Data and Information Security Audit Using IT Baseline Protection Manual at PT. XYZ

I Made Adi Bhaskara[1], Luh Gede Putri Suardani[2], and Wayan Arta Wijaya[3]
[1][2] Department of Electrical and Computer Engineering, Post Graduate Program, Udayana University.
[3] Department of Electrical Engineering, Udayana University
Email: adibhaskara39@gmail.com

***Abstract*—Development of technology security issues is one important aspect of an information system. Data security and information governance in an enterprise has an important role in maintaining the confidentiality of data in the company and keeping the data intact. Without good data security governance it will arise various problems such as vulnerable to hacker attacks and theft of important corporate data, the identity of employees in the company prone to be stolen by using phishing websites, and loss of data caused by technical things like sudden power outages or lost internet connection . The IT Baseline Protection Manual provides an effective way of understanding needs and priorities in securing data through the process of measuring the level of maturity (Capability Level). Audit of data and information security at PT. XYZ aims to measure the level of data security process capability using domains available in the IT Baseline Protection Manual. The audit stage starts from the case study survey, the selection of the IT Baseline Manual Protection domain and the results of the questionnaire obtained as a representation of the level of maturity with the assessment standard using Maturity Level. Maturity Level value obtained from the results of data security and information security using the domain of IT Baseline Protection Manual that is equal to 2,695 of the maximum score 5. Audit results show that the maturity level of dataI security process at PT. XYZ is at Level 2 (Managed) which still needs to be improved to achieve maximum data security.**

***Index Terms*—Audit, IT Baseline Protection Manual, Maturity Level.**

I. INTRODUCTION

Information technology era, data or information is a very valuable asset and must be protected. This is also followed by advances in computer technology. Advances in computer technology help all aspects of human life. From the simple little thing to the very complicated thing even the computer can do. But with the advances in information technology, communications and computer then new problems arise, namely the security of data and information and in this case will open the opportunity for people who are not responsible for using it as a crime. And certainly will hurt certain parties. Generally servers are always in danger and attackers are generally very difficult to detect. [8]

The above problems also occur in PT. XYZ. At PT. XYZ network security is less good so that if there are hackers who attack the server easily the person can gain access to the network. In addition, employees who are browsing the internet are vulnerable to identity theft cases. This allows hackers to access employee data by pretending to be a website that employees trust. Other problems that a sudden power outage or lost internet connection result in massive data loss. Data and information has become an important asset in the company. To anticipate the things that are not desirable related to the misuse of data and information it is necessary to do an audit. The policy on system security is one of the most important aspects in protecting the assets of data and information.

To overcome these problems required suggestions and solutions. The solution to solve the problem is by implementing an audit about data security and information so that the gap of crime through internet network can be minimized. Security audits are an important solution that allows traceback and analysis of any activity including data access, security breaches, application activity, and so on. [10]

The audit process collects data on system activity and analysis to find security breaches or to diagnose the cause [9]. IT audits are conducted periodically to provide risk assessments and test system control [3]. The audits do not force the system, but detect abuse of control, but detect administrative abuse or criminal acts that occur. [4]

Currently available a variety of tools to audit data security and different assessment methods to measure the security of IT in an organization or company. Various tools to audit data security, one IT Baseline Manual Protection. IT Baseline Protection Manual is the best tool that provides recommended steps to meet the mid-level protection of requirements within an organization. [7].

II. LITERATURE REVIEW

A. Definition Audit System Information

Information systems is a system within an organization that brings daily transaction processing needs, support operations, are managerial and strategic activities of an organization and provide certain outside parties with the required reports. [12]

Audit SI as the process of collecting and evaluating the evidence to determine whether the information system can protect the assets, the technology that has maintained the integrity of the data so that both can be directed towards the

achievement of business goals effectively by using resources efficiently. [11]

B. IT Baseline Protection Manual

Baseline Protection in German IT-Grundschutz) that early emergence from the German Federal Security Information Office (FSI) is a methodology for identifying and implementing computer security measures within an organization. The goal is to achieve an adequate level of security and appropriate for IT systems. To achieve this goal, FSI recommends "well-proven technical, organizational, personnel, and infrastructure protection". Federal organizations and agencies demonstrate their systematic approach to securing their IT systems (eg Information Security Management System) by obtaining ISO / IEC 27001 Certificate under IT-Grundschutz.

Issues to be addressed in security management can be summarized as follows [5]:

- address the complexity of the business support information process and understand the issues of de-pendence and linkage,
- Supporting stakeholders (IT responsibles, IT security officers, management) in their cooperation and task fulfillment,
- Provide relevant security information at the appropriate level of abstraction,
- building ongoing security management.

C. IT Baseline Analysis Structure

IT network covers the entire infrastructure, organizational, personnel, and technical components that serve task fulfillment in the area of information processing applications. The IT network can cover the entire IT character of an institution or personal, partitioned by an organizational structure such as, for example, departmental networks, or shared IT applications, for example, personnel information systems. It is necessary to analyze and document the information technology structure concerned to generate IT security concepts and especially to implement the Basic IT Protection Catalog. Because most networked IT systems today, the network topology plan offers a starting point for analysis. The following aspects should be considered.

- Infrastructure available,
- Organizational and personal framework for IT networks,
- Network and non-network IT systems used in IT networks.
- Communication connection between IT and external systems,
- IT applications run on the IT network.

D. IT Baseline Protection Catalog

IT Baseline Protection Catalog, or IT-Grundschutz-Kataloge, ("IT Baseline Protection Manual" prior to 2005) is a collection of documents from the German Federal Security Information Office (BSI) that provides useful information for detecting flaws and eradication. attack in the environment of information technology (IT). The collection includes over 3000 pages, including introduction and catalog. It serves as the foundation of the basic IT protection certification of a company.[1]

E. IT Baseline Protection Catalog Components

Catalog component is the main element, and contains the following five layers: overall aspects, infrastructure, IT systems, network and IT applications.

Partition into the layer clearly isolates the personal group affected by the particular layer of the layer on which it is located. The first layer is addressed to management, including personnel and outsourcing. The second is addressed to in-house technicians, regarding the structural aspects of the infrastructure layer. System administrators include the third layer, looking at the characteristics of the IT system, including clients, servers and private bidding or fax machines. The fourth layer is included in the task area of the network administrator. The fifth is from application administrators and IT users, regarding software such as database management systems, e-mail and web servers.

Based on these five layers, the Components of the IT Baseline Catalog are as follows:

- IT Security Management
- Organization
- Personal
- Backup Plan Concept
- Data Backup Policy
- Privacy Data Protection
- Computer Virus Protection Concepts
- Crypto concept
- Handling of Security Incidents

F. Domain IT Baseline Protection

There are 2 domains contained in IT Baseline Protection as follows:[2]

a) Threats Catalog

Threat Catalog consists of 5 categories:

1. T 1 Threats Catalog - Force Majeure
2. T2 Threats Catalog Organizational Shortcomings
3. T 3 Threats Catalog Human Failure
4. T 4 Threats Catalog Technical Failure
5. T 5 Threats Catalogue Deliberate Acts

b) Safeguard Catalog

Threat Catalog consists of 5 categories:

1. Majeure S 1 Safeguard Catalog Infrastructure
2. S 2 Safeguard Catalog - Organizations
3. S 3 Safeguard Catalog - Personnel

4. S 4 Safeguard Catalog - Hardware & Software
5. S 5 Safeguard Catalog - Communications
6. S 6 Safeguard Catalog: Contingency Planning

Based on the domain catalog above 2 domains there are many sub domains. Sub domain in accordance with the realm that is taken as follows:

G. Maturity Level

Maturity Level describes how a core process in the organization runs. This description is needed to know which processes are already running in accordance with expectations and which processes are still lacking, so it can be given special attention and improvement. It also provides performance or performance measurement of processes in the area of governance and management. But the security of audit efficiency is low because security officers in the data management process are very large from the audit track record data, so literally it is not possible. [6]

There are six levels of process capability that can be achieved, from Incomplete Process (level 0) to Optimizing (level 5). Explanation of the level on Capability Level is more details as follows (ISACA, 2013).

1. Level 0: Incomplete Process

Organizations at this stage do not implement IT processes that should or have not achieved the objectives of the IT process.

2. Level 1: Performed Process

Organization at this stage has successfully carried out IT processes and IT process objectives have been achieved.

3. Level 2: Managed Process

Organizations at this stage in carrying out the IT process and achieving its objectives are implemented in a well managed manner. So there is more assessment because the implementation and achievement is done with good management. Management here means its implementation through planning, evaluation and adjustment processes for the better.

4. Level 3: Established Process

Organization at this stage has a standardized IT process within the overall organization. This means that there are standard IT processes that are applicable throughout the organization.

5. Level 4: Predictable Process

Organization at this stage has run the IT process within definite limits, eg time constraints. These limits result from measurements that have been made during the implementation of the IT process before.

6. Level 5: Optimizing Process

In this stage the organization has made innovations and made continuous improvements to improve its capabilities.

Incomplete	Performed	Managed	Established	Predictable	Optimised
0	1	2	3	4	5

Figure 1. Maturity Level Index

III. Research Methods

The information security management framework is process stages of preparing phases, asset identification, information security management policies and documents, IT operations, communications networks, information security. This research uses descriptive qualitative research type. The nature of this study is descriptive, descriptive method can be interpreted as a problem-solving procedure investigated by describing or describing the state of the subject or object of research at the present moment based on facts that appear.

Descriptive research is intended to:

1. Gathering information in an actual and detailed manner
2. Identify the problem.
3. Make a comparison or evaluation.
4. Determine what others are doing in the face of the same problem and learn from their experience to decide future plans and decisions.

This research to obtain data and information, then the method used in the process of data collection is a questionnaire. The questionnaire provided contains several questions based on the IT Baseline Manual Protection framework to audit data and information security at PT. XYZ.

Subjects in this study is the level of network security at PT.XYZ. While the object of research is the existing employees in PT.XYZ. Maturity level measured from the questionnaire distributed to 35 people in PT.XYZ. 31 people (85.6%) filled the questionnaire completely, while 4 people (11.4%) did not fill out the questionnaire. Questions from the questionnaire are based on points relevant to the network security and user use of the computer based on the IT Baseline Protection Manual domains.

T 5.2	Checking of software used to prevent counterfeit software that can retrieve employee information	2.911
T.5.23	Security by performing routine scans to optimize computer performance that can be interrupted by computer virus	2.914
T 5.3	Security uses authentication on the computer to avoid theft of valuable files	2.911
T 5.4	Security uses anti malware applications to avoid data theft from malware attacks	2.756
T 5.76	Avoids unlocking unknown email links to avoid email bombs	3.600

T 5.78	Enable firewalls and set filters on the computer to avoid DNS spoofing	2.511
T.5.9	Protection by installing anti virus on computer to avoid attacks of vandalism such as virus	2.914
Maturity level of data security level		**(2.911 + 2.914 + 2.756 + 2.911 + 2.914 + 3.600 + 2.511) /7 = 2.931**

Table 1. Questionnaire Results

IV. *RESULT AND DISCUSSION ANALYSIS*

Based on the results obtained questionnaire generated graphs as follows:

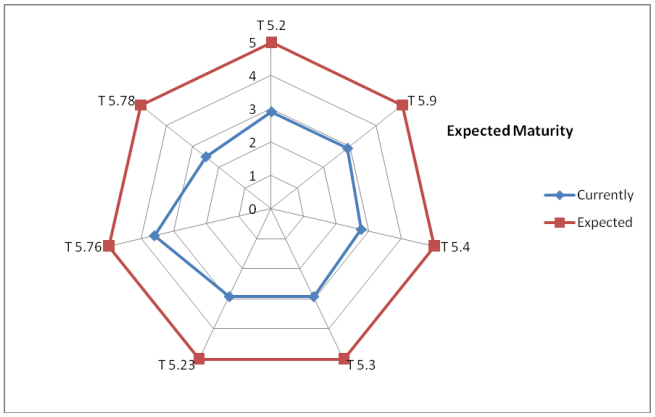

Figure 2. Expected Maturity Graph

Graph in Figure 2 shows the results of the questionnaire obtained by averaging the total score of 7 questions in the IT Baseline Manual Protection in accordance with the realm of the taken. Here is the stages of the analysis of the results of questionnaires conducted at PT. XYZ.

T 5.2 Security from manipulation of data or software
Located at level 3-Established

Checking is quite often against software used to avoid fake software that can retrieve employee information

T 5.23 Security from Computer Viruses
Located at level 3-Established

Security with routine scan is done every time on all computers by setting auto scan every week to optimize computer performance that can be disrupted by computer virus

T 5.3 Security from unauthorised entry into a building
Located at level 3-Established

Security using authentication on the computer to avoid theft of valuable files on average done almost every computer

T 5.4 Security from theft
Located at level 2-Managed

Security using anti-malware applications to avoid data theft from malware attacks just a few computer

T 5.76 Security from Mail Bombs
Located at level 3- Established

Avoiding unlocking unknown email links to avoid email bombs is done by assigning to all employees to browse the work-related stuff on the office computer

T 5.78 Security from DNS Spoofing
Located at level 3- Established

Enabling firewalls and setting up filters is done on multiple office computers to avoid DNS spoofing

T 5.9 Security from unauthorised use of IT System
Located at level 3- Established

Protection by installing anti virus on the computer to avoid attacks that are vandalism like virus is done on almost every computer

V. CONCLUSION

Based on the result of security rating of PT.XYZ, the following conclusions are obtained:

1. The results of the assessment using the Maturity Level approach by using IT Baseline Protection Manual shows that the level of security has a Maturity Level score on Level 2 obtained from the questionnaire filled by user employees.
2. Score Maturity Level 2.931 obtained shows the level of network security still needs to be upgraded to comply with the procedures or risk management standards at PT. XYZ, either from the application side (SOP in Information Security must be the same as SOP in the company), from the human resources side (user must follow the proper usage of the Information Security according to SOP rules in the field), as well as the parties who support for data security and well maintained information and can handle and handle risks well.

ACKNOWLEDGMENT

Thank you to Lecturer and to all parties who have helped and supported the author, as well as the support of fellow writers in the environment until the research is completed.

REFERENCES

[1] IT-Grundschutz-Catalogues 13th Version 2013.

[2] IT Baseline Protection Manual Standard Security Measure Version: October 2000

[3] R. Teeter and R. Brennan, "Aiding the Audit : Using the IT Audit as a Springboard for Continuous Control Monitoring", Collected Paper of the Seventeenth Annual Research Workshop on: Artificial Intelligence and Emerging Technologies in Accounting, Auditing, and Tax Anaheim, CA USA, August 2008, p. 129-136.

[4] C. Clifton and D. Marks, "Security and Privacy Implications of Data Mining", Proceedings of the 1996 ACM SIGMOD Workshop on Data Mining and Knowledge Discovery, 1996,

[5] F. Innerhofer-Oberperfler and R. Breu, "Using An Enterprise Architecture for IT Risk Management", unpublished

[6] L. Me, "Information Gassata, a Genetic Algorithm as an Alternative Tool for Security Audit Trails Analysis", unpublished.

[7] E. Von Solms and J.H.P Eloff, "Information Security Development Trends", unpublished.

[8] J. E. Holt, "Logcrypt : Forward Security and Public Verification for Secure Audit Logs", unpublished

[9] R. Sandhu, "Authentication, Access Control, and Audit", ACM Computing Surveys Vol. 28 No. 1, CRC Press, March 1996, p. 241-243.

[10] Y. Zhu, H. Wang, Z. Hu, G. Ahn, H. Hu, S. S.Yau "Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds", ACM 978-1-4503-0113-6/11/03, USA, 2011, p. 1550-1557.

[11] S. Gondodiyoto and H. Hendarti, "Audit Sistem Informasi", Jakarta: Erlangga, 2006.

[12] Indrajit and Richardus Eko, "Sistem Informasi dan Teknologi Informasi", Jakarta: Gramedia, 2001.