Assessing Information Security on Academic Educational Institution in Indonesia

MISNI HARJO SUWITO[†1] SHINCHI MATSHUMOTO[†2]
JUNPEI KAWAMOTO[†3] DIETER GOLLMANN [†4]
KOUICHI SAKURAI [†5]

Abstract: Information systems are essential for every organization to access its information. However, these systems need to be secure in terms of confidentiality, integrity, and availability of the information. Securing the information systems is the concern of the ISMS adopted by the organization. Information systems of the universities are critical systems due to the rapid growth demand of students enrolling in universities. This paper contribute, an evaluation of the information security level at the Indonesian Academic Education Institution a case study targeting the University of Mercu Buana (UMB). The case study focuses on analysing the risks from two different perspectives (organizational and technical risks) by applying vulnerabilities assessment and penetration testing, finally organized into a risk assessment plan. Since the case study, an ISO/IEC 27001:2005 ISMS has been developed in order to eliminate the risks that face the UMB information systems.

Keywords: Risk assessment, Information Security Management System, ISO/IEC 27001, Vulnerability assessment.

1. Introduction

Information systems are essential for every organization to access its and one of the most important assets in the 21st century for almost every organization. Vulnerability assessment comes as a solution for identifying the security holes in (a) specific information system(s), by identifying the threats that pose a serious exposure to the organization's assets, which leads to identifying unattended threats and quantifying the reactive measures. A unique set of testing processes, tools, and techniques are followed to detect and identify vulnerabilities in information systems. The penetration testing goes beyond the level of identifying vulnerabilities and hooks into the process of exploitation, privilege escalation, and maintaining access to the information system, showing the real value of the threat and how it can affect the information system. Vulnerability assessment and penetration testing are not a good indemnity for a secure information system. Since most of the highest impact security breaches come from inside the organization, there should be a control mechanism for the information system users/implementer to protect the system from being compromised internally, this could extend also to insuring that the information system business continuity do not exclusively depend on a specific individual existence which could lead to a serious system halt/crash based on the availability of specific personnel. Information Security Management Systems (ISMS) provide a complete solution for a better information security experience by providing the needed policies, tools, and procedures for enhancing and maintaining a secured information system.

Recently, most of the Indonesian universities for example, the University of Mercu Buana (UMB), have been facing a rapid growth demand of students enrolling in its programs, both undergraduate and graduate. As the number of student's increases, the organization and maintainability of its information, which is one of the most important assets affecting the business continuity of the universities, are becoming more and more complicated due to huge amount of paper work to do as well as the hard copy that should be stored and retrieved regularly. Moreover, hard copies must be stored in a secure manner to avoid their sensitive content from being disclosed, tampered, modified, or disrupted, which could lead to the destruction of organization's reputation. This might lead to damaging the credibility of the organization concerning the protection of its own information properly or even to scepticism about the legitimacy of the organization's information as well as the validity of its graduate student's certificates.

The University of Mercu Buana is one of the highly reputable universities in Indonesia. The Information, Communication and E-learning Centre (ICET-UMB) has been working closely with different departments since 2005 in order to computerize its operations such as (student's registration, student's exams, students/employees portals, mailing services, and financials). Computerizing manual operations and some of the paper work comes as a magical solution by using computer-based applications to complete complex, time-consuming, redundant operations in order to organize and maintain student's information efficiently time-wise and effort-wise. These computerized operations must insure information Confidentiality, Integrity, and Availability, unless they can be very easily disclosed, tampered, modified, or disrupted.

Computerized systems are usually built by adopting one of the common solutions such as Microsoft, Oracle, or others. Security holes in these solutions would make the computerized system weak and easy to penetrate. Moreover, lack of awareness about the usage and the configuration for a specific solution leads to more dangerous vulnerabilities in the resulting system. For example, allowing default login credentials on a specific solution allows unauthorized users to get authenticated to a specific system using default login credentials.

Therefore to evaluate of the information security level at the Indonesian universities has been developed by launching a case study targeting UMB. The case study focuses on analysing the risks that face UMB information systems from two different perspectives (organizational and technical risks) by applying vulnerabilities assessment and penetration testing, which is finally organized into a risk assessment plan. Furthermore, a risk mitigation plan is developed in order to eliminate these identified risks. During the case study, ISO/IEC 27001:2005 ISMS have been developed in order to eliminate the risks that face the UMB information systems. The ISMS provides the required policies and controls in order to minimize the identified risks and minimize the likelihood of new vulnerabilities emersion. The provided ISMS should facilitate examining and enhancing the information security experience of UMB-ICET.

In this paper, we have introduced an information security policy, the ICET. Section 2 of this paper includes a brief background material on topics concerning vulnerability assessment, penetration testing, and ISMS. It starts with a brief overview of the vulnerability assessment and penetration testing and its importance for information systems; moreover, it addresses one of the methodologies used in penetration testing, which is the backtrack methodology. In addition, ISMS is discussed in details and reflected on ISO27001 ISMS, showing the importance of this standard as a complete solution for information security against the rapidly growing number of security breaches. In Section 3, we introduce the steps of implementing ISO27001 ISMS; it starts

with identifying the scope of implementation. Also proposed information security policy contains that have two different perspectives: technical and organisational. An example for technical perspective is the password policy which addresses the confidentiality technique to be used and organisational policies is the strategy and planning policy. Section 4 will conclude the paper. Moreover, it will present our future plans concerning this research. The main contributions of this paper are the following:

- To enrich knowledge in the fields of Information Security (IS), Information Security Management Systems (ISMS), and Penetration Testing.
- To evaluate the information security level at Indonesian Universities generally and the UMB specifically by applying a case study on the UMB, one of the leading university in Indonesia
- To define and prioritize the UMB information assets affecting its business continuity.
- To define and prioritize vulnerabilities affecting the information assets of ICET at technical and organizational levels.
- To implement ISO/IEC 27001:2005 ISMS for the scope of ICET, including development of an information security policy in addition to risk assessment and risk mitigation plans to provide the solutions needed to eliminate the existing vulnerabilities.

2. Background

2.1. Vulnerability

In the security system vulnerability is a weakness point of an asset or group of assets that can be exploited by one or more threats [2], and results can potentially compromise the confidentiality, integrity and/or the availability of services. Attacks are the processes of exploiting an existing vulnerability. Attacks are divided into two sub-categories based on their effect on the security requirements, namely, active, and passive attacks. They are called active when the attacks affect the services by compromising the integrity or availability, and passive when they affect the information confidentiality only. The attack itself is a threat for the information system, and every threat has a specific risk based on the vulnerabilities. Figure 1 illustrates the relationship between vulnerabilities, threats, and risk [3].

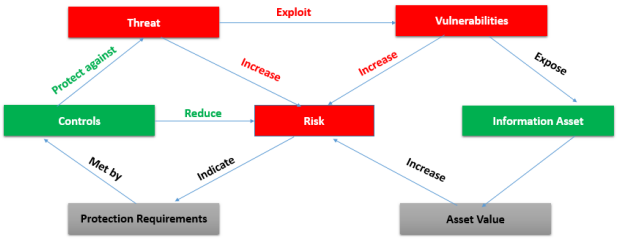

Figure 1. Relation between threat, vulnerabilities, and risk

The most frequently exploited vulnerabilities by attackers are network vulnerabilities. Because all internal and external communications of any company are based on a network, unprotected communication lines and insures network architecture is serious risks. To reduce this vulnerability, it is important to build the network infrastructure securely and use suitable cabling methods in an appropriate way from the beginning. Using a firewall is a good idea, even though it has its own problems.

Personnel risks are more difficult to manage because they are abstract. The key risk indicators refer to the poorly recruited candidates, and the current employees who are not aware of the security process. In response to personnel vulnerability, audit employees access the IT systems, set access privileges for everyone, train employees to increase security awareness, including ethics and the use of policies, and separate employees duties by setting standards and guidelines for the system's development staff.

The lack of monitoring and auditing policies and procedures causes organizational vulnerabilities. To reduce them, the organization should build preventive IT controls. Tests to confirm and validate the correctness of data, auditing, and monitoring must be done.

2.2. Vulnerability Assessment and Penetration Testing

Vulnerability Assessment and Penetration Testing came as tools to identify and quantify the system weakness points in order to improve the security controls and services that protect the information assets. They also give a better understanding about the weaknesses in the existing information system.

Vulnerability analysis can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use.

A. Reasons for Vulnerability Existence
- Insecure coding practices
- Developer education not focused on security
- Limited testing budget and scope
- Disjoined security processes
- More resources outside than inside

B. Steps for Vulnerability Analysis
- Defining and classifying network or system resources.
- Assigning relative levels of importance to the resources.
- Identifying potential threats to each resource.
- Developing a strategy to deal with the most serious potential problems first.
- Defining and implementing ways to minimize the consequences if an attack occurs.

Once analysis has been completed, if security holes are found as a result of vulnerability analysis, a vulnerability disclosure may be required.

Penetration Testing is the process of exploiting the discovered weakness points by a malicious user. The tester needs to gather information, enumerate the vulnerabilities, and finally exploit the given vulnerabilities and gain access to the system [4].

There have been various methodologies introduced to address security assessment needs. The BackTrack testing methodology is one of the methodologies proposed for these purposes. BackTrack is a Linux-based platform aimed for the purpose of penetration testing and security auditing with advanced tools to identify, detect, and exploit any vulnerabilities uncovered in the target network environment. This platform provides users with large collection of security related tools ranging from port scanners to password crackers, applying appropriate testing methodology with defined business objectives and a scheduled test plan will result in robust penetration testing of your network.

Figure 2. BackTrack testing methodology

No.	Activities	Description Activities
1.	Target scoping	To make a successful penetration testing, we must take into consideration the technology under assessment and its basic functionality. An auditor must understand the given scope for the target network environment before starting the security assessment; this step will take him one step closer to the purpose
2.	Information gathering	It is also called reconnaissance phase. During this phase, we should gain information using a number of publicly available resources; the more information we gather, the more chances for the success of penetration testing we gain. This information can be gathered using various methods.
3.	Target discovery	This phase deals with identifying the target status, operating system, and its network architecture. This process provides a full image of the technologies interconnected. By using tools available in Backtrack, it is possible to determine the live network hosts, and identify the operating systems running on these machines.
4.	Enumerating target	This phase is for finding the open ports on the target systems. Scanning may help in determining the port visibility with a number of port scanning techniques such as full open, half-open, and stealth; it sometimes works even if the host is behind a firewall or an Intrusion Detection System (IDS). These ports can be enumerated for the running services
5.	Vulnerability mapping	This phase tends to identify the vulnerabilities based on the valuable information that has been gathered about the target network. This process can be done through using a number of automated network vulnerability assessment and Backtrack tools
6.	Social engineering	When there is no other way available for an auditor to enter the target, the art of deception takes place. A successful penetration may require watching the human psychology before applying the suitable deception technique against the target.
7.	Target exploitation	After examining the revealed vulnerabilities, now it is possible to penetrate the target system. This phase may require modification on the existing exploit; backtrack tools are provided to accomplish this process.
8.	Privilege escalation	Once the target is acquired, the penetration is successfully done. Now we can escalate access privileges using any local exploit that matches the system environment; once they are executed, super-user access or system-level access privileges are attained. After this phase, it is possible to launch other attacks against the local network systems
9.	Maintaining access	Sometimes maintaining access to the system without applying any noisy behaviour is required for a specific period of time. Such activity can be used demonstrating illegal access to the system without applying the penetration testing process again, which saves time, cost, and resources being used. Using some secret tunnelling methods, that make use of protocol or end-to-end connection strategy leads to establishing a backdoor access and maintains the auditor's presence in the target system as long as required
10.	Documentation and reporting	Presenting Documentation and reports about the vulnerabilities found and exploited is the ethical and the final step in the penetration testing methodology. These documents are very important because the concerned technical team will check the method of penetration and will try to close any security loopholes that may exist.

2.3. Information Security Management System (ISMS)

Information Security Management System (ISMS) is a management plan which specifies the requirements for the implementation of security controls customized to the needs of organizations. The ISMS is designed to protect the information assets from any security breaches. ISO27k is a series of international standards for Information security management. This standard covers all types of organizations (e.g., commercial enterprises, government agencies and non-profit organizations) and all sizes from micro-businesses to huge multinationals.

ISO/IEC 27001:2005 standard is a process of applying security management controls on organizations to obtain security services in order to minimize assets' risks and ensure business continuity. The main security services that present the C-I-A triad taken into consideration are [7]: Confidentiality, Integrity and Availability.

This international standard adopts a model called Plan-Do-Check-Act (PDCA) model, which is applied to structure all ISMS processes.

1. **Plan:** Process of establishing the ISMS by applying the policies and objectives of the ISMS as well as developing the procedures concerning managing the risks.
2. **Do:** Process of implementing and operating the ISMS which was planned in the previous step.
3. **Check**: Process of monitoring and reviewing the ISMS by measuring the performance against the applied controls including policies, and, finally, exporting the results to management review.
4. **Act:** According on management reviews, in the previous step, improvements of the applied ISMS is taking place.

We will discussing the details of implementation steps in section 3.

3. Proposed ISO27001 based ISMS

3.1. Proposed Scheme

In this section, we will be addressing the ISMS management framework in addition to the implementation steps of ISO/IEC 27001:2005. ISMS management framework describes the systematic and structural approach of managing information security at ICET. Figure 3 illustrates the implementation steps needed for the ISO27k. This will be discussed in details in the next subsections.

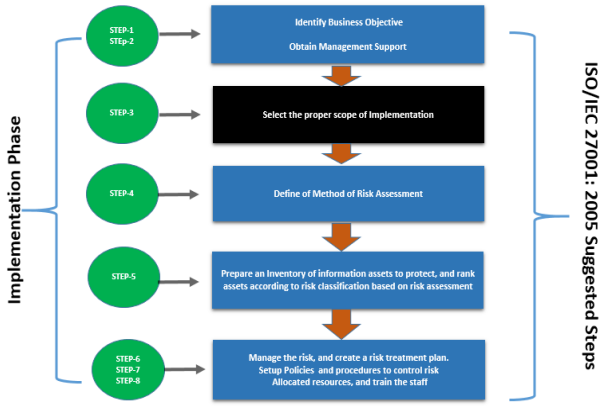

Figure 3. ISO27K implementation steps

Planning is the process of establishing the ISMS by applying the policies and objectives of the ISMS as well as the developing of the procedures concerning managing the risks, in addition to finishing most of the required documented works which are the policies, scope, risk assessment methods, risk assessment plan, risk mitigation plan, and statement of applicability (SoA).

By this the ICET will be ready to start the step by steps which is the process of implementing and operating the ISMS, which was planned in the previous step.

After this steps, there will be some checking which is the process of monitoring and reviewing the ISMS by measuring the performance against the applied controls including policies and finally exporting the results to management review. It is to be noted that the first organization who got the certificate was TELKOM-Indonesian Company [10]. We defined the scope of our study to be the University of Mercu Buana ICET Computer Centre. The main problem we faced was in step (3) where we adopt a black-box methodology, which means that we should treat the ICET as a black box. We made our own assets inventory by identifying the most important assets in the centre.

3.1.1. Establish the ISMS for ICET

A. Determine the scope of the ISMS.
B. Determine an ISMS policy.
C. Define a systematic approach to risk assessment.
D. Identify the risks.
E. Assess the risks.
F. Identify and evaluate options for the mitigation of risks.
G. Select control objectives and controls for the mitigation of risks.
H. Prepare a Statement of Applicability (SoA).
I. Obtain management approval of the proposed residual risks and authorization to implement and operate the ISMS.

3.1.2. Risk Management Methodology

Risk management will be presented and designed to mitigate the Mercu Buana University network. By applying this step, the ICET will be able to operate, monitor, maintain and improve its Information Security Management System according to the requirements of ISO/IEC27001:2005. Table 1 shows the information security risk management activities according the four phases of the ISMS. process [1]:

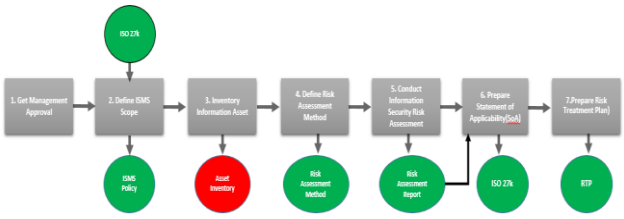

Figure 4. Security process

Table 1. Alignment of ISMS and information security risk management process

ISMS Process	Information Security Risk Management Process
PLAN	Establishing the context Risk Assessment Developing Risk Treatment Plan Risk Acceptance
DO	Implementation of Risk Treatment Plan
CHECK	Continual Monitoring and reviewing of risks
ACT	Maintain and improve the Information Security Risk Management Process

The University of Mercu Buana, as any other organization, faces a struggle in keeping its network secure from inside and outside influences (threats), and in order to keep the business continuity, we need to draw a plan that defines these threats and their impact on the organization and propose a method of how to mitigate them before they pose a great risk on the institution. Advantage to continue monitoring the risk management plan on the organization. The ISO 31000 standard is designed to and intended for implanting risk management codified by the Standardization; the purpose of these standards is to set some boundaries and guidelines regarding the risk assessment and management. Figure 5 illustrates the risk management process. We explain each step and show how we implemented it on the ICET below.

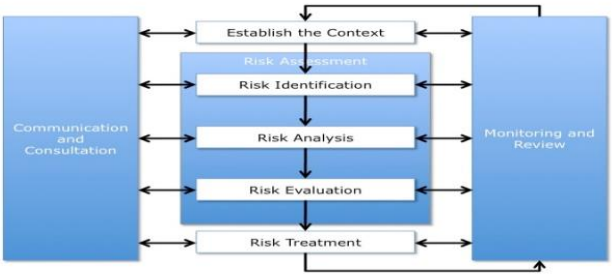

Figure 5. ISO 31000 risk management process

Risk management process consists of many stages according to the ISO 31000:

- Communication and consultation

The communication is needed with the stakeholders in order to document their perception of the risks and their classifications of the assets values. All the risk information obtained from the risk management must be exchanged or shared between the decision-maker and the stakeholders based on an agreement.

- Establishing the context

Defining the scope of our work is performed by discovering all the assets using many vulnerabilities scanners such as Nexpose, Metasploit Pro, Web-security [11].

- Risk assessment

This is the step where we identify the information assets that are of value to the University of Mercu Buana ICET Centre, the threats and the vulnerabilities of information assets, the existing controls present to counter the identified threat and assess the probability and the impact of the threats on the Mercu Buana University Computer Centre. Then risks are determined and prioritized. Finally, the control effectiveness of the implemented controls are measured. Figure 6 illustrates the stages of risk assessment:

Figure 6. ISO 31000 Risk Management Process

- Risk Identification

In this steps we define the scope of risk assessment includes the services provided by the assets listed in the Information Asset Inventory based on their importance to University of Mercu Buana ICET Centre, then we can specify the application of controls as required by ISO/IEC 27001:2005 and ICET Centre Standards (if available). We identify and list all the supporting assets that compliment and support supplying the information technology services provided. As in the information asset inventory, each identified supporting assets shall be mapped to relevant service offering covered under the scope of Risk Assessment, which is describes previously in Figures 3 and 4.

- Risk Analysis

Risk analysis is the process to decide the nature of risk and to determine the level of the risk; it provides the basis for risk evaluation and decisions about risk treatment. Risk analysis includes risk estimation; when estimating the level of the risk two factors should be taken into consideration:

a) The impact of the vulnerability:

The impact rating of each identified supporting asset shall be high, medium or low, taking into consideration the availability importance of services. The severity of each vulnerability is usually defined by global organizations such as CVE (common vulnerabilities and exposures), and CERT which is the United States computer emergency team [12].

b) The likelihood:

In this context, it refers to the chance of occurrence of a specific threat based on the vulnerability, it can be determined objectively or subjectively, qualitatively or quantitatively. Likelihood is defined as the chance of something happening. The ratings are identified as high, medium or low. In the calculation of risk assessment, the term “Probability” is the equivalent of the likelihood [13].

The following will provide the factors to be considered during the rating of an identified vulnerability:

HIGH	In order to exploit the vulnerability, it would require minimal resources and have maximum probable opportunities.
MEDIUM	In order to exploit the vulnerability, it would require minimal resources but have little opportunity or low probabilities. Or, to exploit the vulnerability, it would require a high degree of resources and have maximum probable opportunities.
LOW	In order to exploit the vulnerability, it would require a high degree of resources and have minimal opportunity.

Risk is the outcome of an incident, when a threat successfully exploits the weakness present in an asset. Risk will have a negative impact on an entity or organization. Risk can be measured as the product of an asset impact and a probability that a weakness in an asset will successfully be exploited by a threat action. Risk Assessment Methodology:

- Risk evaluation

The purpose of this step is to assist in making decisions and, especially, in risk treatment and the priority for the treatment implementation based on the outcomes of risk analysis. The risk evaluation can lead to a decision not to treat the risk (risk acceptance). Figure 7 illustrates the risk determining matrix. Based on the determined risk, the risk should be rated from 1 to 6 as illustrated in Table 4. Risk rating helps in the prioritization of risk treatment which will be discussed in the next step, i.e., risk treatment.

Probability \ Impact	HIGH	MODERATE	LOW
HIGH	H/H	H/M	H/L
MEDIUM	M/H	M/M	M/L
LOW	L/H	L/M	L/L

Figure 7: Risk Determining Matrix

- Risk treatment

The second stage of risk management and it is the process of applying adequate protection, based on a management decision to reduce, avoid, transfer and accept risk. An overall planning for the treatment of identified risks should be formulated based on the risk assessment report. Risk treatment involves suggesting options for modifying risks, and implementing those options plus prioritizing risk treatment and offering risk mitigation techniques as well as defining the risk treatment option. Detailed planning and management approval sorting shall be done before treating the identified risks. For all the assets investigated, we offered the risk treatment option and added the required controls plus the ISO 27001 compliance for each vulnerability.
After analysing all these risks and threats, we found out that most of the solutions to these vulnerabilities were:

1. Turning off some services or capabilities related to the vulnerability.
2. Adding access controls using firewalls or network borders.

3. Increasing monitoring to detect or prevent attacks (monitor the intrusion, prevention system) for 24 hours a day.
4. Raising the employee awareness about the vulnerability, giving them courses regarding these matters.
5. Testing and evaluating the patches, before installing, to ensure that they are effective and will not be any side effects.

3.2 Information Security Policies

3.2.1. Planning Policy

The objective of planning is to implement information security, and establish information security plans for the systems.

- Information Security Planning Policy

a) Information Security Officer must be established and filled by ICET that will be responsible for the leading and management of the ICET information security program.
b) The scope of each service must be defined in terms of its supporting assets, assets owners, and its technologies.
c) A risk profile must be created for each included service which should include identification of risks to the assets. Identification of risks must include threats to assets, vulnerabilities that may be exploited by the threats, and the possible impact that loss of CIA (confidentiality, Integrity, and Availability) on the assets.

3.2.2. Requirement Policy

The objective of policies and standards is to define the requirements and responsibilities that the users/employees must follow.

- Information Security Policy
- Statement Policy

3.2.3. Risk Management Policy

The objective of risk management is to manage threats and vulnerabilities facing ICET assets.

• Risk Assessment Policy

a) A risk assessment must be executed on all services at least once every two years or whenever major changes to the services occur.
b) Ongoing monitoring as well as mitigation of risks against different risks must be conducted.

3.2.4. Awareness Policy

The objective of awareness and training is to provide a formal technique for educating the employees of the ICET regarding their responsibilities with respect to information security.

3.2.5. Performance Management Policy

The objective of performance management is to provide metrics to measure progress of the information security program.

a) ICET shall develop measurement procedures to measure the performance of the implemented information security management system, in-line with ISO27001:2005 standard.
b) The Security Officer shall monitor the effectiveness and efficiency of controls in-line with standard requirements.

3.2.6. Assets Management Policy

The objective of asset management is to maintain appropriate protection of assets by assigning assets owner(s) and the acceptable use of assets.

- Inventory of Assets Policy
- Ownership Policy
- Classification policy

3.2.7. Physical Security Policy

The objective of physical security is to provide standards for the protection of personnel, hardware, software, and data from physical circumstances that could cause serious losses or damage to the ICET. This includes protection from fire, and natural disasters.

- Physical Security Policy
- Supporting Utilities and Equipment's Policy
- Cabling Security Policy

3.2.8. Operation Management Policy

The objective of operation management is to introduce procedures to manage the information processing and administer their management.

- Operating Procedures Policy
- Capacity Management Policy
- System Acceptance Policy
- Backup Policy
- Removable Media Policy
- Information Exchange Policy
- Patch Management Policy
- Server Access Management Policy
- Perimeter Security Controls
- Routers & Switches Security Policy
- Desktop Security
- Wireless Network Controls
- E-mail Management Policy

3.2.9. Access Management Policy

The objective of access management is to ensure good management of users' identities, and granting access to these users.

- User Access Management Policy
- Password Policy
- Lockout Policy
- Network Security Policy
- Encryption Policy

3.2.10. Business Continuity Management Policy

The purpose of business continuity management is to create a practiced plan for how the ICET will recover within a specific time period after a disaster or disruption.

a) Business continuity plans must be established.
b) Each business continuity plan must clearly specify the conditions for its activation.
c) Each plan must have a specific owner.
d) Emergency procedures must take place in every plan and must be within the responsibility of the owner of the plan.
e) Business continuity plans may fail upon being tested, usually due to incorrect assumptions or change in equipment's or employees. They must therefore be tested regularly to ensure that they are up-to-date and effective. Such tests must ensure that all members of the recovery team and all ICET staff are aware of the plan.
f) Test schedule must be established, which ensures that the plan(s) will operate in real life.

3.2.11. Acceptable Use Policy

ICET must specify the acceptable use of every information system assets, in which all asset end users must be documented.

4. Conclusions

Organizations and governments spend millions of dollars annually to recover from attacks' negative impact on their information assets. Security breaches have been addressed as a major threat for organizations around the world. Many statistics have stated that most of the security breaches caused by an internal organization problem or can be prevented by eliminating an internal problem. Hence, information security management systems are being adopted by many organizations in order to have appropriate controls to eliminate possible internal organizational problems that may introduce some serious security breach. In this paper, we have taken UMB as a case study (most of Indonesian universities have similar IT setup) and it is concluded that Indonesian universities information systems are facing real possible dangerous security breaches due to the presence of a huge number of different kinds of vulnerabilities in their information systems. The vulnerabilities can be categorized as:

- Inadequate information security awareness for the organization personnel.
- Organizations do not adopt an information security management system to control the security process of the information systems.

We have presented a full package solution for different kinds of vulnerabilities whether technical or organizational by implementing ISO27001 information security management system ISMS, which should eliminate all the vulnerabilities identified during vulnerabilities assessment phase. The main focus was to identify the risks in Indonesian universities' information systems as well as planning for implementing ISO27001 by developing the needed controls. Hence, it enables University of Mercu Buana to start the stages of eliminating the identified risks. With the introduction of these procedures and documents, the University of Mercu Buana will be ready to start the *Do stage***,** which is applying the ISMS on the ICET toward getting an ISO accreditation.

References

[1] Jacobs, S., Security Management of Next Generation Telecommunications Networks and Services, Wiley-IEEE Press, 2014
[2] ISO/IEC, "Information technology-Security techniques-Information security risk management", ISO/IEC 27005:2011, 2011.
[3] Tipton, Harold F. and Micki K., Information Security Management Handbook, 4th Edition. New York: Auerbach Publications, 2000.
[4] Donald Waters. Supply Chain Risk Management: Vulnerability and Resilience in Logistics, 2nd Edition. London, UK, Kogan page, 2011.
[5] G. N. Ericsson, "Cyber security and power system communication—Essential parts of a smart grid infrastructure", *in* IEEE Transaction. Power Del., vol. 25, no. 3, pp.1501 -1507, 2010
[6] Shakeel Ali, Heriyanto Tedi, "Master the art of penetration testing with BackTrack", BackTrack 4: Assuring Security by Penetration Testing, 2011.
[7] British standards (BS) ISO/IEC 27001:2005, British standards (BS)ISO/IEC 27002:2005.
[8] C. Alberts and A. Dorofee, "Managing information security risks: The OCTAVE SM approach". Boston: Addison-Wesley Anderson, 2002.
[9] Moyo, M. ; Abdullah, H. ; Nienaber, R.C., "Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems" *in Proc*. of Information Security for South Africa, pp. 1-6, 2013
[10] *www.telkom.co.id/download/File/UHI/2013/.../Telkom_2012English.pdf*
[11] R. Munir, A. Alhomoud, J. P. Disso, and I. Awan, "On the Performance Evaluation of Intrusion Detection Systems," *in Proc*. of Advances in Security Information Management: Perceptions and Outcomes, pp. 117-138, 2013.
[12] Vogt, M., Hertweck, D. Hales, K. *in Proc*. 44th Hawaii International Strategic ICT Alignment in Uncertain Environments: An Empirical Study in Emergency Management Organizations, conference on System Sciences (HICSS), pp. 1-11, 2011.
[13] H. Kumamoto, and E. J. Henley Probabilistic Risk Assessment and Management for Engineers and Scientists, Wiley-IEEE Press, 2000.