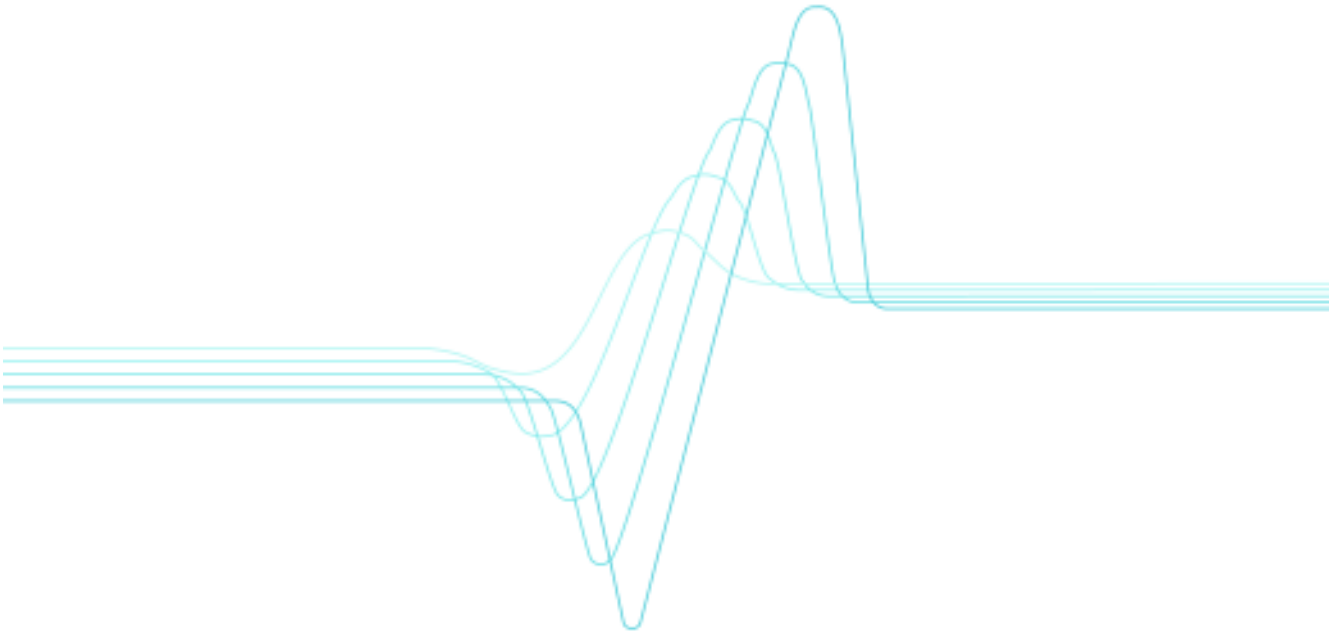
ESPOO 2004 VTT PUBLICATIONS 544

Anni Sademies

Process Approach to Information Security Metrics in Finnish Industry and State Institutions



VTT PUBLICATIONS 544

Process Approach to Information Security Metrics in Finnish Industry and State Institutions

Anni Sademies
VTT Electronics

ISBN 951–38–6406–5 (soft back ed.)
ISSN 1235–0621 (soft back ed.)

ISBN 951–38–6407–3 (URL: http://www.vtt.fi/inf/pdf/)
ISSN 1455–0849 (URL: http://www.vtt.fi/inf/pdf/)

JULKAISIJA – UTGIVARE – PUBLISHER

VTT, Vuorimiehentie 5, PL 2000, 02044 VTT
puh. vaihde (09) 4561, faksi (09) 456 4374

VTT, Bergsmansvägen 5, PB 2000, 02044 VTT
tel. växel (09) 4561, fax (09) 456 4374

VTT Technical Research Centre of Finland, Vuorimiehentie 5, P.O.Box 2000, FIN–02044 VTT, Finland
phone internat. + 358 9 4561, fax + 358 9 456 4374

VTT Elektroniikka, Kaitoväylä 1, PL 1100, 90571 OULU
puh. vaihde (08) 551 2111, faksi (08) 551 2320

VTT Elektronik, Kaitoväylä 1, PB 1100, 90571 ULEÅBORG
tel. växel (08) 551 2111, fax (08) 551 2320

VTT Electronics, Kaitoväylä 1, P.O.Box 1100, FIN–90571 OULU, Finland
phone internat. + 358 8 551 2111, fax + 358 8 551 2320

Technical editing Marja Kettunen

Otamedia Oy, Espoo 2004

Sademies, Anni. Process Approach to Information Security Metrics in Finnish Industry and State Institutions [Prosessinäkökulma tietoturvan mittaamiseen suomalaisessa teollisuudessa ja valtionhallinnossa]. Espoo 2004. VTT Publications 544. 89 p. + app. 2 p.

Keywords information security (IS), security metrics, IS metrics, security level, auditing, security processes

Abstract

In today's information technology world, there is a growing need for security solutions: information systems are more and more vulnerable because of the increased complexity and interconnection of insecure components and networks. Even though appropriate security approaches can be found, the resulting security level often remains unknown. It is a widely accepted principle that an activity cannot be managed well if it cannot be measured. Information security (IS) metrics offers work as a research field.

This thesis focuses on studying the use of IS metrics in certain Finnish industrial companies and state institutions. The objective is to study the state-of-practise and its relation to the literature in the research field. The use of IS metrics is particularly studied from the perspective of processes. The aim is to reveal how development and implementation of the metrics is carried out in the organisations. In addition, the techniques used in implementation and analysis of metrics, as well as their usefulness and future targets are studied. The research consists of a literature study followed by a survey study, and an analytical phase. The survey study is implemented by conducting eight interviews in different industrial corporations and state institutions. The method used is a semi-structured, theme-centred interview. The results are categorised applying suitable classifications found in the literature and analysed using an interpretative analysis method.

The survey clearly shows that measuring IS is important, but the benefits of measurements can only be seen when the metrics use is applied as a process, with the experience gained from the use of history data. Technical metrics and risk assessment metrics are commonly used, but there is a need to measure individual expertise as well as to automate and rationalise measurements. Most of the organisations do not use IS metrics as a process. However, there are intentions to implement an IS metrics process, as well as to integrate the IS metrics process into quality and business processes. Legislation, customers and technical development especially affect the future development of IS metrics.

Sademies, Anni. Process Approach to Information Security Metrics in Finnish Industry and State Institutions [Prosessinäkökulma tietoturvan mittaamiseen suomalaisessa teollisuudessa ja valtionhallinnossa]. Espoo 2004. VTT Publications 544. 89 s. + liitt. 2 s.

Keywords information security (IS), security metrics, IS metrics, security level, auditing, security processes

Tiivistelmä

Tietoturvaratkaisujen tarve lisääntyy koko ajan nykypäivän informaatiotekniikkaa painottavassa maailmassamme. Tietojärjestelmät ovat haavoittuvia monimutkaisuutensa vuoksi ja niihin kuuluu tietoturvattomia osia ja verkkoja. Vaikka turvaratkaisuja on olemassa, jää turvaratkaisun taso usein epäselväksi. Tunnettu periaate on, että kohdetta ei voida hallita hyvin, ellei siitä saada mittaustietoa. Tietoturvan mittaamiseen ei ole tutkimuksessa kiinnitetty suurta huomiota.

Tässä tutkimuksessa selvitetään tietoturvamittareiden käyttöä eräissä suomalaisissa teollisuus- ja valtionhallinnon organisaatioissa. Tietoturvan mittaamisen käytännön sovelluksia ja niiden yhteyttä tutkimuskirjallisuuteen tarkastellaan erityisesti prosessinäkökulmasta. Tutkimuksessa analysoidaan, millä tavoilla ja tekniikoilla tietoturvan mittausta kehitetään ja toteutetaan, sekä arvioidaan tulevaisuuden näkymiä tällä saralla. Tutkimus koostuu kirjallisuustutkimuksesta sekä haastattelu- ja analyysiosioista. Haastatteluosiossa haastateltiin kahdeksaa eri teollisuuden ja valtionhallinnon organisaation edustajaa käyttäen puolistruktukturoitua teemahaastattelumenetelmää. Haastattelutulokset luokitellaan soveltuvaa luokittelumenetelmää käyttäen ja analysoidaan tulkitsevalla analyysimenetelmällä.

Tutkimus osoittaa selvästi, että tietoturvan tason mittausta pidetään tärkeänä, mutta mittaamisen edut tulevat esille vasta, kun mittareita sovelletaan prosessimuodossa, jolloin voidaan hyödyntää historiatietoja. Teknisiä mittareita ja riskinarviointia käytetään yleisesti. Tarvetta on erityisesti henkilöiden tietoturvakäyttäytymisen mittaamiselle, samoin kuin mittauksia automatisoinnille ja järkeistämiselle. Useimmat organisaatiot eivät hyödynnä mittareita prosessimuotoisina. Monilla on kuitenkin aikomuksena toteuttaa tietoturvan tason mittaaminen prosessina, samoin kuin integroida kyseessä oleva prosessi osaksi laatu- ja liiketoimintaprosesseja. Tietoturvan mittaamisen tulevaisuuden kehitykseen vaikuttavat erityisesti lainsäädäntö, asiakkaat ja tekninen kehitys.

Preface

This study is a thesis for the University of Oulu and based on the work carried out in the strategic theme project TRUST at VTT Electronics in Oulu, Finland, during 2004. The work was funded by VTT Electronics.

I wish to express my deep gratitude to the supervisor of this thesis, Mr. Jorma Kajava of the University of Oulu (Department of Information Processing Science). I would also like to thank Mr. Reijo Savola of VTT Electronics for his supervision and valuable comments, which have been crucial for the success of this thesis. I similarly wish to thank Prof. Petri Pulli of the University of Oulu (Department of Information Processing Science) for commenting on this work.

I am also grateful to the interviewees. Their contribution to the development of this thesis has been crucial.

I similarly wish to thank Mr. Jarkko Holappa, Ms. Seija Komi-Sirviö, Mr. Hannu Honka and Prof. Eila Niemelä for commenting on this work at VTT Electronics.

I also want to thank my family and friends for their support and encouragement.

In Oulu, May 19, 2004,

Anni Sademies

Contents

Abbreviations

BS	Base Practises
BS 7799	Specification for Information Security Management
CC	Common Criteria
CEO	Chief Executive Officer
CVE	Common Vulnerabilities and Exposures
DoD	Department of Defence
GQM	Goal Question Metric
HTTP	Hypertext Transport Protocol
IA	Information Assurance
IA-CMM	Infosec Assessment Capability Maturity Model
IDS	Intrusion Detection System
IS	Information Security
IS*	Synonym for metric, measure, score, rating, rank or assessment result
ISACA	Information Systems Audit and Control Association
ISO 17799	Code of Practise for Information Security Management.
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
NIST	National Institute of Standards and Technology
NSA	National Security Agency
PA	Process Area
PC	Personal Computer
PP	Protection Profile
SSAM	SSE-CMM Appraisal Method
SSE-CMM	Systems Security Engineering Capability Maturity Model
ST	Security Target
TCSEC	Trusted Computer System Evaluation Criteria
TOE	Target of Evaluation
TQM	Total Quality Management
TSM	Total Safety Management
TSEM	Total Safety and Environmental Management System
VAHTI	Information Security Executive Group of State Administration

1. Introduction

A growing number of security solutions are used in today's information technology world. However, the achieved security level is often unclear. There is not much research about what kind of information security metrics are used in Finnish industry and state institutions. Therefore, the aim of this study was to investigate the issues focused especially on the development and use of the metrics within production processes. The topics cover what kind of techniques are used in implementation and analysis of these metrics, how useful these metrics are for an organisation, and what the future targets for the use of information security metrics are.

1.1 Background

Without measurement and metrics the level of information security hinges on guesswork and estimates. Information security is often considered as purely an add-on quality factor, and its utilisation level depends greatly on the attitude of the management within the organisation (Kajava & Leiwo, 1994). As the importance of information security utilisation slowly becomes apparent, the urgency for use of IS work processes within an organisation grows and new processes are gradually implemented. It can then be understood that, due to the infancy of the subject, the maturity level of IS metrics and their measurement still requires a vast amount of development work.

The following questions guide the literature study:

- What is the definition of information security metrics?
- What kind of classifications and categorisations does the literature offer for IS metrics?
- What kind of methods and techniques are proposed for IS metrics?
- What is the direction of IS metrics research and development?
- What can we expect as the outcome of the experimental phase of this study, the interviews?

1.2 Research subject

The research problem is: "What kinds of IS metrics do Finnish industrial companies and state institutions use, and why?" In addition, the purpose is to find out the answers to the following questions:

1) What kinds of techniques are used in the implementation and analysis of IS metrics?
2) How useful are metrics for the organisations and why?
3) How should the future work in IS metrics be directed?

The emphasis in this study is placed on processes, that is, to resolve principally whether and how the IS metrics are developed and located within time as a process-like manner, and also how well are IS processes are integrated within the organisation's "basic" processes.

1.3 Research method

The research method used in this study is a literature study followed by an empirical, survey-type study. The data for the empirical study is collected by interviews. A semi-structured, theme-centred interview technique (Hirsjärvi & Hurme, 2001) is used. The research method is illustrated in Figure 1. The interview sample size is eight Finnish organisations. The organisations represent different types of industry enterprises or state institutions. Appropriate representatives, being one of the main responsible people for the information security of the organisations, in each organisation are interviewed.

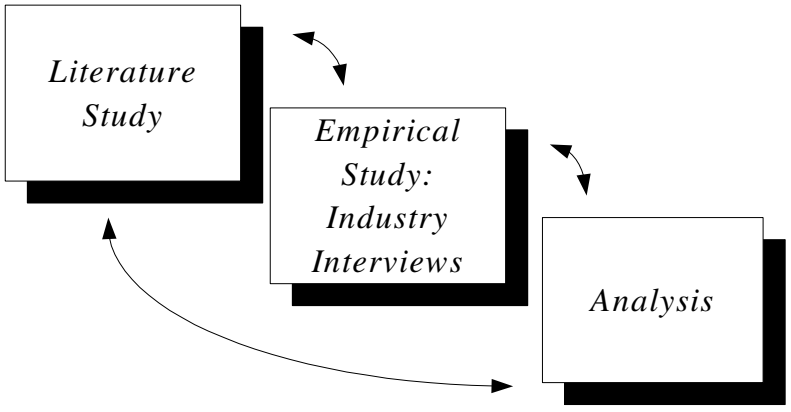


Figure 1. Research method.

1.4 Role of literature study

The literature study provides an overview of the general metrics classification and definition proposed in the literature.

1.5 Role of empirical analysis

The interview technique requires that the questions to be asked not be overly rigid but flexible. In addition, instead of having written-down formal phrasing of the questions, the interviewer should prepare for the interviews by making a list of themes. This allows the interviewee to use his own frame of reference more freely. This may have a huge effect on the originality of the answers. Finally, the interview results are analysed and categorised with help of theory obtained from the literature study, and then compared with how they correspond to each other and the techniques proposed in the literature, as illustrated in Figure 1. The result is a classification of different kinds of security metrics and techniques, which gives a general background for the analysis of the current state of practise in information security metrics in Finnish organisations.

1.6 Structure of the study

The structure of the study is as follows: Chapter 2 reviews what kind of definitions, classifications, techniques, problems and development suggestions for IS metrics can be found in the literature. Chapter 3 describes the preparation for the interviews, presents the analysis technique and analyses the interview results by themes. Chapter 4 analyses and evaluates the state of practise in Finnish industry and state institutions and proposes guidelines for further research. Chapter 5 offers conclusions. Finally, Appendix explains the interview themes and presents them with the interview questions.

2. Information security metrics in literature

Several approaches can be found to metrics research and implementation within the IS field literature.

2.1 Concepts

A few basic concepts are defined in order to understand the application of the concept of metrics in the IS area.

2.2 Information security and its dimensions

Code of Practise (ISO 17799, 2000) defines the purpose of information security as "to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents". Information security is defined as the protection of information for confidentiality, integrity and availability (Parker, 1981). These dimensions can be explained as follows:

- **Confidentiality**: information is accessible only to those authorised to have access,
- **Integrity**: accuracy and completeness of information and computer software is safeguarded, and
- **Availability**: authorised users have access to information and associated assets when required.

2.3 Difference between measurement and metrics

Measurements provide a one-time view of specific measurable parameters and are represented by numbers, weights or binary statements. On the other hand, *metrics* are produced by taking measurements over time and comparing two or more measurements with predefined baselines, thus providing a means for interpretation of the collected data (Jelen, 2000). Henning (2001) notes that there is often "considerable controversy" when the term "metrics" is used within the IS area. Therefore, he suggests that the expression IS* be used as a synonym for

the following: metric, measure, score, rating, rank or assessment result with the definition: “An IS* is a value, selected from a partially ordered set by some assessment process, that represents an IS-related quality of some object of concern. It provides, or is used to create, a description, prediction, or comparison, with some degree of confidence”. IS* is also used in this thesis according to its definition, as a synonym for the multiple attributes where it has been considered appropriate to describe in a broader context than just the word “metrics”.

2.4 Security metrics classifications

In order to understand how different IS* can be constructed, one must take a look at definitions and constructions proposed in the literature for the security metrics model along with various classifications and categorisations for IS*. According to Katzke (2001), a security metrics model consists of three components:

- The object being measured,
- The security objectives, i.e. the “measuring rod” that the object is being measured against, and
- The method of measurement.

The model is illustrated in Figure 2, as well as how the security objectives are divided into:

- Security requirements, such as specifications, standards, control objectives and CC- (Common Criteria, 1999) Protection Profiles,
- Best practises,
- Security base lines,
- Due diligence, i.e. security management based on experience, and
- Maturity models like SSE-CMM (Systems Security Engineering Capability Maturity Model, 2003) and IA-CMM (INFOSEC Assessment Capability Maturity Model, 2003).

Methods of measurement include

- Direct testing (like functional, red team/penetration),
- Evaluation (for example with Common Criteria),
- Assessment (like risk/vulnerability assessment),
- Accreditation,
- Training/education/level of competence and
- Observation of system performance, such as intrusion detection.

Lindqvist et al.(1998) categorise the security guidelines according to the audience for whom they offer the most advantage. They claim that, for vendors and manufacturers, the functionality of the system and the development process have been the target of standards [TCSEC (Trusted Computer System Evaluation Criteria, 1985), ITSEC (Information Technology Security Evaluation Criteria, 1991) and CC] that specify criteria against which security evaluations can be made. In their opinion, baseline security documents have been created for producers to set a minimum set of requirements for security features that an information technology should possess. Security policies are useful to managers, operators and users of information technology system, because they need to follow certain rules in order to minimise potential threats. In this contect, standards mostly mean guidelines and codes of practises.

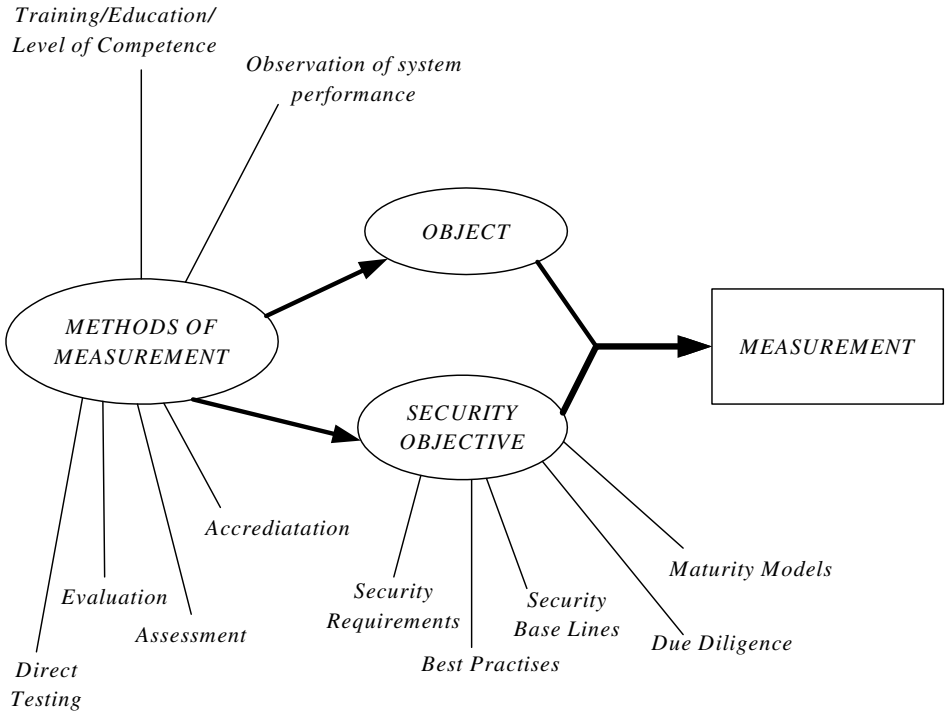


Figure 2. Security metrics model according to Katzke (2001).

Jonsson (2003) sorts the methods of measurement into the following techniques: risk analysis, certification and measures of the intrusion process.

- **Risk analysis** is an estimation of the probability of specific intrusions and their consequences and costs, and it can be thought of as a trade-off to the corresponding costs for protection,
- **Certification** is the classification of the system in classes based on design characteristics and security mechanisms, "The 'better' the design is, the more secure the system.", and
- **Measure on the intrusion process** is a statistical measure of a system based on the effort it takes to make an intrusion. "The harder it is to make an intrusion, the more secure the system" (Jonsson, 2003).

The security metrics model can be seen as an abstraction in Henning's (2001) definition: it divides IS* into four categories:

- Technical,
- Organisational,
- Operational IS*, and
- "Brainstormers", which refer to synthesis, big-picture type of metrics.

Henning emphasises that some viewpoints are excluded from this classification, i.e. individual IS* (describing individual expertise) and environmental IS* (describing security-relevant aspects of an organisation's or operation's environment, in particular, threats). Figure 3 clarifies this abstraction and binds the IS* to the process. The model is considered from the perspectives of "type of object", which means IS*, "purpose", in other words how the IS* is to be used, and "intended audience", which means the people who primarily use the information gained by the use of IS*. However, Table 1 presents the main features of each IS* category, complemented with individual and environmental IS* in order to offer an overall impression of the IS* effect area.

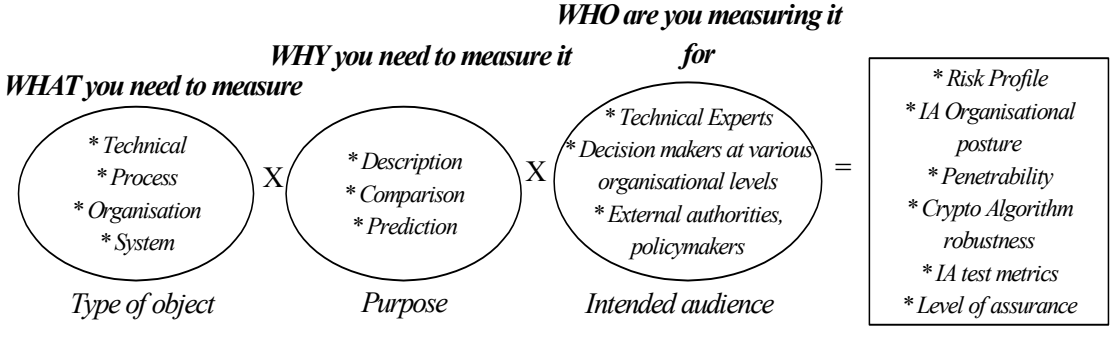


Figure 3. Characterisation of IS (Henning, 2001).*

According to Henning (2001), the purpose for which the IS* are being developed can be divided into decision support and mandated reporting of IS status or posture. According to Figure 3, IS* can be used to describe, compare and predict the behaviour and attributes of a system or its components. The IS* categories by Henning will be reviewed briefly, as well as the security objectives and methods of measurements by Katzke (2001).

Swanson et al. (2003) offer a different classification in their Security Metrics Guide:

- Implementation metrics to measure implementation of security policy,
- Effectiveness/efficiency metrics to measure results of security services delivery, and
- Impact metrics to measure business or mission impact of security events.

As stated, there are many varying classifications and categorisations for IS* which can be used as a basis when evaluating IS metrics. Building a security metrics program is discussed later in Chapter 2.6.

Miettinen (1999) divides metrics into qualitative and quantitative. Qualitative metrics use discrete variables and measurement is thus conducted by assessing. Examples of qualitative metrics are measuring the criticalness of a corporation's activity, measuring the level of management's IS awareness, and personnel and risk assessment. Quantitative metrics use numeric measures, such as probabilities, percentages, ratios and numbers. Quantitative values are gained by measuring technical issues, the costs resulting from activities and the number of development acts. (Miettinen, 1999.)

2.4.1 Technical Information Security Metrics

Technical IS* can be used to describe, and hence compare, technical objects. This includes algorithms, specifications, architectures and alternative designs, products, and as-implemented systems at different stages of the system life cycle. Thus technical metrics represents quantitative metrics using Miettinen's classification. Common Criteria can be considered a standard for writing technical IS*, as the Common Vulnerabilities and Exposures (CVE, 2003) list can serve as a basis for comparing vulnerability-scanning tools. (Henning, 2001.)

Intrusion detection metrics is a typical example of technical IS* for which a reasonable amount of research can be found. This research details intrusion detection systems (IDS), which, due to their technical nature, can be modelled and parameterised for further modularising and quantifying. A notable point according to Henning (2001), is that technical IS* are generally supposed to handle objects so that they can be compared. Therefore, they offer a way of

measuring and comparing progress and state similarities between systems handling similar objects.

Henning (2001) also states that researchers should focus on handling particularly abstracted objects when developing technical IS*, such as cryptographic algorithms or protocol specifications, rather than implemented objects. This is because the development cycle of the product implementation is fast. Therefore, once the appropriate metrics have been developed for the product, it may have already been superseded by the newer version, to which the same IS* cannot be applied. The other alternative would be to focus on evolutionary life cycle within IS* development. (Henning, 2001.)

Deswarte et al. (1999) also recognise this in their validation of the security metrics system. They state that IS* should evolve according to system modifications influencing its security, because any modification can bring new vulnerabilities or correct previous ones, and the security measure should be sensitive to such modifications. They study and develop the structure of IDS models and give further examples of the desired qualities of its IS*. One quality of note is that a system and its measures should remain independent of the potential amount and skill level of the attacker, and the security measure should also be directly related to security objectives. The latter definition explicitly includes an interesting assumption that the system may include several vulnerabilities, yet be secure as long as the vulnerabilities do not defeat the security objectives defined for the system.

However, when two secure systems are combined, the result is not necessarily an explicit combination of the two; there might be unexpected behaviour. Thus, the predictions made for such system behaviour cannot always be reliable. There is a need to develop better models of acceptable systems behaviour limited to the behaviour characteristics of the technical objects. The other point is that in order to make reliable predictions, technical IS* will need an underlying model of IA (Information Assurance) in which the values associated with technical objects are significant factors in system security and also in which the future resembles the past. (Henning, 2001.)

2.4.2 Organisational Information Security Metrics

Organisational IS* are for describing and tracking the effectiveness of organisational programs and processes, such as the percentage of personnel trained in security and the percentage of systems accredited. Thus, organisational IS* represent both quantitative and qualitative metrics in Miettinen's (1999) model. One example of this is the study by Kajava & Leiwo (1994) about information security staff in organisations. They discuss the approach to measure the amount of IS staff and its applicability in Finland, based on research carried out in the U.S. by Wood (1989). They point out that the size of an organisation is a relative concept when interpreting these kinds of results, as a staff size of 2500 people is not small in Finland, even though this is the case in the U.S. This is why using this kind of IS* as an indicator of the state of IS requires common sense, yet can be one important indicator about investment in IS.

Commercial organisations aim mainly at the use of metrics to resolve the effectiveness of organisational programs and processes, as well as the amount and quality needed for security actions. Governmental units mainly measure how well the organisation meets the requisite mandates (reporting metrics). The IS metrics for these organisations often serves as a tool for decision support. The difference between the aims of these sectors can result in different needs for IS*. (Henning, 2001.)

A similarity for both sectors is that both usually have a functioning security program for the IT modernisation process, which comprises the same steps: requirements, approvals, development and installation. There are also established procedures for both sectors that include approval points as well as IS integrated into any program/business case. Both rely on auditors, penetration testing and configuration management procedures. The difference is that government procurements are constrained by national and organisational policies and architectures (policy-driven), while the commercial enterprises rely on the personal judgements of the security practitioner (profit-driven). Due diligence on the part of the individuals is expected and forms the basis for management approval in commercial units, while the government approval process is more structured. (Henning, 2001.)

2.4.3 Operational Information Security Metrics

Henning (2001) refers to the use of operational IS* as to describe and manage the risks to operational environments, including as-used systems and operating practises. Operational IS* are hence mainly risk assessment metrics for which their component metrics related to asset values, impact severity, threats, vulnerabilities and effectiveness of security measures. But they also represent the number of advisories responded to, the time devoted to patch installation and the percentages of systems patched that are assessment components. Hence operational IS* are mainly qualitative metrics (risk assessment) but can also represent quantitative metrics in Miettinen's (1999) model.

In order to manage and measure operational attributes, it must be understood what constitutes the organisation's operational environment: controllable areas, external areas and assumable or predictable matters. Controllable areas consist of physical, procedural and personnel security measures, as well as information systems owned or operated by the organisation. External areas consist of systems that have an interface with the organisation's own systems, or systems that the organisation's own system is dependent on.

2.4.4 Brainstormers

"Brainstormers", according to Henning (2001), refer to concepts of synthesis, cross-track issues and big-picture concerns. In her work, a system engineering approach was applied to aggregate measurement, as this would accommodate the complete system life cycle, meaning that technical, operational and organisational measurement techniques and IS* could all be integrated into this framework most effectively. It can be assumed that brainstormers mainly represent qualitative metrics in Miettinen's (1999) model, which takes advantage of the accuracy gained by quantitative metrics.

Table 1. IS classification according to Henning (2001) with complementary qualities.*

	Tech. IS*	Org. IS*	Oper. IS*	Brainst.	Indiv. IS*	Env. IS*
Describe	Technical objects	Effectiveness of programs and processes of the organisation	Risks to operational environments including as-used systems and operating practises	Synthesis, cross-track issues and big-picture concerns	Individual expertise	Security-relevant aspects of the environment of organisation or operation
Example	Logs	Percentage of systems accredited	Asset values	Combination of other 3 IS* into one framework	Awareness or educational level of an employee	Threats caused by functioning in environment
Challenges	May contain a lot of useless data, often need to be filtered and rationalised	Require viewpoint of the whole organisation, not necessarily directly applicable in other organisations	Require that the operational environment and its effects are understood, this can often be just assessed	Require viewpoint of the whole system life cycle	Difficult to level on the organisation scale	Possibly difficult to model functions of an environment, can contain unexpected factors and combinations

2.5 Problems in application of metrics in information security

There are a few disturbing factors that may be faced when applying metrics in the area of information security. Some concluded problems are illustrated in Figure 4.

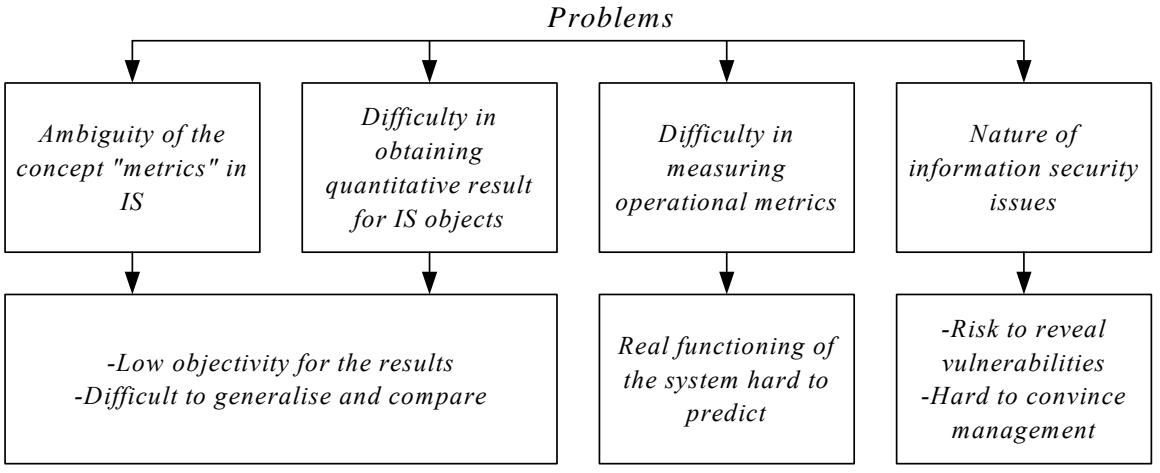


Figure 4. Problems related to IS metrics.

2.5.1 Ambiguity of the concept "metrics" in IS

One can easily find why it is challenging to apply the concept "metrics" to information security. There are several classifications and different viewpoints on the subject, as discussed earlier. Katzke (2001) points out that unless the target objects are defined, the term "security metrics" can be rather ambiguous. Examples of different definitions that he highlights range from measurements of a security program's effectiveness to a security professional or organisation's competence to the security of a system or a product. He refers to security metrics as an immature discipline that lacks precision and contains considerable uncertainty.

The variety of applied fields and multiple approaches constitutes confusion between different audiences and the effecting factors. Henning (2001) states that some seek to reserve it for the results of measurements based on scientific principles, but others use it to include results of assessments based on subjective judgements. In addition to this, the used IS* contexts might be different from what they were meant for. For this reason she proposes that any definition of IS metric, measure, score, rating, rank or assessment result should include a specification of the process used to construct and evaluate it.

2.5.2 Difficulty in obtaining quantitative result for IS objects

According to the definition by Jelen (2000), the concept of metrics demands that the result of a measurement has to be quantitative. Yet, there is no absolute standard definition for any of the dimensions of information security. Therefore, the measurements for determining sub-areas of information security and results gained by them are not objective or comparable until there is a common and indisputable definition for any of those sub-areas. However, organisations might find a general definition of them useful when using the definition for defining security objects for the system. Difficulties often occur when one tries to quantify such concepts in a reliable and adequate manner. It must be noted that there are definitions for the sub-areas concerning technical systems such as intrusion detection systems, but the definitions do not encompass broader concepts such as whole functioning organisations.

Henning (2001) also classifies IS* into numeric and non-numeric forms. Instead of Miettinen's (1999) division of quantitative and qualitative values, in her perspective, qualitative attributes, such as "red/yellow/green"-types of classifications, still need quantitative measures for the results, such as when "green" applies to zero vulnerabilities found, and so on. If there were common definitions for the IS*, it would be much easier to develop common methods and gain quantitative, comparable results.

2.5.3 Difficulty in measuring operational metrics

Jonsson (1998) expresses that the existing way to measure security is to use the classes or rankings in the Orange book (TCSEC, 1985) or other evaluation criteria. According to him, the problem is that static design properties of the system are reflected and the uncertainty and dependence of the operational environment are not incorporated in a probabilistic way, similar to the way in which reliability is commonly expressed. Similar problems were discussed earlier concerning technical IS*. The behaviour of the system, especially when combining two systems into one functioning system, should be taken into account. Furthermore, the metrics should evolve as the processes around them evolve, so that the metrics is constantly measuring real time qualities.

The literature emphasises a quantitative approach to operational IS*: Typically, the number of vulnerabilities, intrusions and virus outbreaks are counted. This approach does not help in assessing operational readiness and does not often aid managers in understanding the potential for security violations in a system or process. The measurements delivered by system security evaluation tools should represent, as accurately as possible, the security of the system in operation. (Henning, 2001).

One can comprehend that there is a need for constant, systematic development of the used IS*, based on the history data and particularly in a process-like manner. The surrounding environment and interfacing systems should be taken into account. According to Henning (2001), the IS properties of an operational environment frequently cannot even be measured directly. Indirect indicators can be useful, but they must be defined and used carefully.

2.5.4 Nature of information security issues

The purpose of measuring information security is ultimately to be aware of the current security level. This process reveals the strengths of the system, but also the vulnerabilities, which require some kind of reaction. The reaction may sometimes be as simple as leaving vulnerabilities as they are, that is, fixing them might be less valuable than taking the risk caused by the vulnerability. Often the cost of a certain threat is hard to define. This mechanism, which is part of the risk analysis process, is using security metrics itself, but the object might also be other types of IS metrics.

The concept of metrics is overlapping and complex. In organisations where the management is not aware of IS issues, it might be extremely hard to convince them to invest in better security. What makes things worse is that security issues are invisible. The better the security is, the more invisible IS becomes in an organisation's life. Therefore, investments in security do not show visible results in daily life, and this is why there may be pressure to reduce investment in security if "nothing happens".

Often the measurement process may require outside knowledge, for example, in audit sessions, or long-term commitment from the staff. This itself may become

too high a risk for the organisation compared to the benefits gained by the use of effective metrics. Human factors are considerable for any IS, and the competitive benefit of gaining access to the organisation's precious information, its weaknesses, and strengths may become too attractive for some people. The information, when in the wrong hands, can even be devastating to the trustworthiness of the company (Kajava & Leiwo, 1994). Therefore, many organisations may ask themselves: "can we afford good security?"

2.6 Security objectives

Using the classification from Katzke (2001), security objectives can be divided into the following: security requirements (such as specifications, standards, control objectives and Common Criteria Protection Profiles), best practises, security base lines, due diligence and maturity models like SSE-CMM and IA-CMM. These are compared in Table 2.

Table 2. Security objectives.

Security objective	Application method	Expected result	Example
Security requirements	Security actions are compared to requirement	Suggestions for improvements	Standards, Common Criteria Protection Profiles
Best practises	Safe procedures for certain activity are given or determined	Instructions for secure procedures	Instructions for viruses, e-mail handling
Security base lines	Organisation security inspection and assessment	Minimum set of security actions needed	Required access controls
Due diligence	Security management based on expertise	Security level of own organisation or business partner	Evaluation of security controls
Maturity models	Security practises are inspected and compared to the model	Explicit security level	SSE-CMM

2.6.1 Security requirements

IS can be considered one quality factor of the organisation's products and services. Therefore, many common factors can be found when considering security issues and organisation's quality actions. The standards used in quality assessment can act as a model when developing information security quality issues, since quality standards have been implemented and tested for a much longer period of time, and far more broadly in industry organisations than have security standards, and the development is therefore further advanced.

The application of quality models naturally depends on the character of the organisation. Some frequently used quality criteria are the ISO 9000 series (The ISO Survey of ISO 9000 and ISO 14001 Certificates, 2002) Total Quality Management (TQM, Gummer & McCallion, 1995) and The Malcolm Baldrige criteria (The Baldridge Criteria for Performance Excellence, 2004). Total Safety Management (TSM, Miettinen, 2001) and Total Safety and Environmental Management System (TSEM, Miettinen, 2001) are quality criteria that are specialised in issues of security management. However, Miettinen (2001) considers the "common" standards to be far more effective when applied to improving the quality of the security management in organisations.

Finnish State Administration gives a broad IS instruction set that covers all IS subareas. The instructions have been developed by VAHTI (Valtionhallinnon Tietoturvallisuuden Kehitysohjelma, 2004). It helps to ensure and backup IS in organisations under the supervision of State Administration. Its development targets are, for example, virus protection, ensuring information systems, management of log data and e-mail and issues concerning electronic services.

Malcolm Baldrige criteria are standard for self-assessment in order to measure and improve organisation excellence. The criteria is divided into seven sub-areas, 1) leadership, 2) strategic planning, 3) customer and target focus, 4) measurement, analysis and knowledge management, 5) human resource focus, 6) process management and 7) business results. Details defined in the sub-areas are detected in the target organisation and evaluated against the criteria.

The Goal Question Metric (GQM) Approach (Basili et al., 1994) is based upon the assumption that for an organisation to measure in a purposeful way it must

first specify the goals for itself and its projects. Then, it must trace those goals to the data that are intended to define those goals operationally and finally provide a framework for interpreting the data with respect to the stated goals. Thus the organisation's informational needs have to be clarified, so that they can be quantified whenever possible, and the quantified information can be analysed regarding whether or not the goals have been achieved. (Basili et al., 1994) Figure 5 illustrates the GQM process:

- **Conceptual level** (GOAL): Goal is defined for an object.
- **Operational level** (QUESTION): A set of questions is used to characterise the way the assessment/achievement of a specific goal is going to be performed based on some characterisation model.
- **Quantitative level** (METRIC): A set of data is associated with every question in order to answer it in a quantitative way.

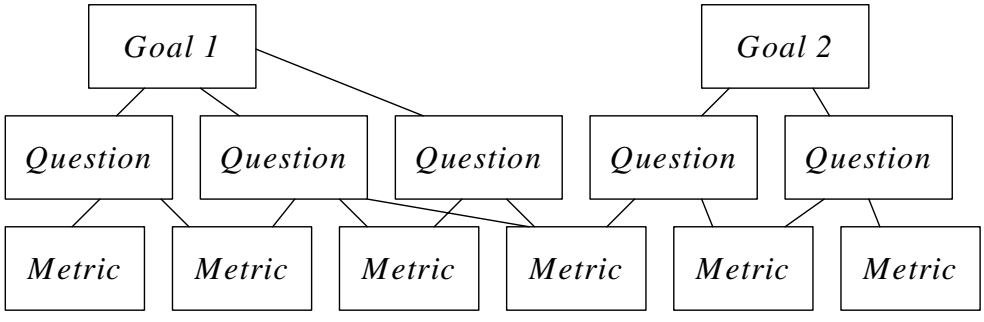


Figure 5. GQM process (Basili et al., 1994).

Common criteria (CC, 1999) are a "catalogue or dictionary of requirements" for constructing the basis for evaluation of the security properties of IT products and systems. It comprises Protection Profiles (PP) and Security Targets (ST). Their concepts differ from each other in that PP are implementation-independent and ST are implementation-specific. Therefore, ST can be considered to be security objectives as well, only targeted for a different audience (product vendors and implementers). CC present a similar concept described earlier in this paper, namely "security objectives", which is the main element of PP and ST. In CC the security objective is described as to "reflect the intent to counter identified

threats and address any identified organisational security policies and assumptions".

CC defines security functional requirements and security assurance requirements. Functional requirements define the desired security behaviour, while assurance requirements enable an assessment of the trustworthiness in the effective implementation of the specified security measures. CC exclude the following security features: evaluation criteria pertaining to administrative security measures not directly related to the IT security measures, evaluation of the technical physical aspects of IT security specifically, evaluation methodology or the administrative and legal framework under which the criteria may be applied by evaluation authorities, procedures for use of evaluation results in product or system accreditation or as the subject of criteria for the assessment of the inherent qualities of cryptographic algorithms. Figure 6 depicts the major elements that form the context for evaluations.

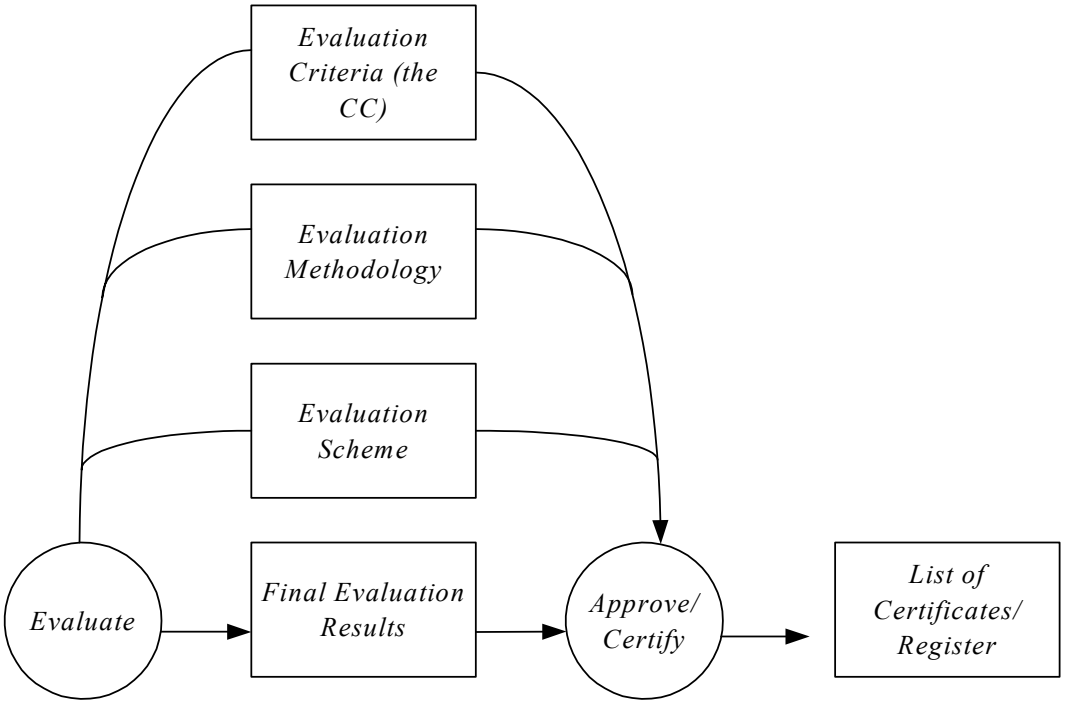


Figure 6. Evaluation context of the Common Criteria (Common Criteria, 1999).

2.6.2 Best practises

Best practises are established security procedures for certain activities, sometimes based on experience or determined more formally, for example, by applying a standard or checklist. Examples of best practises are instructions for handling e-mail in a secure way, keeping documents safe and how to act in case of a virus attack.

2.6.3 Security baselines

Establishing security policy is related to business management issues, as it requires the upper level management to be concerned about the level of IS and undertake actions for resolving it. Policy establishment can be done with the assistance of a consulting firm, that offers expertise to understand, review and learn the methods and techniques needed to develop and implement the security baseline for an organisation. The purpose is to reduce risk, limit liability and improve the business process. The gained baseline is used to identify the suggested minimum physical, operational and information security framework requirements necessary to run an organisation. Therefore, the concept of establishing security baseline is a reminder of the concept of risk management.

2.6.4 Due diligence

Due diligence refers to applying expertise in order to manage information security. It is needed, for example, when outsourcing services and implementing activities where the security level of the business partner (outsourcer) is detected.

2.6.5 Maturity models

Maturity models provide IS requirements that an organisation has to fulfil in order to reach certain levels of IS maturity. The requirements of the lower levels have to be fulfilled in order to reach the higher level.

One of the most used maturity models is SSE-CMM. The purpose of SSE-CMM is to act as a tool for determining the organisation's capability of providing security products, services or operations. It defines activities for improving security in the organisation, called Base Practises (BP), which are associated within a certain Process Area (PA). SSE-CMM defines different maturity levels from 1-5, with 5 being the highest. Each can be achieved by fulfilling the required Generic Practises (GP) and certain BP's in the corresponding PA. The SSE-CMM process is illustrated in Figure 7. The method for appraising the organisation's system security engineering process capability and process maturity defined in SSE-CMM is presented in the SSE-CMM Appraisal Method (SSAM, 1999). The metrics system consists of Process Metrics and Security Metrics. The latter is defined by Kormos et al. (1999): "A measurable attribute of the result of an SSE-CMM security engineering process that could serve as evidence of its effectiveness. A security metric may be objective or subjective, and quantitative or qualitative". Therefore using one requires the use of the other.

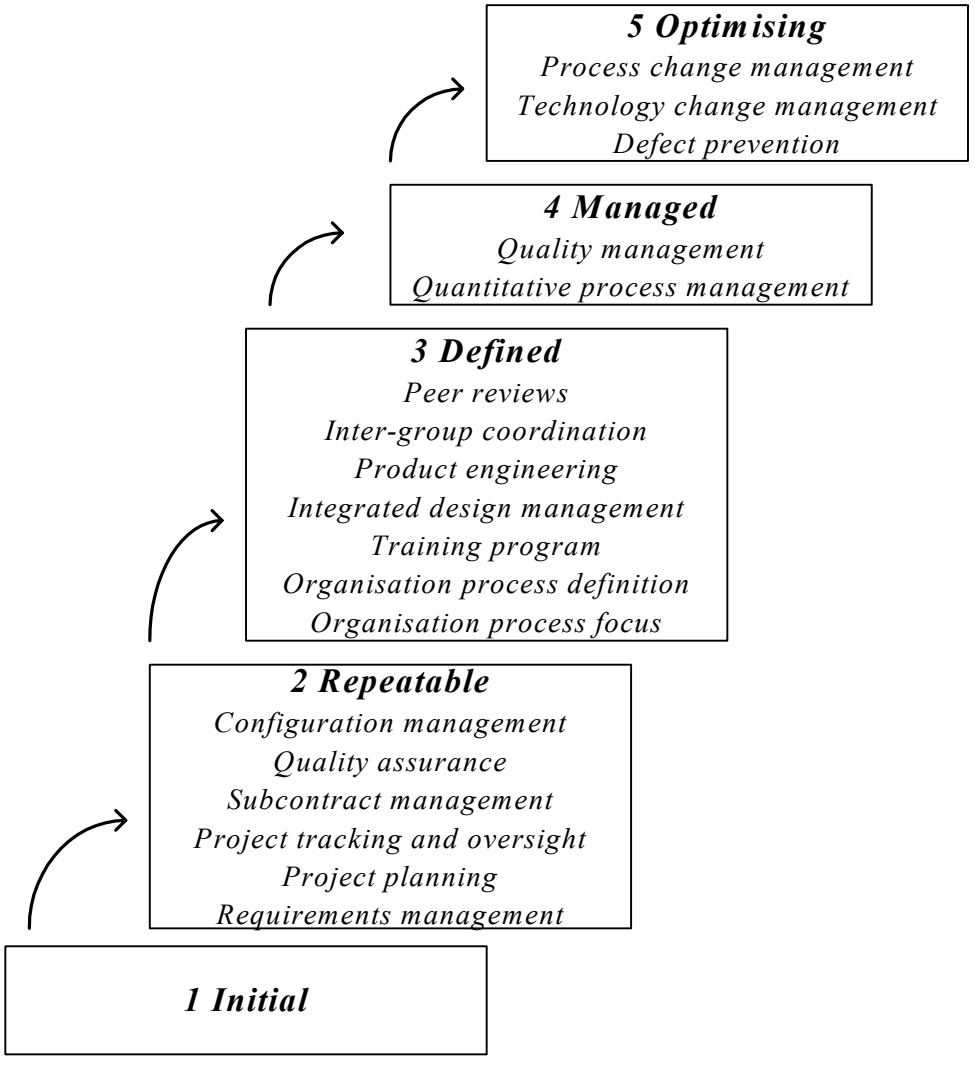


Figure 7. Continuous Capability Maturity Model (Kormos et al., 1999).

The weaknesses recognised in this model are the ones generally associated with in maturity models. They do not adjust to the organisation's characteristics; instead they require the same attributes to be fulfilled from all that apply this method, whether or not it is relevant to the security of the organisation in question. Instead, the maturity models might ignore security requirements that are highly essential for the organisation. Kormos et al. (1999) recognise this by stating that, for example, maturity level number 3 is not completely applicable for service provider types of organisations. It does not require measurement of

the security of the customer's system as a result of applying security engineering processes in the target organisation, even though this was considered to be essential.

2.7 Methods of measurement

Methods of measurement according to Katzke (2001) include direct testing (like functional, red team and penetration testing), evaluation, assessment (like risk and vulnerability assessment), accreditation, training, education and level of competence as well as observation of system performance, such as intrusion detection. The methods of measurement are compared in Table 3.

Table 3. Methods of measurement.

Method of measurement	How applied	Expected result	Example
Direct testing	System state is assessed by testing its qualities	Operational state of a system	Penetration testing
Evaluation	Security measures are compared with criteria	Baseline establishment, suggestions for improvements	Audits
Assessment	Security measures are assessed	Prioritised actions, suggestions for improvements	Risk analysis techniques
Accreditation	Security measures are assessed	Possible certificate, suggestions for improvements	ISO 9000 Series Certificate
Training, education, level of competence	Personnel and organisation knowledge is assessed and increased	Possible certificate, improvement in individual expertise	Conferences, skill tests, meetings
Observation of system performance	System is monitored with technical tools	State or quantity of some technical feature in a certain moment or period	Intrusion detection, network load measurement

2.7.1 Direct testing

Penetration testing is used during the development process, as part of the certification and accreditation, and to reflect the current operational state of a system. Process-based penetration testing (methodically conducted and repeatable) versus ad hoc penetration testing is the only resource available to accurately assess the state of a given system. Penetration testing is an accurate way to assess the state of a system. (Henning, 2001).

Penetration testing is a proactive way to measure security incidents. As an example of the versatile opportunities for test method implementations, Codenomicon's testing tools test the protocol interface for IS defects and robustness shortcomings. The testing tools are based on the work done by the PROTOS-project (Kaksonen, 2001). These kinds of tools can be used for example in:

- Establishing a baseline for new implementations of a protocol,
- Acceptance testing,
- Product evaluation, and
- Regression testing.

2.7.2 Evaluation

Evaluation is independent assessment of the security measures' efficiency in meeting a given set of requirements. Evaluation is carried out against certain criteria, such as CC, with which some baseline is first established. The concepts for evaluation of the security target (ST) include:

- Target of evaluation (TOE),
- Threats to be countered,
- Security objectives to be met,
- Security functionality to be implemented,
- Assurance level to be reached by the product,
- Claimed minimum strength of security functions/mechanisms, and
- Criteria against which the evaluation is to be performed.

Evaluation methods can be divided into:

- Analysis of deliverables/evidence produced by the developer,
- Site visits,
- Testing (replay of developer tests, complementary conformance tests or penetration tests), and
- Independent vulnerability analysis.

This measurement method classification is not exclusive, as, for example, penetration tests are not only an evaluation method but also a direct testing method. On the other hand, the definition depends on the applied area and conceptual environment, like the employed standard. Two evaluation types can be recognised: concurrent, where TOE is under development and consecutive, where TOE is already developed and implemented.

2.7.3 Assessment

Assessment refers mainly to risk or vulnerability assessment. Vulnerability analysis, applied in conjunction with penetration testing, seems to be one of today's most common assessment measures. Risk assessment is often needed before IS functions can be applied, in order to prioritise the organisation's assets, their threats and to resolve what actions are needed to protect them. The main steps in risk management are recognising the risk, analysing it and controlling the risk. The last part is therefore excluded in actual risk assessment. One approach for assessing the quality of different assessment methods and tools used in workplaces is a method presented by Mikkonen et al. (2003). They present techniques that can be used either separately or combined for assessing the applicability of certain risk assessment methods. These are questionnaires, interviews, SW usability tests, web questionnaires, and a development group composed of users.

2.7.4 Accreditation

There are several commercial as well as governmental IS accreditation services and projects available. As an example of accreditation criteria, NIST's project FISMA's (Ross et al., 2004) purpose is:

- Promotion of the development of standards and guidelines to support the Federal Information Site visits,
- Security categorisation of information and information systems in accordance with the Security Management Act,
- Selection of appropriate security controls for information systems,
- Verification of security control effectiveness and determination of information system vulnerabilities, and
- Operational authorisation for processing (security accreditation) of information systems.

2.7.5 Training, education and level of competence

Training is relevant for producing relevant and necessary security skills and competency, education for integrating all (security skills and competencies) into a common body of knowledge and adding a multidisciplinary study of concepts, issues, and principles. (Wilson, 1998). Level of competence can be determined by meeting a standard through application of evaluation or measurement criteria that is carried out by appropriate organisations or certification.

2.7.6 Observation of system performance

Examples of the most common system performance observation techniques are intrusion detection techniques and network load measurements. Hence the gained results represent mainly technical IS*.

The goal of an Intrusion Detection System (IDS) is to detect an intrusion of an information technology system as it happens by monitoring it, and to be able to respond to the intrusion (Babaoglu, 2003, Science Applications International Corporation, 2002). An IT system may range from a computer system to a computer network. An IDS consists of sensors, scanners and analysers, with optional elements such as load balancing and management units. Sensors and scanners collect information regarding IT system activity and vulnerabilities, and they forward the collected data to analysers. Analysers perform intrusion analysis and report on the collected information. (Science Applications International Corporation, 2002.)

There are two concepts that relate closely to the measurement technique of IDSs: false positives and false negatives. A false positive is a situation where something abnormal (as defined by the IDS) happens, but it is not an intrusion, whereas a false negative is a situation where an intrusion is really happening but the IDS does not catch it. Thus, the goal of an IDS is to find intrusions and, in addition, to minimise both false negatives and positives in order to obtain accurate results. (Babaoglu, 2003.)

IDSs can be characterised by the data source (i.e. where the audited data is collected from), or by the models that intrusions represent. Thus, the IDSs can have different kinds of detection mechanisms. Characterisation by data source divides IDSs into host-based, multihost-based and network-based. Different intrusion models are the anomaly detection model and the misuse detection model. When using the anomaly detection model, the IDS detects intrusions by looking for activity that is different from a user's or system's normal behaviour, whereas when using the misuse detection model, the IDS detects intrusions by looking for activity that corresponds to known intrusion techniques (signatures) or system vulnerabilities. (Babaoglu, 2003.)

2.8 Building a security metrics program

Payne (2001) proposes seven key steps for guiding the process of building a security metrics program. They are:

- Defining the metrics program goals and objectives,
- Deciding what metrics to generate,
- Developing strategies for generating the metrics,
- Establishing benchmarks and targets,
- Determining how the metrics will be reported,
- Creating an action plan and acting on it, and
- Establishing a formal program review/refinement cycle.

Another approach, the NIST's metrics program by Swanson et al. (2003), consists of the four independent components: Results-Oriented Metrics Analysis, Quantifiable Performance Metrics, Practical Security Policies and Procedures, and Strong Upper-Level Management Support.

Leach's (2003) definition is much more abstract, but it recognises the key problems in the IS* development area well. He suggests four steps to be taken when aiming towards better IS* solutions:

- The first would be to take a fresh approach in a sense that one should have an attitude towards learning to interpret data in a reliable way, not according to beliefs,
- The second step would be to develop a framework for describing the security characteristics of threats and solutions in terms that can be quantified. The essential aspect pointed out here is that "we need an agreed definition of what the security dimensions are and what their yardsticks should be so that our security terms can be quantified",
- The third step would be to develop mechanisms for quantifying risk aversion and how much insecurity business management is prepared to tolerate for a given system or environment, and
- The fourth step, "calibrate security steel, our security components", is essentially the easiest part once the appropriate methods and practises would be at hand.

Bayuk (2000) presents an audit-based approach, which utilises audit steps as the basis for metrics. Her approach contributes to defining the objectives of information security controls and the corresponding system control framework, then processing the audit steps that cover both, i.e. the steps to verify that the control objectives are met.

These different approaches are examples of the many methods available for constructing an effective security metrics program. Despite the differences, they all agree on the importance of understanding the framework and establishing the security objectives that are to be measured and met by the metrics.

2.9 Results of the literature study

According to the literature study, IS metrics are an ambiguous concept, but are at least an attempt to achieve a numeric or non-numeric value describing the level of some security attribute. Techniques vary depending on the security objective and the object being measured.

There are several classifications available for IS metrics according to their use, their users, or the method or standard applied (for example CC). The definitions for security objects and varying methods of measurement concepts may overlap and depend on the applied area and the conceptual environment. The classification of Henning (2001) and Katzke (2001) were discussed to gain understanding of the diversity of the area.

One of the most disturbing problems is, as Nielsen (2000) summarises, that there is a need for a common vocabulary, a common basis for communication. According to her, there is also the need for more and continued interaction and sharing between and across civilian agencies and the national security community. The other areas that require attention to are the need for increased awareness and attention to information security, the need for increased resources and the need for more personnel skilled in security technologies and techniques. When building a security metrics program, one can find and utilise numerous guidelines. They all share some common basic features, with the establishment of security objectives being the most essential one.

3. Interviews

According the diverse definitions of IS metrics in the literature, it can be expected that the interview answers are varied and dependent upon the interviewee's job description and organisation's field of activity. Based on Henning's (2001) discussion of organisational IS*, it can also be expected that, to some extent, government organisations use a more structured process. This results in a slower development speed than that of commercial representatives, as they are more committed to the standards.

However, Yliluoma (2001) points out that hypotheses should not be generally made before carrying out a qualitative interview. This is because the purpose is to gain new knowledge and to find new areas that cannot necessarily be derived from theory. An open attitude is therefore needed when defining interview themes, even though some expectations and preconceptions assist in this.

3.1 Interview questions

The interview questions were formulated in a way that they would not be too focused on comparing the level of security metrics between the organisations in the analysis. Rather, the purpose was to resolve and analyse the situation generally, and the factors behind situations, which in turn required that the individual features of different organisations to be taken into account.

However, a classification model is needed to analyse the state of the organisations as well as to assist in analysis. Therefore, the models of Katzke (2001) and Henning (2001), are used for this purpose. Furthermore, the aim is to discover the needs and opinions about the use of metrics in order to get state-of-practise information for the metrics research. This means that there is a need for some questions that allow the interviewee to express their own individual expertise, without being limited to the viewpoint of his/her own organisation.

Seven interview themes were chosen. The themes covered 20 questions that could be adjusted during the interview according to the answers. If the answer had already been given in earlier questions, it did not have to be asked again. It can be criticised that some of the questions are too detailed for the theme

interview method. However, this was considered to be the appropriate approach, as the topics represent diverse concepts for different people, and the purpose was to be able to compare the answers to some extent.

3.2 Characteristics of qualitative analysis

According to Myers (1997), there is no clear distinction between data gathering and data analysis in qualitative research. For example, from a hermeneutic perspective it is assumed that the researcher's presuppositions affect the gathering of the data - the questions posed to informants largely determine what you are going to find out. The analysis affects the data and the data affect the analysis in significant ways. For this reason, he prefers to speak about *modes of analysis* rather than *data analysis* in qualitative research. According to him, modes of analysis are different approaches to gathering, analysing and interpreting qualitative data. The common thread is that all qualitative modes of analysis are primarily concerned with textual analysis (whether verbal or written).

It is also difficult to distinguish between data collection (interviews) and data analysis in this study, since the research was cyclic and analysis of the material began while the questions were still being asked. The questions were adjusted according to the answers when necessary in order to get a true understanding of what the interviewee was explaining. Often there was a need for specifying questions.

It seemed that the interviewees had quite a realistic view of the issue, because they were able to discuss the weaknesses and the advantages of their current practise and the situation of IS metrics in general in the industry. The opinions and views offered a valuable basis for the interpretation, and it indicated a strong interest in the issue. Hopefully, the interviews acted, in their own way, as a catalyst to focus attention on the issues of IS metrics and its development in general.

Before the interviews, it was assumed that there would be varying answers both with respect to the content and views of the issue. This was because the

organisations represented divergent operational environments and also because the interviewees held different positions in their organisations.

Eskola & Suoranta (1998) agree that there are no unambiguous instructions for interpreting results in qualitative analysis, but according to them, two principal approaches can be considered for this. The first is to make interpretations straight from the material; the other is to use the material as the basis or tool for theoretical thinking or as the basis for interpretations. The theories that are used in analysis are merely an assistance tool for interpretation, helping to describe the phenomena in the text.

The group of organisations considered in this study can be considered to represent a part of the Finnish organisation types, but not a pure basic group. Consequently, the results have to be treated like concepts of the reality more than a fundamental set of it. Thus, the analysis work concentrates on understanding reality rather than explaining it. There are hypothetical causal connections presented though, so the analysis method does not purely represent understanding reality. However, the results cannot be purely generalised, i.e. the causal connection does not necessarily apply to any organisation. There are unknown factors that would need a more profound study to be carried out in order to make such generalisations.

3.3 Analysis approach used

Myers (1997) discusses three different approaches to analysing qualitative data: hermeneutics, semiotics and narrative/metaphor. Hermeneutics is primarily concerned with the meaning of a text or text-analogue. The essential idea of semiotics is that words/signs can be assigned to primary conceptual categories, and these categories represent important aspects of the theory to be tested. The importance of an idea is revealed by the frequency with which it appears in the text. The word “narrative” is defined by the Concise Oxford English Dictionary as a "tale, story, recital of facts, especially a story told in the first person." Metaphor is the application of a name, descriptive term or phrase to an object or action to which it is not literally applicable (e.g. a window in Windows 95). (Myers, 1997).

The approach that was used for interpreting the results was more or less hermeneutic, even though the method can also include elements of the other approaches. According to Myers (1997), the use of hermeneutics in information systems research is justified because the object of the interpretative effort becomes one of attempting to make sense of the organisation as a text-analogue. Therefore, the aim of the hermeneutic analysis becomes one of trying to make sense of the whole, and the relationship between people, the organisation, and information technology. Because the purpose was to discover IS metrics use that encompasses the whole organisation, people and technology, the approach seemed appropriate. In addition to presenting his/her own opinions, the interviewee describes and speaks for the whole organisation, aiming to reveal how the entire system is organised. The questions were targeted to discover different aspects of organisations, for example, from the operational point of view (risk analysis, strategy), the technical point of view and hierarchy (personnel questions). In addition, there was emphasis on the interaction between the interviewee and interviewers in order to better understand the answers. Thus, the hermeneutic interpretative view can be justified.

3.4 Interpretation of the answers

The results of the literature study were used to help with interpretation of the interview answers. However, as Yli-Luoma (2001) points out, all information gained by interviews cannot be necessarily derived from theory, because a qualitative interview particularly strives to discover new areas of knowledge.

The target organisations represent different lines of business and sizes, but they are all either medium or large-scale organisations. Unfortunately, neither the names of the organisations or the interviewees can be revealed because of the sensitivity of the subject. Nor can the whole interview of any organisation be shown in this study for the same reason. In the following, answers will be discussed according to the themes. No particular order will be followed when processing the answers, i.e. the implemented interview order does not have any effect on the answer order. The themes used are described in Figure 8.

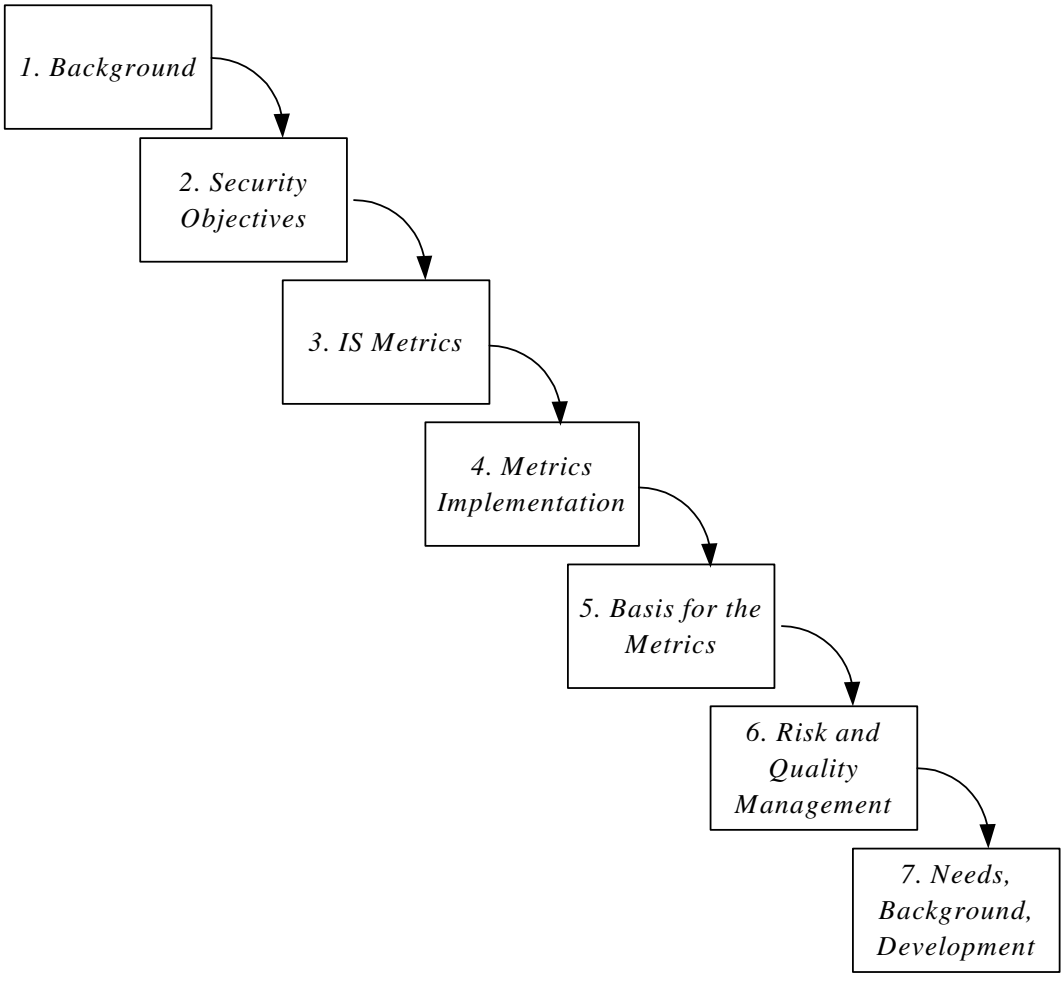


Figure 8. Interview themes, in the order the interviews were carried out.

3.5 Theme 1. Background

Question 1.1:

1. Background, branch (personal professional details, organisation).

Background needs to be resolved in order to facilitate interpretation of the answers from the researcher's point of view.

The interviewees represent the following professions:

- Product manager (IS services),
- Data administration manager,
- Internal audit representative,
- Senior technology manager,
- Main architect of system management,
- Administrator and network design responsible (part of IS programming group),
- Expert on quality management (venture knowledgist), and
- Product manager of IS products specialised in risk management and IS inspections.

3.6 Theme 2. Security objectives

Question 2.1:

2. Security objectives in your organisation. How is responsibility for them assigned?

Interpretation of answers to Question 2.1:

It can be seen early in the interview answers that the security objectives are dependent on the organisation, and that business corporations typically emphasise business continuity, while state institutions focus on congruence with legislation. One interviewee emphasises that before defining the security objectives, the situation has to be considered from the viewpoint of the organisation and particularly by those that run the organisation, not by the experts: "*and there is a contradiction as the IS experts consider it from the viewpoint of expertise"*. Thus, the situation is best understood by the management that have total responsibility for the company. Only after that can the objectives be derived from the corporation's strategy.

As seen from the results, the same business-oriented principles and views cannot necessarily be applied in state institutions when defining security objectives. This indicates the same phenomena that Henning (2001) recognised concerning

organisational IS*. National and organisational policies are more determinant factors in state institutions, and commercial organisations rely more on the personal judgements of the security practitioner.

One of the industrial corporations described the objectives, but referred to the situation as "*according to the measurements, it is a bit better than the average*" indicating that there are not only objectives behind the actions, but their effectivity is also evaluated. A summary of the results of Question 2.1 is given in Table 4.

Table 4. Security objectives behind security actions in state institutions and industry.

State institutions	Industry
❑ **Maintain and build customer trust** ❑ **Ensure** safety of the **money flow process** in the organisation and between it and its interest groups ❑ **Backup main activities** ❑ **Ensure congruence between the main tasks and legislation** (also when the organisation mission is changing, back up the change) ❑ Keep **network open and usable**, do not tighten IS policies, not too a heavy hierarchy	❑ **Integrate IS work into business processes**, **ensure business continuity**, because business is based on information networks and information systems ❑ **Backup corporation's business strategy**

The responsibility of IS is mainly divided according to location or functional unit and between top management and security staff. The CEO usually has the main responsibility and the IS managers have responsibility for the expertise. The responsibility of the top management affects the whole company, as they decide how the IS responsibilities are divided, whether the IS staff is professional enough to handle IS issues and whether the IS staff is granted enough resources and rights. The management should be aware of IS issues as they should be ultimately responsible for all company issues. See Table 5 for a summary of the responsibility division in organisations, classified into state institutions and industry.

Table 5. Responsibility division in organisations.

State institutions	Industry
❑ In line organisation within **security departments**, business units responsible for their own IS ❑ **CEO: final responsibility**, **IS manager:** general instructions and administrative actions. **IT unit**: technical architecture. **IS manager:** education and dissemination ❑ Assigned between **Safety Manager and IS manager**, **Branch Managers:** final responsibilities, **Data Administrator Managers:** responsibility **unit (location) level**	❑ Important **sub-areas** have an **owner** and actors. ❑ **IS manager** is organisationally responsible to **Administrative Manager**, in a crisis directly to **Business Manager.** Issues presented either through official channels or directly to **Management Group**. Employees responsible for own tasks (defined in IS policy). ❑ Security in **change process**, **CEO** responsible according to directive rules, but **in practise Administration Manager** responsible → tasks transferred to **experts**

Question 2.2:

3. Documentation and description of security objectives. Are they documented e.g. as policies and procedures?

Interpretation of answers to Question 2.2:

The interviews resolved that in general, IS documentation is handled more formally in industry organisations than in state institutions. Tables 6 and 7 explain how the documentation of security objectives is handled. The importance of good policies is understood, but maintenance is seen as the most critical issue. One approach to policy handling is the *constructive approach* meaning that policies are constantly validated so that all details in it could be implemented, otherwise it should be changed. This is the hardest part. In addition, there were signs of using too many resources for doing extra work:

"There are very strict procedures because of the lack of policy (things are handled 'just in case'). The strictness can sometimes be even restricting."

The main weaknesses are the lack of personnel responsible for IS and the unclear responsibilities making documentation maintenance hard when situations change. The benefits of the policies are clearly appreciated but good

ways to implement them are needed. In addition, a complicating factor in policy maintenance is the complexity of the systems, which is constantly increasing.

Table 6. Documentation of security objectives in state institutions.

Opinions	Complicating factors in policy implementation and development
❑ The most important feature in the policy is the **awareness** that it brings. ❑ If a policy is **general and flexible** enough, it can be more easily adjusted and updated. Incidents provide material for this.	❑ Personal issues like **responsibility division** cause the most confusion. ❑ **Heterogeneous organisational architecture** complicates policy update. ❑ Because of **complex systems policies and procedures accuracy is only on the general level**, according to system units.

Table 7. Documentation of security objectives in industry organisations.

Opinions	Requirements for knowledge management	Complicating factors in policy implementation and development
❑ Good policy: **close to practise, updated** and **monitored** several times a year, a **constructive approach** ❑ Policy should be **in line with the organisation structure** and **general guidelines** for actions, **not too accurate**. ❑ Should be **constructed by those that run the organisation** ❑ **Specific instructions will always exceed** the policy.	Documentation **requires defining the responsibilities** appropriately. **Tacit knowledge** is often forgotten.	Documentation mostly handled well, **no IS responsible person**. Document **update** and **version management** responsibility **unclear**

Implementing working and realistic documentation requires constant dialogue between work practises and documentation update. One approach describing that is learning environment (see Figure 9). It includes circle, process-like motion, where tacit knowledge is transformed into an explicit form, documentation, which then produces new tacit knowledge as it is applied in practise. Documentation is explicit knowledge, but the value of tacit, implicit knowledge is often forgotten. This, however, constitutes a large amount of all knowledge. Thus, the significance of documentation can be maximised when it is combined

with the tacit knowledge and both complement each other in a "learning organisation"; a constant process where both develop each other.

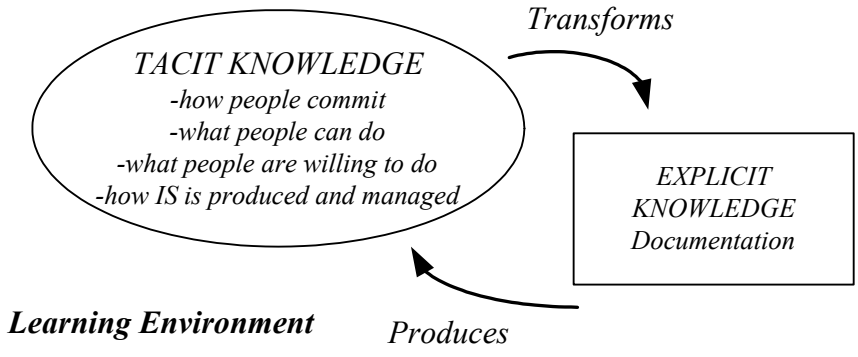


Figure 9. The organisation as a learning environment.

3.7 Theme 3. IS Metrics

Question 3.1:

4. How is the concept of information security metrics understood in your organisation?

Interpretation of answers to Question 3.1:

IS metrics is usually understood as *evaluation* (auditing, vulnerability analysis, penetration testing) or as *observation of system performance*, presented mainly by technical IS*, such as logs and firewalls. The different meanings understood by the term are described in Table 8 and classified according to the methods of measurements presented previously in Table 3. It must be noted that the different measurement methods are not exclusive and in some cases not necessarily even comprehensive for describing the method used in the organisation.

Table 8. Metrics in different organisations.

State institutions	Method of measurement
How employees act (e.g. how many hours are **external connections** used, what types of connections), reported to nearest superior if needed. Audits, internal and external.	Observation of system performance, evaluation
Monitoring the **network reliability** (certain points checked)	Observation of system performance
Server, network disk and e-mail monitoring as security metrics for the disk quota monitoring	Observation of system performance
Yearly assessment of implementation level with respect to conformed policy, part of the quality system yearly inspections, conducted **by the head of the concern**.	Evaluation/assessment
Every **business unit** sees that **policy and procedures** are heading in the right direction.	Evaluation/assessment
Attacks against IS, scenarios that are implemented in practise	Direct testing
Auditing once: **technical testing** was carried out, **boundary protection** monitored → could be carried out in a shorter time period, like every 2 years.	Evaluation/assessment/direct testing
Industry	**Method of measurement**
Ensuring **IS in computers** in the **information system conform** with **software and systems**	Observation of system performance
Product security, difficult: **complex** software, every level and combination should be known. In practise, accomplished by the **comprehensiveness of the tests**.	Direct testing
Yearly audit with partner, **technical and administrative** audits	Evaluation/assessment
Amount of incidents, their cause and origin	Assessment

Auditing and system evaluation is used externally with consultants or partners and internally with different methods. There are opinions that auditing should be a continuing, process-like action and for some it is that already, being for example part of the quality system. An example of an evaluation method:

"...vast penetration test, they pretended to be hackers and on our side only a few people knew about this. The reactions of the administrative personnel and how

well the process worked were observed and a meeting was held about it afterwards. We gained good knowledge but a few critical details were revealed, which was good. Audits are usually carried out by another party; we do have internal inspections, but nothing systematic."

The following issues should be considered when IS measurements are generated for the system:

- The most important thing is to find out the phenomena and objects in the organisation that are connected with IS,
- Corresponding indicators have to be found which describe the phenomena, and
- It has to be resolved how the indicators could be measured.

Almost every respondent mentioned the human factors and estimated their effect on the IS. It is clearly considered the hardest, most significant and most challenging issue to be measured. An interesting note, from one of the interviewees is that *"More than the fact that we measure, the idea, common belief that you are measured, works best"*. This refers to the concept that personnel do not necessarily know if they are being monitored, but they might suspect that their actions are being detected somehow. This can cause them to act in a more secure way, even if they were not actually monitored.

There are some experiences of measuring personnel behaviour and increasing their awareness about IS (individual IS* by Henning, 2001):

- IS should be part of quality and quality assurance,
- IS should be part of a merit pay system, so that the used means would be "a carrot instead of a stick",
- Measurement has to be objective, and
- Measurement has to be controlled somehow.

But:

- It is hard to find metrics for measuring the IS level of work practices when the employee implements IS in his/her work.

One answer to this is web questionnaires. Interviewees of this study have the following experiences of web questionnaires:

- E-learning methods have been applied to promote IS education, and it has IS measurement connected to it,
- Questionnaire reliability is uncertain *"A person answers just what he wants to answer, especially if there is a merit pay system"*,
- Questionnaire information can be transferred to a personal register according to the answers and it is usable and utilisable, and
- One way to motivate people to respond is prizes.

One factor affecting the absence of a need for measuring the personnel IS behaviour issue in certain organisations could be their open working culture. They have an open and flexible atmosphere, and tasks divided are indirectly among the skilled operational group. There is clearly an indication of personnel trust and appreciation for the responsibility.

Question 3.2:

5. What kind of security objectives cause the need for IS metrics?

Interpretation of answers to Question 3.2:

According to the interviews, the origin of state institutions' security objectives is usually a compromise of their own action group recommendations and the legislation directions. The most common objectives that cause the need for IS metrics is the effect on the personnel IS behaviour and ensuring the business goal and fulfilment, as presented in Table 9.

Table 9. Security objectives causing a need for information security metrics.

Security objectives	Related issues
State institutions	
Confidentiality, access control monitoring, integrity	Protection of existing information
Maturity of the IS processes, responsibility assignment, reporting activities	Pervasive IS process
Industry organisations	
Measurement of work practises	System administrators are big risks. ❑ Skills good, but the morale can be low. ❑ Low usability caused by laziness, inexperience, negligence → threats
Measure personnel behaviour and **integrate** it in**to the** used **business process assessment techniques** in quality monitoring.	Personnel behaviour is one of the greatest risks. Integration would raise process effectiveness.
Raise personnel awareness so that they would pay attention to IS in their routine work tasks.	No ways to measure it now; benefits gained by reducing incidents caused by ignorance.
Enable business	Resolve the level of IS where incidents are manageable and understandable.
Availability of the network	Importance of the indicators: resolve which equipment is working and whether the network is functioning.
Integrity/accuracy, availability and confidentiality	Attributes can be described with certain phenomena; some have many aspects.

3.8 Theme 4. Metrics implementation

Question 4.1:

6. Metrics implementation in practise. Can it be described as a process?

Interpretation of answers to Question 4.1:

Experiences of metrics are described in Table 10. The implementation is generally handled as a process in industrial and larger-scale organisations. According to one interviewee, there are four issues that have to be considered in IS metrics development and implementation:

1) Meaning
2) Who measures
3) Methods (depends on 1 and 2)
4) Classes of inspection

A problem in metrics implementation is the absence of processes. Interviewees are not that worried about the kind of metrics they lack, but rather the process concerning the current metrics use, or the lack thereof. It can be concluded that even though there are a variety of different measurement technologies or methods are applied, they cannot be considered as useful as if they were applied as a process-like manner. The most hindering factors in this seem to especially be the lack of readiness or ignorance of the top management to commit to IS issues, together with an absence of documentation caused by unclear or inappropriate responsibilities. This indicates that the personnel involved should have the right expertise. Futhermore, metrics use should be part of quality thinking and corporate management, so that it would become a part of yearly planning. Responsible persons should be at least somewhat aware of IS issues:

"The Quality Manager does not necessarily know what the results are and how they should be assessed and verified and what they should be compared with."

One example of the processes used is the cyclic evolutionary process, where development and implementation phases are located on different sides of the cycle, which changes every six months. However, the processes complement each other constantly:

"There is always a development process and implementation process ongoing simultaneously, and at the same time as we develop, we gather material for implementation. For example, if we make a script and see how it works in practise, the practise gives us material for improving the design."

Table 10. Metrics implementation in organisations as a process.

Metric process in the organisation	Problems and requirements
State institutions	
❑ **Firewall, virus control** and **server-side** administration (e-mail control), metrics process restricted to **using standards** ❑ **Two-sided actions** with partners involving process activities (e.g. reporting) → improvement strategies → learning process ❑ **Cyclic evolutionary process** model: theory and practise combined	❑ Inside business units the process is **not well managed** because of the **complexity of the environment.**
Industry organisations	
❑ The process is an essential concept because "unless it is a process, it is random", and can not be improved	❑ Processes are not documented, it is unclear how things are applied in production → **responsibilities open** ❑ **Has to be integrated into quality** and **management**, problem finding metrics

Question 4.2:

7. Responsibility for metrics implementation.

Interpretation of answers to Question 4.2:

The responsible persons for metrics implementation are mainly operative personnel. There are again some opinions about the management's effect on responsibilities and thus the functioning of the organisation, as can be seen from Table 11.

A notable problem related to the responsibilities is its effect on the costs:

*"In fact it is a **remarkable cost factor**, say when you are detecting connection traffic speed, for example usability issues…there might be some application that is very jammed, and they can't be used because the connections are so jammed. The fault may be server capacity sufficiency or weak connection speed. It is extremely hard to understand that we think, ok, let's raise connection speed, let's buy a server that costs 20,000 euros, so it is expensive. However, no one*

considers that if 20 people are idle for a week, it does not cost anything. There is a huge contradiction. The real expenses are huge."

This indicates that there is:

- Not enough understanding on the management side, difficulties in explaining and concretising issues, and
- Expense-focused thinking.

Table 11. Responsibility division for metrics implementation in organisations.

Government	Industry
❑ Normal division like the **normal IS division** ❑ **Operational staff** of IS and data communications techniques (5–10 people) ❑ **Centralised IT department** maintaining vulnerability table managed by system administrators, vulnerability tool development within units, **information security group** responsible for risk analysis ❑ **Administrative group** responsible as a unit: implementation and design knowledge and tasks, ideas for changes from user response	❑ **Division in site-level** and in production according to **certain functionalities**, on the architectural level. Both geographical and architectural level **based on the location** ❑ **Every process has an owner**, who is responsible for an adequate level and the functionality of the process ❑ **IS design and maintenance responsibility** with **system administrators**, responsibility for measuring how well instructions are followed is difficult

Question 4.3:

8. The relationship of IS metrics process to work flow processes. Is it embedded?

Interpretation of answers to Question 4.3:

Only one respondent utilises a process model that can be understood as completely embedded: a cyclic evolutionary process model. The other organisations' IS metrics processes are more or less random and separate from other processes. However, the interviewees recognise the need to have the IS metrics process integrated into other processes. There are clear views about how it should be done and what kind of development can be expected. Table 12

illustrates the opinions and experiences concerning IS metrics process development.

In general, the problem is that IS metrics are not applied as processes. There are some processes implemented, but they do not cover the whole system. In addition to this, some IS metrics processes can be hard to point out, not to mention integrate into the system. Factors that affect the metrics process evolution are legislation restrictions and responsibility questions.

Table 12. IS metrics process development.

Opinions and experiences regarding the IS metrics process	**Problems and development suggestions**
State institutions	
❑ **System scanning embedded,** easy: networks planned and not public → no legislation problems ❑ **Corporate tolerance concept** will most likely affect how processes are embedded. *"...so that in the future, the CEO most likely has to give warrant, he himself has to sign the contract."* ❑ Pressures to improve processes in a way that the **work processes** built **can be supervised** in order to prevent misuse.	❑ Aim: **embed processes in quality management processes**, part of the quality manual → tailored requirements analysis/standard → basis for IS ❑ Biggest challenge to get measurement embedded → **no means or operation models** ❑ In some network-related activities **legislation** deterrent or problematic
Industry Organisations	
Physical side (access control): easily embedded in actual work (education and motivation) as **immaterial requirements like quality** → hard to see the presence → comes along by knowledge	**Certificate** not a complete solution, a way for an organisation to find a suitable level of requirements analysis and to **prove IS level**.

Question 4.4:

9. Validation of the gathered metrics data (testing, reviews, verification). How is the responsibility allocated?

Interpretation of answers to Question 4.3:

In general, there is no concern about the same personnel implementing and validating the data. There are no opinions, for example, regarding dangerous work combinations, where there is a risk caused by the same person operating the metrics and validating it. The same personnel that operate the metrics usually handle the validation, often due to their experience and because there are no other procedures defined for this. Typically, interviewees understand metrics as logs and network management; thus the answers concern validation of them. Table 13 presents how the validation is handled.

The problem concerning validation is that often there are no separate IS responsible people for validating metrics, but the need for one is common in most organisations.

Table 13. Validation in organisations.

State institutions	Industry
❑ **Monitoring approach** in metrics implementation ❑ **Operative staff validates, access rights** and **log storing**: accurately defined and restricted ❑ In a **reactive situation logs are beneficial**, would be even more so if they could be systematically used. ❑ **Network-related testing** by using it constantly when network functions are essential ❑ **Administrators handle together** and share observation responsibility, one person for tracing individual incidents	❑ **Handling is reactive and all processing is in the same place.** ❑ **Product security** is **also tested** with IS-emphasised testing.

Question 4.5:

10 a) Use of technical metrics. E.g. network load measurements, intrusion detection data, software security features)

Interpretation of answers to Question 4.5:

Technical metrics is used in all organisations and their implementation is more developed than any other metrics. The use, volume and quality of technical metrics depend on the organisation type. As Table 14 shows, the majority of the organisations use more reactive than proactive methods. This can relate to the lack of an IS metrics process. Intrusion detection is not very commonly used as the costs often override benefits. There are indications of interest in proactive methods:

- External threats are not considered to be as harmful as internal threats,
- One of the biggest problems is peer-to-peer software, and
- IPS (intrusion prevention system) could be a solution to peer-to-peer software problems, because it would monitor e.g. HTTP protocol, and this way IS risks caused particularly by own personnel could be blocked.

The problem associated with technical metrics use is that there is usually a massive amount of data to be analysed. There are tasks that could be automated and a need for tools that could find out the relevant data. This is the problem that especially concerns log monitoring and analysing.

Table 14. Technical metrics use in organisations.

Use of technical metrics	Organisation type		Method type	
	State	**Industry**	**Reactive**	**Proactive**
Log use extensive, no policy: "Just In Case Approach": procedures even too accurate, still not too many resources	X		X	
Network, firewall and intrusion detection management, **malicious software management**	X		X	
User load (weekly reports, logins by domain): **load generated by the network**, deviations detected from the results or from the deceleration of the network, **intrusion detection**: abnormal network traffic with alerting sniffer computers	X		X	
IS software considered **harmful:** massive code amount: a lot of defects → IS risks themselves, if network is designed, implemented and updated well, no need for outside IS SW	X			X
No intrusion detection or supervision of what SW program is launched, **protocol firewalls**, no application level firewalls, **barrier defence auditing** with **own procedures** and with **one external** auditor	X		X	
Normal analysis, IDSs under consideration, functions **reactive because of the lack of resources**, workload with **spam** mail, some **denial of services**		X	X	
Load measurement, network detection, **no intrusion detection** (**no added value,** consumes resources). **Firewall** and **log** monitoring, firewall administration, system administration and monitoring, centralised **log collection**		X	X	
Constant, large-scale external audits, administrative and technical side		X		X

Question 4.6:

10 b) Do you use technical tools for IS metrics or for a part of it? If yes, what tools?

Interpretation of answers to Question 4.6:

Organisations use many technical tools. Typically technical tools are equipment for monitoring the network, such as firewall solutions and log analysers. The tools are mainly used by operative personnel. One organisation does not use any tools at all. The following types of tools were used:

- **Self-made tools**; for example programmed tools for detecting activity of the base stations, activity of the user logins,
- **Firewall logs**, server system follow-up on the operating system and application level (using Microsoft active directory and Unix-based applications), interpreting and filtering data from data collection system,
- **Virus protection**,
- **Normal tools** by operative managers, and
- **Analysis software**: a questionnaire that provides a profile of the risks.

3.9 Theme 5. The basis for the metrics (Standards and other documentation)

Question 5.1:

11. What is the basis for the metrics that you use? A standard? Is the standard perhaps adapted for your own purposes? If so, how?

Interpretation of answers to Question 5.1:

Almost every organisation uses a standard or several of them, more or less directly. The most common standards are BS 7799 Code of Practise (BS 7799-2, 2002), VAHTI (Valtionhallinnon Tietoturvallisuuden Kehitysohjelma, 2004) and general legislation. Standards are not followed directly, rather used as guidance:

"Besides legislation, the policy is based on standards that are commonly used…but not in respect that we could be audited by the use of the standard."

"Never directly used, rather interpreted. We have tried checklists but they didn't work. Maybe the level of standards is too general? *And when you think of how they are constructed. Fellows sit around the table and think what should be done."*

"…for the purpose that essential things are considered. Would such a standard that classifies upper level issues and then different lower levels, with different priorities be useful? *Yes it would, and in fact we do that, but it happens during risk analysis."*

Question 5.2:

12. How does the standard respond to your guidelines (and procedures) for the implementation of information security?

Interpretation of answers to Question 5.2:

In every case where a standard is used, it does not respond directly to the documented guidelines and procedures, but usually partly. Almost every organisation uses a standard partially – applying it for itself:

"Not details, but issues like document classification and management instructions are quite similar to VAHTI, they respond to them, they are created through a process of consideration."

"Every application is different and it's more important to understand the idea of the framework than the actual content. Human Intelligence Approach is my favourite approach – used more an expert than a checklist. This is what I offer as a solution to all immaterial requirements. The checklist has to be read by someone who understands the basic ideology, otherwise it is useless."

3.10 Theme 6. Risk and quality management

Question 6.1:

13. Do you use risk analysis techniques? How? Is it part of your process? How do they relate to your documentation?

Interpretation of answers to Question 6.1:

Almost every organisation uses risk analysis and, in particular, somehow applied to their own purposes; some have even developed their own methods for this. For some organisations there are no systematic methods and risks are managed through practical experience:

"...how much it costs for a certain device to be down, if it costs more than the price of it then we get one."

Experiences of risk analysis techniques are presented in Table 15. It can be seen that when risk analysis techniques are applied, they are adjusted to the processes and are clearly seen as a benefit. The organisations whose work is strongly based on risk assessment results have paid more attention to it than the others.

Table 15. Experiences of risk analysis techniques in organisations.

Risk analysis experiences	Organisation
Risk analysis most **essential for the process**, no systematic risk analysis techniques	S
Work should be based on current risk analysis → used **every year**: future needs assessed with own mathematical tool, "risk mapping", neither analysis nor management	S
"**Static**": risk analysis due to developing and operation of the system, testing the system	S
Risk analysis is a **means of communication**.	S
For **ensuring availability and integrity**, light methods: for example ensuring whether certain computer or network equipment essential for the network, there has to be a backup plan for the most critical equipment. Risk analysis **managed with practical experience**.	S
No certain methods. **Security group administratively responsible**: "which is this assemblage that has only collective responsibility, which, in my opinion, does not work with any issue concerning security; it is just a discussion forum."	I
Threat analysis: all possible threats recognised, arranged in order → become risks, emphasis on brainstorming	I
Concerning information systems every couple of years → **recognition of the systems** that are **most valuable from the business point of view**, continuity production and updating recovery plan for them. Risk analysis and management process that encompasses the whole system.	I
Methods used depend on the actor. VAHTI offers one assessment model. Documentation is a target.	I

Question 6.2:

14. Are the risks related to the metrics assessed?

Interpretation of answers to Question 6.2:

Risks related to the metrics are not assessed to a large degree. The type of organisation clearly affects this. Large organisations and those state institutions that have significant responsibilities in the society use risk techniques more to assess the risks of IS metrics. Some examples of the approaches:

- Risks are assessed by means of the daily work of the responsible person – no systematic methods,
- Logs are not assessed, but risk analysis is used concerning work methods and with "dangerous work combinations" (for example, the same person orders something, accepts the bill and pays it),
- Risk analysis is not officially used, experts think about issues that concern problems, and
- There is an open policy in the organisation – all administrators can access everything, but misuse will probably be caught in one way or another.

Question 6.3:

15. Quality assessment (of the metrics system)

Interpretation of answers to Question 6.3:

According to the interviews, quality assessment of the metrics is not usually handled in a process-like manner, but there are intentions to improve the situation as customers demand high quality in IS issues. Interviewees understand that information security itself is a quality factor, but if the assessment would be more systematic, it would be given more attention by the management. The word IS quality clearly refers more to product quality on business side, because it depends more on the customer requirements. In state administration, IS quality mainly represents issues concerning personnel behaviour and responsibilities. Audits are also considered a suitable way to assess quality. One example of an assessment method is the following:

"We try to incapacitate all our systems with all kinds of tools available at that moment. And that of course is a kind of quality assessment event for measuring durable development."

The problem is generally that IS should be part of the quality management process instead of applying *best effort* methods when evaluating information security quality. The process would utilise more proactive methods instead of using reactive quality assessment by counting incidents, which it often does. The approaches to quality issues are presented in Table 16.

Table 16. Quality assessment in organisations.

State institutions	Industry
❑ Not much need for logs but **concerning user rights procedures the process is very systematic, requires** a lot of **development**. ❑ "**Best effort**" method ❑ **Self-made methods:** few incidents and yearly low downtime with a few administrators → quality rather good ❑ **Own quality system** for acquiring and implementing the metrics system. A process → adheres to **internally classified quality system**, but **not a complete** quality system ❑ **Audits represent quality assessment**	❑ **Customers demand high IS quality and documentation**. Aim to get **risk, quality and metrics issues within the normal planning process** that includes business representatives, managers and people from all groups → issues mobilised **further into production processes**. ❑ **Security** to be **included in business processes** Main objective to **raise IS awareness → increase process quality** ❑ **Quality assessment incidents count (testing, inspections)**. Methods **checked with a big group → weaknesses**

Question 6.4:

16. Gathering of history data and its use. Is the process further developed according to history data?

Interpretation of answers to Question 6.4:

Interviews showed that some organisations do not have a particular metrics process, thus the collected history data is mainly log collection and analysis. The practises used are presented in Table 17.

Table 17. History data handling in organisations.

State institutions	Industry
❑ **Backup copy** on a certain time scale. **Log handling and storing** similar ❑ **Logs and auditing**. External audits not necessary due to own expertise. IS development target: process description development ❑ **System developed with limiting values**, **problems with old systems** → no sense in patching them ❑ **Separate log collection from servers, logins and connections monitored**. **User actions can be traced** but used only to resolve network fault situation. **System is developed according to the history data and users** (contact concerning the problems).	❑ **Target a secure product**: history data by incident collection and analysis. Refined and accessible all the time → usable learning material, examples ❑ **Finnish Communications Regulatory Authority regulates log collection**, storage time ordered → disk space consuming. When **IS is integrated** into quality processes, instructions are more accurate. ❑ **Organisation should use a balanced method** when utilising history data: **1) What has happened vs. what issues act as future drivers** **2) Short-term issues vs. long-term issues** **3) Objective vs. subjective issues** **4) Strategic vs. operational point of view**

3.11 Theme 7. Needs for the metrics, background, development

Questions 7.1, 7.2:

17 a) Usefulness of metrics for the system 17 b) Usefulness of metrics for the business

Interpretation of answers to Questions 7.1 and 7.2:

There is need for certification and standardisation since they might help to prove the level of IS. This would add credibility among business associates, but it would also help to determine the current level of IS in the organisation itself. The usefulness of the metrics is represented in Table 18, both from the system and business point of view.

Metrics enable analysis of what has happened particularly in fault situations, but it requires systematic data collection and analysis. The metrics are found most useful when predicting or trying to understand future situations. Therefore, it can be assumed that there are some kind of IS metrics processes in most organisations, even though they are not explicitly defined. The problem experienced when estimating metrics usefulness is that there is usually a need to find out the relevant data among all the metrics information. If there is no history data collection and analysis, the situation remains usually purely reactive.

Table 18. Usefulness of metrics from the system and business point of view.

Useful for the system	Useful for the business	Factors that decrease usefulness
State institutions		
❑ **Knowledge gained** by people, can always configure a system in a better way as an organisational structure	❑ **Enables grading the processes with a standard** → help to recognise the IS level	❑ **Log analysis** hard, a lot of useless data → **need for** tools that **rationalise** the process, help find out the **relevant data** ❑ "Best effort" method: **lack of history data and benefit from experience**: low usefulness
Industry organisations		
❑ Helps to **automate the system observation** (for instance, giving automatic alerts) ❑ Useful **if verified** that the right things are measured, results reliable, analysis method appropriate → need for the right tools and skilful staff	❑ **Helps to increase and formalise the metrics,** shows partners IS quality ❑ **Enhances history data study, trend analysis**: speed and direction ❑ Helps in understanding systems: history data useful because of **complex systems**	❑ Lack of systemacy

Question 7.3:

18. Is there a need for IS metrics? Why? / Why not?

Interpretation of answers to Question 7.3:

The aim of the question was to resolve how useful the interviewees experience the current metrics to be, and based on what qualities. The needs are presented in Table 19. The most common need is to have a constantly developing metrics system. Many respondents emphasise and justify the importance of a process. The process would enhance the definition of IS issues and update the policy when history data produced comparison material. It would probably enable definition of the current level of IS as there are expectations of being able to indicate it, as one respondent expresses:

"You can't go asking 'how have you handled documents today?' from every employee."

The problem is the contradiction between IS and user privacy; there is the need to preserve valuable information by strict procedures, but at the same time the aim is to offer usability and gain confidence from users.

Table 19. Needs for IS metrics.

Need for metrics	Type of metrics	Org. type
Customer expects high-quality services with IS as an expectation value → need for **means that show the IS quality level** of the service	Organisational	S
Logs and their analysis need development (rationalisation), **detection** of **what launched applications**, **what equipment connected to the network**	Technical, organisational	S
Detecting listening computers → protocol firewall does not help much.	Technical	S
Audit methods that could be sustained continuously, **self-directing method that could be used, for example, continuously** as a part of normal work process and **included as internal auditing concepts**	Technical, operational	S
New personnel should be **educated**, including security managers that have not worked with the metrics. Through **meetings and educational events**	Organisational, individual	S
Complex systems → reality and policies separate → need for measurement system that checks how and whether policy is derived from business, are the IS risks managed, how well the policy adheres to the actual processes or structures → policy **can be adjusted** easily	Technical, organisational, operational	S
Need **in administration**. **The process of IS**: from business strategy, proceeding through IS policy to IS strategy → objectives. But how to measure IS work executed within business processes, via guidelines, procedures and policies → **a tool for quality control**	Organisational, operational	I
Optimal system protection level with risk and business analysis, **checking it with some points**	Operational	I
Measure **every day IS work within processes**, who is obeying instructions	Operational, individual	I

Question 7.4:

19. Strategy for metrics development in the long run

Interpretation of answers to Question 7.4:

Strategy is a sum of many factors, thus there is no absolute direction that could be pointed out exactly. The strategies are described in Table 20. The situation

will get more complicated as the systems become more complex, threats more diverse and attackers more skilful. The system has to adjust to altering situations by detecting its current state and studying history, thus making predictions for the future. There is a need for education and continuous awareness maintenance. There will be requirements set by legislation, customers will demand more secure products, actions and proof of them. These issues all affect each other. As one interviewee pointed out, there has to be on-going study of what the customer wants, and the development has to proceed according to it:

"Normally we offer log monitoring, measure things that way, the number of attacks per time period or whatever the customer wants. We have to detect and study these things, and possibly using IDS, time will show if it's worth it or does it just cause extra work load compared to the gained benefits."

Difficulties caused by disordered systems are described in the following example:

"If we consider a monolithic system that has one or two protocols between the server and the user, it is easy to set up IDS. Then as time goes by and system size increases, there are suddenly 50 different protocols. The IDS becomes so noisy that it is difficult to gain any benefitt. You can't set the threshold values of an IDS in such a wa, that it would be possible to detect attackers in all that noise. So we can't say, lets make an IDS-strategy and implement it. Instead we have to live according to the development of our processes, what kind of information systems back up these processes, how all that old information system environment and data communications system develops. It is a very dynamic field."

Table 20. Strategies for metrics development in organisations.

Strategy	Affecting factors
State institutions	
Process description is part of the documentation and attachment of the **IS policy**, **IS administration** system → once the process is described and studied, it can be improved. **External audits** become **internal**.	**Common standard would help**.
Documentation volume increases and **will already be included in the early stages**. Issues that have to be defined in this: the **levels the documentation has to preserve** and what has to be taken into account with it. Management has to provide **guarantees**.	Process thinking within 1-2 years from the Ministry of Finance (U.S. practices)
Requirements both from **outside** (legislation, doctrine), **and inside** (requirements caused by threat scenarios), which provides its own structure and the base.	Legislation, doctrine, scenarios
Disordered field (complex systems, numerous protocols), **strategies** concerning one system are **hard to come up with**.	**Requirements** from **business** and **system changes**. Requirements for metrics in the information management strategy
Different views of IS in the organisation **affect strategy development**: a quality within a product and IS is a value in itself (IS manager's view). **IS** can be separated from **a) product b) process c) structure** and managed separately.	Organisational structure, different views
Measurement systems will **become more complicated** and heavier (enterprise solutions), require more from the staff, and probably **cause bigger problems,** thus adding the **need for increasing observation**.	Information systems become more complicated.
Industry organisations	
IS embedded in Quality Control	IS personnel responsibility division
Pressure for certain measures and services, like firewall services	Customers

Question 7.5:

20. What should be measured if possible, what would you want to be measured in the future?

Interpretation of answers to Question 7.5:

One of the most critical, yet hardest issues to measure is the human factors, behaviour and awareness. The means with which the behaviour would be

measured could also help add awareness. However, it is recognised that there are ethical questions involved and a maximum amount of monitoring is not the target. People's privacy is respected. Furthermore, different audiences have different views about it and the challenge is to understand what one person can do and what not: *"A fellow can answer all questions with the correct answers, but he never adheres to them"* ("enemy inside"). The other general aim in industrial organisations is to get IS processes connected with business processes and measure its succession. Table 21 presents the issues that are most useful for the organisations.

Personnel monitoring is a sensitive area. There are restricting and complicating factors that have to be considered:

- Regulators restrict employees' traffic monitoring even though tools for this exist,
- Yet, some claim: *"In Finland legislation would enable us to monitor far more than we do now. But we don't want to proactively monitor in that way"*,
- Privacy protection issues have to be considered, also in the legislation, and
- Too difficult to supervise one person among a vast amount of employees: *"It would be an optimal system if we had built-in integrity control, in a way that everything you do forms a personal profile, a baseline. And once you deviate from this profile, an alarm goes off. But how do you do it when the system changes, the process changes, work tasks changes…in a more dynamic environment or process it is more difficult. You can only measure probabilities."*

On the other hand, there is an goal to achieve results by positive actions:

*"I hope there would be some kind of **encouragement**, we could justify why we have to act this way and we could achieve IS behaviour as a natural way to act, because everyone would want to act this way."*

Management should take a more significant role when leading IS management, as this also affects the succession of measuring IS:

*"Managers recognise the importance of IS ... But what they don't see is that they have to **lead and manage** the organisation on the part of IS as well, instead they see themselves as just one actor in the organisation IS. They often move the responsibility to the IS managers, and this might lead to a situation where IS manager is obligated to act in a hazardous way."*

Table 21. Useful metrics for the organisations and affecting factors.

What measures organisations need	Affecting factors
State institutions	
Common **standard**	**IS emphasises a process** more than a product.
IS culture	**Different audiences** have **different views**. And yet it is included in all policies. "**Enemy inside**"
Technical tools	Only parts that are easily **predictable can be automated.**
To get the **spectrum** that comes **from different tasks** so well **profiled** that illegal actions could be separated from there	**Different zones** in the system *"outside you can do anything but the closer you get to the kernel the more restricted it becomes, tools, protocols, policies."*
Data concurrently from several metrics	The **more sensors** provide combined and analysed data, the **better picture** of the whole situation every moment or on every time scale. **Data rewind**, **checkpoints**
Usability metrics: to be able to measure the capacity of a functioning production system	**Notification when** the **usability** of the system **is** so **low** that is has to be replaced by another system *"we are constantly losing time, and in business money."*
Measure **all OSI 7 layers and** the 7th layer, the **application layer,** in several ways at several points	A need for a covered checkpoint system
Measure network in a way that user privacy is not threatened	Network availability is a primary target.
Absolute metrics whether the **computer** is **broken into or not**.	One viewpoint to intrusion detection
Virus tracing and localisation in the computers in the network	Includes the **questions of privacy, tracing people**
User behaviour	Complex systems, people might not even know they have threatened IS instructions
Industry	
User behaviour	Privacy protection issues
Personnel behaviour	Probably one of the main issues
Education	Customers not very aware of IS issues → depends on the corporation size whether they demand documentation → sales personnel should be educated.
Automation of IS metrics	**Checkpoints** to the system that can be measured.
The **minimum** IS metrics **amount required**	Determined at all times to **minimise the costs**
IS metrics use should be **integrated into business management.**	Otherwise it will be experienced as an extra cost, a trouble that does not promote business.
Absolute security in a product, process, premises or practises	**Absolute modelling**, not necessarily exact, but accurate enough
Self-learning SW	SW can learn from its own functioning and spend endless time **testing itself**, which can never be done with human work.
Staff IS behaviour, not only awareness	No need for technical tools or system solutions

4. Discussion

The interviews show that the IS metrics situation in Finland depends to a great extent on the organisation type. The metrics that organisations use is different and there are many factors that affect why a certain organisation chooses certain metrics.

4.1 State of practise in Finnish industry and state institutions

Typically, the security objectives of state institutions include building and maintenance of customer trust, ensuring critical process functioning and backup of the main activities, as well as ensuring the congruence between the main tasks and the legislation. State institutions' other security objectives are to back up the change and keep the policy optimised so that it is not too strict and thus adding to the user's ease of use. Typical industrial organisations' security objectives are to integrate IS work into business processes, back up the business strategy and ensure product security. There is a common objective to raise the IS awareness and educational level. The reasons for using metrics are the need to raise the level of IS awareness, the risk factors of human behaviour and to ensure availability, integrity and confidentiality.

The technical metrics used is mainly PC and network monitoring, incident counting, auditing and risk management. IS metrics is connected with general IS management. Metrics implementation depends strongly on what kind of decisions the responsible people in the organisation are able to make about the IS resources and investments. One restricting factor in this is the inability of the management to understand the needs of IS and give enough authority to knowledgeable IS people. The other extreme is that managers that do understand the significance of IS, force the IS managers to take all responsibility. This leads to a situation where management does not commit to the decisions and there is a lack of strategic leadership concerning information security.

There is certainly need for knowledgeable leaders who understand that they have to guide the organisation's activities from the point of view of IS and its measurement. The term "knowledge management" encompasses this idea and is

recognised more often when quality issues are concerned. This is why IS process development could learn a great deal from quality process management.

Lack of interoperability between subsystems that contribute to IS is a problem. Some subsystems are old and as new subsystems are added to this assembly, they cannot necessarily communicate with each other. The systems are complex and difficult to control, not to mention measure. Security policies are considered problematic from the perspective of responsibilities. How up-to-date they are is dependent on skilful staff with enough views on IS issues as well as perceiving it in organisational strategic management. This problem refers to the lack of evolution process. The significance of documentation and construction of security policies is not as great as the significance of adjusting it to the organisation's working culture.

The utilisation skills of the tools and methods on the technical level are high and the area is very well understood. Generally, risk assessment is handled well and it is mostly applied so that it adjusts to the organisation's own processes and purposes. However, there are limitations when the risks of assessing the metrics themselves are concerned. Because the idea of measuring IS level and its benefits are typically poorly understood by the organisation management, the risks concerning this are neither recognised nor acted upon. Quality issues are considered important as a functioning, developing process, with active history data collection and improvement being an essential part of it. Some organisations explicitly recognise IS as a quality factor in itself, and aim to make the IS process a part of quality management and processes.

The organisations feel that metrics is useful not only for defining the IS level in the organisation, but also for proving it to the partners. It is already considered a competitive benefit, not to mention in the future. Some kind of general standard is a suggestion to define the level of IS issues objectively. However, it is recognised that such a standard may be impossible to define so that it would be applicable to everyone as the current standards merely provide guidelines. Measurement of essential things is seen as important and there is a need for tools to rationalise the measurement overload. Rationalising is important in order to get better results, but it also helps to justify the need for effective IS methods to the management.

Most of all, metrics, regardless of the type, is considered useful when applied as a process. The benefits of a constantly developing and functioning IS process are recognised and it is seen as a means to improve policies and practises as well as raise IS awareness and personnel commitment. The most significant factor concerning IS and measurement are without a doubt the human factors.

4.2 Directions for further research

Future development depends, for example, on the management, systems, customers (in industry) and the legislation (governmental side). Because of the large number of stakeholders, its direction is hard to predict. There are intentions to integrate the metrics process into the business management as well as quality control systems. This is an inevitable direction for those whose business is based on IS in one way or another, and whose development requires process optimisation. In the future, the value of a functioning IS process can be appreciated more than now as systems become more complicated and decentralised.

Measuring human behaviour is considered important. However, the contradiction between measurement and privacy protection is recognised and there is no particular desire to injure privacy of an individual unnecessarily. The rationalisation of IS can be one approach to this, but also motivating people to commit to IS issues, which is one of the greatest challenges. The level of knowledge amongst the stakeholders, the manageability and measurability of IS, including skills to prioritise and continuously optimise the dialogue between IS and organisation actions, will be a competitive value in the future. These enable security issues to be made a visible and inseparable part of organisation life.

Tables 22, 23 and 24 summarise the most common needs brought out in the interview answers and offer possible directions for the solutions. Table 22 presents issues concerning personnel or user behaviour, Table 23 organisational and operational issues and Table 24 technical issues. The classification of problems into different metrics classes is overlapping. The same problem might represent various metrics types.

Table 22 shows that there is a need for educational programmes that would motivate people to commit to act according to given IS instructions and constantly learn more. This way the need to measure IS behaviour would decrease. However, sometimes there is a need to measure behaviour, and in theses cases there would be a need for metrics that would separate risk behaviour from the data. This also refers to one type of operational metrics presented in Table 23, where spectrums from different tasks would be profiled.

Table 22. Suggestions for the most common problems concerning user behaviour.

Need	Quality of the problem	Type of metrics	Development suggestion
Security methods **taught** to new personnel and security managers that have not worked with them before	For example tailored, continuously developing audit methods	Individual	Meetings and educational events
Measuring every day **IS work within processes**, who is obeying the instructions	*"You can't go asking 'how have you handled documents today?' from every employee."*	Operational, individual	Tests, motivation
Need to measure **IS culture**, especially in own organisation	**Different audiences** have **different views** ("**enemy inside**").	Individual	Questionnaire, tests
User behaviour	**Complex systems**, people **might not even know** they have threatened IS instructions	Individual	Educational programs
User behaviour	Privacy protection issues vs. control	Individual	Awareness
Education	**Sales personnel need to be aware** of the IS issues → inform customers	Individual	Educational programs, motivation
IS behaviour of the staff, not only awareness	No need for technical tools or system solutions, the problem is administrative.	Individual	Tests, motivation

Table 23 suggests measuring systems based on checkpoint measurement, and standardisation, whereas Table 24 suggests technical metrics that focus

especially on automation, rationalisation and self-learning qualities of the measurement target.

Still, general competent solutions are hard to find. As Deswarte et al. (1999) state, the metrics used should focus on determining the qualities of an individual organisation rather than comparing the states of different organisations. The organisations in this study represent different types of units, therefore there is a need for a more targeted study for one particular branch, for instance in the mobile telecommunications industry. That kind of study could benefit from interview questions modified according to the field. After a number of targeted studies a quantitative analysis would be useful for handling the answers, as there would be a lot of source material.

Table 23. Suggestions for the most common problems concerning organisational and operational metrics.

Need	Quality of the problem	Type of metrics	Development suggestion
To **show the IS quality level of the services** and its development further	Customers require evidence of the IS level.	Organisational, operational	Standardised, formalised methods, certificate, or maturity models
Self-directing audit method that could be used continuously	Part of the normal work process, **included as internal auditing concepts**	Technical, operational	Organisation process study, constant audits as part of quality management
Measurement system that checks how and whether a policy is derived from business	E.g. are the IS risks managed, how well the policy adheres to the actual process or structure	Technical, organisational, operational	Risk management tool, checkpoints
How to measure **the process of IS** that is executed in business processes via guidelines, procedures and policies	IS process comes from business strategy, then proceeds through IS policy to IS strategy, this way objectives,that have to be fulfilled are gained.	Organisational, operational	Quality control tool, process modelling, checkpoints
Optimal system protection level	Need to establish a baseline for the system	Operational	Risk analysis and business analysis, checking it at some points

Common **standard**	**IS probably emphasises the process more than the product** also in view of project work.	Organisational	Standardisation of IS measures
Spectrum from different tasks profiled so that illegal actions can be separated	**Different zones in the system**	Operational	Access right management, *"tools, protocols, policies"*
Usability metrics: measure the capacity of a functioning production system	**Notification when** the system **usability** is so **low** that it has to be replaced by another system	Organisational, operational, technical	Checkpoints
Automation of IS metrics	To rationalise tasks that can be automatised, needs often determine what they are	Technical, operational	Checkpoints to the system that can be measured
The **minimum required metrics amount** is determined	To minimise the costs	Organisational, Operational	Analyser tool that constantly detects the system and updates itself
IS metrics use should be **integrated into business management.**	**Otherwise experienced as an extra cost**, a trouble, does not promote business	Organisational	Process study for IS, creating IS process, applied with the business model

Table 24. Suggestions for the most common problems concerning technical metrics.

Need	Quality of the problem	Type of metrics	Development suggestion
Logs and their analysis development (**rationalisation**)	Logs impractical, contain massive amounts of data, which is hard to resolve	Technical, organisational	Rationalisation tools
Detection of what kind of **applications launched**, what kind of **equipment connected to the network**	Need for network analysis	Technical, operational	Analyser tools
Detecting listening computers → protocol firewall does not help much.	Protocol firewall does not help.	Technical	Analyser tools
Need for technical **tools that enable automation**	Only easily **predictable** parts **can be automated.**	Technical	Automation tools
Data concurrently from several metrics, like what is the user doing on the Internet, and concurrently in the confidential department	The **more sensors** give combined and analysed data, the **better the picture** of the whole situation every moment or on every time scale.	Technical	Data collection and analysis, data can be **rewound** or some **checkpoints** just checked. **Data filter**.
Measure **all OSI 7 layers and** the 7th layer, the **application layer,** in several ways at several points	The whole picture of the network activity	Technical, operational	Checkpoint system
Measure the network without threatening user privacy	The target is to maintain availability.	Technical, operational	Network analyser
Absolute metrics whether the **computer** is **broken into or not**	One viewpoint to intrusion detection	Technical	Intrusion detection system
Virus tracing and localisation in the computers in the network	Includes the questions of **privacy, tracing people**	Technical	Network analyser
Absolute security in a product, process, premises or practises	Does not have to be exact, but accurate or accurate enough	Brainstormers	Baseline for a certain product, process or practise
Self-learning SW	**SW that can learn** from its **own functioning,** endlessly **test itself** → can never be done with human work	Technical, organisational	Self-learning, self-monitoring, self-testing software

5. Conclusions

Even though the literature offers several models and methods for measuring the maturity of information security processes in an organisation, they serve best when the organisation's own operational environment, frame of reference and other individual factors are taken into account. Solutions that would benefit all organisations are hard to come up with. Security is an invisible concept that depends on numerous factors, such as technical development, legislation, customers and the environment.

This study clearly shows that most of all information security metrics use is beneficial when applied as a process. Personnel behaviour is one of the most critical issues to be measured. However, there are restricting factors: privacy protection and the requirements of legislation. There is a need for knowledgeable management that understands the importance of managing information security and providing information security managers with enough authority to improve metrics development.

Allocation of responsibility is considered to be an important factor that affects the quality of implemented IS metrics. The knowledge and skills of the IS staff, as well as co-operation with other teams is valuable to the success of a continuously developing metrics process. Most of all, there is need for means that enable construction of a process that is able to take the organisational culture into account. Means are also needed to help integrate the security process into existing processes, especially quality management and business processes. Understanding quality models and software process models is essential in achieving that goal.

A well-managed security metrics program requires effective documentation management. Documentation concerning security policies and procedures has to be constantly updated and close to the implemented practises. The dialogue between theory and practise is optimally a cyclic process, where the significance of tacit knowledge is understood and used as a source for the development and updating of documentation. Again, the allocation of responsibility affects the success of this process.

In terms of technical metrics, there is need for automation, rationalisation and self-learning. In order to rationalise resource management, the minimum amount of needed metrics has to be measured. The rationalisation could be implemented with automated tools that inspect the system's state and prioritise actions. Furthermore, routine tasks could be automated with appropriate systems. This would all help to justify the need for attention to a pervasive information security process, as savings could be achieved by rationalisation.

The topic of measuring IS in Finnish organisations has not been well studied before. In order to get a comprehensive picture of the topic, a more profound study is needed. Because the organisations used in this study represent very different organisation types and business segments, the results can not be generalised to represent a comprehensive IS metrics usage situation in Finland.

There are several possible directions for further work. More interviews might be valuable, first targeting the situation in one particular branch, for example within the mobile telecommunications industry area and network-related industry, and then making conclusions within that particular branch. The interview questions could be refined further according to the studied branch in order to gain the characteristics related to it. This kind of study could benefit from a quantitative analysis approach, as there would be enough relevant material for comparison. There is a need for educational programmes that would motivate people to commit to act according to given IS instructions and to constantly learn more, after which the need to measure IS behaviour would decrease. There is still a need to measure personnel behaviour, in a way that risk behaviour could be pointed out from the data using profiles. In addition, one development target could be a checkpoint-based measurement system that would provide data from several sources, and this data could be profiled and prioritised so that most vulnerable or critical points could be taken into account. In addition, this could enable task automation and rationalisation by recognising them with self-learning capabilities. Yet another development target could be a common standard or maturity model for Finnish organisations.

References

Bayuk, J. L. 2000. Information Security Metrics: An Audited-based Approach. NIST and CSSPAB Workshop, Washington, D.C., 14 June 2000. [Web-document]. Available: http://csrc.nist.gov/csspab/june13-15/Bayuk.pdf . [Referenced 1.3.2004].

Babaoglu, O. 2003. Intrusion Detection Systems. Course Material, University of Bologna, Department of Computer Science. [Web-document]. Available: http://www.cs.unibo.it/babaoglu/courses/security/lucidi/IDS.pdf . [Referenced 14.3.2004].

Basili, V.R., Caldiera G. & Rombach, H.D. 1994. The Goal Question Metric Approach. Encyclopedia of Software Engineering. Wiley. Available: http://www.cs.umd.edu/projects/SoftEng/ESEG/papers/gqm.pdf . [Referenced 1.4.2004].

BS 7799-2. 2002. Specification for Information Security Management. ISO/IEC.

Common Criteria (CC) version 2.1. 1999. National Institute of Standards and Technology. Available: http://csrc.nist.gov.cc . [Referenced 1.4.2004].

Common Vulnerabilities and Exposures List, version 20030402. 2003. The MITRE Corporation. [Web-document]. Available: http://www.cve.mitre.org/cve/downloads/full-cve.html. [Referenced 1.4.2004].

Deswarte, Y., Kaâniche M. & Ortalo, R. 1999. Experimental Validation of a Security Metrics. [Web-document]. Available: http://philby.ucsd.edu/~cse291_IDVA/papers/rating-position/Deswarte.pdf. [Referenced 1.3.2004].

Gummer, B. & McCallion, P. 1995. Total Quality Management in the Social Services: Theory and Practise. Albany, NY: Rockefeller College Press.

Henning, R. (ed.) 2001. Workshop on Information Security System Scoring and Ranking. Information System Security Attribute Quantification or Ordering (Commonly but improperly known as “Security Metrics”). [Web-document].

Available:http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf. [Referenced 28.1.2004].

Hirsjärvi, S. & Hurme, H. 2001. Tutkimushaastattelu – Teemahaastattelun teoria ja käytäntö. (In Finnish). Helsinki: Helsinki University Press.

Eskola, J. & Suoranta J. 1998. Johdatus laadulliseen tutkimukseen. (In Finnish). Vastapaino. Tampere.

INFOSEC Assessment Capability Maturity Model version 3.0. 2003. Information System Security. [Web-document]. Available: http://www.iatrp.com/iacmm.cfm. [Referenced 1.4.2004].

Information Technology Security Evaluation Criteria version 1.2. 1991. Department of Trade and Industry. Available: http://nsi.org/Library/Compsec/eurooran.txt . [Referenced 1.4.2004].

ISO 17799. 2000. Code of Practise for Information Security Management. ISO/IEC.

Jelen, G. 2000. SSE-CMM Security Metrics. NIST and CSSPAB Workshop, Washington, D.C., 13-14 June 2000. Available: http://csrc.nist.gov/ispab/june13-15/jelen.pdf .
(10 July 2001). [Referenced 27.1.2004].

Jonsson, E. 2003. Dependability and Security Modelling and Metrics [Web-document]. Available: http://www.ce.chalmers.se/undergraduate/D/EDA261/03/oh03/oh_F13_security_evaluation_6pp.pdf. [Referenced 28.1.2004].

Jonsson, E. 1998. An Integrated Framework for Security and Dependability [Web-document]. Proceedings of the New Security Paradigms Workshop 1998, Charlottesville, VA, USA, September 22-25 1998. Available: http://www.ce.chalmers.se/staff/jonsson/Paradigms-nspw98-print.rev0001.fm55.pdf. [Referenced 23.1.2004].

Kajava, J. & Leiwo, J. 1994. Tietoturvahenkilöstö organisaatioissa. (In Finnish). Working Papers Series B 34. University of Oulu.

Kaksonen, R. 2001. A Functional Method for Assessing Protocol Implementation Security. Espoo. VTT Publications.

Katzke, S. 2001. Security Metrics [Web-document]. Available: http://philby.ucsd.edu/~cse291_IDVA/papers/rating-position/Katzke.pdf. [Referenced 23.1.2004].

Kormos, C., Givans, N., Gallagher, L. & Bartol, N. 1999. Using Security Metrics to Assess Risk Management Capabilities. [Web-document]. Available: http://csrc.ncsl.nist.gov./nissc/1999/proceeding/papers/p29.pdf . [Referenced 28.2.2004].

Leach, J. 2003. Security engineering and security RoI. Computers and Security. Vol. 22, Issue 6, 482–486.

Lindqvist U., Kaijser, P. & Jonsson, E. 1998. The Remedy Dimensions of Vulnerability Analysis. In: Proceedings of the 21st National Information Systems Security Conference, pages 91-98, Arlington, Virginia, October 5–8, 1998. National Institute of Standards and Technology/National Computer Security Center. [Web-document]. Available: http://www.ce.chalmers.se/staff/ulfl/pubs/nissc98l.pdf. [Referenced 23.1.2004].

Miettinen, J. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. (In Finnish). Helsinki: Kauppakaari Oyj.

Miettinen, J. 2001. Yritysturvallisuuden käsikirja. (In Finnish). Helsinki: Talentum Media Oy.

Mikkonen, P., Murtonen, M., Valtonen, P. & Järvinen-Taubert, J. 2003. Työpaikkojen riskien arviointimenetelmien käyttö. (In Finnish). Tampere, VTT Tuotteet ja tuotanto. Research report BTU044-031197. [Web-document]. Available: http://www.vtt.fi/tuo/44/tuloksia/btu044-031197.pdf. [Referenced 9.3.2004].

Myers, M. D. "Qualitative Research in Information Systems," MIS Quarterly (21:2), June 1997, pp. 241-242. MISQ Discovery, archival version, June 1997, http://www.misq.org/discovery/MISQD_isworld/. MISQ Discovery, updated version, last modified: February 27, 2004 www.qual.auckland.ac.nz. [Referenced 1.4.2004].

Nielsen, F. 2000. Approaches to Security Metrics. A Report of the Workshop Held June 13–14 at the National Institute of Standards and Technology (NIST) In conjunction with the Computer System Security and Privacy Advisory Board (CSSPAB) Meeting. Washington, D.C. [Web-document]. Available: http://csrc.nist.gov/csspab/june13-15/metrics_report.pdf . [Referenced 1.3.2004].

Parker, D.B. 1981. Computer Security Management. Reston: Prentice Hall.

Payne, S. 2001. A Guide to Security Metrics [Web-document]. Available: http://www.sans.org/rr/papers/5/55.pdf . [Referenced 24.1.2004].

Ross, R., Swanson, M., Stoneburner, G., Kazke, S. & Johnson, A. 2004. Guide for the Security Certification and Accreditation of Federal Information Systems. National Institute of Standards and Technology. [Web-document]. Available: http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf. [Referenced 15.5.2004].

Science Applications International Corporation. 2002. Intrusion Detection System System Protection Profile. Version 1.4. NSA. Available: http://niap.nist.gov/cc-scheme/PP_IDSSYPP_V1.4.pdf. [Referenced 1.4.2004].

Swanson, M., Bartol, N., Sabato, J., Hash, J. & Graffo, L. 2003. Security Metrics Guide for Information Technology Systems. NIST. [Web-document]. Available: http://www.csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf . [Referenced 1.3.2004].

Systems Security Engineering Capability Maturity Model version 3.0. 2003. The International Systems Security Engineering Association. [Web-document]. Available: http:// www.sse-cmm.org/librarie.htm. [Referenced 29.1.2004].

Systems Security Engineering Capability Maturity Model Appraisal Method version 2.0. 1999. The International Systems Security Engineering Association. [Web-document]. Available: http://www.sse-cmm.org/docs/SSAM.pdf. [Referenced 29.1.2004].

The Baldridge Criteria for Performance Excellence. 2004. NIST. [Web-document]. Available: http://www.quality.nist.gov/PDF_files/2004_Business_Criteria.pdf. [Referenced 28.4. 2004].

The ISO Survey of ISO 9000 and ISO 14001 Certificates. 2002. [Web-document].Available: http://www.iso.org/iso/en/iso900014000/pdf/survey12thcycle.pdf. [Referenced 28.4. 2004].

Trusted Computer System Evaluation Criteria.1985. DoD. Available: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html . [Referenced 1.4.2004].

Valtionhallinnon Tietoturvallisuuden Kehitysohjelma 2004–2006. (In Finnish). 2004. VAHTI. [Web-document]. Available: http://www.vm.fi/tiedostot/pdf/fi/70508.pdf. [Referenced 30.4.2004].

Wilson, M. 1998. Information Technology Security Training Requirements: A Role-and Performance- Based Model. NIST. [Web-document]. Available: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf [Referenced 15.3.2004].

Wood, C. 1989. How many information security staff people should have? Information integrity investments, Sausalito, California, USA.

Yliluoma, P. 2001. Ohjeita opinnäytetyön tekemiseen. (In Finnish). University of Oulu.

Appendix A: Interview questions

Interview themes can be classified according to effective security metrics program components proposed by Swanson et al. (2003):

1) Strong Upper-Level Management Support (→ resources)
2) Practical Security Policies and Procedures (backed by authority to necessary to enforce compliance, attainable, provide meaningful security through appropriate controls, → metrics are not easily obtainable if there are no procedures in place)
3) Quantifiable Performance Metrics (based on security performance goals and objectives, easily obtainable, feasible to measure, repeatable, provide relevant performance trends over time and be useful for tracking performance and directing resource)
4) Results-Oriented Metrics Analysis (results are used to apply lessons learned, improve the effectiveness of existing security controls and plan future controls to meet new security requirements as they occur, → essential for the improvement of the overall security program)

The questionnaire themes respond to corresponding component indicated by number in parentheses:

Background

1. Background, branch (personal professional details, organisation).

Security objectives

2. Security objectives in your organisation. How is responsibility for them assigned? (1)
3. Documentation and description of security objectives. Are they documented e.g. as policies and procedures? (3)

IS Metrics

4. How is the concept of information security metrics understood in your organisation?
5. What kind of security objectives cause the need for IS metrics? (3)

Metrics implementation

6. Metrics implementation in practise. Can it be described as a process? (3)
7. Responsibility for metrics implementation (2)
8. The relationship of IS metrics process to work flow processes. Is it embedded? (2,3)
9. Validation of the gathered metrics data (testing, reviews, verification). How is the responsibility allocated? (4)

10 a). Use of technical metrics. E.g. network load measurements, intrusion detection data, software security features) (3)

10 b). Do you use technical tools for IS metrics or for a part of it? If yes, what tools? (2,3,4)

Basis for the metrics (Standards and other documentation)

11. What is the basis for the metrics that you use (3)? A standard? Is the standard perhaps adapted for your own purposes (2)? If so, how?
12. How does the standard respond to your guidelines (and procedures) for the implementation of information security? (2)

Risk and quality management

13. Do you use risk analysis techniques (2)? How? Is it part of your process? How do they relate to your documentation (3)?
14. Are the risks related to the metrics assessed? (2,3,4)
15. Quality assessment (of the metrics system) (4)
16. Gathering of history data and its use. Is the process further developed according to history data? (4)

Needs for the metrics, background, development

17 a). Usefulness of metrics for the system (4)

17 b). Usefulness of metrics for the business (4)

18. Is there a need for IS metrics? Why? / Why not?
19. Strategy for metrics development in the long run (1,4)
20. What should be measured if possible, what would you want to be measured in the future?

Published by

Series title, number and report code of publication

VTT Publications 544
VTT–PUBS–544

Author(s)
Sademies, Anni

Title

Process Approach to Information Security Metrics in Finnish Industry and State Institutions

Abstract

In today's information technology world, there is a growing need for security solutions: information systems are more and more vulnerable because of the increased complexity and interconnection of insecure components and networks. Even though appropriate security approaches can be found, the resulting security level often remains unknown. It is a widely accepted principle that an activity cannot be managed well if it cannot be measured. Information security (IS) metrics offers work as a research field.

This thesis focuses on studying the use of IS metrics in certain Finnish industrial companies and state institutions. The objective is to study the state-of-practise and its relation to the literature in the research field. The use of IS metrics is particularly studied from the perspective of processes. The aim is to reveal how development and implementation of the metrics is carried out in the organisations. In addition, the techniques used in implementation and analysis of metrics, as well as their usefulness and future targets are studied. The research consists of a literature study followed by a survey study, and an analytical phase. The survey study is implemented by conducting eight interviews in different industrial corporations and state institutions. The method used is a semi-structured, theme-centred interview. The results are categorised applying suitable classifications found in the literature and analysed using an interpretative analysis method.

The survey clearly shows that measuring IS is important, but the benefits of measurements can only be seen when the metrics use is applied as a process, with the experience gained from the use of history data. Technical metrics and risk assessment metrics are commonly used, but there is a need to measure individual expertise as well as to automate and rationalise measurements. Most of the organisations do not use IS metrics as a process. However, there are intentions to implement an IS metrics process, as well as to integrate the IS metrics process into quality and business processes. Legislation, customers and technical development especially affect the future development of IS metrics.

Keywords
information security (IS), security metrics, IS metrics, security level, auditing, security processes

Activity unit
VTT Electronics, Kaitoväylä 1, P.O.Box 1100, FIN–90571 OULU, Finland

ISBN			Project number
951–38–6406–5 (soft back ed.) 951–38–6407–3 (URL:http://www.inf.vtt.fi/pdf/)			E4SU000157
Date August 2004	Language English, finnish abstr.	Pages 89 p. + app. 2 p.	Price B
Name of project		Commissioned by	
Series title and ISSN VTT Publications 1235–0621 (soft back ed.) 1455–0849 (URL: http://www.vtt.fi/inf/pdf/)		Sold by VTT Information Service P.O.Box 2000, FIN–02044 VTT, Finland Phone internat. +358 9 456 4404 Fax +358 9 456 4374	

Julkaisija

Julkaisun sarja, numero ja raporttikoodi

VTT Publications 544
VTT–PUB–544

Tekijä(t)
Sademies, Anni

Nimeke

Prosessinäkökulma tietoturvan mittaamiseen suomalaisessa teollisuudessa ja valtionhallinnossa

Tiivistelmä

Tietoturvaratkaisujen tarve lisääntyy koko ajan nykypäivän informaatiotekniikkaa painottavassa maailmassamme. Tietojärjestelmät ovat haavoittuvia monimutkaisuutensa vuoksi ja niihin kuuluu tietoturvattomia osia ja verkkoja. Vaikka turvaratkaisuja on olemassa, jää turvaratkaisun taso usein epäselväksi. Tunnettu periaate on, että kohdetta ei voida hallita hyvin, ellei siitä saada mittaustietoa. Tietoturvan mittaamiseen ei ole tutkimuksessa kiinnitetty suurta huomiota.

Tässä tutkimuksessa selvitetään tietoturvamittareiden käyttöä eräissä suomalaisissa teollisuus- ja valtionhallinnon organisaatioissa. Tietoturvan mittaamisen käytännön sovelluksia ja niiden yhteyttä tutkimuskirjallisuuteen tarkastellaan erityisesti prosessinäkökulmasta. Tutkimuksessa analysoidaan, millä tavoilla ja tekniikoilla tietoturvan mittausta kehitetään ja toteutetaan, sekä arvioidaan tulevaisuuden näkymiä tällä saralla. Tutkimus koostuu kirjallisuustutkimuksesta sekä haastattelu- ja analyysiosioista. Haastatteluosiossa haastateltiin kahdeksaa eri teollisuuden ja valtionhallinnon organisaation edustajaa käyttäen puolistruktukturoitua teemahaastattelumenetelmää. Haastattelutulokset luokitellaan soveltuvaa luokittelumenetelmää käyttäen ja analysoidaan tulkitsevalla analyysimenetelmällä.

Tutkimus osoittaa selvästi, että tietoturvan tason mittausta pidetään tärkeänä, mutta mittaamisen edut tulevat esille vasta kun mittareita sovelletaan prosessimuodossa, jolloin voidaan hyödyntää historiatietoja. Teknisiä mittareita ja riskinarviointia käytetään yleisesti. Tarvetta on erityisesti henkilöiden tietoturvakäyttäytymisen mittaamiselle, samoin kuin mittauksia automatisoinnille ja järkeistämiselle. Useimmat organisaatiot eivät hyödynnä mittareita prosessimuotoisina. Monilla on kuitenkin aikomuksena toteuttaa tietoturvan tason mittaaminen prosessina, samoin kuin integroida kyseessä oleva prosessi osaksi laatu- ja liiketoimintaprosesseja. Tietoturvan mittaamisen tulevaisuuden kehitykseen vaikuttavat erityisesti lainsäädäntö, asiakkaat ja tekninen kehitys.

Avainsanat
information security (IS), security metrics, IS metrics, security level, auditing, security processes

Toimintayksikkö
VTT Elektroniikka, Kaitoväylä 1, PL 1100, 90571 OULU

ISBN			Projektinumero
951–38–6406–5(nid.) 951–38–6407–3(URL: http://www.vtt.fi/inf/pdf/)			E4SU000157
Julkaisuaika	Kieli	Sivuja	Hinta
Elokuu 2004	Englanti + suom. tiiv.	89 s. + liitt. 2 s.	B
Projektin nimi		Toimeksiantaja(t)	
Avainnimeke ja ISSN VTT Publications 1235–0621 (nid.) 1455–0849 (URL: http://www.vtt.fi/inf/pdf/)		Myynti: VTT Tietopalvelu PL 2000, 02044 VTT Puh. (09) 456 4404 Faksi (09) 456 4374	

VTT PUBLICATIONS

Tätä julkaisua myy	Denna publikation säljs av	This publication is available from
VTT TIETOPALVELU PL 2000 02044 VTT Puh. (09) 456 4404 Faksi (09) 456 4374	VTT INFORMATIONSTJÄNST PB 2000 02044 VTT Tel. (09) 456 4404 Fax (09) 456 4374	VTT INFORMATION SERVICE P.O.Box 2000 FIN–02044 VTT, Finland Phone internat. +358 9 456 4404 Fax +358 9 456 4374

ISBN 951–38–6406–5 (soft back ed.)
ISSN 1235–0621 (soft back ed.)

ISBN 951–38–6407–3 (URL: http://www.vtt.fi/inf/pdf/)
ISSN 1455–0849 (URL: http://www.vtt.fi/inf/pdf/)