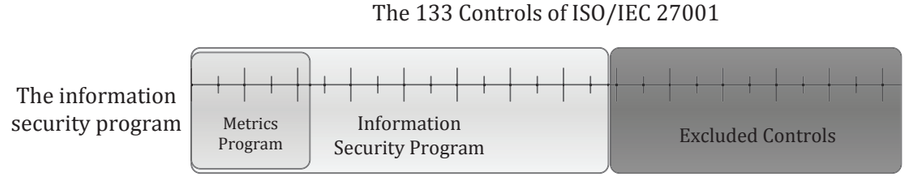
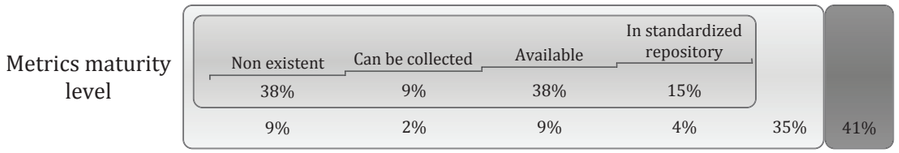
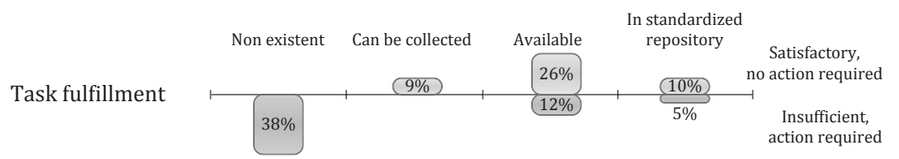
A Framework for Inter-Organizational Comparisons of Information Security Capabilities

HELENA GRANLUND, KRISTOFFER LUNDHOLM,
JONAS HALLBERG, MARGARETHA ERIKSSON







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

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

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

www.foi.se

FOI-R--3186--SE
ISSN 1650-1942

Methodology Report
March 2011

Information Systems

Helena Granlund, Kristoffer Lundholm,
Jonas Hallberg, Margaretha Eriksson[1]

A Framework for Inter-Organizational Comparisons of Information Security Capabilities

[1] Stockholm University, DSV

Titel	Ramverk för inter-organisatoriska jämförelser av informationssäkerhetsförmåga
Title	A Framework for Inter-Organizational Comparisons of Information Security Capabilities
Rapportnr/Report no	FOI-R--3186--SE
Rapporttyp Report Type	Metodrapport Methodology Report
Månad/Month	Mars/March
Utgivningsår/Year	2011
Antal sidor/Pages	26 p
ISSN	ISSN 1650-1942
Kund/Customer	Myndigheten för samhällsskydd och beredskap, MSB
Projektnr/Project no	B7110
Godkänd av/Approved by	Hans Frennberg

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

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

Sammanfattning

Förmåga att bedöma organisationers informationssäkerhet är grundläggande för kvalitén hos relaterade riskhanteringsbeslut. Svenska myndigheter ska hantera informationssäkerhet i enlighet med etablerade standarder för ledningssystem för informationssäkerhet (LIS), såsom standarderna ISO/IEC 27001 och ISO/IEC 27004.

Ramverket som presenteras i denna rapport stödjer detta arbete genom att tillhandahålla ett tillvägagångssätt för att värdera mognadsgraden hos det metrikprogram vilket ska vara en del av varje LIS. Nyttjande av ramverket ger indikationer på mognadsgraden hos metrikprogrammet liksom hur långt införandet av ett LIS har kommit. Dessa resultat kan nyttjas för jämförande av organisationer samt utgöra en grund för diskussioner och utbyte av erfarenheter relaterade till LIS och metrikprogram för informationssäkerhet.

Vi anser att ett nyttjande av ramverket bland svenska myndigheter kommer att förbättra förutsättningarna för:

- lärande avseende informationssäkerhet, såväl inom enskilda myndigheter som myndighetsöverskridande
- kontrollerad styrning av myndigheters informationssäkerhet
- granskande myndigheter att bedöma lämpligheten hos specifika LIS

Nyckelord: Informationssäkerhet, Metrik, Ledningssystem för informationssäkerhet (LIS), ISO/IEC 27001, ISO/IEC 27004

Summary

The ability to evaluate the information security capabilities of organizations is vital for the adequateness of the associated risk decisions. Swedish government agencies are supposed to address information security in accordance with the established standards for Information Security Management Systems (ISMS), such as the ISO/IEC 27001 and ISO/IEC 27004.

The framework presented in this report supports this effort by providing means to evaluate the maturity of the information security metrics program that is supposed to be part of the ISMS. Applying the framework will provide illustrations of the maturity of the metrics program, as well as the overall results of the implemented information security metrics. These results can be used for comparisons of organizations as well as the basis for discussions and exchange of knowledge related to ISMS and information security metrics programs.

We foresee that the application of the framework among Swedish government agencies will support their intra- and inter-organizational learning as well as the strategic management of the ISMS. Moreover, the ability of regulatory authorities to evaluate the ISMSs of agencies will benefit from the potentially increased transparency.

Keywords: Information security, Metric, Information security management system (ISMS), ISO/IEC 27001, ISO/IEC 27004

Contents

1 Introduction

Information security is a crucial quality aspect of government agencies. Among other things, agencies need to maintain business efficiency, protect employees and citizens, and meet regulatory requirements. Traditionally, information security has been handled mainly as a technical issue. The ISO/IEC 27000 series of standards, starting with ISO/IEC 27001, acknowledges the need for information security management systems (ISMS) in order to integrate information security aspects with the overall organizational development (ISO/IEC, 2005).

Swedish government agencies are mandated to act in accordance with the standards (Hedström, 2009). The ISO/IEC 27001 sets strict demands for an operational control environment; an adequate risk analysis and information security policy is mandated; active work with controls should be performed; structured IS education should be given to employees; regular monitoring, management and development of the ISMS should be performed.

The COntrolled INformation Security (COINS) research project, funded by the Swedish Civil Contingencies Agency, was established in order to address the needs of understanding, learning, and managing information security. The COINS project aims at providing knowledge, methods, and tools to support the improvement of the information security abilities in organizations, with a focus on Swedish government agencies. The framework presented in this report is based on the results of case studies performed within the COINS project, on the ISO/IEC 27000 series of standards and on the capability maturity model of the National Institute for Standards and Technology (NIST) (Chew et al., 2008).

1.1 Motivation

Experience has shown that even motivated government agencies with opportunities and resources for an adequate information security program can fail to implement a functioning ISMS (RiR, Swedish National Audit Office, 2007). The difficulty originates from the need to consciously control a number of parallel processes like the monitoring, management, and development of information security in accordance with current policy.

The possibility to compare the information security programs at different agencies would provide several benefits. A common framework would first and foremost support learning and shared experiences between organizations, which would motivate the agencies that have not yet established a functional ISMS. A framework would also provide the agencies with a tool for strategic management of their information security maturity and thus encourage the agencies that

already have a functional ISMS. Moreover, external parties, such as regulatory authorities, would gain from the potential transparency.

1.2 Problem Formulation

In order to provide a framework for inter-organizational comparisons of the maturity of information security programs, there are several issues that need to be considered. The framework should serve as a long-term support for organizations to systematically ensure that their information security measurement process and information security capabilities are in line with other organizations. It should also serve as a support for inter-organizational reflection and learning about possibilities and solutions for controlled and effective information security activities.

Information security metrics designed through the process specified by the standard ISO/IEC 27004 supports the instrumentation of separate parts of the ISMS, such as the controls prescribed in the standard ISO/IEC 27001. However, there is a lack of a comprehensive picture capturing the overall status of the ISMS. A framework for the comparison of the maturity of information security programs should provide such a comprehensive picture, without revealing sensitive information.

1.3 Contributions

The main contribution is a framework that captures the maturity level of the information security programs in organizations and allows inter-organizational, as well as intra-organizational, comparisons. The framework proposes a common assessment base rooted in the standards ISO/IEC 27001 (ISO/IEC, 2005) and ISO/IEC 27004 (ISO/IEC, 2009) as well as the capability maturity model proposed by NIST (Chew et al., 2008).

2 Background

This chapter describes two concepts which are essential for understanding the context of the framework; first the ISO/IEC 27001 and ISO/IEC 27004 standards, then the NIST capability maturity model visually represented by a five path staircase (Chew et al., 2008).

2.1 ISO/IEC 27001 Standard for ISMS

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

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

ISO/IEC 27001 prescribes a set of 133 information security controls for an ISMS. Not all of these controls will be applicable to all organizations, which is why a Statement of Applicability (SoA) should be defined in each specific organization. The SoA is a document in which all the controls are listed with a motivation to why each is chosen to be included or excluded from the ISMS. For the framework described in this report the SoA is of special interest, as it is the base for the organizations information security program. For included controls the SoA should state which are currently implemented and when the remaining controls are planned to be implemented.

2.2 ISO/IEC 27004 standard on Metrics

The ISO/IEC 27004 standard concerns the design and use of an information security *measurement program*. To define such a program, metrics (named measurement constructs in ISO/IEC 27004) are designed for each of the controls in the ISMS of the organization. The standard assumes that there is an implemented ISMS as described in ISO/IEC 27001. Even if there is no ISMS, it is still possible to use the method described in ISO/IEC 27004 for the design of metrics to measure other controls than those prescribed in ISO/IEC 27001.

The design process for a single metric according to ISO/IEC 27004 is shown in Figure 1. The process is performed for each control to be measured. If such a control is too extensive for one metric, several metrics may be designed.

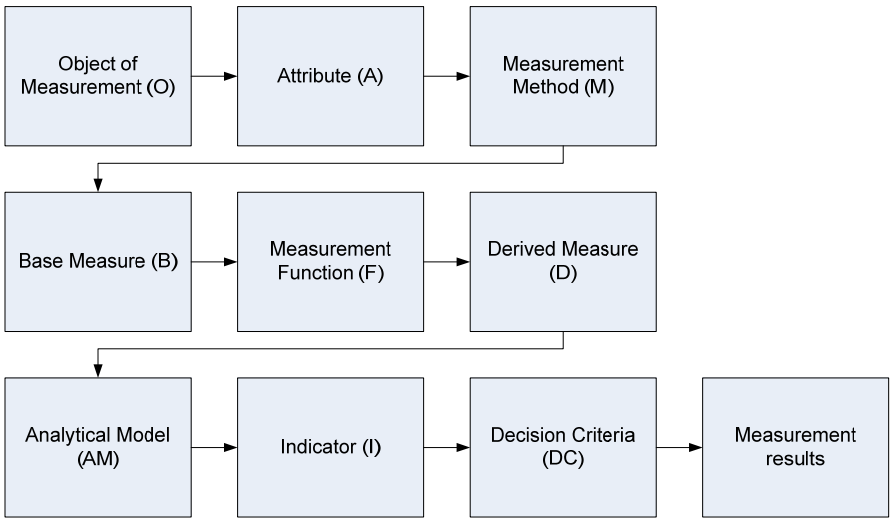


Figure 1: The process steps in designing measurement constructs as described in the standard ISO/IEC 27004

The process starts by identifying *objects of measurement (O)*, i.e. actual places from which information can be gathered. A set of *attributes (A)* is defined. The attributes determines which data to be extracted from the objects of measurement. The *measurement method (M)* states how the data collection defined by the attributes is to be made, and the result from this data collection is called *base measures (B)*. The base measures can then be combined using *measurement functions (F)* which aggregate data. The result from this aggregation is called a *derived measure (D).*

An *analytical model (AM)* use the derived measures and/or some base measures to further aggregate the data. The aggregation produces an *indicator (I)* which is compared to the reference values defined in the *decision criteria (DC)*. The comparison of the reference values with the actual values gives the *measurement results*.

2.3 The NIST Staircase

The NIST staircase (Figure 2) for the maturity of an information security program consists of four steps where each step represents an increased level of maturity. The maturity of the information security program determines the type of measures (the NIST definition of a measure is close to what this report defines as a metric) that can be collected. Once *IT security goals* have been defined, *implementation* measures should be created in order to measure how far the security program is in its implementation. When a process is mature enough to be

considered fully implemented, *effectiveness/efficiency* measures should be used to support the alignment of the security processes to the security goals. Finally, *business impact* measures should be used to gain knowledge concerning how the security program is affecting the operation of the organization (Chew et al., 2008).

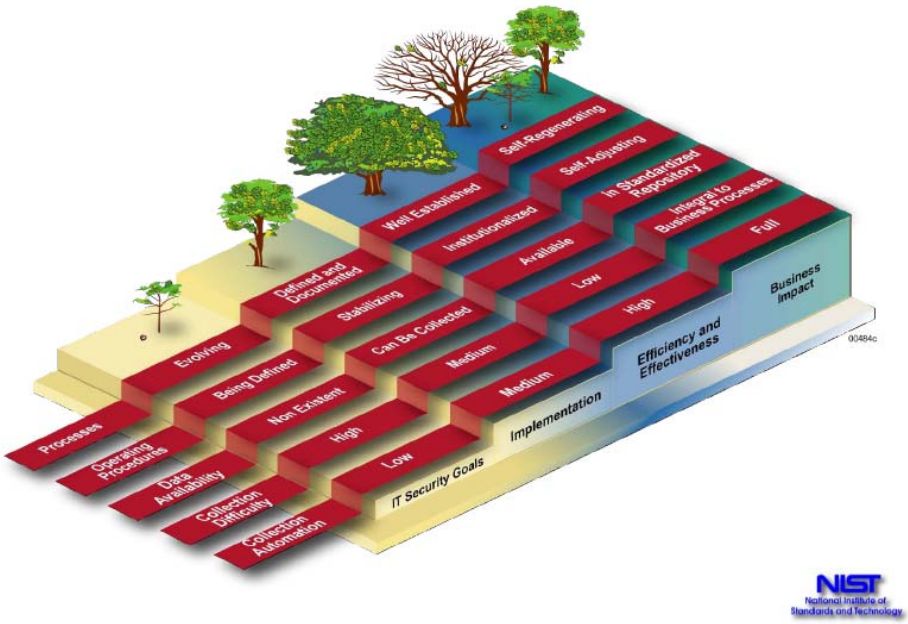


Figure 2: The information maturity levels as specified by NIST

The NIST staircase and its five paths can be used as a model to add comprehension in an organization to the metrics designed according to the process described in ISO/IEC 27004. The path *Data availability* concerns the state of the organizations data and is crucial for the metrics program as measurements can not be performed without data. The framework described in this report is based on this path (Figure 2). However, the data availability path is coupled to the other paths. As *processes* become more standardized and repeatable and as *operating procedures* become more detailed and documented, the information security program may produce a greater amount of data. The additional data can be used as input for the metrics program. Thus, the maturity of the metrics program depends on the maturity of the security program.

2.4 Terminology

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

Control. In this context, controls signify means to manage risk. That is, the information security is supported by a number of controls, whose implementation address social and technical aspects of information security. The standard ISO/IEC 27001 (ISO/IEC, 2005) includes 133 controls to be considered when establishing an **information security management system** (ISMS).

Information security. Information security relates to information assets and the ability to uphold security-related characteristics, such as confidentiality, integrity, and availability (Gollmann, 2006; ISO/IEC, 2009a). Consequently, information is a vast area including administrative as well as technical security issues. Contrary to IT security, information security includes issues related to information processing not connected to information (IT) systems, such as transmission by speech or paper documents.

Information security assessment (security assessment). Information security assessments are performed in order to establish how well a system meets specific security criteria. The aim of an IT security assessment is to produce knowledge, which can, for example, be used to improve the security levels of the assessed system. Although perfect security should be the goal, it cannot be achieved. By increasing the knowledge of the assessed system, security assessments improve the validity of the corresponding actors' perception of the information security. Although security assessments cannot guarantee any level of security, they can provide a basis for confidence in the assessed system (Bishop, 2003). Thus, the trust in the system may be increased.

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

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

Information security metric (security metric). The purpose of information security metrics is to support the measurement and computation of security values characterizing the information security posture of entities. Studied entities can be, for example, organizations, humans, and routines. There are many interpretations of the term security metrics. Here the following definition is adopted. A security metric contains three main parts: a magnitude, a scale and an interpretation. The security values of systems are measured according to a specified magnitude and related to a scale. The interpretation prescribes the meaning of obtained security values. (Hallberg et al., 2004)

The presence of magnitude and scale means there should be values that can be measured or computed. Moreover, the interpretation of the values, in the context of information security posture, should be possible. However, to achieve measurability and computability on one hand and interpretability on the other hand has proved to be difficult.

Information system. Information systems collect, process, store and distribute information. The term has a general meaning, but is most often used for computer based information systems. The definition includes the technical equipment of a system as well as its human activities and routines (Encyclopædia Britannica, 2011).

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

3 The Framework

The purpose of the framework is to enable inter-organizational comparisons of the maturity of information security programs. In order for such comparisons to be possible, the comparing organizations need a mutual baseline. The ISO/IEC 27001 standard with its 133 controls can serve as such a baseline. To capture the development of information security processes, the framework must be applied at regular intervals. Then it can be used for internal assessment of the individual information security activities as well as for long-term inter-organizational comparisons.

The structure of the framework is divided into three phases. Each of the three phases visualizes one aspect of the information security program. *Phase one* illustrates the extent of the information security program as described by the SoA, *phase two* illustrates the maturity of each of the metrics in the metrics program, and *phase three* illustrates the goal fulfillment for each of the metrics in the metrics program. The framework can be presented as a figure representing the information security program of an organization at one point in time (Figure 7).

During the first phase, a SoA should be derived from the 133 controls of ISO/IEC 27001, Appendix A. The SoA illustrates the extent of the information security effort (Figure 3) by stating which of the 133 controls that should be part of the organization's information security program, as well as providing a motivation for why the rest of the controls are excluded.

During the second phase, the individual metrics of the metrics program are classified according to the NIST staircase (Chew et al., 2008). Each metric is analyzed and mapped to one level in the staircase. To illustrate this, all metrics are summarized at each level to provide an overview of the maturity of the complete metrics program (Figure 5).

During the third and final phase, the fulfillment of the goal for each metric is recorded in the appropriate step of the NIST staircase (Figure 6).

It should be noted that the framework indicates the ability of organizations to evaluate the maturity of their information security program. A good evaluation result does not automatically guarantee that the information security is adequate. However, what gets measured can be acted on; hence the evaluation may improve the security level as a side-effect.

3.1 Phase one: Illustrating the Extent of the Information Security Program

The first phase is based on the 133 controls in the standard ISO/IEC 27001. It should be noted that if the organization already has defined a SoA and already maintains an information security metrics program, this phase will only require data on the number of included and excluded controls (Figure 3).

3.1.1 Definition of a SoA

Defining a SoA consists of reviewing the 133 controls in ISO/IEC 27001, Appendix A, and for each control document whether it is relevant for the organization to implement, or if it should be excluded. It is important to thoroughly motivate all exclusions of controls. The controls that are selected as relevant, forms the information security program of the organization. The classification of controls as included or excluded is the basis of the framework (Figure 3).

3.1.2 Definition of a Metrics Program

The *metrics program* consists of all controls of the information security program for which there are security metrics implemented. The design of metrics to measure the fulfillment of the goals provided by the selected controls can be done according to the method described in the standard ISO/IEC 27004 (ISO/IEC, 2009). To illustrate the portion of the information security program that is currently the subject of a metrics program, the metrics program is displayed in the figure as a sub-area of the information security program (Figure 3).

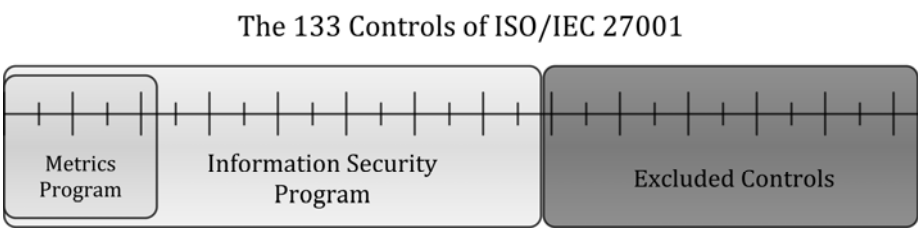


Figure 3: The first phase, the extent of the information security program

3.2 Phase Two: Maturity Level of Metrics

The second phase classifies the individual metrics in the metrics program. To do this, the maturity level of each metric is evaluated and categorized according to

the *data availability path* of the NIST staircase. Each metric is mapped to one step in the staircase, resulting in a set of metrics from the information security metrics program belonging to each of the steps. This provides the organization with an overview of the maturity of the whole metrics program.

3.2.1 The Data Availability Path of NIST Staircase

The NIST staircase (Chew et al., 2008) is used to define maturity levels for the metrics of the information security metrics program. The NIST staircase consists of four steps and five paths (Figure 2). In this phase, only the *data availability path* is used. For the other four paths, it is assumed that data availability is supported by sound and relevant processes and instructions, as well as some degree of data collection automation.

3.2.2 Classification of Metrics for the Measurement of Control Objectives by Using the Data Availability Path

This classification of a metric is related to the maturity of the process for collecting security related data, that is, the metric itself, not the maturity of the measured processes. There is no known correlation between the maturity of the process to collect data in a metrics program and the actual security level of the organization. The data collection process for a control may be mature; however the maturity of the actual security control may still be insufficient. Still, without measurement it is impossible to know whether the information security processes are mature or not.

In the example illustrated in Figure 4, there are 32 controls in the metrics program. These 32 controls must be reviewed with regard to how mature the process of collecting the data for the corresponding metrics actually is. As an example, consider the following distribution. There are 12 metrics for which the data availability is *non existent* (38%), 3 metrics for which data *can be collected* (9%), 12 metrics for which data is *available* (38%), and 5 metrics for which data is *in standard repository* (15%) (Figure 4). The figures in this example are fictive and selected to provide an illustrative example.

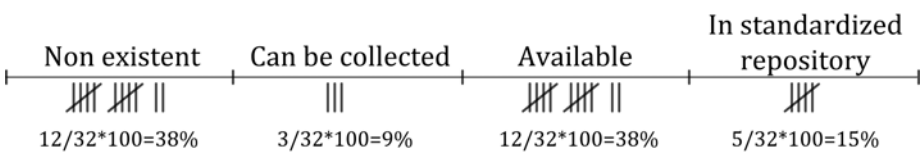


Figure 4: Classification of metrics as presented in the example

One control may have more than one metric. When this is the case, the metric with the highest maturity rating will represent the control in the calculation. The

motivation for this approach is to ensure that an organization with several metrics for one control continues working with the less developed metrics. It could be tempting to skip metrics with low maturity level in order to improve the visible result.

3.2.3 Results for the Metrics Classification

The second phase consists of a classification of the maturity levels of the metrics used by the organization. The metrics are classified according to the steps in the NIST staircase. This is illustrated by the innermost frame in (Figure 5). In order to provide a complete overview of the metrics program in relation to the information security program, the distribution of the maturity of the metrics is complemented by indicating the maturity of the metrics for each step, in relation to the whole information security program. This is illustrated by the numbers at the bottom of (Figure 5). The dark gray area (41%) represents the controls that are excluded from the information security program and the 35% adjacent to the dark gray area represents the controls that are going to be implemented but currently are not measured by any metrics.

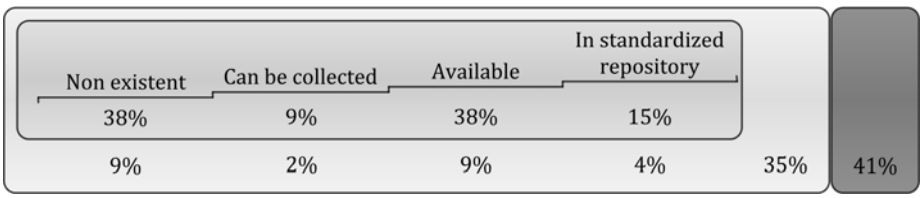


Figure 5: The second phase, the classification of metrics

3.3 Phase three: Summarizing Fulfillment of Metrics Goals

The third phase deals with the result of each metric mapped to the steps of the NIST staircase. The comparison presents the percentage of controls for which the goals for the measurement are fulfilled, as well as the controls that did not fulfill the goals. The percentages are presented for each step to give an overview of the quality of the controls instrumented by the metrics (Figure 6). The illustration extends the upper part of Figure 5 by adding information on the fraction of controls whose metrics have satisfactorily or insufficiently fulfilled goals respectively. Thus, the sum of the percentages presented for each step of the NIST staircase in Figure 6 equals the percentages in the upper part of Figure 5 and the total in Figure 6 equals 100%.

In the fictive example there is a high percentage (38%) of metrics with *non existent* data availability. For these metrics the fulfillments automatically are

insufficient and actions are required. A large set of metrics at the first maturity level, *non existent*, may pose a risk that the controls to design metrics for have been chosen without prior knowledge of what is possible to measure in the organization. It could be a sign of the organization having a clear picture of what metrics are needed. However, choosing a realization course that includes too much work with developing data collection abilities might take focus from what actually matters, that is the intended information security. In order not to stretch the resources of the metrics program, it might be more productive to focus on a few selected metrics.

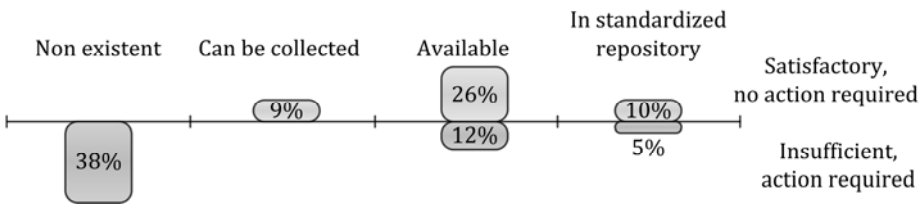


Figure 6: The third phase, the rating of task fulfillment

3.4 Compiled Results

The concluding illustration of the framework is a combination of Figure 3, 5 and 6. It provides insights for intra- and inter-organizational information security comparisons and discussions (Figure 7).

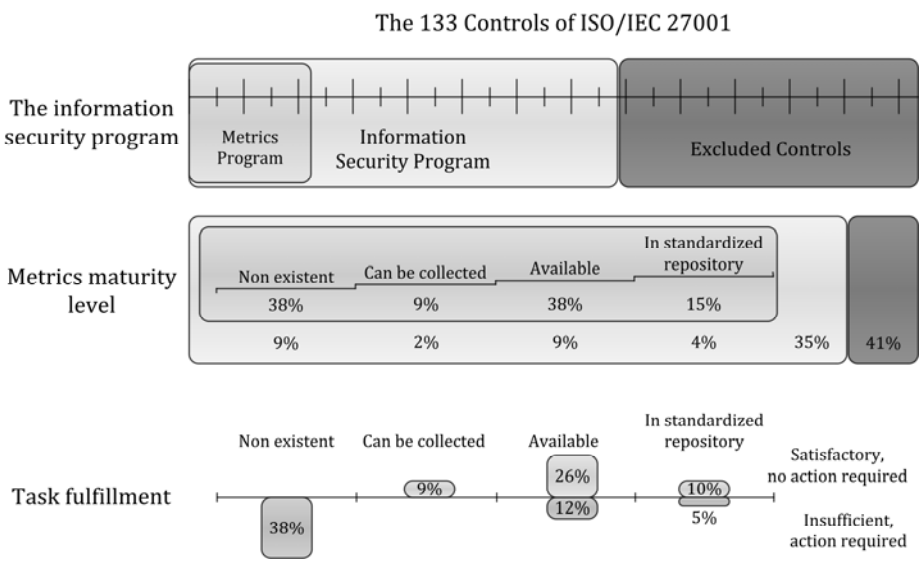


Figure 7: The concluding illustration of the three phases of the framework

4 Case Study

To provide insight into how the framework can be applied to information security measurement programs of organizations, the experiences form a preceding case study is presented. The case study uses a set of five metrics from a recently started metrics program at a Swedish government agency.

The agency did not have a SoA and no SoA was developed in the context of the study. Thus, the case study will only illustrate how the framework can be used for internal comparisons concerning the maturity development of a metrics program over time.

The metrics used are connected to the controls; 8.2.2 Information security awareness, education and training, 9.1.2 Physical entry controls, 10.5.1 Information back-up, 13.1.1 Reporting information security events, and 13.2.2 Learning from information security incidents from ISO/IEC 27001 appendix A. The report *Design and Use of Information Security Metrics: A Case Study* provides a complete description of the definition of the metrics used (Lundholm et al., 2011).

4.1 Classification of the Metrics

A classification of the five metrics, each connected to the respective control, is presented in Table 1. The classification of the *data availability* according to NIST staircase for each metric was obtained by a subjective judgement performed by one of the researchers. It should however be straight forward to perform a classification by simply making a judgement for each metric concerning the data availability for the measurements performed.

Table 1: Maturity classification of the studied metrics

Control	Data availability classification	Motivation for classification
8.2.2 Information security awareness, education and training	Can be collected	Manual questioning of managers required for measurement
9.1.2 Physical entry controls,	Can be collected	Manual calculations on the log data required
10.5.1 Information back-up	Available	Data can be obtained through database queries
13.1.1 Reporting information security events	Can be collected	Information is collected through a manual process
13.2.2 Learning from information security incidents	Can be collected	Data acquisition is performed by a manual process

From analysis in the metrics report it was found that none of the five metrics, fulfilled the criteria specified in the metric (Lundholm et al., 2011). The decision criteria for the metrics were intentionally set to not automatically be fulfilled, since improvements of the corresponding controls were desired.

Combining the information about classification according to the NIST staircase with the information about fulfillment of the metrics provides the result shown in Figure 8.

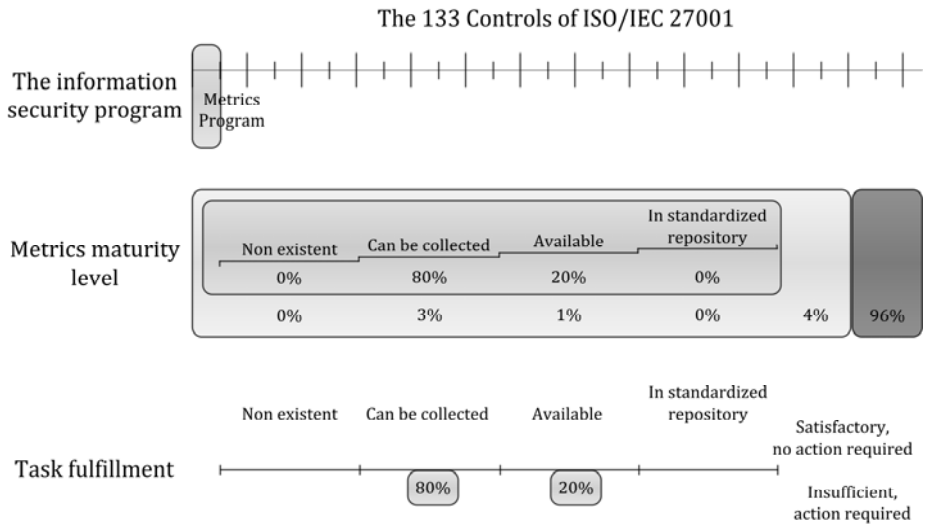


Figure 8: The three phases for the 5 controls in the case study

4.2 Possible Comparisons of Results

As mentioned above, the agency for which the metrics were designed had no SoA. Since there is no SoA, the result of the case study can only be used for internal comparisons, and not for inter-organizational comparisons. Considering the small sample size, it might not be useful to perform inter-organizational comparisons at this early stage in metrics development.

The framework provides an easy way of illustrating the current maturity level of an organizations information security metrics program, it is well suited for managers to gain quick insight in how the program is developing. If the framework is used regularly, comparisons about the maturity level can be made from one point in time to the next.

5 Discussion

A framework for comparison of information security metrics programs has evident benefits. It supports learning and the sharing of knowledge and experience between organizations. The gained knowledge may be used as the basis for informed decisions.

The framework itself is developed with the intention not to impose too much additional work for the organization. However, the preparatory work needed to use the framework may require a substantial effort, especially considering the process of defining a SoA. The effort required to start using the framework is discussed in section (5.1). The two different ways of performing comparisons, with or without common baseline, both benefit learning for the organization and is further discussed in section (5.2). The discussion concludes with reflections and recommendations (5.3).

5.1 Required Effort

In order to use the framework to its full extent, an organization needs to have a SoA and an implemented metrics program. If the organization has neither of these, three activities must be performed in order to use the framework; establish a SoA, design and implement a metrics program, and classify the metrics according to the NIST staircase. Most likely few organizations have a defined SoA or a documented metrics program.

Establish a SoA is the most demanding activity for an organization since it involves performing a risk analysis for each of the 133 controls of the standard ISO/IEC 27001(ISO/IEC, 2005), followed by a decision about whether the risk conveyed by the control can be disregarded or not. The presence of a SoA is beneficial for the organization as a basis for informed information security decisions. However, since a lot of work is required to establish a SoA, there is a risk for organizations abandoning their intentions due to lack of visible results.

In order to provide the organization with intermediary result, the framework was designed with the ability to illustrate an organizations measurement maturity development without an explicit SoA. The value of using the framework without a SoA is further discussed in the next section (5.2), whereas some recommendations for parallel development of the SoA and the metrics program are presented in section 5.3.

A metrics program is needed in order to use the framework and has to be designed and implemented, if it does not already exist. The design and implementation can be performed with two opposite approaches, and any intermediate combination of the two. The first approach is to strictly follow the workflow as recommended by the standards ISO/IEC 27001 (ISO/IEC, 2005)

and ISO/IEC 27004 (ISO/IEC, 2009). The second approach is to follow a workflow where the needs systematically defined by information security professionals are matched to available data.

The first approach will, if strictly implemented, result in an information security metrics program with full coverage of the controls for which the metrics are designed. When strictly followed, the first approach will require a lot of work, especially if the information security program is immature. This approach is only recommended for organizations with mature information security programs.

The second approach will allow the organization to learn and develop a broad ability to handle metrics. It will let the information security program mature with less work effort. However, it might not result in an information security metrics program with full coverage of the controls for which the metrics are designed. Lundholm et al. (2011) thoroughly discuss the design of metrics using the second approach. This approach is recommended for all information security programs that are not yet mature enough to use the first approach.

Classifying the metrics to the steps of the NIST staircase requires subjective judgments. Thus, this task needs to be performed by persons familiar with the metrics. The effort required to perform the classification should be low, in comparison to establishing the SoA.

5.2 Comparisons With and Without Common Baseline

If organizations want to utilize the framework as intended, that is, perform inter-organizational comparisons, a SoA is required. On the other hand, if an organization only intends to use the framework as an internal evaluation tool, any other approach to identify the controls to be measured than the SoA can be used.

For inter-organizational comparisons the SoA serves as the baseline which all involved organizations have in common. It is the means for organizations to be able to refer to common concepts and have a common understanding of the controls referred to by the framework. Without common concepts the comparison *between* organizations becomes ineffective.

This being said, even without a SoA the framework can still be used for internal assessment *within* the organization. By doing so, the organization will have a tool for learning about its information security development over time.

Relating to the case study presented in chapter 4, the studied agency did not have a SoA but still designed a set of metrics for the evaluation of the information security work. In this initial phase the framework can not be used for full comparisons with other organizations. The framework can however be used standalone as an illustration of the organizations internal development in terms of

maturity. When the SoA finally is developed and the metrics program adjusted to it, the utility of framework can be extended to comparisons between organizations as well as providing an insight to the maturity development of the metrics program.

5.3 Reflections and Recommendations

A suggestion for initial work with the framework is to work in parallel to develop both the SoA and the metrics. The development of the SoA will require a lot of work, and to be able to show some intermediate results it is recommended that metrics for the most relevant controls are developed in parallel with the SoA. Developing metrics while establishing the SoA can provide the organization with knowledge about the information security risks and, thus, facilitate the risk analysis that forms the basis for the SoA. If a SoA has already been defined in the organization, a large part of the prerequisites for using the framework inter-organizational is already available.

The framework is meant to enable inter-organizational comparisons of information security measurement programs, which serves as an indicator for the maturity of the information security program itself. Although the framework is designed to compare the information security metrics programs between organizations, another value in using it will be a common base for the discussion of the management of and the approaches to the information security program.

When an organization defines a SoA, it verifies that it has taken all the controls from ISO/IEC 27001 Appendix A into consideration. However, the list of controls in the standard does not cover all areas of information security. Defining specific controls for each organization could be necessary. These controls should be included to generate an expanded SoA. A problem with adding organization-specific controls to the SoA is that the ability to compare the information security metrics programs to other organizations will be impaired. It would be beneficial to have a central repository of controls for organizations that wants to be able to compare their measurement program to other organizations. Thus, an organization can re-use the controls added by other organizations.

For Swedish government agencies, the central repository for additional controls could be managed by for example the Swedish Civil Contingencies Agency. Each agency would have access to all controls the other agencies have defined as relevant for their information security program. Each agency may then consider additional controls and add them to their information security program, if relevant.

It is important that agencies perform a risk analysis concerning each of the controls they add to the repository and that the controls deemed irrelevant for the information security program are excluded. Since the goal is to eventually have

measurements for all controls in the information security program, measuring irrelevant controls is a waste of resources.

6 References

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

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

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

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

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

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