

An Analysis of IT Assessment Security Maturity in Higher Education Institution

Misni, Harjo Suwito
University of Mercu Buana

Shinichi, Matsumoto
Institute of Systems, Information Technologies and Nanotechnologies

Junpei Kawamoto
Faculty of Information Science and Electrical Engineering, Kyushu University

Gollmann, Dieter
SVA Security in Distributed Application, Hamburg University of Technology

他

<https://hdl.handle.net/2324/1566107>

出版情報 : Information Science and Applications (ICISA) 2016, pp.701-713, 2016-02-15. Springer
Singapore

バージョン :

権利関係 :



An Analysis of IT Assessment Security Maturity in Higher Education Institution

Misni¹, Shinchi Matsumoto², Junpei Kawamoto³, Dieter Gollmann⁴, Kouichi Sakurai⁵

1. Faculty of Computer Science University of Mercu Buana, Jakarta, Indonesia.
misni.muhammad@mercubuana.ac.id
2. Institute of Systems, Information Technologies and Nanotechnologies (ISIT), Kyushu, Japan
smatsumoto@isit.or.jp
3. Faculty of Information Science and Electrical Engineering, Kyushu University, Kyushu, Japan
kawamoto@inf.kyushu-u.ac.jp
4. SVA Security in Distributed Application, Hamburg University of Technology, Germany
diego@tu-harburg.de
5. Faculty of Information Science and Electrical Engineering, Kyushu University, Kyushu, Japan
sakurai@csce.kyushu-u.ac.jp

Abstract: The information technology (IT) has been applied widely in Indonesia Higher Education Institution for various services. Many organizations responsible for managing the IT infrastructure, however, rarely have a framework for assessing the security maturity level of their information management. The implementation of a framework is one of solutions, but has not been yet maximized. Therefore we suggest to combine several frameworks in hope that they can be complementary. The combination of different frameworks will be more effective to monitoring the security maturity level by using an assessment security maturity management. This assessment security maturity management is a combination of framework control objective from IT Governance COBIT® 4.1 (Control Objectives for Information and related Technology) with Management Service in ITIL v3 (Information Technology Infrastructure Library) and ISO/IEC 27001. Since assessment of security maturity management is measured using COBIT® 4.1 assessment framework, and before it was adjusted with the ISO 27001 framework applied maximal. This paper present the results of assessment maturity security management, mapping of combination framework providing an indicator of security maturity level at one of university in Jakarta. A case study conducted shows that combination of some frameworks to support assessment of security maturity management level becomes more effective and efficient.

Keywords: COBIT® 4.1, ITIL® V3, ISO/IEC 27000, Risk Assessment, Information Technology Security, Service Management, Maturity

1. Introduction

The information technology (IT) has been applied widely in Indonesia Higher Education Institution for various services. Many organizations responsible for managing the IT infrastructure, however, rarely have a framework for assessing the security maturity level of their information management. The purpose of this paper is to explain to business users and senior managements the importance of IT best practices and how to easily harmonize, implement, and integrate these best practices. To attract attention and challenge the companies when building IT best practices by making combinations between the three IT standards (COBIT® 4.1, ITIL ® V3, and ISO / IEC 27002) and highlight their features. All three standards discussed in this paper have their own useful rules: COBIT® 4.1 and ISO / IEC 27002 can be used to determine what should be done and ITIL ® V3 provide a service management aspect. There is a major risk from the implementation of these practices, where usually the best practices can be costly and unfocused if they are treated as a pure technical guideline. To be most effective, best practices should be applied in the context of the business and focus on providing the most benefit to the organization. IT best practices are very important in

the organization because of their support not only in management of IT, which is critical to the success of the company's strategy, but also the effective governance of IT activities, ITGI (2008). An IT best practices framework also enables the effective management of policies, internal controls, and practices, as well as many other business benefits, including efficiency gains, less reliance on experts, fewer errors, confidence of business partners, and respect of the regulator. This paper proposes a method for information security management through a combination of several standards for the evaluation of maturity and control of continuous improvements. The main contribution of this paper are:

- To identify the security maturity objectives that can be used to achieve the strategic goals.
- To obtain as soon as possible a instead of return on investment from using a security maturity model.
- To make a decisions about the security maturity, accounting for hidden costs, and future considerations.

The paper is organized into six sections. Section 2 presents motivation and related work. Section 3 presents the methods and materials. Section 4 is an overview of IT governance. Section 5 discusses the design maturity assessment. In section 6 present a case study and the last section presents the conclusions.

2. Motivation and Related Work

The motivation for this paper is to assess the implementation of security challenges in an organization. In addition to the challenges of implementation, the present work tries to fulfil the requirement of best practices implementation and provide self-learning organization that can be used to measure their information security practices. Several attempts have been made to establish information security management maturity models. The ISM3 system was introduced to prevent and mitigate attacks, errors, and accidents that jeopardize security [2]. While this attempt recognized three levels of management responsibility, it did not provide best practices for the implementation of security. Information security management maturity model [3], NIST (PRISMA)¹ information security maturity model, Generic security maturity model (GISMM) [2][14], and SUNY's information security initiative [2], represent one of the standards from the information security area, whose main goal, apart from achieving the admissible level of security, is achieving business results. Although it has been presented widely about information security, there are similarities for the solutions application with all the three standards described earlier. The idea of achieving business results, regardless of the information security issues, appears also in COBIT® 4.1. It should be underlined that other standards do not mention explicitly how to maintain efficient business, but they imply that the business continues in spite of the security problems. Maturity Model, which is integrated into this standard, provides management tools to measure business results, and that is why ISM3 is characteristic compared to all other standards.

3. Method and Materials

3.1 Information Security Maturity Model

The information security maturity model (ISMM) is intended as a tool to evaluate the ability of organizations to meet the objectives of security, namely, confidentiality, integrity, and availability while preventing attacks and achieving the organization's mission despite attacks and accidents. The model defines a process that manages,

¹ NIST Special Publications (SPs) such as NIST SP 800-53 (Revision 3), Recommended Security Controls for Federal Information Systems; existing federal directives including FISMA; and other proven techniques and recognized best practices in the area of information security.

measures, and controls all aspects of security. It relies on four core indicators for benchmarking and serves as an aid to understanding the security requirements of the organization. These indicators are goal-driven to achieve security needs. Many of these models are quite detailed and target security with regard to the technological requirements, usually leading to a very expensive program to work for implementing security that focuses on technology, but is not business oriented. There has been a use of other models, including restricting the scope for individual business units or given its scope in terms of the company's business processes. An analysis of developing IT governance model is shown in Figure 1 to illustrate the basics of theoretical approaches. This model starts with COBIT® 4.1 Maturity which is presented in Table 1 and ending with COBIT® 4.1 using the RACI (Responsible, Accountable, Consulted and Informed) control embedment process. A combination of IT governance maturity model, COBIT® 4.1, ISO 27001 and ITIL ® V3 achieved at the level of standards and processes within the framework rather than at the level of objective control. Process key of ITIL ® V3 is for change management and release management process models mapped to ISO 27001 and then presented in a conventional EPM program management structure for reporting and ongoing management. Each concept of security, building or type of device that has a dimension associated with the changes is identified in this model.

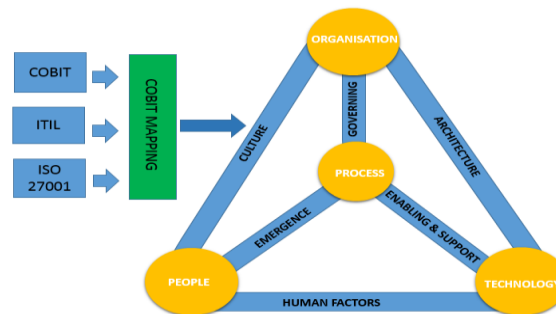


Fig. 1.Information Security Model

The goal of information security is to properly protect this asset and to ensure business continuity, reduce damage to the business, and improve the return on investments made in the business. As defined by ISO 27001, the information security is described as preservation [7], *Confidentiality*: This is to ensure that information is accessible only to those who are authorized and have the right to access, *Integrity*: This is to ensure that information is accurate and now must modify and securely maintain the accuracy and completeness of information and processing methods, *Availability*: this is to ensure that authorized users have access to information and associated assets when required.

3.2 Combination Standards

As a framework and different standards evolve, they create confusion, especially when using one of them. When taking a closer look at them, it is very clear that they can be successfully aligned. To carry out the process to provide IT-services without really defining measures to monitor the process will lead to a higher risk and it would not be more efficient and effective. It is one of the arguments for the combination COBIT® 4.1, ITIL ® V3, and ISO / IEC 27001. Therefore, IT best practices need to be adapted to business needs and integrated with each other and with internal procedures. COBIT® 4.1 can be used at the highest level, providing an overall control framework based on the IT process model that should suit every organization in general. Specific practices and standards such as ITIL ® V3 and ISO / IEC 27002 cover discrete areas can be mapped to the COBIT® 4.1 framework, thus providing a hierarchy of guidance

materials. It is much clear that security is the main concern at this time so that for each process application of security standards shown in Table 1.

COBIT® 4.1	ITIL® V3	ISO/IEC 27001
Services Support DSS02 Manage service request and incident APO11 Manage quality	Service desk	6.3.2 reporting security weakness
DSS02 manage problems and incidents	Incident management	13.2.1 establish incident response responsibilities and procedures
DSS04 manage problems	Problem management	13.2.1 establish incident response responsibilities and procedures
BAI010 manage configuration	Configuration management	
BAI06 manages changes	Change management	10.5.1 change control procedures 8.2.1 operational change control
BAI06 manages changes	Release management	10.4.1 control of operational software 10.5.2 technical review of operating system changes release
Service Delivery APO09 manage service agreements	Service level agreement	4.2.2 security requirements for third party contracts 10.2.1 manage third party service agreements
APO006 manage budget and cost	Financial management	
DSS04 manage continuity	Continuity management	14 business continuity management
BAI04 manage availability and capacity	Capacity management	8.2.1 capacity planning
BAI04 manage availability and capacity	Availability management	8.5.1 network control 9.5.5 use of system utilities

Table 1. Combination of IT Governance Standard

The table mentioned above is a clear mapping between themes of COBIT® 4.1, ITIL® V3, and ISO 27001 that might make us believe that the objectives of three standards instead of are comprised the same security instructions and guidance. However, it is interesting to note that although the themes are the same, there are minor differences in the implementation requirements which drastically affect the planning and budgeting for implementing these standards. Thus, a manager is expected to carefully understand all the objectives of the three documents, despite having a clear representation of their mappings – as this will enable him/her to make a better decision on using these frameworks, in case he/she feels the need to use these in complement to each other.

4. Overview of the IT Governance

IT Governance is part of a wider Corporate Governance activity, but with its own specific focus. The benefits of good IT risk management, oversight, and clear communication not only reduce the cost and damage caused by IT failures – but also engenders greater trust, teamwork, and confidence in the use of IT itself and the people trusted with IT services. The following is an analysis combination of three standards IT governance: COBIT® 4.1, ITIL ® V3, and ISO27002, which have different characteristics but they have a role in best practice guidance on how to efficiently use this standard within the organization's IT environment. An analysis is presented in Table 2 and can be seen that there are similarities and differences of those three standards:

Combination IT Governance Standards					
Standard/ Framework	Control Objective	Issuer	Implementation	Function	Professional
COBIT® 4.1	34 Processes and 4 Domain	ISACA	Information System Audit	Mapping IT Process	Accounting Company, IT Consulting Company
ITIL ® V3	9 Processes	OGC	Manage Service Level	Mapping IT Service Level Management	IT Consulting
ISO 27002	10 Domain	ISO Board	Compliance with Security Standards	Information Security Framework	IT Consulting Company, Security Company, Network Consultant

Table 2. Combination Standard IT Governance

The Table 2 shows the first of three standards issued by different organizations with different areas of activity and target. The general role of the standard are also found to be slightly different. COBIT® 4.1 provides the best practices and tools for monitoring and mapping of IT processes while ITIL ® V3 aims to map IT service level management

and ISO 27002 provides guidance for implementing an information security framework standard. COBIT® 4.1 consists of 4 domains and 34 processes necessary for implementation of information systems audit. For ITIL best practice framework includes a total of 9 processes and enables the implementation of IT service level management that is focused on achieving business effectiveness and efficiency in the management of IT services. At the time of determining or selecting the appropriate standard, managers must also consider the type of vendors that can offer them the preferred solution of IT application standards.

4.1 Framework COBIT® 4.1

COBIT® 4.1 is a set of documentations of best practices for IT governance that can help the auditor, management and users to bridge the gap between business risks, implement controls as well as technical problems [8]. In practice provided by COBIT® 4.1, provided measures to ensure servicing and administering standards of measurement to assess when there is an error in its use. There are 13 control objectives to ensure delivery of services and support is good, ranging from. COBIT® 4.1 also provides parameters for the assessment of the IT management in an organization by using maturity models that can be used for assessment awareness of officials and maturity levels using the method of assessment.

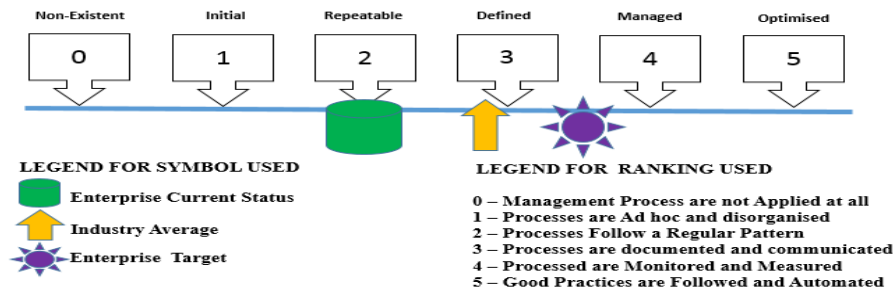


Fig. 2. Maturity Model of COBIT® 4.1

4.2 Framework ITIL® V3

Information technology infrastructure library (ITIL® V3) is a standard of practices associated with information technology services and provides for good practice in guiding the management of IT service management [9]. Service is all about delivering value to the consumer, and also defines services as a means of delivering value to customers in order to facilitate the results customers want without adding cost or specific risk [10]. ITIL® V3 defines service management as a set of specialized organizational capabilities for providing value to customers in the form of a service. There are five stages in [10]. ITIL® V3 is a collection of best practices for the management of IT services; helps organizations to become aware of the business value that their IT services provide to internal and external stakeholders; security management process describes the structured fitting of security in the management organization [11]. Integration of security best practices like ISO/IEC 27001 into service management best practice processes like ITIL® V3 enables the organization to lower the overall cost of maintaining acceptable security levels, effectively manage risk and reduce overall risk levels [12].

4.3 Framework ISO 27000:2005

The goal of information security is to protect all assets to ensure continuity, business keep running, minimize business risk and maximize company profit [13] series is a

standard for information security management that is recognized internationally. The ISO 27002 will be used in working on this research.

4.3.1 ISO/IEC 27001:2013

This is a standard for building information security management system (ISMS). Inside are four steps to implement and how to define, implement, monitor and maintain the ISMS [14].

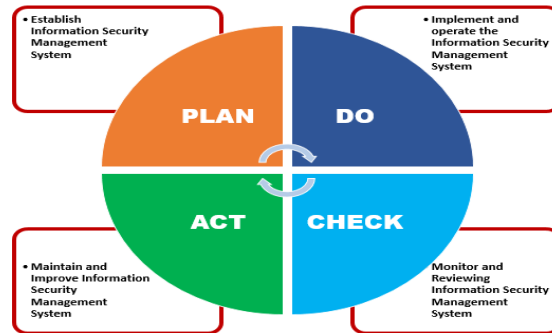


Fig. 3. PDCA model applied to ISMS processes ISO 27001:2005

4.3.2 ISO/IEC 27002:2005

This standard is originally published to replace previous standard, i.e. ISO 27002:2005 used as a best practice information security management. Basically, it has hundreds of potential control mechanisms and its control, which will be implemented in, and follow outlined theory in [11]; set guidelines that are used as a general principle to initiate, implement, maintain and improve information security within an organization; has 14 areas. These areas are as follows:

1. Framework-Acceptable Use of Information Technology Resources
2. Information Security Definition & Terms
3. Risk Assessment
4. Security Policy
5. Organization of Information Security
6. Asset Management
7. Human Resources Security
8. Physical and Environmental Security
9. Communications and Operations Management
10. Access Control
11. Information Systems Acquisition, Development and Maintenance
12. Information Security Incident Management
13. Business Continuity Management
14. Compliance

4.4 Combining Frameworks COBIT® 4.1, ITIL® V3 and ISO/IEC 27000 series

Combining the three standard can be very useful as a system of interconnected networks that can support service management structure by offering some standard compliance rules within each organization. This can be tested by combining three management specifications (COBIT® 4.1, ITIL ® V3 and ISO 27002) is a very complicated process and become a very important thing in this study to obtain harmony between them in

order to facilitate the mapping of IT standards in the organization. Here is a model of the interconnection of three standards:

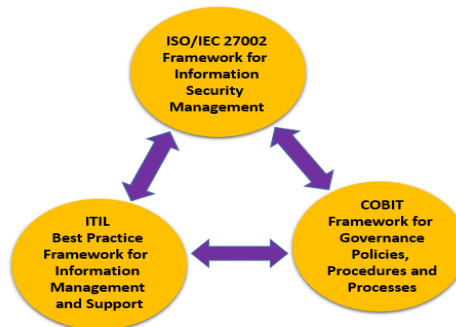


Fig. 4. Combinations Framework

Gehrmann [9] highlights that security and control of implementation COBIT® 4.1 standard combined is able to reduce critical threats can interfere with project results. That is the main structure which must be applied in the overall security assurance organization at all levels. Administrative and management issues that are not addressed in the standard ISO / IEC 27000 and COBIT® 4.1. This is possible because it has features to maintain confidentiality, integrity and availability of information within the organization. The availability of this information in COBIT® 4.1 dealt with aspects of quality, reliability and maintenance. The method used to determine strategies, concepts, and processes related to security services carried out within an organization, a service provider in one of the universities in Jakarta has a function as a technical unit that carried out the field of data processing. IT management is used to evaluate critical success factors, metrics, indicators and audits, ISO / IEC 27001 IT management standards guide on issues of security relations.

5. The Design of Assessment Maturity

This chapter explains the design of assessment to be built on research. The combination designs several standards types that have been outlined in the previous chapter.

5.1 Concepts/processes

In the discussed processes of security, perspectives, there are five cycles. It is based on the ability to describe processes, functions and organizational structure to support major areas within IT service management. From the perspective of security, it also discusses Information Security Management (ISM) in each stage of service [9].

5.2 Area

In perspective of the discussed security management services, it is based on purpose, of combination COBIT® 4.1, ITIL® V3 and ISO/IEC 27002 for security information technology services management that expected to be done effectively and efficiently, security risks are minimized and accordance with the requirements applicable law [9].

5.3 Mapping Component of Assessment Maturity

Mapping assessment maturity security service management using a combination concept based on needs organization, i.e. not only ensure its services can run well in accordance with planned quality, but also able to ensure that the service runs safely.

	Service Strategy				Service Design				Service Transition				Service Operational		Service Continual								
	Strategy Generation	IT Fundamental Management	Service Portfolio Management	Demand Management	Service Catalogue Management	Service Level management	Availability management	Capacity Management	Service Continuity Management	IT Security Management	Supplier Management	Change Management	Service Asset and Configuration	Release and Deployment	Transition Planning and Support	Service Validation and Testing	Evaluation	Knowledge Management	Incident Management	Problem management	Event management	Access Management	The Seven Step Improvement
COBIT DS-1 : Define and Manage Service Levels																							
Security Policy	N	N	N	Y	Y	N	N	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N
Organization of Information Security	Y	N	N	Y	Y	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	Y	N	Y	N
Asset Management	N	N	N	N	N	N	N	Y	Y	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N
Human Resources Security	N	N	Y	N	Y	N	N	N	Y	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N
Physical and Environmental Security	N	N	N	N	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
Communications and Operations Management	N	N	N	N	N	N	Y	N	Y	Y	N	Y	N	Y	N	N	N	Y	Y	N	Y	N	N
Access Control	N	N	N	N	N	N	Y	N	Y	Y	N	N	N	N	N	N	N	N	Y	N	N	N	N
Information Systems Acquisition, Development and Maintenance	N	N	N	N	Y	Y	N	N	N	N	N	N	Y	Y	N	N	N	N	N	N	N	N	N
Information Security Incident Management	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N	N	N	Y	N	Y	N	N	N	N
Business Continuity Management	Y	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	Y	Y	Y
Compliance	N		N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N

Fig. 5 Mapping Component Assessment

The combination is processed to produce maps more assessment directional of security service management with required security management in each phase with the control objective strategy IT all using best practice.

5.4 Setting of Scoring and Status Assessment

Determination of scoring and status parameter assessment using COBIT® 4.1, which have been elaborated. In assessment, there are six steps assessment levels, namely:

Score	Status	Description
0	Non Existent	Management Processes are not applied at all
1	Initial	Processes are ad hoc and disorganized
2	Repeatable	Processes Follow a regular pattern
3	Defined	Processes are documented and communicated
4	Managed	Processes are monitored and measured
5	Optimized	Good practices are followed and automated

Table 3. Scale used for maturity levels

5.5 Mapping of Assessment Maturity

Mapping assessment based on the needs of organization, i.e. not only to ensure the service can run well according to the planned quality, but also able to ensure that existing services are run with secure combining process derived from mapping assessment component.

ITIL® V3	ISO/IEC 27001	COBIT® 4.1	Maturity Model
Service Strategy	Security Policy Organizational structure	DS1-Define and Manage Service Level DS2- Manage third-party services	
Service Design	Asset Management Security Human Resources	DS1-Define and Manage Service Level DS2- Manage third-party services	
	Physical and Environmental Security	DS3- Manage performance and capacity DS4-Ensure continuous service DS5-Ensure systems security DS11- Manage data	
Service Transition	Addition, Development and Maintenance Information System	DS7-Educate and train users DS9- Manage the configuration DS12- Manage the physical environment DS13- Manage operations	
Service Operation	Communications and Operations Management Access Control Management of security incidents	DS8- Manage service desk and incidents DS10- Manage problems DS13- Manage operations	
Continual Service Improvement	Business Continuity Management Fulfilment Requirements		

Table 4. Mapping Assessment Maturity

5.6 Assessment Process

The initial assessment process obtained conditions existing incentives that are still not in accordance with ideal conditions based on standard security services because there are still some discrepancies and availability of IT governance. Security problems in implementing a service are not yet concentrated, in case studies still looking for a suitable pattern used to measure the level of maturity security services management IT. By combining framework and some of the best practices, it is expected to be able to answer those needs.

6. Case Study and Results

IT Governance Institute recently developed a maturity model of specific IT governance. According to this model, company/organization is rated at level 0 is characterized by a complete lack of any recognizable IT governance process. To rise to the level 1, organization at least needs to recognize the importance of addressing issues of IT governance.

Maturity level 5 implies understanding of advanced and forward-looking IT governance issues and solutions, supported by a framework established and best practices of the structures, processes, and relational mechanisms. It should be noted that the desired "to be" the position must be identified in function of the context in which one operates (business, industry, geography, size, etc.) and corporate strategy. When the "as is" and "to" position is known, the gap can be determined, the project is defined and specific actions can be taken.

A case study that makes maturity security assessment service management done, service providers, one of university in Jakarta that has functioned as a unified technical implemented in the field of data processing. An organization has tasks in collecting, processing, storing, and presenting data and information as well as providing service education programs, research, and community service.

To organize this, the tasks are functioned in a good organizational structure with few equipped standard operating procedure (SOP). The organization distributed a detailed questionnaire to collect data to find concentrated existing conditions. The following table is based on the collected data from the assessment:

Management Process	Existing Condition	Ideal Conditions	Description
Organizational Readiness	2.87	4	Not Appropriate
Asset management	2.96	4	Not Appropriate
Preparation of IT	2.25	4	Not Appropriate
Implementation of IT	2.34	4	Not Appropriate
Development Planning	1.59	4	Not very Appropriate

Table 5. Results of Data Collection

It was found that the organization does not yet have a standardized security management or a good service. This is reflected by completeness of SOP and compliance organization owned.

7. Conclusions

Based on the test results from case studies and analysis that have been done in this research, the conclusions as follows:

The creation of security assessment services management combining with standard service delivery and assessment based on maturity model is relevant.

1. The combination between IT management methodology using the COBIT® 4.1 and ISO/IEC 27002 give a more comprehensive results and the most efficient in the preparation of implement features.
2. Assessment decision can be made to contain the features of devoted public organization service providers, especially university.

References

1. Zacarias, M., & Martins, P.V. (2011). Collaborative Methods for Business Process Discovery. Spatial and Organizational Dynamics, 7 , 45-55
2. Lessing, MM. 2006. A Model for Best Practice Driven Information Security Governance. Unpublished dissertation. Johannesburg: University of Johannesburg.
3. ISM3 Consortium. (2007), "Information Security Management Maturity Model version 2.10" Consortium, (Also available at <http://www.ism3.com/>, Last access September, 2010).
4. Aceituno, V. (2007), "ISM3 - Information Security Management Maturity Model – v. 2.1." ,available at: <http://www.ism3.com/> (accessed 18/June/2013)
5. Karokola, G., Kowalski, S. and Yngström, L. (2011), "Towards an Information Security Maturity Model for Secure e-Government Services: A Stakeholders View" in Proceedings of the Fifth International Symposium on Human Aspects of Information Security & Assurance in London, UK, pp. 58-73.
6. The Open Group (2011), Open Information Security Management Maturity Model (O-ISM3), Van Haren Publishing.
7. Daminda, P., 2008. ISO/IEC 27001 Information Security Management System. ISO 27001 Family, pp: 2-21.
8. The IT Governance Institute, COBIT 4.1, USA: the IT Governance Institute, 2007.
9. Gehrmann, *Combining ITIL, COBIT and ISO/IEC 27002 for structuring comprehensive information technology for management in the organization*, 2012.
10. The IT SMF International, Foundation of IT Service Management based on ITIL V3, Van Haren, 2007
11. ISO/IEC, Information Technology-Security techniques-Code of Practice for Information Security Management, Switzerland: ISO/IEC in 2005, 2005.
12. Warre KV (2010) Security controls in service management. SANS Institute reading room. From <http://www.sans.org/search/results>
13. Calder and s. Watkins, IT Governance A manager's Guide to Data Security and ISO 27001/27002, London: Kogan Page Limited, 2007
14. Architecture, Security Management Framework, Security Architecture, 2009.
15. Lijnse, "Service Management Art," 2006. [Online].