Measuring effectiveness of control of information security management system based on SNI ISO/IEC 27004: 2013 standard

A P Aldya, S Sutikno and Y Rosmansyah

1 Informatics Engineering Siliwangi University, Indonesia
2 3 School of Electrical Engineering and Informatics Institute Technology of Bandung, Indonesia

Email: aldy@unsil.ac.id

Abstract. One of the keys to the successful implementation of information security management in an organization is the selection and implementation of an information security management system control that is good and in accordance with the needs of the organization, the information security management system control can be adopted based on ISO/IEC 27001: 2013 standard document. To ensure the success of information security controls, it is necessary to measure the effectiveness of each control applied. SNI ISO/IEC 27004: 2013 is a standard that provides guidance on the development and use of measures and measurements to assess the effectiveness of controls and control groups in the information security management system as stated in the ISO/IEC 27001 standard, but to do the measurement process, required objects and measurement attributes and metrics, which are not explained in detail in the ISO ISO/IEC 27004: 2013 standard. This study aims to assist in measuring the effectiveness of information security management control by generating the flow of steps in determining the object and measurement parameters and the metrics used based on the provisions contained in the ISO ISO/IEC 27004: 2013 standard.

1. Introduction

Managing information security is as important as managing the core of the business itself. Nowadays, business organizations are becoming more concerned about the security of their information, as well as legal and audit institutions expect every organization to follow certain security rules compliance in line with the implementation of information security management infrastructure in its business. Therefore, build and implement appropriate information security infrastructure is one of the priority needs for most business organizations.

In this context, what is meant by 'information' that includes all forms of data, knowledge, documents, communications, conversations, messages, recordings, and images. Since the information, information systems, and computer are all interrelated, most of the information security means protecting all related assets including hardware, network, Internet connectivity, software, databases, the data (both data stored or data sent and received), file, directory, file reports, telephone, fax, documents, etc., such that only the authorities and legitimate users can access the information [1].

Practice in the field indicates that the problem of information security often caused by bad management. The comparison itself is 30% on the technical side and 70% on the management side. If
the technique is the key to information security problems, then management is the core \[2\]. Therefore, we need to implement good information security management system. In the information security management system standard set forth by ISO/IEC 27000 standard series, the approach presented in the process of ISMS standard is based on the principle that is commonly known as the Plan - Do - Check - Act (PDCA):

a. Plan - set goals and make plans (analyze the situation of the organization, define the overall objectives and set targets, and develop plans to achieve them);
b. Do - implement the plan (do what was planned to be done);
c. Check - measure (measure and monitor the extent to which the implementation is done to meet the planned objectives); and
d. Act - to improve and enhance the activity of (learn shortage to boost activities in order to achieve better results).

As has been described above that one of the principles approach to the process of the ISMS (check) where the process is made by measuring the implementation of information security management systems, one of them is a measure of the effectiveness of the implementation of information security management system controls.

2. Literature Review

2.1. Measurement of information security management system

Security management, such as computer technology management, sales management, production management, and other functions of a company or organization well, should be measured, because something cannot be measured then it will not be evaluated. The evaluation is done to determine whether the measures taken for the organization are correct and also whether the resources provided are adequate \[3\].

Here is the definition of measurements according to some sources of reference:

a. According to the great dictionary of Indonesian word measurement meaning process, how, or deed measure.
b. According Atzeni and Lioy \[4\] measurement that is a process that aims to obtain quantitative values of attributes or qualitative in the real world. Attribute real world is any property of an existing entity, may be abstract or concrete.

While the definition of the measurement of information security management systems according to the document ISO/IEC 27 004: 2013 \[5\], which is the process of getting information about the effectiveness of the ISMS and control using measurement methods, measurement functions, analytic models and decision criteria.

Security management measurements help calculate and measure the effectiveness of the ISMS processes and controls. Measurement facilitates decision making and improve performance and accountability. Measurements can also help managers decide where to place controls and identify unproductive control \[6\].

A good measurement includes the following qualities: "SMART" (Specific, Measurable, Attainable, Repeatable, and Time-Dependent). Characteristics metrics, including accurate, precise, valid, and true, meaningful, reproducible, objective and unbiased, and is able to measure progress toward the goal, can be measured consistently, cheap to do, expressed as cardinal numbers or percentages and use at least one unit of measure, and contextually specific. \[6-7\].

2.2. Information security metrics

Metrics can provide an overview for the organization, to prioritize threats or vulnerabilities and risks generated. The metric is a tool designed to facilitate decision making, improve performance, and accountability, so that can be aligned with the goals and objectives of the organization \[8\].

Here is a list of definitions of metrics:
a. Measure: A variable whose value, its main purpose is to measure the data in order to facilitate insight.

b. Metric: measure or unit of measure that is designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant data is proposed.

c. Metric: broad category of tools used by decision makers to evaluate the data. A metric is a system of related measures that facilitate quantification of some particular characteristics. In simple terms, the metric is a measurement that is compared with the scale or benchmark to yield useful results.

d. Security metrics: measurement of computer security standards.

Metrics can be used to improve the effectiveness of information security. The metric is a system parameter or quantitative assessment and periodic way of the process to be measured, along with procedures for carrying out the measurement and interpretation procedures for assessment from the standpoint of prior assessment or comparable. Metrics are usually devoted to the subject area, in this case the metric is only applicable in a particular domain and cannot directly refer to or interpreted outside of it [9-10].

Mostly of scientists agree that there are at least two approaches are important in the development of metrics. The first type is a mathematical or formal approach and the second is the definition of pragmatic [10-11].

Generally, security metrics can be considered as a part or an extension of the system or the organization's information security management program. Security metrics also have an important relationship with risk management. It can be said that many decisions are supported by security metrics in risk management decisions, because the ultimate goal of all activities of security management is a security risk management. Therefore, metrics can complement certain risk management activities, directly contribute input to the analysis and the overall ability of the organization to deal with the risks faced by facilitating continuous improvements to security [12-14].

2.3. Information security controls

Information Security controls are a set of information security policies that must be defined, approved by management, published and communicated to employees and relevant external parties [15].

Table 1 shows the control area, and the amount of control contained in the document of ISO/IEC 27001: 2013 Annex A.

2.4. Information security measurement model

Here's a picture of the information security measurement model described in ISO/IEC 27004: 2013 [5].

![Figure 1. Model of information security measures](image)
| Clause number | Area Control                                      | Control Amount |
|--------------|--------------------------------------------------|----------------|
| 5            | Information security policies                     | 2              |
| 6            | Organization of information security              | 7              |
| 7            | Human resource security                           | 6              |
| 8            | Asset management                                  | 10             |
| 9            | Access control                                    | 14             |
| 10           | Cryptography                                      | 2              |
| 11           | Physical and environmental security                | 15             |
| 12           | Operations security                               | 14             |
| 13           | Communications security                           | 7              |
| 14           | System acquisition, development and maintenance   | 13             |
| 15           | Supplier relationships                            | 5              |
| 16           | Information security incident management          | 7              |
| 17           | Information security aspects of business continuity management | 4 |
| 18           | Compliance                                        | 8              |
|              | Total Amount of Control                           | 144            |

Information security measurement model is the structure that connects the needs of the information with the relevant measurement objects and attributes. The object of measurement can be planned or implemented process, procedures, projects and resources. The information security measurement model illustrates how the relevant attributes are measured and converted into indicators that provide a basis for decision making.

3. Method and results
In this research, the development of methods of measurement and metric measures, the development of methods of measurement carried out to facilitate the measurement, especially for ease in determining the measurement object and its attributes, and to assist in making the metric measures. Development of measurement methods and metric measurement performed in this study was developed and adopted from the measurement model contained in the ISO standard of ISO/IEC 27004: 2013.

3.1. Determining the measurement objects and attributes
The main stage in measuring and making information security controls metric is to determine the measure of the measurement object and its attributes, the following is a flowchart that outlines the image stages in determining the measurement object and its attributes:
3.1.1. Determine the scope of measurements and information needs. The first phase to measuring information security management system is determining the scope of measurement and information needs. The broad scope of the measurement depends on the capabilities and resources of the organization, the scope of the organization's initial measurement activities will be limited to elements such as certain controls, information assets are protected by a specific control, special activities for the information security with highest priority. Each measurement’s construction must comply with at least one information’s need.

The following activities can be carried out to identify the needs of the relevant information [5]:

a. Check-up the ISMS and processes, such as:
   1. ISMS policy and objectives, control objectives and controls;
   2. Laws, regulations, contracts and organization of information security requirements;
   3. The results output from the information security risk management process, as described in ISO/IEC 27001.

b. Prioritize information needs that identified based on criteria, such as:
   1. Risk management priorities;
   2. Capabilities and resources of an organization;
   3. Stakeholders' interests;
   4. Information security policy;
   5. The information necessary to meet legal requirements, regulations, and contracts;

![Figure 2. The steps to determine the measurement object and attribute.](image-url)
6. The value of information in relation to the cost of measurement;
   c. Select a subset of information that should be addressed in the measurement of the list of
      priority activities; and
   d. Document and communicate the needs of selected information to all relevant parties.

All measurements that applied to the implementation of the ISMS control or control group should be
implemented based on the needs of the selected information. Information needs to measure the
effectiveness of controls is limited to controls contained in the document ISO/IEC 27001: 2013 Annex
A, which controls contained in the document ISO/IEC 27001: 2013 Annex A is directly derived from
and aligned with those listed in the ISO/IEC 27002: 2013.

3.1.2. Study of best practice or reference. Best practice is needed to assist in determining the
measurement object and its attributes, best practice used in this research is the document of ISO/IEC
27002: 2013, but it also used another references that is COBIT 5 for Information Security
document for other additional materials consideration.

3.1.3. Determine the control objective. Before determining the measurement object, control
objectives need to be identified first, control objective is a statement of desired results or objectives
to be achieved by implementing control procedures. The purpose of determining the control objective
is to target the goal of every control on each clause, so that the measurement object can be achieved
precisely in accordance with the target of control.

3.1.4. Determining control design and control effectiveness. In this research, the measurement itself
is done to get the effectiveness of any control that implemented on the ISMS, therefore, need to be
separated between the control design with control effectiveness measurement’s selected so that the
object can be in accordance with the requirements for the measurement itself. Control
design is planning, or the description how a control is assembled or formed so that the controls can
functionate in accordance with the expected goals or objectives, while the control effectiveness is an
indicator of the success achieved by the control of the objective, or goals that have been set
previously.

3.1.5. Determining the measurement object. Control objectives, control design, and control
effectiveness that have been determined can be used to assist in determining the measurement
object. The object that will be used by the measurement should be selected based on the priority
information in accordance with the needs of the organization. Examples are included in the
measurement object, i.e. [5]:
   a. Products and services;
   b. Process;
   c. Applicable assets such as facilities, applications, and information systems as specified in
      ISO/IEC 27001: 2013 (Inventory of assets, A.8.1.1);
   d. Business Unit;
   e. Geographical location; and
   f. Third-party services

3.1.6. Determining the measurement attribute. One object of measurement can have one, or more
attributes that can be used to take measurements. To make it easier to determine the attributes, as well
as the measurement object, it needs to be reconsidered, control objective, control design and control
effectiveness of each of the control order attributes can be determined in accordance with the target
control, and can be used for measuring the effectiveness of controls, measurement attributes also
should be selected based on the priority information in accordance with the needs of the organization.
Values that will serve as the basis of the relevant measure is obtained by applying the method of
measurement in accordance with the selected attributes. This option should also ensure that:
a. A base measure is relevant and appropriate measurement methods can be identified; and
b. Valuable measurement results can be developed based on the values obtained and measures developed.

Characteristics of selected attributes determine the type of measurement method used to obtain the values that will serve as the base measure (e.g. qualitative or quantitative).

3.1.7. Evaluating the measurement attribute. Attributes that have been determined to be evaluated or reviewed to ensure that [5]:
   a. Attributes for measurements have been appropriated; and
   b. Data collection has been made to ensure the selected attribute can be used to perform effective measurement.

Only attributes that are relevant to the appropriate base measure should be selected. Although the selection of attributes should consider the level of difficulty in obtaining the attributes to be measured, so it is not just because the data is easily obtainable or attributes that are easy to measure.

3.1.8. Documenting the measurement object and attribute. Henceforth, the object of measurement and the attributes that have been evaluated shall be documented.

3.2. Developing metrics

After the measurement object and attribute obtained, the next step is to apply the measurement object and attribute it to the metric measure, stage of implementation of the measurement object and its attributes depicted in the figure flowchart as follows:

**Figure 3.** The steps to applying object attributes into the measurement and metrics measure.

3.2.1. Determining the base measure. Base measure is the simplest measure that can be obtained. Base measure is the result of the application of the method of measurement for the selected attribute of an object of measurement. A measurement object may have many attributes, but only a
few that can provide useful value to be used as a base measure. A given attribute can be used for several different base measures. Measurement method is a logical sequence of operations used in connection with the scale to measure certain attributes. In the operation may involve activities such as counting occurrences or observing the passage of time. Given the measure of the base can be input for some measure of derivatives, but there is also a base measure that cannot be used as input for the derived measures, but can be directly used as an estimate or evaluation that results in the measurement’s indicator.

3.2.2. Determine derived measure. Derived measure is a measure derived or developed from one or more base measure, based on measurement functions is used. Scale and the unit of derived measure depends on the scale and measure of the basic unit combined with the measurement function. Function measurement or calculation algorithm itself is used to combine two or more base measures to create the derived measure. Measurement functions can involve a variety of techniques, such as the average measure of the base, applying the base measure weights, or assign qualitative values for the measure of the base. Measurement functions can combine base measure that uses a different scale, as a percentage and qualitative assessment results.

3.2.3. Determining the indicator. Indicator is a measure that provides an estimate or evaluation of certain attributes, derived from the model analysis of information needs are defined. The indicator is obtained by applying the analytical model of the measure of the base or the derived measure. Scale and measurement methods influence the selection of the analytical techniques used to produce indicators.

3.2.4. Analyzing indicator. The results of measurement were developed by analyzing or interpreting the applicable indicators based on the criteria set out decisions, and should be considered in the context of the overall measurement goal of assessing the effectiveness of the ISMS controls. Decision criteria used to determine the need for further action or investigation, as well as to describe the level of confidence in the results of measurement. Decision criteria can be applied to a set of indicators, for example, to perform a trend analysis based on the indicators are received at different times.

3.2.5. Metrics Evaluation. Metrics that have been made subsequently evaluated, to ensure metric measures are made in accordance with the target effectiveness of the ISMS controls.

3.2.6. Metrics Documentation. Results of metrics that have been made and evaluated subsequently then documented, so it can be used as a reference in measuring the effectiveness of the ISMS controls.

3.3. Result of objective control, control design and control effectiveness, measurement objects and attributes
Here is an example of the control objective, control design and control effectiveness, as well as measuring objects and attributes that have been determined to control [A.12.1.1] Documented operating procedures:
Table 2. Examples of control objective, control design, and control effectiveness, as well as the measurement object and its attributes.

| A.12 Operations security | Documented operating Procedures |
|--------------------------|--------------------------------|
| A.12.1 Operational procedures and responsibilities | Control objective: The whole operation is done in accordance with operating procedures |
| | Control design: Operating procedures are documented and available for users who need it |
| | Control effectiveness: Operating procedures are executed by the relevant users |
| | Measurement’s object: 1. Employees, 2. Operation procedure that shall be performed |
| | Attribute: 1. Employees who have access to the document operating procedures, 2. Executed operation procedure |

3.4. Metrics result example

Here is an example of the measurement object and attributes applied into metrics, to control [A.12.1.1] Documented operating procedures:

Table 3. Examples of metrics.

| Measurement construct identification |
|-------------------------------------|
| Measurement construct name          |
| A.12.1 Documented operating procedures |
| Logical identifier                  |
| A.12.1.1 Documented operating procedures |
| Purpose of measurement construct    |
| To ensure the document is executed with an effective operating procedures. |
| Control/process objective           |
| Clause [A.12.1.1] Documented operating procedures |
| Control/process                     |
| Clause [A.12.1.1] Documented operating procedures. Operating procedures shall be documented and made available to all users who need them |
| Object of measurement and attributes |
| 1. Employees, 2. Operation procedure that shall be performed |
| attribute                           |
| 1. Employees who have access to the document operating procedures, 2. Executed operation procedure, |
| Base measure specification          |
| 1. The number of employees who have access to the document operating procedures, 2. The number of operational procedures performed, in accordance with the operating procedures documents |
| Measurement method                  |
| 1. Count the number of employees who have access to the document operating procedures, 2. Count the number of operational procedures performed in accordance with operating procedures documents |
| Type of measurement method          |
| 1. Objective; 2. Objective, |
| Scale          | 1. Numerical; 2. Numerical, |
|---------------|----------------------------|
| Type of scale | 1. Nominal; 2. Nominal,     |
| Units of measurement | 1. Personnel; 2. Procedures, |
| Derived measure | 1. The percentage of the number of employees who have access to the document operating procedures |
|                | 2. The percentage of the number of operational procedures performed in accordance with the operating procedures document. |
| Measurement functions | 1. (Number of employees who have access to the operating procedures/total number of employees) * 100 |
|                | 2. (The number of operational procedures performed in accordance with operating procedures document/total operating procedures to be performed) * 100 |
| Indicator      | 1. The bigger percentage of employees who have access to the document operating procedures is better, |
|                | 2. The bigger percentage of the number of operational procedures performed in accordance with the operating procedures document is better. |
| Analytical model | 1. Compare percentage of the number of employees who have access to the document operating procedures with the total number of employees who should have access to documents of operating procedures, |
|                | 2. Compare percentage of the number of operational procedures performed in accordance with operating procedures document to the total number of operating procedures that must be met. |
| Decision criteria | 1. Percentage of employees who have access to the document of operating procedures should be above 85% |
|                | 2. The percentage of the number of operational procedures performed in accordance with operating procedures documents should be above 85% |
| Measurement results | 1. If the percentage below 85% it is necessary to be reviewed, |
|                | 2. If the percentage below 85% it is necessary to control and better monitoring of the implementation of operating procedures. |
| Indicators interpretation | 1. Pie chart |
|                | 2. Pie chart with furnished information about the reason for the procedure was not in accordance with the operating procedures document. |
| Stakeholder    | Information security managers and human resource development manager |
|                | Information Security Auditor or information security manager |
|                | Operational managers and human resource development (HRD) managers |
|                | Staff of operational and or information security staff |
|                | Information security manager |
| Frequency/period | Monthly |
### 4. Conclusions

Based on the results of research conducted, the conclusion that can be drawn from this research are as follows:

1. Has been performed and resulted the development of methods of measurement, which can be used to help create measurement metrics of the effectiveness of information security management system controls.
2. Has applied the measurement object and attributes acquired in metric measures, which can be used to measure the effectiveness of information security management system controls.
3. Standard of ISO/IEC 27004: 2013, can be used to develop measure and measurement controls contained in document ISO/IEC 27001: 2013 standard (Annex A), or ISO/IEC 27002: 2013.

### References

[1] M. Dey 2007 in *Proc. AFRICAN Conference* p 1-6
[2] Qingguo L and Wei Z 2009 *Int. Conf. on Multimedia Information Networking and Security* (Los Alamitos: IEEE Computer Society) p 182
[3] Bilbao A and Bilbao E 2013 *47th Int. Carnahan Conf. on Security Technology (ICCST)* (Los Alamitos: IEEE Computer Society) p 1
[4] Atzeni A and Lioy A 2005 *Adv. Inf. Secur.* 23 1-12
[5] ISO/IEC 2009 *International Standard ISO/IEC 27004 techniques—Information security management—Measurement* (Jenawa: International Organization For Standardization)
[6] Hong-li L and Ying-ju Z 2009 *Int. Symp. on Computer Network and Multimedia Technology* (Los Alamitos: IEEE Computer Society) p 1
[7] R. Barabanov 2011 DSV Report series No 11-007
[8] Karabey B and Baykal N 2009 *43rd Int. Carnahan Conf. on Security Technology (ICCST)* (Los Alamitos: IEEE Computer Society) p 144-48
[9] Azuwa M P, Ahmad R, Sahib S and Shamsuddin S 2012 *Int. J. Cyber-Security Digit. Forensics* 1 280-88
[10] Magott J and Woda M S 2008 *IJCCBS* 1 161-77
[11] Brothby W K and Hinson G 2013 *PRAGMATIC Security Metrics: Applying Metametrics to Information Security* (New York: CRC Press)
[12] Barabanov R, Kowalski S and Yngström L 2011 *Information Security Metrics: Research Directions* (University of Stockholm)
[13] Bayuk J L 2000 *Information Security Metrics: An Audited-based Approach* (Washington, D.C: NIST and CSSPAB Workshop)
[14] Lundholm K, Hallberg J and Granlund H 2011 *Design and Use of Information Security Metrics Application of the ISO/IEC 27004 standard* (FOI-Swedish Defence Research Agency)
[15] ISO/IEC 2013 *International Standard ISO/IEC 27002 Information technology—Security techniques—Code of practice for information security controls* (Jenawa: International Organization For Standardization)