Comparative Study Between the Integration of ITIL and ISO / IEC 27001 with the Integration of COBIT and ISO / IEC 27001

Nur Kholis Gunawan*, Raden Budiarto Hadiprakoso, Herman Kabetta
Cryptography Engineering Department
Sekolah Tinggi Sandi Negara, Bogor, Indonesia.

*nur.kholis@stsn-nci.ac.id, budiarto.hadiprakoso@stsn-nci.ac.id, herman.kabetta@stsn-nci.ac.id

Abstract. This paper tries to get a comparison between the integration of Information Technology Infrastructure Library (ITIL) and ISO / IEC 27001 with Integration of COBIT and ISO / IEC 27001. Factors to be considered are the increased level of information security services credibility, cost of the two standards integration of, the time of implementation, the multiple processes removal, and the increase in understanding between parts of the organization. A literature study is used as a research method. The results of the research can be a reference for organizations to consider two information security standards that will be integrated.

1. Introduction

Information is an asset for individuals, even organizations; this is because information affects the achievement of the organization's vision and mission[1]. Therefore, the organization must manage information to be safe from threats and risks in order to successfully achieve its objectives[14]. Some best practices, such as ITIL and ISO / IEC 27001, can be used in developing information security processes in organizations[6]. Besides, there are also COBIT which helps Executive Managers ensure that the application of Information Technology (IT) supports the achievement of organizational goals and targets. The researchers agree that COBIT, ITIL, and the ISO / IEC 27000 family are the most popular best practices currently implemented[13]. Several studies have tried to integrate two best practices. This integration is carried out for several reasons, for example, improving information security services and combining the advantages of two best practices. Integration has several advantages including the elimination of multiple processes because if one point in a best practice is mapped equally in another best practice, then the point does not need to be done twice (ISO/IEC 27013).

The discussion on integration is, for example, the integration of COBIT and ISO / IEC 27001 so that both complement each other's deficiencies to increase the benefits for the organization especially in terms of IT security[8]. The integration conducted by Mataracioglu and Ozkan was done because COBIT excelled in the application of IT governance, but the explanation in it was general and lacked details regarding how to do it. Whereas ISO / IEC 27001 explains in more detail the things that need to be done in an information security system. There is also research that discusses the integration of two best practices, namely ISO / IEC 27001, can also be integrated with ITIL to improve information security and IT services[11]. This study tried to get an overview of the integration ratio of ITIL and ISO / IEC 27001 with the integration of COBIT 5 and ISO 27001 when seen from the advantage when the integration factor of two best practices in information security is done. The superiority factor for integrating the two best practices of information security is to increase the level of credibility of information security services, the cost of integrating two best practices, implementation time, eliminating multiple processes, and increasing understanding between parts of the organization[3]. This paper only discusses three factors: increasing the level of...
credibility of information security services, eliminating multiple processes, and increasing understanding between parts of the organization.

2. Method
The method approach in this research uses a literature study. A literature study is a study used in gathering information and data with the help of various materials available in the library such as documents, books, magazines, historical stories so on[7]. The following are the steps in library research, according to Kuhlthau[5]:
1. The choice of topic is best practice in implementing information security
2. Exploration of information is the integration between two best practices
3. Determine the focus of research, namely the comparison between two integrations by comparing
4. Collection of data sources namely thesis, paper, practitioner's writing about the integration of two best practices
5. Presentation of data
6. Compilation of reports.

3. Results and discussion
3.1. The results of the comparison of the level of credibility of information security services
According to Heru Susanto[2] COBIT focuses on the scope of IT Governance, ITIL focuses on Service Management, while ISO / IEC 27001 focuses on Information Security Management Systems. The integration between ITIL and ISO / IEC 27001 will improve information security and IT service levels[11]. While the integration between COBIT and ISO/ IEC 27001 will increase the benefits for the organization, especially in terms of IT security and the benefits of IT for the organization[8]. However, according to Heru Susanto[2], the three best practices have different numbers of countries using the following data ISO / IEC 27001 several 163 countries, ITIL several 50 countries and COBIT 160 countries. Thus, there will be differences in global recognition between the integration of COBIT and ISO / IEC 27001 with the integration of ITIL and ISO / IEC 27001.

3.2. The results of the comparison of multiple process removal factors
According to Mark Sykes[9] by mapping the control objectives and controls in ISO / IEC 27001, some are relevant to ITIL. Total control of the ISO / IEC that can be supported by processes and activities that are part of the ITIL can be seen in Table 1.

| Area                                      | Number of process-control relations |
|-------------------------------------------|------------------------------------|
| A.5 Security Policy                       | 2                                  |
| A.6 Organization of Information Security  | 22                                 |
| A.7 Asset Management                      | 2                                  |
| A.8 Human Resources Security              | 10                                 |
| A.9 Physical and Environmental Security    | 13                                 |
| A.10 Communications and Operations Management | 32                              |
| A.11 Access Control                       | 12                                 |
| A.12 Information Systems Acquisition, Development and Maintenance | 12 |
Sheikhpour and Modiri present a reverse mapping of ISO / IEC 27001 control and control objective into the ITIL processes and activities. As a result, many of the controls and control objectives in ISO 27001 are part of Service Management which makes integration of the two more natural[10]. Mapping the number of ISO / IEC 27001 control and control objective into the ITIL processes and activities can be seen in Table 2.

**Table 2. Relationship between ISO / IEC 27001 control and control objective into the ITIL processes and activities**

| ITIL Process               | Number of control-process relations |
|---------------------------|-------------------------------------|
| Service Strategy          | -                                   |
| Service Design            | 31                                  |
| Service Transition        | 36                                  |
| Service Operation         | 27                                  |
| Continual Service Improvement | 19                                |

Whereas in the integration between COBIT and ISO / IEC 27001, the ISO / IEC 27001 will cover the DS5 section, namely Ensure Systems Security. However, the topic of information security is spread across other domains, so many controls and control objectives are mapped to the process in COBIT domains. Mapping the number of controls and the objectives of ISO / IEC 27001 controls related to COBIT can be seen in Table 3, as mentioned by Sheikhpour dan Modiri[12].

**Table 3. Relationship between ISO / IEC 27001 control and control objective to COBIT processes and activities**

| Domain                | Number of process-control relations |
|-----------------------|-------------------------------------|
| Plan and Organize     | 52                                  |
| Acquire and Implement | 45                                  |
| Deliver and Support   | 68                                  |
| Monitor and Evaluate  | 14                                  |

Thus, many of the objectives of ISO / IEC 27001 control are related to COBIT if the integration process is carried out.

3.3. The results of the comparison of understanding between parts of the organization based on improvement factors

According to Kristian Beckers[4], the integration of ITIL and ISO / IEC 27001 will facilitate coordination and alignment between the Information Security Section that will implement ISO / IEC 27001 and the Risk Management Section that has implemented ITIL. The Information Security Section will quickly identify which ISO / IEC 27001 parts have been implemented and which have not. ITIL and ISO 27001 are both based on the Plan-Do-Check- Act (PDCA) process model. According to ITIL's perspective, almost all security controls in ISO / IEC 27001 are part of ITIL.
There are various sequences in the application of integration between ITIL and ISO / IEC 27001, be it ITIL applied before ISO / IEC 27001 or vice versa, all of which continue to facilitate the Information Security Section and the Risk Management Section to keep coordinating and aligning[11].

ISO 27001 only focuses on information security, while COBIT generally focuses on IT control to benefit the organization. COBIT has a broader scope on IT Governance but does not have detailed information security control requirements such as ISO / IEC 27001. Thus ISO / IEC 27001 will support COBIT in implementing Information Security Governance[12]. With a variety of scenarios in the order of application to the integration of COBIT and ISO / IEC 27001, the information security department will continue to work efficiently with other sections such as the Management and Audit Sections. It is because if the information security department implements the controls in ISO / IEC 27001, many parts of COBIT have been covered and vice versa if the order of integration is implemented[12]. Coordination and alignment between the fixed part are easy to do.

4. Conclusion

The integration between ITIL and ISO / IEC 27001 will increase the credibility of information security in IT service management, while the integration between COBIT and ISO / IEC will increase the credibility of information security in IT Governance. Both integrations have many dual processes that can be done once in the integration process and equally facilitate understanding and coordination between parts of the organization. The difference between the two integrations is the global recognition that COBIT is more widely applied globally.

References

[1] Alberts, C., 2003 Introduction to The OCTAVE Approach. USA: Carnegie Mellon University.
[2] Heru Susanto, Mohammad Nabil Almunawar, Yong Chee Tuan, 2011 Information Security Management System Standards: A Comparative Study of the Big Five, International Journal of Electrical & Computer Sciences IJECS-IJENS Vol: 11 No: 05 21-27.
[3] International Organization for Standardization (ISO), 2012 ISO/IEC 27013 Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1, ISO Copyright Office. Published in Switzerland.
[4] Kristian Beckers, Stefan Hofbauer, Gerald Quirchmayr, Christopher Wills, 2013 A Method for Re-using Existing ITIL Processes for Creating an ISO 27001 ISMS Process Applied to a High Availability Video Conferencing Cloud Scenario, 1st Cross-Domain Conference and Workshop on Availability, Reliability, and Security in Information Systems (CD-ARES), Regensburg, Germany. pp.224-239.
[5] Kuhltau, C. C., 2002 Teaching The Library Research, USA: Scarecrow Press Inc.
[6] Larrocha ER., Minguet JM, Díaz G., Castro M. and Vara A., 2010 Filling the gap of Information Security Management inside ITIL®: proposals for postgraduate students. IEEE EDUCON Edu. Engg. pp: 907-912.
[7] Mardalis, 1999 Metode Penelitian Suatu Pendekatan Proposal, Bumi Aksara : Jakarta.
[8] Mataracioglu, T., & Ozkan, S., 2011 Governing Information Security In Conjunction With COBIT and ISO 27001. 1-5.
[9] Mark Sykes and Nigel Landman, 2013 How ITIL can be used to support the delivery of compliant practices for Information Security Management Systems. Fox IT SM Resourcing Ltd and QT&C Group Ltd.
[10] Razieh Sheikhpour and Nasser Modiri, 2011 Mapping Approach of ITIL Service Management Processes to ISO/IEC 27001 Controls, Journal of Computing, Volume 3, Issue
[11] Razieh Sheikhpour dan Nasser Modiri, 2012 A best practice approach for integration of ITIL and ISO/IEC 27001 services for information security management, Indian Journal of Science and Technology Vol 5 No. 2, 2170-2176.

[12] Razieh Sheikhpour and Nasser Modiri, 2012 An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls, International Journal of Security and Its Applications Vol. 6, No. 2, 13-28.

[13] Sahibudin Sh, Sharifi M and Ayat M, 2008 Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. Proc. 2nd Asia Intl. Conf. Modelling & Simulation. pp:749-753.

[14] Tryfonas, T., 2009 Information Security Management and Standards of Best Practice. World Scientific.