Design and Use of Information Security Metrics

Application of the ISO/IEC 27004 standard

KRISTOFFER LUNDHOLM, JONAS HALLBERG,
HELENA GRANLUND

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--3189--SE
ISSN 1650-1942

Scientific report
March 2011

Information Systems

Kristoffer Lundholm, Jonas Hallberg,
Helena Granlund

Design and Use of Information Security Metrics

Application of the ISO/IEC 27004 standard

Titel	Design och användning av metriker för informationssäkerhet baserat på ISO/IEC 27004
Title	Design and Use of Information Security Metrics: Application of the ISO/IEC 27004 standard
Rapportnr/Report no	FOI-R--3189--SE
Rapporttyp Report Type	Scientific report
Månad/Month	Mars/March
Utgivningsår/Year	2011
Antal sidor/Pages	57 p
ISSN	ISSN 1650-1942
Kund/Customer	Myndigheten för samhällsskydd och beredskap, MSB
Projektnr/Project no	B7110
Godkänd av/Approved by	Magnus Jändel

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

Den internationella standarden för framtagande av ett ledningssystem för informationssäkerhet (LIS), ISO/IEC 27001, har funnits tillgänglig sedan 2005. I denna standard finns det ett krav på att mätningar som påvisar hur väl en organisations LIS fungerar, ska genomföras. En metod för utveckling av dessa mätningar publicerades 2009 i standarden ISO/IEC 27004.

Denna rapport presenterar en studie som genomförts på en Svensk myndighet. Syftet med studien var att utvärdera en metod för att ta fram informationssäkerhetsmetriker. Den metod som användes i studien är en utökad version av den metod som presenteras i standarden ISO/IEC 27004. I standarden finns en mall för vilken data som behövs för att definiera en metrik; till denna har användande av medverkande design lagts till för att identifiera den information som behövs vid skapandet av metriker.

Första steget i den använda metoden var *val av åtgärder* som metriker skulle tas fram för, här identifierades fem åtgärder från ISO/IEC 27001. Nästa steg var att *ta fram metriker* för dessa fem. Framtagandet gjordes genom medverkande design bestående av två uppsättningar intervjuer med personal med säkerhetsansvar inom de relevanta områdena, vid myndigheten. Slutligen genomfördes *mätningar med de framtagna metrikerna*. Mätningarna genomfördes av de respondenter som intervjuats vid framtagandet medan sammanställning av resultatet genomfördes av en av de medverkande forskarna.

Från studien drogs slutsatsen att framtagande av ett metrikprogram för organisationer vars informationssäkerhetsprogram ännu inte är mogna bör inledas med identifierande av intressanta områden att mäta på. När detta har gjorts bör metrikprogrammet skapas så att de data som krävs finns lätt tillgängliga. Metrikprogrammet bör sedan successivt utökas till att innefatta insamlande av data som är mer svåråtkomligt. En viktig slutsats är även att närvaron av ett metrikprogram stödjer utvecklingen av organisationens LIS vilket i förlängningen kommer att leda till att mer data kommer att finnas tillgänglig.

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

Summary

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

This report presents a case study performed at a Swedish government agency. The aim of the study was to evaluate a method for the design and implementation of information security metrics. The used method is based on the method outlined in the standard ISO/IEC 27004 augmented with a participatory design approach. The standard provides a template for the specification of metrics, whereas the augmentation is essential in order to extract the information needed from the agency in order to be able to design the metrics.

The first step, *selection of controls* (from ISO/IEC 27001) for which to design metrics, resulted in five controls. The next step was to *design metrics* for these controls. The design was performed through a participatory design process consisting of two sets of interviews with security personnel, whose responsibilities correspond to the security areas of the controls. The final step was *measurement using the metrics*. The measurements were performed by the security personnel involved in the design of the metrics, whereas the actual results presentations were prepared by one of the participating researchers.

From the study it was concluded that the design of metrics programs for organizations with immature information security programs should probably be initiated by identifying areas of interest for measurement. Next, the metrics program should be designed to gather data that is readily available and gradually expanded to measurements requiring data that is more difficult to collect. A vital point is that the presence of metrics programs supports the efforts to make the ISMS more mature and, thereby, improves the availability of data to be measured.

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

Contents

1 Introduction

There are several factors indicating the increasing importance of information security in public organizations. The increased connectivity of government systems to the internet for example leads to increased privacy threats which must be handled in order to retain the trust of the public. The removal of manual routines for information management results in information systems becoming more business-critical. In modern organizations the result is that many business processes are severely hampered when information systems become unavailable. The awareness of the public is stimulated by the continuous debate on privacy issues, as well as individuals' personal experience of security flaws. The increased public awareness leads to an increased demand for organizations to provide trustworthy information systems.

Consequently, the ability to reach adequate levels of information security is important. Since it is not possible to build information systems security on merely technical solutions, successful information security programs have to involve the human, organizational, and technical aspects of organizations. Metrics, measuring the overarching information security includes these aspects of organizations and can be used as a validation of the will of organizations to counter information security risks.

1.1 Motivation

The standard ISO/IEC 27001 for the management of organizations' information security was published in 2005 (ISO/IEC, 2005). It has, since then, been widely accepted as a mean to successful information security programs in organizations. In Sweden, all agencies are mandated to implement information security programs consistent with the standard. In the standard, it is stated that the performance of the management system should be monitored. However, how this is to be implemented is not described in the document. To alleviate this lack of instructions, the standard ISO/IEC 27004 for the measurement of the information security performance of organizations was published in 2009 (ISO/IEC, 2009b). The standard ISO/IEC 27004 includes a general description of a process for the design and use of information security metrics. However, it is unclear how this standard can be introduced in organizations.

1.2 Problem Formulation

In general, the aim of the study is to explore the usability of the ISO/IEC 27004 standard. In more detail, the performed study should answer the following questions:

- How does a metrics design process based on the ISO/IEC 27004 standard work when designing information security metrics in an operative organization? This involves the effort required to produce the metrics and the usability and feasibility of the resulting metrics.
- Are the metrics resulting from design processes based on the ISO/IEC 27004 standard usable in the studied organization? This involves the possibility to obtain the required data as well as the ability to produce adequate results and present results for the stakeholders.

1.3 Contributions

The main results of the performed study are:

- A method for the design of information security metrics, based on the standard ISO/IEC 27004.
- Five information security metrics, designed using the presented method.
- Measurements based on the designed information security metrics.
- Analysis of information security, based on the designed metrics and the performed measurements.
- An evaluation of the usability and feasibility of the approach.

1.4 Report Layout

In Chapter 2, the relevant background to the study is presented. In Chapter 3, the method used to design and use the metrics is presented. In Chapter 4, the results of actual design and measurement efforts in an organization are presented. Finally, in Chapter 5, the results are discussed.

2 Background

In this chapter, the background information relevant for this report is presented.

2.1 Needs and Relevant Information Security Characteristics

Acknowledging that the design of information security metrics should be derived from established assessment needs, an analysis was performed at an agency in order to identify these needs (Lundholm & Hallberg, 2011). The analysis was based on statements extracted from interviews with personnel working at the agency, as well as documentation from the agency. The analysis resulted in a structure consisting of 36 information security assessment needs. Based on the structure of needs, another structure of relevant information security characteristics was formed. This structure includes 42 characteristics. The purpose of formulating these relevant information security characteristics was to create a basis for the design of an information security metrics scheme.

In this report, controls included in the standard ISO/IEC 27001 (ISO/IEC, 2005) are mapped to the presented characteristics. A selection of these controls is further used in the presented study (Section 3.1).

2.2 The ISO/IEC 27001 and 27004 Standards

From the ISO/IEC 27000 family of standards on information security management systems two specific standards are central for the work described in this report. Those are the ISO/IEC 27001 *Information technology — Security techniques — Information security management systems — Requirements* (ISO/IEC, 2005) and the ISO/IEC 27004 *Information technology — Security techniques — Information security management — Measurement* (ISO/IEC, 2009b).

2.2.1 ISO/IEC 27001

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

According to the ISO/IEC 27001 standard, a number of actions must be taken when an ISMS is to be implemented. Examples of actions are to define an

information security policy, to conduct a risk assessment, to prioritize among identified risks, and to approach the risks in an intentional and controlled manner.

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

2.2.2 ISO/IEC 27004

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

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

The process of designing a metric according to the ISO/IEC 27004 is shown in Figure 1. In order to facilitate the creation, the template included in Appendix A of the ISO/IEC 27004 is used. The template is included in this report as Appendix A.

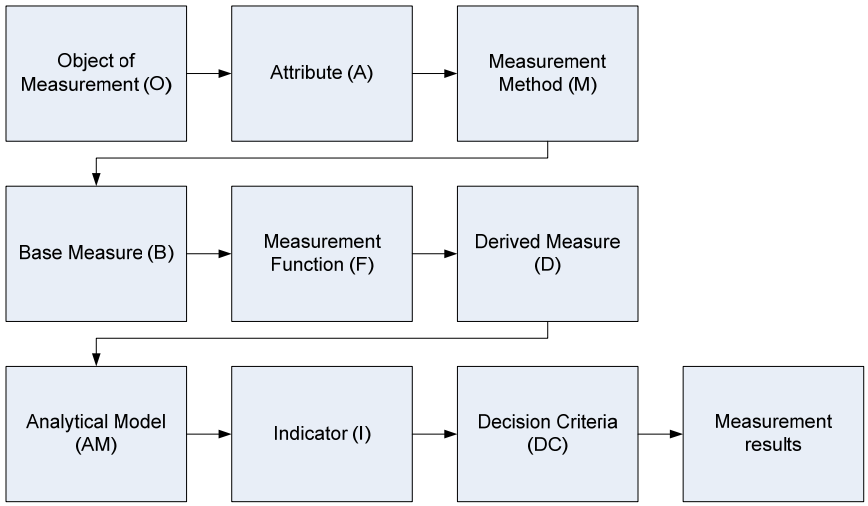


Figure 1: The steps in the design of measurement constructs as described in the ISO/IEC 27004

If the control to be measured is too extensive for one metric, several metrics might need to be designed. The process is then performed for each metric.

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

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

2.3 Study Context

The study was undertaken at one of the largest government agencies in Sweden. The agency uses and maintains comprehensive, centralized data registers. The agency has a close link to the Swedish government and is the central supervisor and coordinator of the local agencies of their branch, with a mission to support

and rationalize their activities. The selected agency may also, by direction of the Government, direct and supervise different activities at the national level.

2.4 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 Method

The aim of this study was, firstly, to design a set of metrics according to the method described in the standard ISO/IEC 27004 and, secondly, to perform measurements of chosen aspects of information security at the studied agency using these metrics. At a general level, the chosen method was to select a small set of controls from the ISO/IEC 27001, design metrics for these controls based on a participatory design process involving personnel from the studied agency and the researchers performing the study, and use the metrics to acquire actual results. The selection of controls was based on an earlier performed needs analysis followed by prioritization by the researchers performing the study. The result from the prioritization was then reviewed and modified by an information security specialist at the studied agency. The metrics design process was based on dialogues between the researchers and the agency personnel and intermediate design work by the researchers. The data collection was performed by the agency personnel, while the aggregation and report generation was performed by the researchers.

The steps taken for designing and using the metrics, presented in chronological order, were:

1. select the controls for which to design metrics
2. conduct a first set of semi-formal interviews
3. design a first version of the metrics
4. conduct a second set of semi-formal interviews
5. finalize the metrics
6. perform measurements using the designed metrics
7. perform aggregations based on the gathered data and create report

Before the interviews, each respondent received:

- a copy of the description of the controls from which the metrics were to be designed
- the template in which the metrics should be documented
- a description of the planned work process for the seven steps above.

3.1 Selection of Controls

This section covers step 1 from the section above.

1. The first thing done in order to start the metrics creation process was to select the controls that the metrics were supposed to measure. To do this, controls from the standard ISO/IEC 27001 were mapped to the relevant information security characteristics describing the view on information security at the studied agency. The analysis resulting in these characteristics was part of a previous study (Lundholm & Hallberg, 2011). The resulting prioritized list of controls from the standard was used as the basis for a prioritization performed by an agency representative, in order to produce a short list of five controls. For this study, five controls were used since it was considered a good compromise between the knowledge gained and the required effort for the studied organization.

3.2 Metrics Design

This section covers step 2 to 5, performing interviews and formulating metrics.

2. At the first set of interviews, a semi-formal discussion of the selected controls was performed with the respondents, using the template from ISO/IEC 27004 (Appendix A) (ISO/IEC, 2009b) as a guide. The purpose of these interviews was to identify relevant measurements for the selected controls, as well as to estimate the effort required to perform these measurements. During the interviews, relevant information was recorded directly in the template when possible. The text inserted into the template was validated by the respondent as the interview progressed. Further information was recorded in personal notes by the interviewers as support for the development during the next step.
3. After the completion of the first set of interviews, the collected material was formalized and structured as to fit into the template. The metrics were completed as much as possible from the gathered data. To facilitate further development of the metrics, suggestions for derived measures, as well as indicators, were prepared in a draft.
4. During the second set of interviews, the drafts were discussed. At this stage, applicable corrections were made and the suggested parts of the metrics were verified or rewritten.
5. Finally, based on the data acquired during the second round of interviews, the metrics were formalized and fully documented. During the finalization of

the metrics any further questions were answered by the respondents via telephone or email.

3.3 Measurements and aggregation

This section covers steps 6 and 7, that is, the measurement and aggregation.

6. The measurements based on the designed metrics were performed by sending the finished metrics to the respondents requesting them to perform the data collection specified.
7. The data from the previous step was aggregated using the approach defined by each specific metric. Further, reports were created according to the specifications of the metrics.

4 The Design and Use of Metrics

This chapter describes how the metrics were designed, including a rough estimate of the time spent on each of the steps described in the method above. The emphasis for the creation of the metrics was usability and feasibility, i.e. the results from measurements should be useful for the organization and the effort required to perform the measurements should be reasonable enough for the metrics to be used.

4.1 Selection of Controls

An earlier study (Lundholm & Hallberg, 2011) resulted in a structure containing 42 relevant information security characteristics (Section 2.1). An initial mapping of the controls from the standard ISO/IEC 27001 to these characteristics resulted in a list of 25 controls. The mapping is illustrated in Appendix B.

The initial prioritization of the controls was performed by a researcher. This prioritization was then reviewed and modified by an information security specialist from the studied agency. Since the security specialist has good insight into which areas it is feasible to design metrics for, the final prioritization was based on knowledge about both the design of security metrics and what parts of the ISMS at the studied agency that were suitable for participation in the study. The prioritization resulted in the five 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
- 13.2.2 – Learning from information security incidents

Further, persons with the knowledge required to design metrics for these controls were identified. Three of the respondents were each associated with one of the controls 8.2.2, 9.1.2, and 10.5.1, while both the controls 13.1.1 and 13.2.2 were assigned to a single respondent. Thus, in this study there are four respondents in total.

4.2 Metrics Design

As described in chapter 3.2, the metrics design was initialized by preparing a draft for an individualized template for each respondent by inserting the selected controls into the template from ISO/IEC 27004. In addition, a short description of the intended method, as well as the expected effort required by the respondent, was documented. These were then sent to the respondents prior to the first interview. The full set of designed metrics can be found in Appendix C

4.2.1 First Set of Interviews

All interviews in the first set followed roughly the same pattern with the main parts being:

- Introduction to the purpose of designing and using the metrics, that is, testing the process outlined in ISO/IEC 27004 as well as providing reports on the measured aspects of security to the respondents.
- A general discussion of the role of the respondent in the organization.
- A specific discussion of the selected control to be measured, including what measurements within this scope that would provide value to the respondent as well as the organization.
- A detailed discussion about what to enter into the fields of the template.

The goal for the first set of interviews was to get a clear view of what to measure, that is, what the object of measurement for each metric should be, which attributes to select as well as a definition of the base measures and the measurement methods. This was, for the most part, accomplished for all five of the controls. Each interview involving a single control lasted for two hours, while the interviews involving two controls lasted for three hours.

Since the controls in the standard ISO/IEC 27001 are not consistent in how much they encompass and since the maturity of the information security management in the organization varied in different areas, the coverage of the metrics varies as well. However, none of the designed metrics fully covers all aspects of the corresponding control. The impact of this is further discussed in chapter 5. The first set of interviews resulted in information on each metric as follows.

4.2.1.1 Control 8.2.2 Information Security Awareness, Education and Training

During the interview it was decided that the metric should include two different areas of measurement. The first to measure the ratio of contractors at a specific

unit who received initial information security training, and the second to measure how many of the units in a specific department that have procedures for providing initial information security training to their employees.

To get the data on the contractors, a document kept by the human resources department was identified as the object of measurement and the attributes needed were records of contractors and whether they have undergone information security training or not. For the second measurement, the manager of each unit were identified as the object of measurement and their knowledge of whether their unit has provided information security training for their employees was identified as the attribute to measure.

The *base measures* that were created during the interview were: number of contractors hired during last month, number of the contractors hired last month that received information security training, and number of units that have an information security training program for contractors.

Since the definition of the metric started with a basic idea of what the measurement function should contain, there was a concluding discussion about how to calculate the desired values as well as the preferred ways to present the data.

4.2.1.2 Control 9.1.2 Physical Entry Controls

Early in the discussion about what to be measured considering this control, a plentitude of alternatives was discovered. Most of these measurements would require a lot of effort from the collector of the data as the interface of the database where the data was stored did not allow for customized queries. Since the motto for the metrics creation was that development and measurement should be possible to do with limited resources, it was decided that the focus for this metric should be to provide data to illustrate a specific problem known to the respondent. The metric was thus decided to be about how often an access card was misused, i.e. how often someone was using their personal access card to open the door for someone else.

The object of measurement was the log database containing data on the use of access cards. Initially the intention was to measure how often access cards are used for multiple admittance for every door in the building. However, the effort required to obtain this data was considered too great. Consequently, only the door perceived as the most troublesome was to be measured. Further, the respondent was mainly interested in checking this door outside office-hours since during office hours there is a guard at the door.

The *base measures* from this interview were: number of times a card has been used for multiple entries outside office-hours, number of entries for each multiple entry, and the total number of entries during non office hours.

The interview progressed from trying to enumerate all kinds of available data, at the start, to trying to limit the amount of effort required for performing the measurement at the end. The reason was that, although the amount of data available was large, the effort required to extract and convert that data into useful information was too great with the limited resources available. During the discussion some notes of potentially interesting ways of aggregating the data was discussed, but no formal decision of what aggregation should be performed was made.

4.2.1.3 Control 10.5.1 Information Back-Up

From this interview it was found that there were a number of goals, set by the agency, for the backup routines, but not all of them were adequately followed up. It was therefore decided to perform measurements that would enable the respondent to show whether or not selected goals were met. The goals to be investigated were that all data requested for restoration actually is restored, and that restoring data should not take longer than 48 hours.

In addition to these measurements, the respondent requested that the metric also included how many restore operations that were performed for two particular systems. The reason for this request was that the respondent knew that restore operations for the first system consume a lot of time, even for small amounts of user data, and that the second system was excluded from the 48 hour requirement.

Since the actual measurements to be performed were quickly identified, the discussions mostly concerned where to acquire the necessary data. The objects of measurement identified for this metric were:

- The system which manages requests for restore operations, with the attribute of interest being the requests for restore operations.
- The logs from the backup system, with the attribute of interest being the amount of time required to perform each restore operation.

The *base measures* found for this metric were: number of recorded requests for restore operations, start and end time for each restore operation, number of restore operations performed for system A, and number of restore opertaions performed for system B.

Since the design of the metric started from goals, the aggregation performed in the metric is meant to show whether or not the goals are fulfilled. Therefore, at

the end of the interview there was a rather clear picture of how aggregation and reporting was to be done.

4.2.1.4 Control 13.1.1 Reporting Information Security Events

During the discussion about what to measure within the boundaries of this control, it became apparent that there were multiple ways of reporting and handling security incidents within the organization. The respondent was responsible for contacting all the different owners of incident data and to periodically summarize the data in a report. It was decided that the measurements should concern how many sources of information that needed to be contacted and how many incidents each of those sources reported. Further, due to some problems experienced by the respondent in obtaining the necessary incident data, it was decided that the metric should also measure the response time, i.e. the time from request to receiving data.

The identified objects of measurement were:

- A spreadsheet used to keep track of incidents with the relevant attributes being those rows in the spreadsheet which concern incidents.
- The person responsible for producing incident reports, i.e. the respondent, where the relevant attributes were knowledge about incident reporting.

The *base measures* found for this metric were: number of sources for incident data during the measurement period, number of reported incidents from each source during the measurement period, and the time taken for gathering the required incident data for the measuring period.

For this metric, only a brief discussion about aggregation was performed but no clear idea of how data should be aggregated was formed during the interview.

4.2.1.5 Control 13.2.2 Learning From Information Security Incidents

The discussion for this control focused on the respondent's work of investigating incidents as well as keeping track of ongoing investigations. Since there is no centralized incident handling within the organization, it was decided to create measurements for those incidents the respondent was in charge of. The discussion about the time taken for investigations, as well as the risk of incidents possibly being uninvestigated for long periods of time, led to the creation of measurements that would indicate any such tendencies. The measurements concern for how long incidents have been under investigation or waiting for investigation as well as how much time, on average, the investigations require.

For this metric only one object of measurement was identified, a spreadsheet used to keep track of incidents, with the relevant attributes being information about the incidents.

The *base measures* for this metric were: the number of incidents that are not marked “finished” or “no investigation”, the time for decisions concerning incidents, the number of incident investigations that finished during the measurement period, time used for the investigation of incidents, and the date of measurement.

Only a brief discussion about how to aggregate data was conducted. During this, it was concluded that it would be good if the report could serve as an early warning for if the time taken for investigations concerning incidents should become excessively long.

4.2.2 First Version of the Metrics

The information obtained at the interviews was used to design a first version of the metrics. The process was facilitated by the ISO/IEC 27004 template, used as a central part of the discussions during the interviews. Further, the design process gained much from the fact that as much information as possible had been written directly into the fields during the interviews. The process consisted of structuring the interview data and formulation of suggestions for the later parts of the metric. This included giving suggestions of how to aggregate the data as well as to give possible interpretations of the aggregated data.

For each metric, some suggestions for derived measures and the corresponding measurement functions were written. The suggested additions were based on the researchers’ understanding of the discussions during the first set of interviews. The work was carried out by a researcher with limited prior knowledge of the studied organization. The total time spent doing the structuring for the five metrics was 20 to 25 hours.

4.2.3 Second set of Interviews

The goal for the second set of interviews was to obtain the information needed to finalize the metrics. During the interviews the draft for the metric was discussed and the suggestions for those parts that were not fully explored during the first set of interviews were accepted or modified. Most of the discussions during the interviews were centered on the analytical model, the decision criteria, and the indicator interpretation.

Like the first set of interviews, two hours, or in one case three, had been allocated for each interview. Unlike the first set however, only half of the time

was needed in order to obtain the information necessary for the finalization of the metrics. The reason for this was that the respondents generally were in favor of the suggestions in the metrics drafts. An overview of the suggestions, both the accepted and the modified, is presented below.

4.2.3.1 Control 8.2.2 Information Security Awareness, Education and Training

The first interview provided a rather clear picture of what was to be accomplished by the measurements in this metric. As a result of this, there was a close to complete suggestion for the remaining fields in the template at the start of the second interview.

The suggestions for derived measures were: ratio of contractors that received information security training during the month and number of departments where the manager states that the department has an information security training program. These were accepted without alteration by the respondent.

The suggestions for indicators were: ratio for security education of contractors should be shown as a pie chart for the current month as well as a histogram showing the trend for previous months, and the ratio for the number of departments that claims to have or have not information security education should be shown as a pie chart. These were also accepted with only a few minor changes to the formulation.

The remaining time of the interview was spent on discussing the decision criteria and how the indicators should be interpreted. It was quickly established that the desired goal to be measured was that all contractors should undergo security training and that all departments should have training programs. Setting values for when to take different actions and what those actions should be however, was not as straightforward. After some discussion, the decided actions to be taken should all contractors not have received training were:

- 90 to 100 % received training, check if remaining contractors received training on a previous assignment
- less than 90 % received training, check the routines for when training is given so that no contractors are forgotten.

For the trend the decision criteria was decided to be: if the trend has been declining for the last two months, start an investigation as to what caused the decline. Finally, if a department does not have a security training program, the issue should be discussed with the manager of the department. All of these actions are investigative, rather than mandating a change. The reason for this is further discussed in chapter 5.

4.2.3.2 Control 9.1.2 Physical Entry Controls

The discussion from the first interview about what the perceived problem was, gave a very good idea of how to aggregate data as well as what the indicators should be.

The suggestions for derived measures were: the number of unauthorized entries, the average number of unauthorized entries per person abusing their right of passage, and the ratio of unauthorized entries. These derived measures were all accepted without modifications.

Two of the three indicators that were prepared before the interview were accepted by the respondent. The indicator that was deemed unnecessary was one concerning the average number of unauthorized entries per time a person abuses their card. The other two, a histogram for the trend for total number of unauthorized entries and a pie chart for the ratio of unauthorized entries were kept as suggested.

Most of the discussion for this metric was spent on what the decision criteria should be, i.e. the ranges for different actions and what those actions should be. Initially, the only values for the indicators that were considered were: no unauthorized entries, the average number of unauthorized entries per person abusing their card should be 0, and the ratio of unauthorized entries should not be higher than 0 %. This, of course, is the goal for the metric but additional values were needed to indicate what should be done if these goals are not met. The intervals that were agreed on were that if less than three persons had abused their cards, the matter would be resolved by addressing these persons individually, but if more than seven had abused their cards the matter would be elevated to the security manager as well as the operations manager. At the time, it was not noted that there was no action for the interval between 3 and 7 persons. This was, along with another issue, in fact not discovered until after the first measurement. More on this in section 4.3.2.

4.2.3.3 Control 10.5.1 Information Back-up

Since the purpose for this metric was relatively well understood from the first interview, there was a close to complete suggestion for the derived measures as well as the indicators presented at the start of the second interview.

The derived measures suggested were: the ratio of requested restore operations that could be performed, the ratio of restore operations that were performed within the time limit, the number of restore operations that were performed for system A, and the number of restore operations performed in system B (the names have been removed for anonymity reasons). The discussions of these derived measures resulted in a split of the second suggested derived measures

since it was deemed too complicated. Instead the two derived measures: number of restore operations performed last month and restore time for each of the restore operations performed last month, were created.

The suggested indicators, represented by pie charts showing the ratio of successful restore operations and the ratio of restore operations completed within 48 hours, were accepted by the respondent without modifications.

The discussion on this metric focused on the intervals for the interpretation of the indicator as well as what the corresponding actions should be. Due to the respondent claiming that the only action to be taken, should a restore operation fail, is to do an investigation of the cause and report the result to those affected, the decision criteria for the indicators were formulated accordingly.

The decision criteria for the indicator concerning ratio of successful restore operations thus state that if less than 100 % of the requested restore operations are successful, an investigation of the cause should be conducted and reported to the persons that requested the failed restore operations.

For the second indicator, that all restore operations should be completed within 48 hours, a similar decision criterion was decided. If the ratio of restore operations completed within 48 hours is less than 100 %, an investigation of the cause should be conducted. The respondent pointed out that the majority of restore operations that cannot be completed within 48 hours cannot be completed at all, meaning that the first decision criterion will be the most commonly used.

4.2.3.4 Control 13.1.1 Reporting Information Security Events

This metric was not particularly well defined at the start of the second interview. Only one derived measure was suggested, the average wait time for requests of incident information. However, although discussions about adding more derived measures were conducted, no necessary additional derived measures could be identified. It was concluded that the necessary data for interpretation was obtained through base measures.

Once this was established, the discussion shifted towards what the indicators for the metric should be. At the start of the interview there was one suggestion of an indicator but this suggestion was found to be irrelevant and therefore rejected. To find what would constitute adequate indicators, the report to be created was discussed and the desired properties of that report were used to formulate the indicators. The indicators that were agreed upon were: a histogram for the time to deliver a report for incidents for each source and a line chart indicating the trend for this time where each source is represented by a line.

The decision criteria for the first indicator was that if the time to deliver a report for a source is more than one week, a request for the reason for the delay should

be issued. The decision criteria for the second indicator was that if the trend was not declining or stayed above one week for three measurements in a row, a discussion with the manager for the slow units should be conducted to gain insight into the managers view of the priority of incident reporting.

4.2.3.5 Control 13.2.2 Learning From Information Security Incidents

At the beginning of the second interview there was only a partly finished suggestion for a derived measure. Discussion was therefore initially focused on what kind of derived measures should be created. The approach used was to focus on what the respondent wanted to show with the report and see what kind of calculations that needed to be done on the base measures in order to create the necessary data. This lead to identifying that the report should contain a trend for the average time unresolved incidents have been under investigation and a trend for the average investigation time for the incident investigations that were finished during the measurement period. From this it was identified that two derived measures were needed corresponding to the desired data.

The indicators for this metric were then defined as histograms showing the trend desired for the report. During the discussions concerning decision criteria, i.e. how to interpret the indicator and what actions to take, only investigative actions could be established. For both trends the decided decision criteria were that if the trend is rising, but only for this month, a judgment of if this is likely to continue should be made and if the trend is rising for two or more months, an investigation should be made to establish the underlying reason. A discussion of probable causes as to why only investigative actions were suggested can be found in chapter 5.

4.2.4 Final Version of the Metrics

From the discussions in the second set of interviews, the final version of the metrics was designed. During the finalization process, some additional information was needed. This information was obtained through e-mail correspondence with the respondents.

The total time taken for the completion of the metrics depended on if any complementary information was needed. An estimate of the time used is 3 to 5 hours per metric.

4.3 Measurement Using the Metrics

When the metrics were completed, the next step was to have the respondents perform the measurements defined in each metric. The purpose of performing these measurements was twofold: Partly a test to see how metrics designed according to ISO/IEC 27004 worked in reality, and partly to provide the respondents with reports on the measured aspects of security.

4.3.1 Measurement

The final metrics were sent, by email, to the respondent for the respective metric. The respondents were then responsible for ensuring that the requested information was collected. They were also instructed to document the time used for the data collection. The respondents used between 10 minutes and 1.5 hours to collect the data. The completed data forms were then returned to the principal researcher.

The data collection for the metrics 8.2.2, 10.5.1, 13.1.1, and 13.2.2 took between 10 and 30 minutes, whereas the collection for the metric 9.1.2 took 1.5 hour. The data collection for metric 9.1.2 included thorough work with manual reviews of the print outs from a database, whose interface did not allow appropriate filtering of the output, that is, the formulation of customized queries.

4.3.2 Results Presentation

The aggregation of the gathered data as well as creating the reports for the metrics was done by the principal researcher. The reason for this was that the amount of time the respondents had at their disposal for participating in this study was limited. However, all calculations needed, how to interpret the results as well as what to include in the report is described in each metric. It is therefore assumed that with the exception of creating a layout for the report, these tasks are purely administrative and could just as well have been done by the respondents.

The result from the measurements showed that the goal was not reached for any of the five metrics. For three of the five metrics there was at least one goal concerning a trend for the measurement, and since only one measurement had been performed these could not be properly compared with the corresponding decision criteria. For each of the measurement results, a report was created according to the reporting format field defined in each metric. An example of a report from a metric can be found in Appendix D

During the creation of the report for metric 9.1.2 it was discovered that since only the number of entries that was performed with one access card was recorded it was not possible to report the number of *persons* that had misused their right of passage. The solution was to change the metric to use the number of times a card had been misused instead of the number of people. This modification did fortunately not require additional measurements. Further, it was during this redefinition of the metric that it was discovered that there was a gap in the specification of the metric. No definition of an action was given if the number of misuses was between 3 and 7. This was solved via email with the respondent.

5 Discussion

In this chapter, the design and use of the metrics as well as some general aspects of the design of security metrics to instrument an ISMS are discussed.

5.1 Assumptions and Preconditions

From the start it was assumed that the agency where the study was performed would not be able to provide a lot of resources for the study. Thus, the guiding principle for the development of metrics presented in this report was that the design and use of metrics should be possible with limited usage of the agency's resources. During the design of the metrics, the research team acted as metrics developers, while the respondents were considered as experts in their respective area. In total, the study was allocated roughly 5 person hours per metric. The original assumption proved to be correct, supporting the approach of designing metrics that are straightforward to use.

5.2 Selection of Controls

The selection of the controls for which the metrics were designed was based on a thorough needs analysis. The needs analysis was based on documentation as well as interviews with security personnel at the agency. The reason for using the needs analysis in the selection of controls was that it had already been performed as part of a previous study and, thus, was available to use instead of a risk analysis performed by the studied agency.

The final selection of the five controls was performed by a security specialist at the studied agency with extensive knowledge of the organization. The same employee also identified the four respondents for the interviews. Access to security personnel with adequate knowledge about the organization identifying areas of interest, as well as people to interview, proved invaluable to the development.

Alternatively, the initial controls could have been selected directly from the ISO/IEC 27001 standard by an agency representative with the required information security authority. This would however, require a lot of effort from that person and, due to resource limitations, this was not a viable option.

It should be noted that, as described above, the controls for which the metrics were designed were *not* selected purely by what could be measured. Rather, a small set of relevant controls were identified, and from this set the selection of controls judged to be the easiest to design metrics for were made. The metrics

program should ideally be designed to instrument the most critical parts of the organizations information security program but in order to get the program going it was assumed to be better to start somewhere and then allow the metrics program to mature towards the controls that, although relevant, are difficult to measure.

Considering the result of the metrics design and use, the selection of controls to design metrics for was successful.

5.3 Metrics Design

As described in chapter 4.2.1, the first set of interviews resulted in metrics at rather varying stages of completion. The reasons for this are several. Most important is the maturity of the underlying process governing the particular security function in the organization. Without a clear, established process for how information security should be managed, it is hard to measure how well it is working.

Another factor, affecting the difficulty of designing a metric for a control, is the comprehensiveness of the control. To exemplify, creating metrics for ensuring the function of the control “Users shall be required to follow good security practices in the selection and use of passwords” (11.3.1) would be easier than creating measurements for the control “Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities” (10.8.1).

In order to ensure that the metrics would be possible to complete as well as provide the agency with valuable information, the base measures were selected using a participatory design process emphasizing the feasibility of the measurements. Thus, the measurements were selected so that data needed would be collected from sources that were known to be available. The consequence of this choice is that the metrics will not provide complete coverage of the corresponding controls. Instead they will cover those parts of the controls that are currently possible for the organization to measure. This is further discussed in the experiences and reflections section (5.5)

For all the five metrics, the suggestions for actions to be taken should a measurement not be fulfilled are concerned with investigating or reporting the problem rather than concrete actions to change the organization. The reason for this might be that performing investigations and reporting the problem is within the authority of the respondent. However, decisions concerning actions affecting the organization are not. For example, decisions about starting education programs or increasing funding to the security program have to be made by

managers at a higher organizational level. Thus, the design of metrics that requires organizational changes requires the participation or support of managers.

5.4 Measurements Using the Metrics

The effort required to perform the measurements was relatively limited for four of the metrics, that is, 10 to 30 minutes. Considering that the specified intervals of measurement are relatively large, the actual measurements will not pose inhibiting for the continual use of these metrics. For one of the metrics the required effort was considerably larger, that is, 1.5 hours. In this case, however, a substantial potential for automation can be seen. In all cases, continual measurement can be anticipated to decrease the required effort.

5.5 Experiences and Reflections

The guiding principle for the metrics was that the design and use should be possible to perform with limited resources. The effort demanded from the respondents in this study was in the order of 4–5 hours per metric. The time spent by the research team on each metric is estimated to be roughly 15 to 20 hours. This figure includes the time used for the interviews. The amount of time used to design the metrics is considered to be short and should be manageable by all organizations that are seriously interested in starting an information security measurement program.

The most important reason for why the design of the metrics went as smooth as it did was the continuous communication with the security experts. The value for the organization in using the metrics is further increased by the metrics being designed to measure those aspects of the information security program that were found important in the needs analysis. From this it can be concluded that even if the standard is meant to be applicable to every organization, a thorough knowledge of the organizations information security goals, as well as an understanding of the maturity of the information security processes connected to these goals, is needed.

For each control, the associated metric was designed using a participatory design approach emphasizing the feasibility of the measurements. That is, once a control had been selected, metrics were designed to use available data in order to provide a result that would support the fulfillment of, at least parts of, the control. However, there is a vital aspect that has to be considered when designing metrics based on available data. The metrics have to be connected to the actual needs of the security professionals of the organization. That is, there has to be stakeholders endorsing the metrics.

A method starting from what metrics are needed to show complete fulfillment of a control would instead be as follows: Once a control is decided, the information needed to show fulfillment of the control is specified followed by defining what to measure in order to collect the corresponding data. This approach will likely provide better measurement coverage of the control and is preferred for organizations with information security programs mature enough to use the method.

There is however a risk that the data needed will be difficult and resource demanding to collect because the information security program may not yet be mature enough. If this is the case and it is still decided to use such an approach, the risk is that the measurement program will be discontinued after much work has been performed without any reportable results.

It must be stressed that we do not advocate approaches based on a “measure-whatever-possible mantra”. Measurements are resource demanding and should always be motivated by need for knowledge about the information security of the organization (Barabanov, 2011, p.38).

We would thus recommend that, when the relevant controls have been selected, the metrics are designed using a participatory design process involving the affected security professionals of the organization. Moreover, using a method where the availability of data is prioritized higher than the completeness of the metrics is recommended in order to test and improve the maturity of the information security program. The metrics which design is based on data that is available can later be replaced or augmented by metrics designed to fully show the fulfillment of the controls, once the maturity of the information security program permits it.

6 References

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

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

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

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

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

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

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

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

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

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

Appendix A: Template for metrics[1]

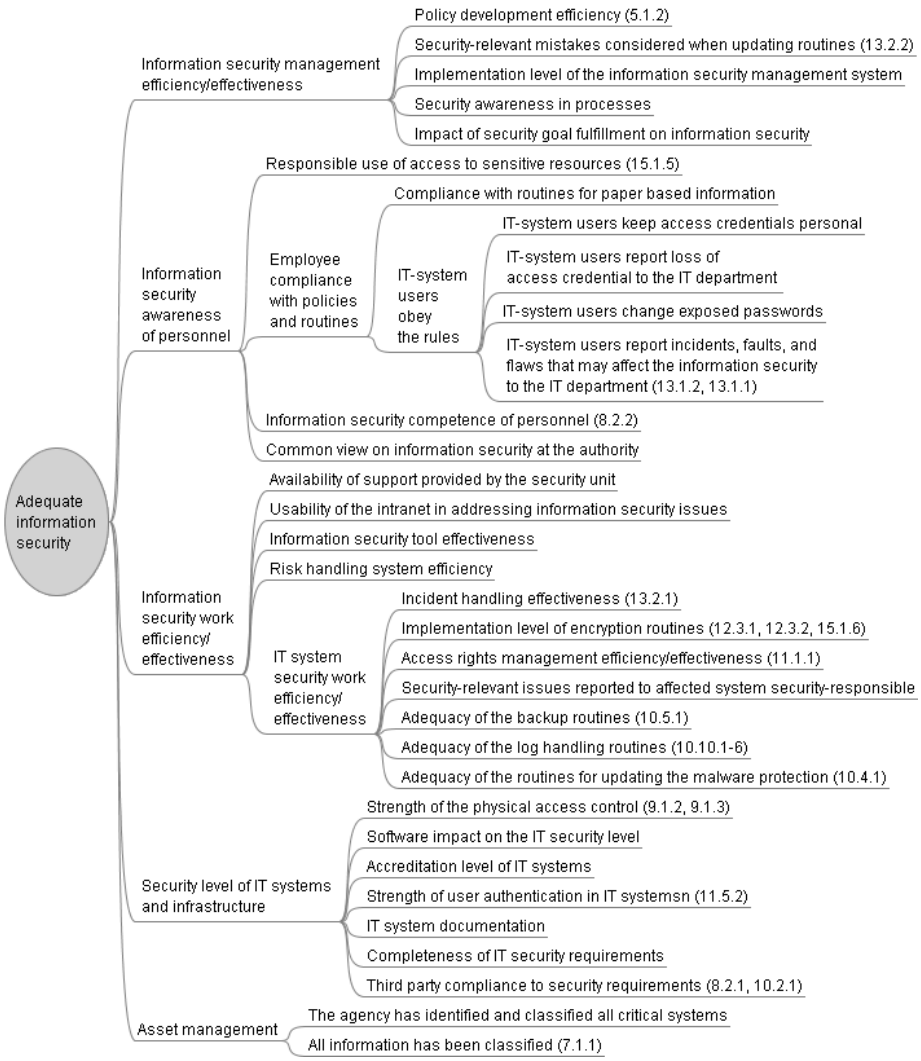
Below is the template used for the creation and documentation of the metrics.

Measurement Construct Identification	
Measurement Construct Name	
Numerical Identifier	
Purpose of Measurement Construct	
Control/process Objective	
Control (1)/process (1)	
Object of Measurement and Attributes	
Object of Measurement	
Attribute	
Base Measure Specification (for each base measure [1..n])	
Base Measure	
Measurement Method	
Type of Measurement Method	
Scale	
Type of Scale	
Unit of Measurement	
Derived Measures Specification	
Derived Measures	
Measurement Function	
Indicator	
Indicator	
Analytical Model	
Decision Criteria Specification	
Decision Criteria	
Measurement results	
Indicator Interpretation	
Reporting Formats	
Stakeholders	
Client for measurement	
Reviewer of measurement	
Information Owner	
Information Collector	
Information Communicator	
Frequency/Period	
Frequency of Data Collection	
Frequency of Data Analysis	
Frequency of Reporting Measurement Results	
Measurement Revision	
Period of Measurement	

[1] Mallen är återgiven från standarden SS-ISO/IEC 27004:2010 med vederbörligt tillstånd från SIS Förlag AB, 08-555 523 10, www.sis.se

Appendix B: The mapping of controls to characteristics

The figure below illustrates the mapping of controls from the standard ISO/IEC 27001 to the relevant information security characteristics presented in (Lundholm & Hallberg, 2011).



Appendix C: The Designed Metrics[2]

This appendix contains anonymized versions of the five metrics that were designed in the study.

Metric for the control 8.2.2

Measurement Construct Identification	
Measurement Construct Name	Information security training for contractors
Numerical Identifier	8.2.2
Purpose of Measurement Construct	To check how many of the contractors, employed by unit A, that are given information security training and to clarify how many of the units in department X that can provide information security training to contractors.
Control/process Objective	**8.2** During employment[3] **Objective:** To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.
Control (1)/process (1)	**8.2.2** All employees of the organization and, where relevant, contractors and third party users shall receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.[2]
Object of Measurement and Attributes	
Object of Measurement	1. Word-document concerning contractors at unit A, owned by administrative unit B 2. Manager for each unit in department X
Attribute	1. Entries concerning contractors at unit A 2. Knowledge about the training of contractors at the department
Base Measure Specification (for each base measure [1..n])	

[2] Mallen är återgiven från standarden SS-ISO/IEC 27004:2010 med vederbörligt tillstånd från SIS Förlag AB, 08-555 523 10, www.sis.se

[3] Controls/control objectives är återgivna från standarden SS-ISO/IEC 27001:2006 med vederbörligt tillstånd från SIS Förlag AB, 08-555 523 10, www.sis.se

Base Measure	1.1. Number of contractors last month 1.2. Number of contractors that received information security training 2.1. Number of units that can provide information security training
Measurement Method	1.1. Count the number of contractors that were hired by unit A last month 1.2. Count the number of contractors last month that were given information security training (contractors that were hired before may have been given training at that time) 2.1. Ask the manager of each unit in department X (unit A, unit B, unit C, unit D, unit E, unit F) if the unit has formal routines for information security training of contractors
Type of Measurement Method	1.1. Objective 1.2. Objective 2.1. Subjective
Scale	1.1. Integer 1.2. Integer 2.1. Binary
Type of Scale	1.1. Ratio 1.2. Ratio 2.1. Nominal
Unit of Measurement	1.1. Number of contractors 1.2. Number of contractors 2.1. None
Derived Measures Specification	
Derived Measures	1. Ratio of contractors that received training 2. Ratio of units providing training
Measurement Function	1. Number of contractors that were employed last month that were given information security training / total number of contractors employed last month * 100 2. Number of units where the manager states that the unit has a documented routine for information security training / 6 * 100
Indicator	
Indicator	a) Pie chart for the ratio of contractors that received information security training last month b) Histogram showing the trend for the ratio of contractors that received information security training c) Pie chart showing the number of units that provides information security training for contractors
Analytical Model	a) The ratio of contractors that received information

	security training during the measurement period should be indicated with green color, whereas the ratio that did not receive training should be indicated with red color. b) Each bar in the histogram represents the ratio of contractors that received information security training during the month the bar represents c) Each unit should have a slice in the pie chart. This slice should be green if the unit provides information security training and red if the unit does not provide information security training.
Decision Criteria Specification	
Decision Criteria	a) The ratio of contractors that are given information security training should not be below 100% b) The trend for the ratio of contractors receiving information security training should be increasing or stable c) All units should provide information security training
Measurement results	
Indicator Interpretation	Indicator a) should be interpreted as follows: • 100%, no action needed. • Between 90% and 100%, check if there are contractors that have been given information security training previously, no additional actions needed. • Less than 90%, check the routines for when information security training should be provided so that training is not put on hold indefinitely. Indicator b) should be interpreted as follows: • Rising or stable trend, no action needed. • Decreasing trend for the last two months, start an investigation to find the cause. Indicator c) should be interpreted as follows: • 100% no action needed. • Less than100%, discuss the issue with the manager for the unit that does not have information security training.
Reporting Formats	The report should be initiated with the name of the metric followed by the purpose of the metric as well as the control the metric is connected to. Thereafter, the diagrams for the indicators described in this metric should be included. A short description of

	the interpretation of each diagram should be presented, including the break points described in the indicator interpretation.
Stakeholders	
Client for measurement	• Manager of department X • Operations manager • Managers of units A-F
Reviewer of measurement	Person Y
Information Owner	Person Y
Information Collector	Person Y
Information Communicator	Person Y
Frequency/Period	
Frequency of Data Collection	Monthly
Frequency of Data Analysis	Monthly
Frequency of Reporting Measurement Results	Monthly
Measurement Revision	Annually
Period of Measurement	One month

Metric for the control 9.1.2

Measurement Construct Identification	
Measurement Construct Name	Abuse of personal access cards
Numerical Identifier	9.1.2
Purpose of Measurement Construct	To show how often employees abuse their right of passage when there is no guard on duty.
Control/process Objective	**9.1** Secure areas[4] **Control:** To prevent unauthorized physical access, damage and interference to the organization's premises and information.
Control (1)/process (1)	**9.1.2** Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.[1]
Object of Measurement and Attributes	
Object of Measurement	Security logs for entrances to the building.
Attribute	Security logs for door 1
Base Measure Specification (for each base measure [1..n])	
Base Measure	1. Number of times multiple, authorized, entries have been made when no guard was on duty during the last week 2. Number of entries made for each multiple entry described in 1 3. Total number of entries when no guard was on duty for last week
Measurement Method	1. Count the number of times during last week where an access card has been used for 2 or more authorized entries in a row, between 16:31 and 07:29, where the authorized entries were performed within one minute 2. For each time an access card has been used more than once in a row, as described in question 1, document how many entries that were made 3. Document the total number of authorized entries, between 16:31 and 07:29, during last week

[4] Controls/control objectives är återgivna från standarden SS-ISO/IEC 27001:2006 med vederbörligt tillstånd från SIS Förlag AB, 08-555 523 10, www.sis.se

Type of Measurement Method	1 – 3 Objective
Scale	1 – 3 Integer
Type of Scale	1 – 3 Ratio
Unit of Measurement	1. Number of multiple entries 2. Number of entries 3. Number of entries
Derived Measures Specification	
Derived Measures	1. Number of unauthorized entries 2. Ratio of unauthorized entries
Measurement Function	Definitions: • Multiple Entries = Total number of entries made when one card was used more than once • Times = Number of times a card was used for a multiple entry • All entries = Total number of entries. 1. Number of unauthorized entries = Multiple entries – Times 2. Ratio of unauthorized entries = (Multiple Entries – Times) / All entries
Indicator	
Indicator	a) Histogram showing the trend for the number of times a multiple entry has been made b) Pie chart showing the ratio of authorized to unauthorized entries for the measured week
Analytical Model	a) Each bar in the histogram represents then number of times a multiple entry was made during that week b) In the pie chart, authorized entries should be represented by a green slice and unauthorized entries should be represented by a red slice
Decision Criteria Specification	
Decision Criteria	a) No unauthorized entries should be made b) The ratio of unauthorized entries should not be above 0%
Measurement results	
Indicator Interpretation	Indicator a) should be interpreted as follows: • No unauthorized entries, no action required • Between 0 and 3 multiple entries, talk to these persons separately • Between 3 and 7 multiple entries, discuss the problem with affected middle-level managers • More than 7 multiple entries, escalate the problem

	to operations manager as well as security manager for the organization Indicator b) should be interpreted as follows: • No unauthorized entries should be accepted. Thus, this indicator should be interpreted as a base for discussions with managers.
Reporting Formats	The report should be initiated with the name of the metric followed by the purpose of the metric as well as the control the metric is connected to. The report should include a diagram showing the trend for the number of times multiple entries were made. Further, a pie chart showing the ratio of authorized entries to unauthorized entries for the week of measurement should be included. Finally, a diagram showing the trend for the total number of entries should be included where each bar should be divided into two parts, one green for the authorized entries and one red for the unauthorized entries.
Stakeholders	
Client for measurement	The security group
Reviewer of measurement	Person Y
Information Owner	Person Y
Information Collector	Technician responsible for logs
Information Communicator	Person Y
Frequency/Period	
Frequency of Data Collection	Weekly
Frequency of Data Analysis	Weekly
Frequency of Reporting Measurement Results	Weekly
Measurement Revision	Yearly
Period of Measurement	One week

Metric for the control 10.5.1

Measurement Construct Identification	
Measurement Construct Name	Restoring back-ups
Numerical Identifier	10.5.1
Purpose of Measurement Construct	To ensure that requested restore operations are performed within 48 hours.
Control/process Objective	**10.5** Back-up[5] **Objective:** To maintain the integrity and availability of information and information processing facilities.
Control (1)/process (1)	**10.5.1** Back-up copies of information and software shall be taken and tested regularly in accordance with the agreed backup policy.[1]
Object of Measurement and Attributes	
Object of Measurement	1. Support management system 2. Back-up tools
Attribute	1. Support requests tagged with “restore operation” 2. Start and finish times for restore operations as well as what system the restore operation was requested for
Base Measure Specification (for each base measure [1..n])	
Base Measure	1.1. Number of support requests tagged with restore operation 2.1. Start and finish times for restore operations 2.2. Number of restore operations performed for system A 2.3. Number of restore operations performed for system B
Measurement Method	1.1. Count the number of support requests that have the tag “restore operation” for last month. 2.1. Document start and finish times for all restore operations that were performed last month 2.2. Count the number of restore operations that were performed for system A last month 2.3. Count the number of restore operations that were performed for system B last month

[5] Controls/control objectives är återgivna från standarden SS-ISO/IEC 27001:2006 med vederbörligt tillstånd från SIS Förlag AB, 08-555 523 10, www.sis.se

Type of Measurement Method	1 – 4 Objective
Scale	1.1. Integer 2.1. Year-month-day time 2.2. Integer 2.3. Integer
Type of Scale	1.1. Nominal 2.1. Interval 2.2. – 2.3. Ratio
Unit of Measurement	1.1. Number of support requests 2.1. None 2.2. – 2.3. Restore operations
Derived Measures Specification	
Derived Measures	1. Ratio of requested restore operations that were completed 2. Number of performed restore operations 3. Time used for completed restore operations 4. Number of restore operations for system A 5. Number of restore operations for system B
Measurement Function	1. Divide the number of restore operations that were made in response to a request with the number of requests for restore operations during last month 2. Calculate how many restore operations that were performed last month 3. For each restore operations performed last month, calculate the time taken = finish time – start time 4. Divide the number of restore operations for system A with the total number of restore operations last month 5. Divide the number of restore operations for system B with the total number of restore operations last month
Indicator	
Indicator	a) Pie chart for the ratio of requested restore operations that could not be performed b) Ratio of restore operations that were performed within 48 hours
Analytical Model	a) The fraction of restore operations that could be performed is indicated with green color whereas those that could not be performed is indicated with red color b) The fraction of restores that could be performed within 48 hours = (Number of restores taking less than 48 hours / total number of restore operations)
Decision Criteria Specification	

Decision Criteria	a) All requested restore operations should be performed b) All restore operations should be performed within 48 hours
Measurement results	
Indicator Interpretation	Indicator a) should be interpreted as follows: • If the ratio of successful restore operations is less then 100%, an investigation should be performed to determine the reason. If the reason is that the requested data is not back-upped, this should be communicated to the affected managers Indicator b) should be interpreted as follows: • If the fraction of restore operation that are performed within 48 hours is less than 100%, an investigation to determine the reason should be initiated
Reporting Formats	The report should be initiated with the name of the metric followed by the purpose of the metric as well as the control the metric is connected to. In addition to this, the following diagram should be presented: • The pie chart from indicator a) • The pie chart from indicator b) in which restore operations performed within 48 hours should be indicated by green color and restore operations taking longer than 48 hours should be indicated by red color • A pie chart that shows the number of restore operations performed for system A, system B, and other systems. The slices in this pie chart should have neutral colors so that no misunderstandings concerning the slices as good or bad occurs It should be stated for each diagram how many restore operations each slice for each diagram represents as well as an explanation as to how to interpret the diagram
Stakeholders	
Client for measurement	• System owner for systems using the back-up service • Management for unit A • The back-up team

Reviewer of measurement	Person A
Information Owner	Person A
Information Collector	Person A
Information Communicator	Person A
Frequency/Period	
Frequency of Data Collection	Monthly
Frequency of Data Analysis	Monthly
Frequency of Reporting Measurement Results	Monthly
Measurement Revision	Yearly
Period of Measurement	One month

Metric for the control 13.1.1

Measurement Construct Identification	
Measurement Construct Name	Time for receiving material for incident reports
Numerical Identifier	13.1.1
Purpose of Measurement Construct	To show how many incidents that are reported from different sources as well as to indicate the time it takes to collect incident data from different parts of the organization.
Control/process Objective	**13.1** Reporting information security events and weaknesses[6] **Objective:** To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
Control (1)/process (1)	**13.1.1** Information security events shall be reported through appropriate management channels as quickly as possible.[1]
Object of Measurement and Attributes	
Object of Measurement	1. Incident handling system, managed by Person A 2. Person in the security group responsible for the compilation of the incident report
Attribute	1. Information about incidents 2. Knowledge about reporting
Base Measure Specification (for each base measure [1..n])	
Base Measure	1.1. Number of sources for the last four months 1.2. Number of reported incidents during the last four months, per source 2.1 Time for receiving incident reports from each source
Measurement Method	1.1. Count the number of sources that reported incident data to Person A during the last four months and document the name of the source. 1.2. For each source in 1.1, count how many incidents were reported. 2.1. Ask Person A how many days that passed, for each source, between asking for incident data for the

[6] Controls/control objectives är återgivna från standarden SS-ISO/IEC 27001:2006 med vederbörligt tillstånd från SIS Förlag AB, 08-555 523 10, www.sis.se

	last four months and receiving the requested data.
Type of Measurement Method	1.1. – 1.2. Objective 2.1. Objective/Subjective
Scale	1.1. – 1.3. Integer
Type of Scale	1.1. – 1.3. Ratio
Unit of Measurement	1.1. Name of source 1.2. Incidents 2.1. Days
Derived Measures Specification	
Derived Measures	Average time for reporting incidents
Measurement Function	(Add up the individual times for receiving an answer from each source) / number of sources
Indicator	
Indicator	a) Histogram for the time for receiving reports from each source for the last four months b) Line chart showing the trend for the reporting time with one line for each source
Analytical Model	a) The histogram should have one bar showing the time for receiving incident reports from each source as well as a line showing the average time drawn across all the bars. b) In the line graph, the time for receiving incident reports from each source for each four month period should be represented. The lines should have different colors and the colors should be possible to distinguish even if the graph is printed in black and white. In addition, each data series should be represented by a different type of dots for the data points.
Decision Criteria Specification	
Decision Criteria	a) When incident data is requested, all sources should send the data within one week b) The trend should be decreasing or less than one week
Measurement results	
Indicator Interpretation	Indicator a) should be interpreted as follows: • If the time from requesting to receiving data is less than one week, no action is needed • If the time from requesting to receiving data is longer than one week for any source, a request should be made concerning the reason for the delay Indicator b) should be interpreted as follows:

	• If the trend is decreasing, no action is required • If the trend is increasing or if the time from request to receiving data is more than one week for three consecutive measurements, a discussion about the priority of incident reports should be initiated with affected managers
Reporting Formats	The report should be initiated with the name of the metric followed by the purpose of the metric as well as the control the metric is connected to. In addition, the graphs created as indicators should be presented along with a short explanation of how each graph should be interpreted and what the limits were
Stakeholders	
Client for measurement	Security CIO
Reviewer of measurement	Person A
Information Owner	Person A
Information Collector	Person A
Information Communicator	Person A
Frequency/Period	
Frequency of Data Collection	Every four months
Frequency of Data Analysis	Every four months
Frequency of Reporting Measurement Results	Every four months
Measurement Revision	Every two years
Period of Measurement	Four months

Metric for the control 13.2.2

Measurement Construct Identification	
Measurement Construct Name	Processing time for incidents
Numerical Identifier	13.2.2
Purpose of Measurement Construct	To show the volume and processing time for incidents.
Control/process Objective	**13.2** Management of information security incidents and improvements.[7] **Objective:** To ensure a consistent and effective approach is applied to the management of information security.
Control (1)/process (1)	**13.2.2** There shall be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.[1]
Object of Measurement and Attributes	
Object of Measurement	Incident handling system, managed by Person A
Attribute	Information about incidents
Base Measure Specification (for each base measure [1..n])	
Base Measure	1. Number of incidents that are not marked as “investigated” “no investigation” or “sent to other unit for investigation” 2. Incident registration date 3. Number of investigated incidents last month 4. Incident investigation time 5. Date of measurement
Measurement Method	1. Count the number of incidents that are not yet marked with ”investigated”, ”no investigation” or ”sent to other unit for investigation” 2. For each incident not yet marked with ”investigated”, ”no investigation” or

[7] Controls/control objectives är återgivna från standarden SS-ISO/IEC 27001:2006 med vederbörligt tillstånd från SIS Förlag AB, 08-555 523 10, www.sis.se

	”sent to other unit for investigation”, extract the date when the incident was registered in the system 3. Count the number of incidents that were marked with ”investigated” last month 4. For each incident that were marked with “investigated” last month, extract the dates when the incident was marked with ”investigated” as well as when the incident was registered into the system 5. Document the date of measurement
Type of Measurement Method	1 – 5 Objective
Scale	1. Integer 2. Date 3. Integer 4. Date 5. Date
Type of Scale	1. Ratio 2. Interval 3. Ratio 4. Interval 5. Interval
Unit of Measurement	1. Incidents 2. Year-Month-Day 3. Incidents 4. Year-Month-Day 5. Year-Month-Day
Derived Measures Specification	
Derived Measures	1. Average time incidents have been under investigation 2. Average investigation time
Measurement Function	1. (Sum [date of measurement – date of registration] for each incident not marked with “investigated”, “no investigation” or “sent to other unit for investigation”) / number of incidents not marked with “investigated”, “no investigation” or “sent to other unit for investigation”) 2. Sum [date for marked as investigated – date of registration] for each incident marked as investigated) / number of incidents marked as investigated
Indicator	
Indicator	a) Histogram showing the trend for incidents under investigation

	b) Histogram showing the trend for the average investigation time for incidents
Analytical Model	a) The histogram should have a bar for each month showing the average time incidents that are not marked with "investigated", "no investigation" or "sent to other unit for investigation" have been under investigation b) The histogram should have a bar for each month showing the average investigation time for the incidents for which investigations were competed this month.
Decision Criteria Specification	
Decision Criteria	a) The trend for the average time an incident have been under investigation should be decreasing or stable b) The trend for the average investigation time for incidents for which investigation was completed this month should be decreasing or stable
Measurement results	
Indicator Interpretation	Indicator a) should be interpreted as follows: • If the trend is stable or decreasing, no action is needed • If the trend is increasing but only for one month, make a judgment if it is a temporary anomaly • If the trend has been increasing for two or more months, make an investigation to determine the cause Indicator b) should be interpreted as follows: • If the trend is stable or decreasing, no action is needed • If the trend is increasing but only for one month, make a judgment if it is a temporary anomaly • If the trend has been increasing for two or more months, make an investigation to determine the cause
Reporting Formats	The report should be initiated with the name of the metric followed by the purpose of the metric as well as the control the metric is

	connected to. In addition, the graphs created as indicators should be presented along with a short explanation of how each graph should be interpreted and what the limits were. To complement the graphs there should be tables stating the number of open incidents as well as the number incidents where investigations were completed during the month
Stakeholders	
Client for measurement	Person A, Security CIO
Reviewer of measurement	Person A
Information Owner	Person A
Information Collector	Person A
Information Communicator	Person A
Frequency/Period	
Frequency of Data Collection	Monthly
Frequency of Data Analysis	Monthly
Frequency of Reporting Measurement Results	Monthly
Measurement Revision	Yearly
Period of Measurement	One month

Appendix D: Results Report for a Metric

This appendix presents an example of a results report based on the measurements that was performed using one of the metrics presented in this report. The results report is translated from the original Swedish version.

Restoring Back-ups

This metric is connected to the control 10.5.1 in ISO/IEC 27001.

Purpose

To ensure that requested restore operations are performed within 48 hours.

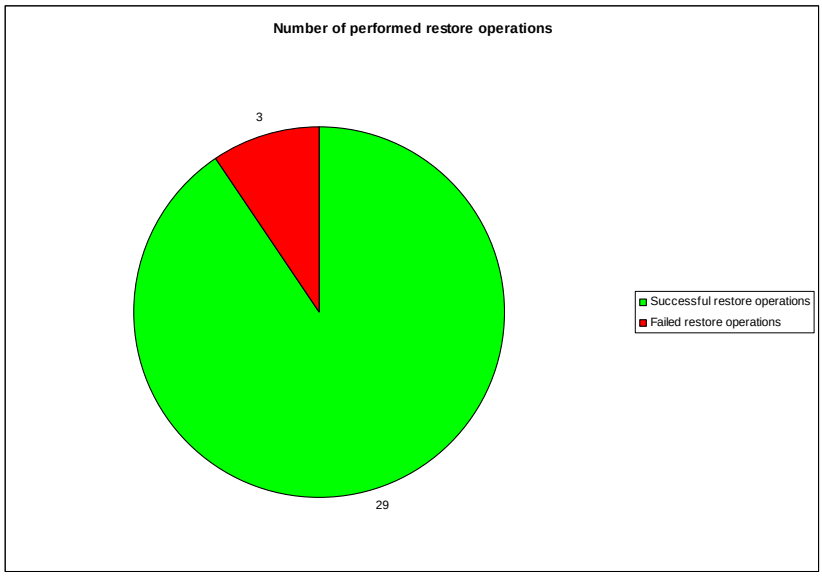
Measurement period

This report concerns measurements for back-ups performed during October 2010

Results

Below the diagrams presenting the measurement results are presented with a short description for each diagram.

Performed restore operations

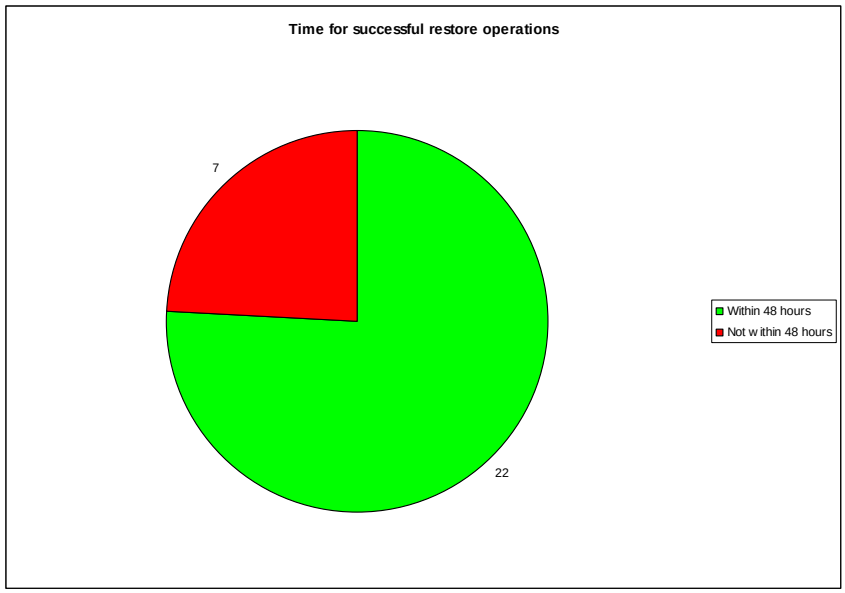


The diagram illustrates the ratio for the restore operations that were performed during October 2010. Of the 32 restore operations that were requested, 29 were successfully performed.

The decision criteria for this measurement states that if less then 100% of the restore operation are successful, an investigation to determine the cause should be initiated and the result reported to affected managers.

Since the fraction of successful restore operations is less than 100%, an investigation and subsequent reporting of the reason should be performed.

Completing restore operations within 48 hours

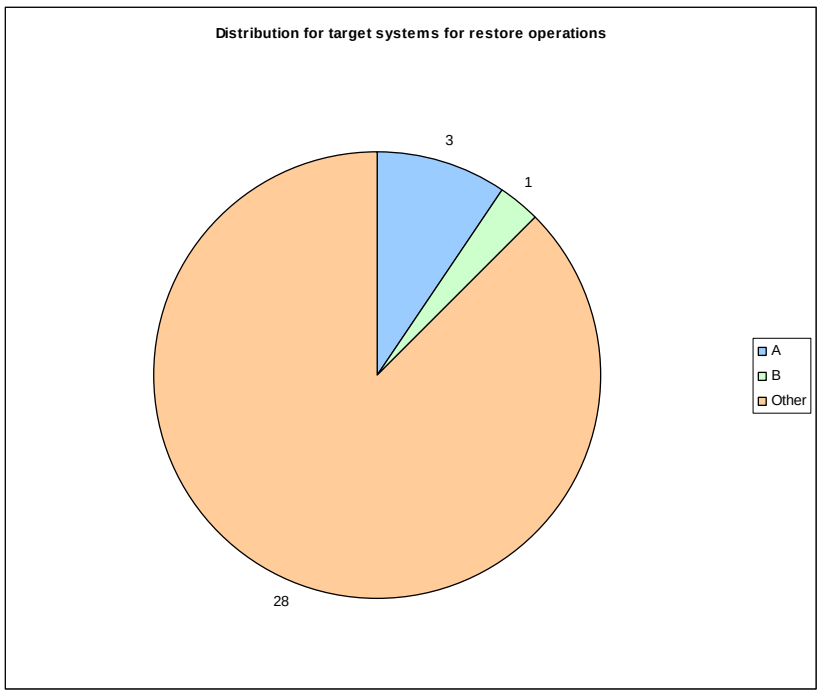


The diagram shows the ratio as well as the number of successful restores that were completed within 48 hours. Of the 29 successful restore operations, 22 were completed within 48 hours.

The decision criteria for this measurement states that if less then 100% of the successful restore operations are completed within 48 hours, an investigation of the cause should be initiated.

Since not all restore operations were successfully completed within 48 hours, an investigation to determine the cause should be performed.

Target system for restore operations



The diagram shows the ratio of restore operations that are performed for system A, system B, and other systems.

This measurement does not have a decision criteria connected to it. It is included in the report to illustrate the distribution of requested restore operation over the two specific systems A and B in relation to all other systems.