into two groups: less important (type α) and more important (type β). Do this so that the groups contain approximately the same number of attributes. Define the weight vector such that the weights for each attribute of type β has twice the weight of each type α attribute, while adhering to the rule that the sum of the weight vector elements should be one.

Example
The following example uses the simple method for weighting the attributes. Category A consists of the attributes A1, A2, A3 and the characteristic A4. Category B consists of the attributes B1, B2, B3 and B4. Characteristic A4 is not relevant for the user, and will thus be removed (weight set to 0). The rest of the attributes are divided into two groups: less important (type α) and more important (type β). We assume that A1, B1, B2 and B4 are of type β, and the

other of type α. Thus, the two groups contain roughly the same number of attributes. With four attributes of type α and three of type β we have 4·2+3=11 "weight shares", so that type α attributes get weight 2/11 and type β attributes get weight 1/11, see Table 2.

Table 2: Example of weights.

	W
Category A	
Attribute A1	2/11
Attribute A2	1/11
Attribute A3	1/11
Characteristic A4	0
Category B	
Attribute B1	2/11
Attribute B2	1/11
Attribute B3	2/11
Attribute B4	2/11

4.2 Attribute measuring

The individual attribute values must be measured with great care since they form the basis for the testing procedure. We define two different approaches for doing this, one more careful and one simpler. Both approaches result in valid attribute value vectors, which are then used for multiplying (inner product) with the corresponding weight vectors, yielding the quality values.

4.2.1 Type I – measuring using real values

When measuring attribute values using real values, preferably used together with AHP weighting of attributes, attribute values are chosen in the range [0, 1] to reflect the levels of attribute fulfillment, with 1 meaning perfect fulfillment and 0 meaning no fulfillment. Using real values is a way to extract as much information as possible from the personal and subjective knowledge of the person doing the measuring. Attributes that are intrinsically binary will still be taken as either 0 or 1, with no value between being possible.

4.2.2 Type II – binary measuring

The second proposed method for measuring the attribute values can be seen as a simplification of the real values measuring. Since there are so many elements in the testing procedure that are approximate, subjective and incomplete, it may be unnecessarily scrupulous to use real valued measurements. Instead, attribute values are chosen as either 0 or 1, with 1 meaning that the attribute is fulfilled in an acceptable way and 0 that it is not. This is still a subjective measurement, but it may be simpler for the person doing the measurement to choose from this reduced value set.

4.3 Performing tests

The test procedure is divided into six activities, which are further explained in this section.

Two important types of actors involved in a test are the *user* and the *test supervisor*. The user is the one in need of a security assessment method, while the test supervisor is the one in charge of the test. The test supervisor may also involve further expertise to perform the testing.

When performing tests the validity of the specified assessment method will remain the same for all tests regardless of user needs. The relevance on the other hand differs since the needs of the user can change between tests. Not only do the needs change, the individual weighting of the relevance-related attributes will probably change, which affects the resulting relevance value of the tested assessment method.

4.3.1 Activity 1 – Identify user needs

Since the user needs are the ground for being able to identify a relevant security assessment method, the first activity of the TSAR procedure is to *identify user needs*. User needs influence weighting of relevance attributes, but do not affect validity attributes.

This activity is carried out by the users, or by the users in cooperation with the test supervisor, in order to clarify what they need from an assessment. User needs can for example be formulated as a textual description or as a checklist.

User needs may be stated directly by the user in the form of a set of user statements. On the other hand, in a more formalized needs analysis, user statements are used as input to a series of analytical activities to transform statements into user needs, (Hallberg et al, 2005). This involves the test supervisor’s engagement in the analysis.

The result of this activity is a set of user needs.

4.3.2 Activity 2 – Choose relevance attributes

The user needs, identified in the first activity, need to be transformed into attributes. The attributes are selected from the relevance-related characteristics in the TSAR tables. This activity is performed by the test supervisor in cooperation with the user to make sure that the transformation is as accurate as possible and reflects the identified user needs.

The result of this activity is a set of relevance attributes.

4.3.3 Activity 3 – Assign weights to relevance attributes

The user shall, together with the test supervisor, assign weights to the relevance-related attributes from the previous activity. Since all relevance-related attributes are not necessarily of the same importance to the user, all characteristics are assigned weights in order to reflect this difference of importance. During a test, this is only done for the relevance-related characteristics since the weights of the validity characteristics are pre-defined in the testing procedure. Details regarding weight assigning are described in Section 4.1.

The result of this activity is a weight vector for the relevance attributes.

4.3.4 Activity 4 – Measure attributes

The test supervisor models the security assessment method by measuring the relevance attributes, chosen in activity 2, and the validity attributes, thereby populating the relevance and validity attribute value vectors. These vectors constitute the model of the security assessment method in the remaining stages of the test procedure. If the validity attributes of the security assessment method already have been measured in previous tests, it is not necessary to redo the measuring. This activity is performed by the test supervisor.

The result of this activity is one attribute value vector for each of the qualities relevance and validity.

4.3.5 Activity 5 – Compute quality values

The computation of quality values for relevance and validity is based on the corresponding attribute value vectors. The relevance attribute value vector is multiplied (inner product) with the relevance attribute weight vector, yielding the relevance value. The computation of the validity value is done likewise. The computations are performed by the test supervisor.

The result of this activity is a quality value for each of the qualities relevance and validity.

4.3.6 Activity 6 – Interpret and discuss the results

After completing the test, the test supervisor and the user discuss and evaluate the test result. By evaluating the results it is possible to trace back through the test and make sure that the user understands the reasons for the achieved test results. When performing this activity it may also be decided whether further tests should be performed on other assessment methods.

5 The TSAR tables

The testing procedure, described in Chapter 3 and Chapter 4, uses the TSAR tables. The TSAR tables are to a large extent an adaptation of the Crossroads framework for classification and comparison of security assessment methods (Hallberg et al, 2006). The TSAR tables consist of two sets of characteristics related to the two qualities relevance (Figure 7) and validity (Figure 8). Some characteristics are related to both qualities and are therefore present in both sets.

Through the adaption of Crossroads, resulting in the TSAR tables, a number of characteristics from Crossroads have been rewritten and some have been removed. The ones being removed were found not to be fully appropriate for the purpose of testing security assessment methods. The TSAR tables are also based on computational principles inspired by measurement theory (Bengtsson, 2007) and a process description for security assessment (Hallberg et al, 2007) stating the activities necessary for performing security assessments.

The TSAR characteristics are used to characterize security assessment methods in a standardized way, which facilitates their inspection. To facilitate the comparisons of assessment methods, the sets of characteristics should be static. However, the set of relevance characteristics has to be adapted to the needs of the security assessment users. Thus, the comparison of assessment methods is only valid in a specific context.

Characterization of security assessment methods are aided by stating how well TSAR characteristics are met. Each characteristic is possible to state as being met, not met at all or something in between. Deciding whether characteristics are met will most likely be non-obvious and possibly be in need of some negotiation involving expertise on test procedures and security assessment. In Appendix A the characteristics of the TSAR tables are presented in detail.

The relevance characteristics, Figure 7, focus on whether the user’s security assessment needs are met by the tested security assessment method. These characteristics include, for example, what system aspects (technical, organizational etc) are in focus in the security assessment method, with what entities (computer components, computers, humans, processes etc) systems are modeled and with what kind of security values (atomic or aggregated) computations are modeled.

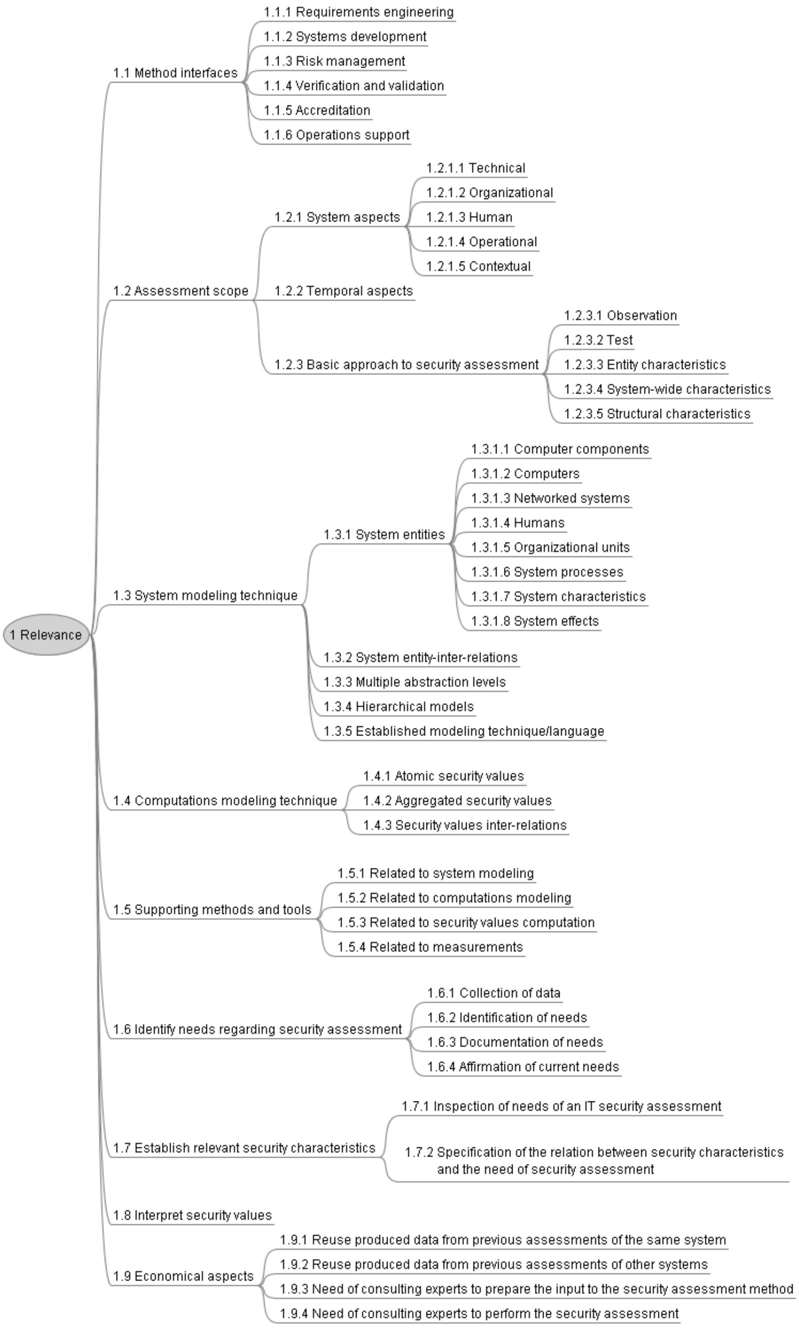
1 Relevance
1.1 Method interfaces
1.1.1 Requirements engineering
1.1.2 Systems development
1.1.3 Risk management
1.1.4 Verification and validation
1.1.5 Accreditation
1.1.6 Operations support
1.2 Assessment scope
1.2.1 System aspects
1.2.1.1 Technical
1.2.1.2 Organizational
1.2.1.3 Human
1.2.1.4 Operational
1.2.1.5 Contextual
1.2.2 Temporal aspects
1.2.3 Basic approach to security assessment
1.2.3.1 Observation
1.2.3.2 Test
1.2.3.3 Entity characteristics
1.2.3.4 System-wide characteristics
1.2.3.5 Structural characteristics
1.3 System modeling technique
1.3.1 System entities
1.3.1.1 Computer components
1.3.1.2 Computers
1.3.1.3 Networked systems
1.3.1.4 Humans
1.3.1.5 Organizational units
1.3.1.6 System processes
1.3.1.7 System characteristics
1.3.1.8 System effects
1.3.2 System entity-inter-relations
1.3.3 Multiple abstraction levels
1.3.4 Hierarchical models
1.3.5 Established modeling technique/language
1.4 Computations modeling technique
1.4.1 Atomic security values
1.4.2 Aggregated security values
1.4.3 Security values inter-relations
1.5 Supporting methods and tools
1.5.1 Related to system modeling
1.5.2 Related to computations modeling
1.5.3 Related to security values computation
1.5.4 Related to measurements
1.6 Identify needs regarding security assessment
1.6.1 Collection of data
1.6.2 Identification of needs
1.6.3 Documentation of needs
1.6.4 Affirmation of current needs
1.7 Establish relevant security characteristics
1.7.1 Inspection of needs of an IT security assessment
1.7.2 Specification of the relation between security characteristics and the need of security assessment
1.8 Interpret security values
1.9 Economical aspects
1.9.1 Reuse produced data from previous assessments of the same system
1.9.2 Reuse produced data from previous assessments of other systems
1.9.3 Need of consulting experts to prepare the input to the security assessment method
1.9.4 Need of consulting experts to perform the security assessment

Figure 7: Relevance characteristics.

Validity characteristics, Figure 8, focus on whether result of the security assessment method reflects reality. These factors include, for example, the capturing of inter-relations of system entities and security values and whether measurements are performed objectively.

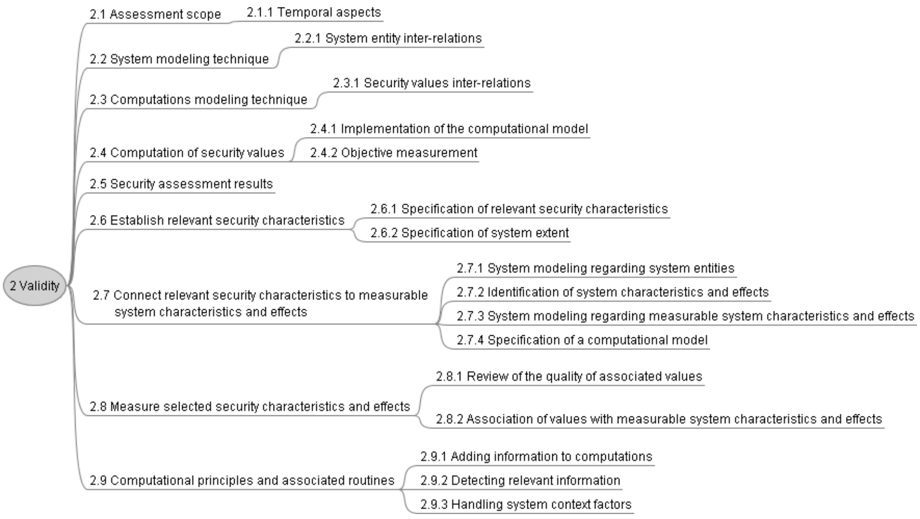
2 Validity
2.1 Assessment scope
2.1.1 Temporal aspects
2.2 System modeling technique
2.2.1 System entity inter-relations
2.3 Computations modeling technique
2.3.1 Security values inter-relations
2.4 Computation of security values
2.4.1 Implementation of the computational model
2.4.2 Objective measurement
2.5 Security assessment results
2.6 Establish relevant security characteristics
2.6.1 Specification of relevant security characteristics
2.6.2 Specification of system extent
2.7 Connect relevant security characteristics to measurable system characteristics and effects
2.7.1 System modeling regarding system entities
2.7.2 Identification of system characteristics and effects
2.7.3 System modeling regarding measurable system characteristics and effects
2.7.4 Specification of a computational model
2.8 Measure selected security characteristics and effects
2.8.1 Review of the quality of associated values
2.8.2 Association of values with measurable system characteristics and effects
2.9 Computational principles and associated routines
2.9.1 Adding information to computations
2.9.2 Detecting relevant information
2.9.3 Handling system context factors

Figure 8: Validity characteristics.

6 Observations and conclusions

The TSAR procedure has been developed in order to provide a fast way to indicate

- if a security assessment method provides the needed assessment results and
- if the method is appropriate for the available type of information system.

We believe that the proposed testing procedure is simple enough to use and that it produces results which can be used to evaluate if the tested security assessment method provides valid results matching the user's needs of security assessment results.

Two different types of quality mappings and attribute measuring, named *Type I* and *Type II*, have been defined in this report. Using the TSAR procedure together with *Type II* provides a more comprehensive test which is believed to be enough in most cases. *Type I* should be used when there is a need for more detailed test. Both the quality mapping and the attribute measuring can be modified to fit the needs of a security assessment method test.

A multitude of qualities have been considered as the result of performing a test using the testing procedure. The quality *reliability* was for a long time during the development process intended as the third quality along with *relevance* and *validity*. The *reliability* of a security assessment method resolved around its capability of providing repeatable results. After some consideration *reliability* was removed since a security assessment method having low *reliability* also would have low *validity*. If the result of a security assessment is not repeatable, it most likely does not reflect the reality. Hence the security assessment method has low *validity*.

The TSAR tables provide characteristics used to characterize the relevance and validity of security assessment methods. Since this is the first version of the TSAR tables, the sets of characteristics should most likely be modified and extended in the future. However, we do feel that it is appropriate to start with a set of characteristics that we consider vital for sound security assessments.

The TSAR procedure, along with the TSAR tables, will be used to test, more or less well-specified, assessment methods in order to detect potential possibilities of improvements. We believe that this can result in future substantial improvement of the methods for security assessment as well as provide novel ideas for assessing security. Furthermore, the use of the TSAR procedure will result in revision and validation of the TSAR tables and also of the procedure itself.

References

Bengtsson, M. (2007). *Mathematical foundation needed for development of IT security metrics,* Master's Thesis, University of Linköping, LiTH-ISY-EX--07/4001--SE

Bishop, M. (2003). *Computer Security – Art and Science*, Addison-Wesley, ISBN 0-201-44099-7

Encyclopedia Britannica. (2008). http://www.britannica.com/EBchecked/topic/287895/information-system

Hallberg, J., Hallberg, N., Hunstad, A. (2005). *Behovsanalys avseende värdering av IT-säkerhet*. Scientific report. FOI-R--1820--SE. FOI, Linköping, Sweden.

Hallberg, J., Hallberg, N., & Hunstad, A. (2006). *Crossroads and XMASS: Framework and Method for System IT Security Assessment*, Scientific report. FOI-R--2154--SE, FOI, Linköping, Sweden.

Hallberg, J., Hunstad, A., & Hallberg, N. (2007). *Handbok för IT-säkerhetsvärdering (in Swedish).* Technical report, FOI, Linköping, Sweden.

Saaty, T. (1994) *Fundamentals of Decision Making and Priority Theory – with the Analytic Hierarchy Process*, Vol. VI. RWS Publications. Pittsburgh, USA.

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

Appendix A Characteristics

The characteristics are presented according to the following table structure:

ID	The ID of the characteristic.
Name	The name of the characteristic.
Type	Type of characteristic. Atomic or compound.
Abstract	A short description stating what measurement of the assessment method the characteristic performs.
Description of results	A description of results produced by the characteristic.
Unit of measure	The unit of measure for the produced result.
Target	A description of desired result. Can be as simple as “low is good”.
Objective	The objective describes a functionality or quality of an information system and measures whether the functionality/quality is considered by the assessment method.
Tags	A reference to the source of this characteristic. Could for example be [Crossroads, 4.2], which would refer to section 4.2 in the Crossroads report.

A.1 Relevance characteristics

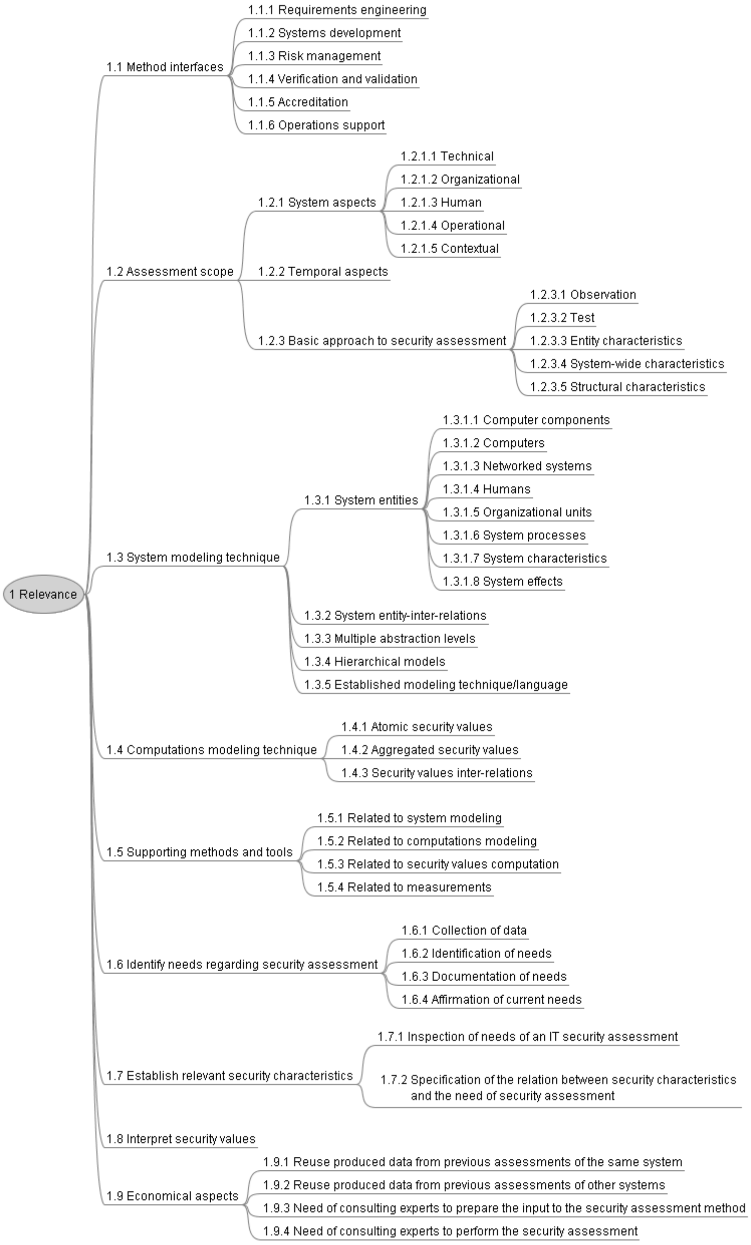
1 Relevance
1.1 Method interfaces
1.1.1 Requirements engineering
1.1.2 Systems development
1.1.3 Risk management
1.1.4 Verification and validation
1.1.5 Accreditation
1.1.6 Operations support
1.2 Assessment scope
1.2.1 System aspects
1.2.1.1 Technical
1.2.1.2 Organizational
1.2.1.3 Human
1.2.1.4 Operational
1.2.1.5 Contextual
1.2.2 Temporal aspects
1.2.3 Basic approach to security assessment
1.2.3.1 Observation
1.2.3.2 Test
1.2.3.3 Entity characteristics
1.2.3.4 System-wide characteristics
1.2.3.5 Structural characteristics
1.3 System modeling technique
1.3.1 System entities
1.3.1.1 Computer components
1.3.1.2 Computers
1.3.1.3 Networked systems
1.3.1.4 Humans
1.3.1.5 Organizational units
1.3.1.6 System processes
1.3.1.7 System characteristics
1.3.1.8 System effects
1.3.2 System entity-inter-relations
1.3.3 Multiple abstraction levels
1.3.4 Hierarchical models
1.3.5 Established modeling technique/language
1.4 Computations modeling technique
1.4.1 Atomic security values
1.4.2 Aggregated security values
1.4.3 Security values inter-relations
1.5 Supporting methods and tools
1.5.1 Related to system modeling
1.5.2 Related to computations modeling
1.5.3 Related to security values computation
1.5.4 Related to measurements
1.6 Identify needs regarding security assessment
1.6.1 Collection of data
1.6.2 Identification of needs
1.6.3 Documentation of needs
1.6.4 Affirmation of current needs
1.7 Establish relevant security characteristics
1.7.1 Inspection of needs of an IT security assessment
1.7.2 Specification of the relation between security characteristics and the need of security assessment
1.8 Interpret security values
1.9 Economical aspects
1.9.1 Reuse produced data from previous assessments of the same system
1.9.2 Reuse produced data from previous assessments of other systems
1.9.3 Need of consulting experts to prepare the input to the security assessment method
1.9.4 Need of consulting experts to perform the security assessment

Figure 9: Relevance characteristics.

ID	1.1
Name	Method interfaces
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the relevance characteristics tree diagram, Figure 9, ID 1.1.1 - 1.1.6.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	Assessment methods can with other processes and give input to a range of different processes and thereby facilitate them.
Tags	[Crossroads, 3.1]

ID	1.1.1
Name	Requirements engineering
Type	Atomic
Abstract	The characteristic specifies whether the tested assessment method provides input to the process of requirements engineering regarding the assessed information systems.
Description of results	Existence of input to the requirements engineering process.
Unit of measure	N/A
Target	True
Objective	Output from the assessment method can be used to facilitate the process of requirements engineering. The objective of this characteristic is to state whether input to the requirements engineering process is provided. Input may concern issues of categorizing, sorting and structuring requirements as well as how to specify relations to stated needs and thereby prioritization of requirements.
Tags	[Crossroads, 3.1]

ID	1.1.2
Name	Systems development
Type	Atomic
Abstract	The characteristic specifies whether the tested assessment method provides sufficient input to the process of systems development regarding the assessed information systems.
Description of results	Existence of input to the systems development process.
Unit of measure	N/A
Target	True
Objective	Output from the assessment method can be used to facilitate the process of systems development. The objective of this characteristic is to state whether input to the systems development process is provided. Input may especially concern issues regarding security architecture of assessed information systems.
Tags	[Crossroads, 3.1]

ID	1.1.3
Name	Risk management
Type	Atomic
Abstract	The characteristic specifies whether the tested assessment method provides sufficient input to the process of risk management regarding the assessed information systems.
Description of results	Existence of input to the risk management process.
Unit of measure	N/A
Target	True
Objective	Output from the assessment method can be used to facilitate the process of risk management. The objective of this characteristic is to state whether input to the risk management process is provided. Input may concern issues of existing risks, threats, associated probabilities of threats being realized and supposed consequences. Input may also facilitate choosing and planning appropriate counter-measures.
Tags	[Crossroads, 3.1]

ID	1.1.4
Name	Verification and validation
Type	Atomic
Abstract	The characteristic specifies whether the tested assessment method provides input to the process of verification and validation regarding the assessed information system.
Description of results	Existence of input to the verification and validation process.
Unit of measure	N/A
Target	True
Objective	Output from the assessment method can be used to facilitate the process of verification and validation. The objective of this characteristic is to state whether input to the verification and validation process is provided. Input may concern issues regarding security measures, their fulfillment of security requirements and their usability.
Tags	[Crossroads, 3.1]

ID	1.1.5
Name	Accreditation
Type	Atomic
Abstract	The characteristic specifies whether the tested assessment method provides sufficient input to the process of accreditation regarding the assessed information systems.
Description of results	Existence of input to the accreditation process.
Unit of measure	N/A
Target	True
Objective	Output from the assessment method can be used to facilitate the process of accreditation. The objective of this characteristic is to state whether input to the accreditation process is provided. Input may concern issues of the development process, intended use, functionality and structure as well as identified risks and requirements of the assessed information system.
Tags	[Crossroads, 3.1]

ID	1.1.6
Name	Operations support
Type	Atomic
Abstract	The characteristic specifies whether the tested assessment method provides sufficient input to the process of operations support regarding the assessed information systems.
Description of results	Existence of input to the operations support process.
Unit of measure	N/A
Target	True
Objective	Output from the assessment method can be used to facilitate the process of operations support. The objective of this characteristic is to state whether input to the operations support process is provided. Input may concern issues regarding configuration, maintenance and incident management.
Tags	[Crossroads, 3.1]

ID	1.2
Name	Assessment scope
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the relevance characteristics tree diagram, Figure 9, ID 1.2.1 - 1.2.3.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	The complex structure of information systems, along with the difficulty for assessment methods to capture all security relevant characteristics, makes it essential to specify the scope of the assessment method. Defining the extent of the system being assessed illuminates both features and limitations of the assessment method.
Tags	[Crossroads, 3.1]

ID	1.2.1
Name	System aspects
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the fourth level of the relevance characteristics tree diagram, Figure 9, ID 1.2.1.1 - 1.2.1.5.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	The scope of the system security assessment can be limited to one or more system aspects. For example, focusing on technical system aspects will result in a radically different assessment than an assessment based on purely organizational aspects.
Tags	[Crossroads, 3.1]

ID	1.2.1.1
Name	Technical
Type	Atomic
Abstract	This characteristic specifies whether support for assessment of technical system aspects exists.
Description of results	Existence of support for assessment of technical system aspects.
Unit of measure	N/A
Target	True
Objective	Assessments of information systems may take into consideration different system aspects. Security relies, among several other aspects, on technical aspects. Technical design, implementation and operation as well as their interaction with factors regarding other system aspects have to be considered during assessment.
Tags	[Crossroads, 3.1]

ID	1.2.1.2
Name	Organizational
Type	Atomic
Abstract	This characteristic specifies whether support for assessment of organizational system aspects exists.
Description of results	Existence of support for assessment of organizational system aspects.
Unit of measure	N/A
Target	True
Objective	Assessments of information systems may take into consideration different system aspects. Security relies, among several other aspects, on organizational aspects. Organizational design, implementation and operation as well as their interaction with factors regarding other system aspects have to be considered during assessment.
Tags	[Crossroads, 3.1]

ID	1.2.1.3
Name	Human
Type	Atomic
Abstract	This characteristic specifies whether support for assessment of human system aspects exists.
Description of results	Existence of support for assessment of human system aspects.
Unit of measure	N/A
Target	True
Objective	Assessments of information systems may take into consideration different system aspects. Security relies, among several other aspects, on human system aspects. Human factors and their effect on system design, implementation and operation as well as their interaction with factors regarding other system aspects have to be considered during assessment.
Tags	[Crossroads, 3.1]

ID	1.2.1.4
Name	Operational
Type	Atomic
Abstract	This characteristic specifies whether support for assessment of operational system aspects exists.
Description of results	Existence of support for assessment of operational system aspects.
Unit of measure	N/A
Target	True
Objective	Assessments of information systems may take into consideration different system aspects. Security relies, among several other aspects, on operational aspects in the sense of work processes involving assessed information systems. Design, implementation and operation of such work processes, as well as their interaction with factors regarding other system aspects have to be considered during assessment.
Tags	[Crossroads, 3.1]

ID	1.2.1.5
Name	Contextual
Type	Atomic
Abstract	This characteristic specifies whether support for assessment of contextual system aspects exists.
Description of results	Existence of support for assessment of contextual system aspects.
Unit of measure	N/A
Target	True
Objective	Assessments of information systems may take into consideration different system aspects. Security relies, among several other aspects, on contextual aspects. Contextual aspects are the settings for the system, such as for example legal aspects, physical environment etc. Contextual factors and their effect on system design, implementation and operation as well as their interaction with factors regarding other system aspects have to be considered during assessment.
Tags	[Crossroads, 3.1]

ID	1.2.2
Name	Temporal aspects
Type	Atomic
Abstract	This characteristic specifies whether time-dependence of security is regarded.
Description of results	Existence of support for assessment of temporal aspects.
Unit of measure	N/A
Target	True
Objective	The dynamic nature of security, and especially the dynamic nature of security threats, necessitates security updates of information systems. Lack of updates will result in a degrading system.
Tags	[Crossroads, 3.1]

ID	1.2.3
Name	Basic approach to security assessment
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the fourth level of the relevance characteristics tree diagram, Figure 9, ID 1.2.3.1 – 1.2.3.5.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	Security assessments can be based on different types of data. It is therefore important to specify what type of data the specific assessment is based upon.
Tags	[Crossroads, 3.1]

ID	1.2.3.1
Name	Observation
Type	Atomic
Abstract	This characteristic specifies whether support exists for handling data based on observations.
Description of results	Existence of support for handling data based on observations.
Unit of measure	N/A
Target	True
Objective	Observations disregard the internal system characteristics and instead view the system from the outside. This gives assessments based on observations of security consequences.
Tags	[Crossroads, 3.1]

ID	1.2.3.2
Name	Test
Type	Atomic
Abstract	This characteristic specifies whether support exists for handling data based on tests.
Description of results	Existence of support for handling data based on tests.
Unit of measure	N/A
Target	True
Objective	Testing of security is based on using vulnerability scanners or red teams. The number of detected vulnerabilities, or effort required by red teams measured as adversary work factor, form the basis for security metrics in security assessments based on tests.
Tags	[Crossroads, 3.1]

ID	1.2.3.3
Name	Entity characteristics
Type	Atomic
Abstract	This characteristic specifies whether support exists for handling data based on entity characteristics.
Description of results	Existence of support for handling data based on entity characteristics.
Unit of measure	N/A
Target	True
Objective	Security assessments can be based on characteristics of entities of the information system. Entities are subjects, objects or subsystems that perform tasks in a system and the tasks themselves. These can be described by performance characteristics, interfaces etc. At the level of describing systems as consisting of entities and their performance, descriptions of entity characteristics are needed
Tags	[Crossroads, 3.1]

ID	1.2.3.4
Name	System-wide characteristics
Type	Atomic
Abstract	This characteristic specifies whether support exists for handling data based on system-wide characteristics.
Description of results	Existence of support for handling data based on system-wide characteristics.
Unit of measure	N/A
Target	True
Objective	System-wide characteristics can be used in security assessments. Examples of system-wide characteristics: system ability to withstand attacks, update policies and their implications etc. At the level of describing systems as a whole, system-wide characteristics are needed
Tags	[Crossroads, 3.1]

ID	1.2.3.5
Name	Structural characteristics
Type	Atomic
Abstract	This characteristic specifies whether support exists for handling data based on structural characteristics.
Description of results	Existence of support for handling data based on structural characteristics.
Unit of measure	N/A
Target	True
Objective	Structural characteristics can be used in security assessments. Examples of structural characteristics are: hierarchical relations between entities and their effects on performance At the level of describing systems as structures and resulting performance, descriptions of structural characteristics are needed
Tags	[Crossroads, 3.1]

ID	1.3
Name	System modeling technique
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics fulfilled at the third level of the relevance characteristics tree diagram, Figure 9, ID 1.3.1 – 1.3.4.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	Security assessment is dependent on information regarding how systems are modeled. Several kinds of system modeling techniques are possible to use and they are often complementary.
Tags	[Crossroads, 3.2]

ID	1.3.1
Name	System entities
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the fourth level of the relevance characteristics tree diagram, Figure 9, ID 1.3.1.1 – 1.3.1.8.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	Security assessment is dependent on information regarding which kinds of entities, constituents as well as processes, are used to model a system.
Tags	[Crossroads, 3.2]

ID	1.3.1.1
Name	Computer components
Type	Atomic
Abstract	This characteristic specifies whether support exists for modeling computer components.
Description of results	Existence of support for modeling computer components.
Unit of measure	N/A
Target	True
Objective	In cases where results of security assessments are influenced by the choice, design, implementation or operation of computer components, it is vital that the assessment method supports modeling of computer components. Computer components may be both hardware and software components.
Tags	[Crossroads, 3.2]

ID	1.3.1.2
Name	Computers
Type	Atomic
Abstract	This characteristic specifies whether support exists for modeling computers.
Description of results	Existence of support for modeling computers.
Unit of measure	N/A
Target	True
Objective	In cases where results of security assessments are influenced by the choice, design, implementation or operation of computers, it is vital that the assessment method supports modeling of computers.
Tags	[Crossroads, 3.2]

ID	1.3.1.3
Name	Networked systems
Type	Atomic
Abstract	This characteristic specifies whether support exists for modeling networked systems.
Description of results	Existence of support for modeling networked systems.
Unit of measure	N/A
Target	True
Objective	In cases where results of security assessments are influenced by the choice, design, implementation or operation of networked systems, it is vital that the assessment method supports modeling of networked systems
Tags	[Crossroads, 3.2]

ID	1.3.1.4
Name	Humans
Type	Atomic
Abstract	This characteristic specifies whether support exists for modeling human interaction with the system.
Description of results	Existence of support for modeling human interaction with the system.
Unit of measure	N/A
Target	True
Objective	In cases where results of security assessments are influenced by the interaction with humans, it is vital that the assessment method supports modeling of human interaction with the system.
Tags	[Crossroads, 3.2]

ID	1.3.1.5
Name	Organizational units
Type	Atomic
Abstract	This characteristic specifies whether support exists for modeling organizational units.
Description of results	Existence of support for modeling organizational units.
Unit of measure	N/A
Target	True
Objective	In cases where results of security assessments are influenced by the choice, design, implementation or operation of organizational units and interaction with these, it is vital that the assessment method supports modeling of organizational units.
Tags	[Crossroads, 3.2]

ID	1.3.1.6
Name	System processes
Type	Atomic
Abstract	This characteristic specifies whether support exists for modeling system processes.
Description of results	Existence of support for modeling system processes.
Unit of measure	N/A
Target	True
Objective	In cases where results of security assessments are influenced by the choice, design, implementation or operation of system processes and interaction with these, it is vital that the assessment method supports modeling of system processes.
Tags	[Crossroads, 3.2]

ID	1.3.1.7
Name	System characteristics
Type	Atomic
Abstract	This characteristic specifies whether support exists for modeling system characteristics.
Description of results	Existence of support for modeling system characteristics.
Unit of measure	N/A
Target	True
Objective	In cases where results of security assessments are influenced by which system characteristics are used to describe the system, it is vital that the assessment method supports modeling of system characteristics.
Tags	[Crossroads, 3.2]

ID	1.3.1.8
Name	System effects
Type	Atomic
Abstract	This characteristic specifies whether support exists for modeling system effects.
Description of results	Existence of support for modeling system effects.
Unit of measure	N/A
Target	True
Objective	In cases where results of security assessments are influenced by which system effects are used to describe the system performance, it is vital that the assessment method supports modeling of system effects. System effects are achieved in the interaction between the system and its environment. In a security assessment focus is on the security aspects of system effects.
Tags	[Crossroads, 3.2]

ID	1.3.2
Name	System entity inter-relations
Type	Atomic
Abstract	This characteristic specifies whether system entity inter-relations are regarded.
Description of results	Existence of support for system entity inter-relations.
Unit of measure	N/A
Target	True
Objective	In cases where results of security assessments are influenced by the choice, design, implementation or operation of system entity inter-relations, it is vital that the assessment method supports modeling of system entity inter-relations. The system entity inter-relations describe how the entities of a system affect each other.
Tags	[Crossroads, 3.2]

ID	1.3.3
Name	Multiple abstraction levels
Type	Atomic
Abstract	This characteristic specifies whether support exists for multiple abstraction levels.
Description of results	Existence of support for multiple abstraction levels.
Unit of measure	N/A
Target	True
Objective	Support for multiple abstraction levels makes it possible to model systems consisting of different types of system entities.
Tags	[Crossroads, 3.2]

ID	1.3.4
Name	Hierarchical models
Type	Atomic
Abstract	This characteristic specifies whether support exists for hierarchical models.
Description of results	Existence of support for hierarchical models.
Unit of measure	N/A
Target	True
Objective	In hierarchical models, the data is organized into a tree-like structure, which makes it possible to, in a specific model, move between different levels of abstraction. Support for hierarchical models facilitates the modeling by making it more flexible.
Tags	[Crossroads, 3.2]

ID	1.3.5
Name	Established modeling technique/language
Type	Atomic
Abstract	This characteristic specifies whether the system model is described using an established modeling technique/language.
Description of results	Existence of a system model described using an established modeling technique/language.
Unit of measure	N/A
Target	True
Objective	A system model can be anything from a description in natural language to a description based on an established modeling technique/language like UML or finite state machines. An established modeling technique/language is preferred since it is more likely to be well defined.
Tags	

ID	1.4
Name	Computations modeling technique
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the relevance characteristics tree diagram, Figure 9, ID 1.4.1 – 1.4.3.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	Security assessment is dependent on information regarding how computations of security values are modeled. Several kinds of computations modeling technique are possible to use and they are often complementary.
Tags	[Crossroads, 3.3]

ID	1.4.1
Name	Atomic security values
Type	Atomic
Abstract	This characteristic specifies whether support exists for using atomic security values.
Description of results	Existence of support for using atomic security values.
Unit of measure	N/A
Target	True
Objective	An atomic value is a value that cannot be split up. Booleans and integers are examples of atomic values.
Tags	[Crossroads, 3.3]

ID	1.4.2
Name	Aggregated security values
Type	Atomic
Abstract	This characteristic specifies whether support exists for using aggregated security values.
Description of results	Existence of support for using aggregated security values.
Unit of measure	N/A
Target	True
Objective	Aggregated security values are used to describe a combination of atomic security values. Aggregated values are typically assigned where inter-relations between security values occur.
Tags	[Crossroads, 3.3]

ID	1.4.3
Name	Security values inter-relations
Type	Atomic
Abstract	This characteristic specifies whether security values inter-relations are regarded.
Description of results	Existence of support for security values inter-relations.
Unit of measure	N/A
Target	True
Objective	In cases where security assessments are influenced by dependencies between security values, it is vital that modeling of inter-relations of security values is supported.
Tags	[Crossroads, 3.3]

ID	1.5
Name	Supporting methods and tools
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the relevance characteristics tree diagram, Figure 9, ID 1.5.1 – 1.5.4.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	The characteristic presents a measure of the extent to which different relevant methods and tools support the assessment methods. Methods and tools includes routines, administrative processes, software tools etc.
Tags	[Crossroads, 3.2, 3.3]

ID	1.5.1
Name	Related to system modeling
Type	Atomic
Abstract	This characteristic specifies whether tools or methods exist for performing the system modeling.
Description of results	Existence of tools or methods for system modeling.
Unit of measure	N/A
Target	True
Objective	The process of system modeling is complex and difficult. Tools and methods may aid and simplify this process.
Tags	[Crossroads, 3.2]

ID	1.5.2
Name	Related to computations modeling
Type	Atomic
Abstract	This characteristic specifies whether tools or methods exist for performing the computations modeling.
Description of results	Existence of tools or methods for computations modeling.
Unit of measure	N/A
Target	True
Objective	The process of computations modeling is complex and difficult. Tools and methods may aid and simplify this process.
Tags	[Crossroads, 3.3]

ID	1.5.3
Name	Related to security values computation
Type	Atomic
Abstract	This characteristic specifies whether tools or methods exist for performing the security values computation.
Description of results	Existence of tools or methods for security values computation.
Unit of measure	N/A
Target	True
Objective	The process of security values computation is complex and difficult. Tools and methods may aid and simplify this process.
Tags	[Crossroads, 3.4]

ID	1.5.4
Name	Related to measurements
Type	Atomic
Abstract	This characteristic specifies whether tools or methods exist for performing measurements.
Description of results	Existence of tools or methods for performing measurements.
Unit of measure	N/A
Target	True
Objective	To perform measurements can be complex and difficult. The existence of tools or methods supporting the performance of measurements may aid and simplify.
Tags	

ID	1.6
Name	Identify needs regarding security assessment
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the relevance characteristics tree diagram, Figure 9, ID 1.6.1 - 1.6.4.
Description of results	Percentage of sub characteristics fulfilled
Unit of measure	Percent
Target	100%
Objective	An assessment should start from the needs of the stakeholder. It is therefore important to have appropriate guidelines for how the needs analysis shall be performed. The objective is to ensure that the appropriate guidelines exist for analyzing the needs regarding security assessment.
Tags	[Process model, 4.1]

ID	1.6.1
Name	Collection of data
Type	Atomic
Abstract	This characteristic specifies whether guidelines for collection of data exist.
Description of results	Existence of guidelines for collection of data
Unit of measure	N/A
Target	True
Objective	The collected data is the basis for identifying the needs of the stakeholder, it is therefore important to have guidelines stating how the collection of data shall be performed. Collected data may consist of interviews with stakeholders and experts, analyzed documents etc.
Tags	[Process model, 4.1]

ID	1.6.2
Name	Identification of needs
Type	Atomic
Abstract	This characteristic specifies whether guidelines for identification of needs exist.
Description of results	Existence of guidelines for identification of needs
Unit of measure	N/A
Target	True
Objective	The process of identifying user needs is complex and difficult. Guidelines for how the identification of needs is performed are therefore needed. The guidelines could for example describe the following three steps: 1. Identification of statements regarding IT security needs 2. Analysis of statements in order to identify security needs 3. Analysis and structuring of the security needs
Tags	[Process model, 4.1]

ID	1.6.3
Name	Documentation of needs
Type	Atomic
Abstract	This characteristic specifies whether guidelines for documentation of needs exist.
Description of results	Existence of guidelines for documentation of needs
Unit of measure	N/A
Target	True
Objective	The identified needs shall be documented in order to allow traceability. The needs shall be documented using applicable and adequate tools such as hierarchical structures, use cases and misuse cases.
Tags	[Process model, 4.1]

ID	1.6.4
Name	Affirmation of current needs
Type	Atomic
Abstract	This characteristic specifies whether guidelines for affirmation of current needs exist.
Description of results	Existence of guidelines for affirmation of current needs
Unit of measure	N/A
Target	True
Objective	The current needs shall be affirmed and possibly also prioritized by the stakeholder in order to establish the needs in the organization.
Tags	[Process model, 4.1]

ID	1.7
Name	Establish relevant security characteristics
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the relevance characteristics tree diagram, Figure 9, ID 1.7.1 – 1.7.2.
Description of results	Percentage of sub characteristics fulfilled
Unit of measure	Percent
Target	100%
Objective	In order to carry out adequate, valid and reliable security assessments, the needs of the stakeholder have to be mapped with relevant security characteristics of the studied system.
Tags	[Process model, 4.2]

ID	1.7.1
Name	Inspection of needs of an IT security assessment
Type	Atomic
Abstract	This characteristic specifies whether guidelines for inspection of needs of an IT security assessment exist.
Description of results	Existence of guidelines for inspection of needs of an IT security assessment.
Unit of measure	None
Target	True
Objective	Detected and approved needs are to be inspected to verify whether they are sufficient to establish a set of relevant security characteristics. This incorporates guidelines to eliminate redundant security needs.
Tags	[Process model, 4.2]

ID	1.7.2
Name	Specification of the relation between security characteristics and the need of security assessment
Type	Atomic
Abstract	This characteristic specifies whether guidelines exist for specification of the relation between security characteristics and the need of security assessment.
Description of results	Existence of guidelines for specification of the relation between security characteristics and the need of security assessment.
Unit of measure	N/A
Target	True
Objective	In order to ensure the traceability from security characteristics to needs and vice versa, the relations between these shall be documented.
Tags	[Process model, 4.2]

ID	1.8
Name	Interpret security values
Type	Atomic
Abstract	This characteristic specifies whether guidelines for selection of routine and establishment of interpretation of security values exist.
Description of results	Existence of guidelines for selection of routine and establishment of interpretation of security values.
Unit of measure	N/A
Target	True
Objective	Security values can be interpreted in many different ways. Therefore it is of importance to select and establish an interpretation of the security values so they are interpreted in the same way.
Tags	[Process model, 4.6]

ID	1.9
Name	Economical aspects
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the relevance characteristics tree diagram, Figure 9, ID 1.9.1 – 1.9.4.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	There are several economical aspects involved when performing a security assessment. Different security assessment methods have different prerequisites which, at the bottom line, give an indication of the costs involved for performing a security assessment using the specified security assessment method.
Tags	

ID	1.9.1
Name	Reuse produced data from previous assessments of the same system
Type	Atomic
Abstract	This characteristic specifies whether it is possible to reuse produced data from previous security assessments of the same system.
Description of results	Existence of support to reuse produced data from previous security assessments of the same system.
Unit of measure	N/A
Target	True
Objective	The possibility to reuse produced data from previous security assessments of a system reduces the time needed to perform new assessments of the same system. Reused data could for example be a system model from a previous assessment which can be modified to reflect the current system. Thereby it is not necessary to redo the system modeling from scratch.
Tags	

ID	1.9.2
Name	Reuse produced data from previous assessments of other systems
Type	Atomic
Abstract	This characteristic specifies whether it is possible to reuse produced data from previous assessments of other systems.
Description of results	Existence of support to reuse produced data from previous assessments of other systems.
Unit of measure	N/A
Target	True
Objective	The possibility to reuse produced data from previous assessments of other systems reduces the time needed to perform assessments of new systems. Reused data could for example be a system model from another system which is similar to the new system to be assessed. The system model from the similar system can be modified to reflect the current system, which means it is not necessary to do the system modeling from scratch.
Tags	

ID	1.9.3
Name	Need of consulting experts to prepare the input to the security assessment method
Type	Atomic
Abstract	This characteristic specifies whether experts are needed in order to prepare the input to the security assessment method.
Description of results	Existence of need to consult experts to prepare the input to the security assessment method.
Unit of measure	N/A
Target	False
Objective	The input to the assessment method can consist of both measured values and assessed values. The existence of assessed values as input indicates a possible need to consult experts in order to perform an assessment. This characteristic regards the economical aspects of consulting experts which, in most cases, indicates an increased cost for preparing the input to the security assessment method.
Tags	

ID	1.9.4
Name	Need of consulting experts to perform the security assessment
Type	Atomic
Abstract	This characteristic specifies whether experts are needed in order to perform an assessment using the security assessment method.
Description of results	Existence of need to consult experts to perform the security assessment.
Unit of measure	N/A
Target	False
Objective	The expertise needed to perform a security assessment can vary between different security assessment methods. More complex security assessment methods can require experts in order to perform a security assessment. An expert can also be needed in order to interpret the assessment result. This characteristic regards the economical aspects of consulting experts which, in most cases, indicates an increased cost for performing the security assessment.
Tags	

A.2 Validity characteristics

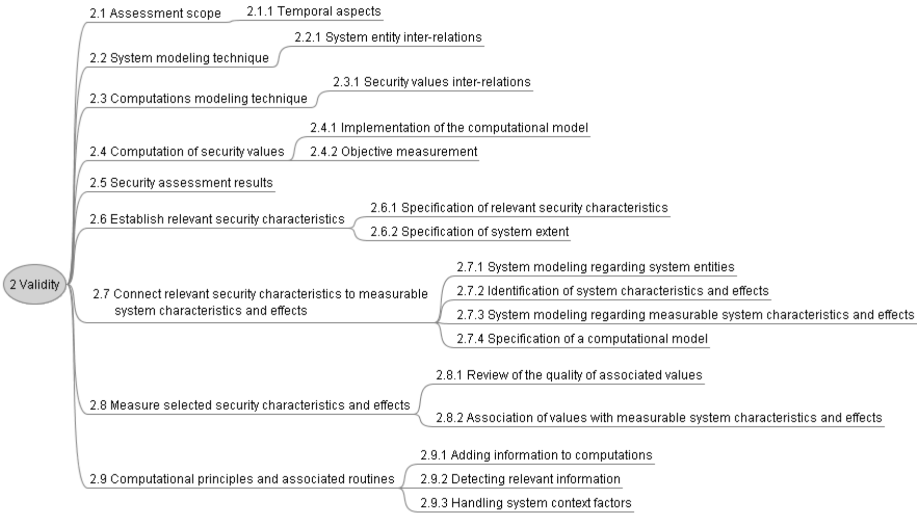
2 Validity
2.1 Assessment scope
2.1.1 Temporal aspects
2.2 System modeling technique
2.2.1 System entity inter-relations
2.3 Computations modeling technique
2.3.1 Security values inter-relations
2.4 Computation of security values
2.4.1 Implementation of the computational model
2.4.2 Objective measurement
2.5 Security assessment results
2.6 Establish relevant security characteristics
2.6.1 Specification of relevant security characteristics
2.6.2 Specification of system extent
2.7 Connect relevant security characteristics to measurable system characteristics and effects
2.7.1 System modeling regarding system entities
2.7.2 Identification of system characteristics and effects
2.7.3 System modeling regarding measurable system characteristics and effects
2.7.4 Specification of a computational model
2.8 Measure selected security characteristics and effects
2.8.1 Review of the quality of associated values
2.8.2 Association of values with measurable system characteristics and effects
2.9 Computational principles and associated routines
2.9.1 Adding information to computations
2.9.2 Detecting relevant information
2.9.3 Handling system context factors

Figure 10: Validity characteristics.

ID	2.1
Name	Assessment scope
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the validity characteristics tree diagram, Figure 10, ID 2.1.1.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	The complex structure of information systems, along with the difficulty for assessment methods to capture all security relevant characteristics, makes it essential to specify the scope of the assessment method. Defining the extent of the system being assessed illuminates both features and limitations of the assessment method.
Tags	[Crossroads, 3.1]

ID	2.1.1
Name	Temporal aspects
Type	Atomic
Abstract	This characteristic specifies whether time-dependence of security is regarded.
Description of results	Existence of support for temporal aspects.
Unit of measure	N/A
Target	True
Objective	The dynamic nature of security, and especially the dynamic nature of security threats, necessitates security updates of information systems. Lack of updates will result in a degrading system.
Tags	[Crossroads, 3.1]

ID	2.2
Name	System modeling technique
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the validity characteristics tree diagram, Figure 10, ID 2.2.1.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	Security assessment is dependent on information regarding how systems are modeled. Several kinds of systems modeling technique are possible to use and they are often complementary.
Tags	[Crossroads, 3.2]

ID	2.2.1
Name	System entity inter-relations
Type	Atomic
Abstract	This characteristic specifies whether system entity inter-relations are regarded.
Description of results	Existence of support for system entity inter-relations.
Unit of measure	N/A
Target	True
Objective	In cases where results of security assessments are influenced by the choice, design, implementation or operation of system entity inter-relations, it is vital that the assessment method supports modeling of system entity inter-relations. The system entity inter-relations describe how the entities of a system affect each other.
Tags	[Crossroads, 3.2]

ID	2.3
Name	Computations modeling technique
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the validity characteristics tree diagram, Figure 10, ID 2.3.1.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	Security assessment is dependent on information regarding how computations of security values are modeled. Several kinds of computations modeling technique are possible to use and they are often complementary.
Tags	[Crossroads, 3.3]

ID	2.3.1
Name	Security values inter-relations
Type	Atomic
Abstract	This characteristic specifies whether security values inter-relations are regarded.
Description of results	Existence of support for security values inter-relations.
Unit of measure	N/A
Target	True
Objective	In cases where security assessments are influenced by dependencies between security values, it is vital that modeling of inter-relations of security values is supported. The security values inter-relations describe how the security values affect each other.
Tags	[Crossroads, 3.3]

ID	2.4
Name	Computation of security values
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the validity characteristics tree diagram, Figure 10, ID 2.4.1 – 2.4.2.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	The measured security values are to be combined into compound security values, which finally results in values for the relevant security characteristics. Guidelines shall describe how to carry through this computation of security values.
Tags	[Process model, 4.5]

ID	2.4.1
Name	Implementation of the computational model
Type	Atomic
Abstract	This characteristic describes whether there exist tools which implement the computational model.
Description of results	Existence of tools implementing the computational model.
Unit of measure	N/A
Target	True
Objective	In order to compute the security values it is necessary to have tools implementing the computational model. A tool can be anything from a specially designed tool to more general software, like a spreadsheet application, which carries out the computations. It is also necessary to have manuals describing how to use the tools.
Tags	[Process model, 4.5]

ID	2.4.2
Name	Objective measurement
Type	Atomic
Abstract	This characteristic specifies whether measurements are objective.
Description of results	Existence of objectively performed measurements
Unit of measure	N/A
Target	True
Objective	The validity of security assessment methods is reduced if measures (input) are subjective. Therefore, it is important that all measurements are objectively performed.
Tags	[Crossroads, 3.4]

ID	2.5
Name	Security assessment results
Type	Atomic
Abstract	This characteristic states whether the validity of the assessment method has been demonstrated/shown.
Description of results	Existence of studies or experiments supporting the validity of the security assessment results.
Unit of measure	N/A
Target	True
Objective	Since it is hard to prove that security assessment methods produce valid results, it is essential to establish the presence of previous experience or results supporting the validity of the tested method.
Tags	[Crossroads, 3.5]

ID	2.6
Name	Establish relevant security characteristics
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the validity characteristics tree diagram, Figure 10, ID 2.6.1 – 2.6.2.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	In order to carry out adequate, valid and reliable security assessments, the needs of the stakeholder have to be mapped with relevant security characteristics of the studied system.
Tags	[Process model, 4.2]

ID	2.6.1
Name	Specification of relevant security characteristics
Type	Atomic
Abstract	This characteristic specifies whether guidelines exist for specification of relevant security characteristics.
Description of results	Existence of guidelines for specification of relevant security characteristics.
Unit of measure	N/A
Target	True
Objective	The purpose of specifying relevant security characteristics is to find security characteristics whose assessment will eliminate the stakeholder's lack of knowledge.
Tags	[Process model, 4.2]

ID	2.6.2
Name	Specification of system extent
Type	Atomic
Abstract	This characteristic specifies whether guidelines exist for specification of system extent.
Description of results	Existence of guidelines for specification of system extent
Unit of measure	N/A
Target	True
Objective	The specification shall include the following factors which describe the system extent: ➢ The boundary between the modeled system and its surroundings. ➢ The system aspects that shall be included in the system model ➢ The part of the system's life-cycle that shall be modeled. ➢ The security characteristics and effects that shall be modeled.
Tags	[Process model, 4.2]

ID	2.7
Name	Connect relevant security characteristics to measurable system characteristics and effects
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the validity characteristics tree diagram, Figure 10, ID 2.7.1 – 2.7.4.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	In order to assess relevant security characteristics not being directly measurable, the security characteristics must be associated with measurable system characteristics and effects. Thereby a computations model is created that describes how measurable system characteristics and effects are compound into values for the relevant security characteristics.
Tags	[Process model, 4.3]

ID	2.7.1
Name	System modeling regarding system entities
Type	Atomic
Abstract	This characteristic states whether routines for creating a system model of the system entities are available.
Description of results	Existence of routines
Unit of measure	None
Target	True
Objective	A system model, which shows the entities available in the system, is needed in order to identify the system characteristics and effects available within the system. Routines for creating a system model of the system entities shall be available.
Tags	[Process model, 4.3]

ID	2.7.2
Name	Identification of system characteristics and effects
Type	Atomic
Abstract	This characteristic states whether guidelines exist for identification of system characteristics and effects.
Description of results	Existence of guidelines for identification of system characteristics and effects.
Unit of measure	N/A
Target	True
Objective	The identification of system characteristics and effects can be done in two principle ways, top-down or bottom-up. Top-down starts with security characteristics and breaks them down into measurable system characteristics and effects. Bottom-up starts with the available measurable system characteristics and effects of the system and maps them with the relevant security characteristics.
Tags	[Process model, 4.3]

ID	2.7.3
Name	System modeling regarding measurable system characteristics and effects
Type	Atomic
Abstract	This characteristic states whether guidelines exist for system modeling regarding measurable system characteristics and effects.
Description of results	Existence of guidelines for system modeling regarding measurable system characteristics and effects.
Unit of measure	N/A
Target	True
Objective	The system model shall describe the available entities regarding measurable system characteristics and effects, and in some cases also the relations between the entities. This constitutes a prerequisite for realization of the measurements.
Tags	[Process model, 4.3]

ID	2.7.4
Name	Specification of a computational model
Type	Atomic
Abstract	This characteristic states whether guidelines exist for specification of a computational model.
Description of results	Existence of guidelines for specification of a computational model.
Unit of measure	N/A
Target	True
Objective	The computational model shall include metrics regarding the measured system characteristics and effects, as well as a description of the relations between the measurable system characteristics and effects and the relevant security characteristics.
Tags	[Process model, 4.3]

ID	2.8
Name	Measure selected security characteristics and effects
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the validity characteristics tree diagram, Figure 10, ID 2.8.1 – 2.8.2.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	In order to compute values for the relevant security characteristics it is crucial that the measurable system characteristics and effects are assigned adequate values.
Tags	[Process model, 4.4]

ID	2.8.1
Name	Review of the quality of associated values
Type	Atomic
Abstract	This characteristic states whether guidelines exist for reviewing the quality of associated values.
Description of results	Existence of guidelines for reviewing the quality of associated values.
Unit of measure	N/A
Target	True
Objective	The reliability of the measured values is, at a review, compared with the affirmed metrics. The review of the quality of associated values aims at identifying situations where ➢ the chosen metric does not describe the reality in an adequate way. ➢ it is not possible to measure a system characteristic or effect with adequate accuracy.
Tags	[Process model, 4.4]

ID	2.8.2
Name	Association of values with measurable system characteristics and effects
Type	Atomic
Abstract	This characteristic states whether guidelines exist for associating values with measurable system characteristics and effects.
Description of results	Existence of guidelines for association of values with measurable system characteristics and effects.
Unit of measure	N/A
Target	True
Objective	Values shall be taken from the system model, or be collected based on the system model, and associated with the measurable system characteristics and effects identified in the computational model.
Tags	[Process model, 4.4]

ID	2.9
Name	Computational principles and associated routines
Type	Compound
Abstract	This is a compound characteristic which specifies the percentage of fulfilled sub characteristics at the third level of the validity characteristics tree diagram, Figure 10, ID 2.9.1 – 2.9.3.
Description of results	Percentage of sub characteristics fulfilled.
Unit of measure	Percent
Target	100%
Objective	This characteristic states whether computational routines, based on computational principles, exist to obtain sound and adequate computations. This entails the existence of routines to handle system context factors and to avoid • inclusion of irrelevant or incorrect information, • disregard of relevant information.
Tags	[Mattias Bengtsson's thesis, 2.4 and 4]

ID	2.9.1
Name	Adding information to computations
Type	Atomic
Abstract	This characteristic specifies whether routines exist to avoid that irrelevant or incorrect information is added.
Description of results	Existence of routines to avoid that irrelevant or incorrect information is added.
Unit of measure	N/A
Target	True
Objective	It is crucial to obtain adequate and correct information to facilitate security assessments. Interpretation of and operations on data need to be based on a sound theoretical foundation maintaining the information contained within the data. To achieve this, routines to avoid that irrelevant or incorrect information is added are necessary.
Tags	[Mattias Bengtsson's thesis, 2.4 and 4]

ID	2.9.2
Name	Detecting relevant information
Type	Atomic
Abstract	This characteristic specifies whether routines exist to avoid that relevant information is disregarded.
Description of results	Existence of routines to avoid that relevant information is disregarded.
Unit of measure	N/A
Target	True
Objective	It is crucial to obtain adequate and correct information to facilitate security assessments. Interpretation of and operations on data need to be based on a sound theoretical foundation maintaining the information contained within the data. To achieve this, routines to avoid that relevant information is disregarded are necessary.
Tags	[Mattias Bengtsson's thesis, 2.4 and 4]

ID	2.9.3
Name	Handling system context factors
Type	Atomic
Abstract	This characteristic specifies whether routines exist to identify, describe and handle factors influencing on the assessment result.
Description of results	Existence of routines for identifying, describing and handling factors influencing on the assessment result.
Unit of measure	N/A
Target	True
Objective	A number of factors in the system context, which are not explicitly handled by the testing procedure, may affect the repeatability of an assessment method.
Tags	

Appendix B Validity weights

This appendix presents the weights of the validity attributes using the Type II definition of quality mapping. Table 3 presents the *more important* attributes while Table 4 presents the *less important* attributes.

Table 3: Type β – More important.

ID	Name	Weight
2.2.1	System entity inter-relations	1/13
2.3.1	Security values inter-relation	1/13
2.4.2	Objective measurement	1/13
2.5	Security assessment results	1/13
2.7.1	System modeling regarding system entities	1/13
2.7.2	Identification of system characteristics and effects	1/13
2.7.3	System modeling regarding measurable system characteristics and effects	1/13
2.7.4	Specification of a computational model	1/13
2.8.2	Association of values with measurable system characteristics and effects	1/13

Table 4: Type α – Less important.

ID	Name	Weight
2.1.1	Temporal aspects	1/26
2.4.1	Implementation of the computational model	1/26
2.6.1	Specification of relevant security characteristics	1/26
2.6.2	Specification of system extent	1/26
2.8.1	Review of the quality of associated values	1/26
2.9.1	Adding information to computations	1/26
2.9.2	Detecting relevant information	1/26
2.9.3	Handling system context factors	1/26