Information Technology Application Audit for Employees Using IT Baseline Protection

Muhammad Ridwan Satrio[1*], I Made Bagus Wiradivka Laksa Wibawa[2], Komang Oka Saputra[3]

[1,2]Department of Electrical and Computer Engineering, Post Graduate Program,
[3]Department of Electrical Engineering, Udayana University
*Email: mridwansatrio@gmail.com

Abstract In the current era of information technology, data or information is a very valuable asset and must be protected. The IT Baseline Protection Manual provides an effective way of analyzing threats and ways to secure data through a Maturity Level measurement process. This method is applied by the German government to regulate information technology audit standards. In this method there is an audit module in the employee area to analyze how well the application of information technology by employees in an agency. An information technology audit at the Badung Regency Communication and Information Department aims to measure the maturity level of employees in applying information technology using the domains available in the IT Baseline Protection Manual. The audit phase starts from the case study survey, the IT Baseline Manual Protection domain selection and gets the results of the questionnaire which is a measure of maturity level by evaluating using Maturity Level. The Maturity Level figures obtained from the audit of the application of information technology to employees using the IT Baseline Protection Manual domain which is equal to 3.43. The results show that the maturity level of the process of applying information technology to employees at the Communication and Information Department of Badung Regency is at Level 3 (Defined), namely there are already good IT process standards in the entire scope of the organization but could be increased to the maximum.

Index Terms— Information Technology Audit, IT Baseline Protection, Maturity Level.

I. Introduction

Developments in the era of globalization and information technology now make data and information security a very important thing. This is to show the professionalism of organizations, especially agencies that serve the community at large. The success in securing public information is not separated from the way work and routine employees in the agency environment. Routines in terms of processing data and channeling these data are carried out by employees with the application of information technology. Then there are security issues of data and information from data processing routines by employees who have not met the standards.

This can open opportunities for people who are not responsible for using it as a crime. And of course it will harm certain parties. These problems may occur in the Badung regency communication and information department. As a public agency, the communication and information department of Badung Regency has the responsibility to manage public information and deliver it to the public, especially the people of Badung Regency. Information that will be conveyed to the public and various relevant agencies must of course be maintained so that no changes can cause misinformation.

To overcome this problem, an information technology (IT) audit is needed. To ensure that the audit process is carried out correctly or in accordance with the procedure, it is necessary to analyze the activities in it, so that it can be seen whether what has been done has achieved the objectives to be achieved by an organization or can be further improved by adding evaluation elements that will improve quality part of the organization that was assessed [3]. Information technology audit is essentially one of the forms of operational audits, but now information technology audits are known as a separate type of audit unit whose main purpose is more to improve IT governance [4]. By doing the audit, it can be known the level of asset security, maintenance of data integrity, can encourage the achievement of organizational goals effectively and use resources efficiently [5]. In order for IT to be utilized as optimally as possible for the benefit of business strategies, IT governance must be considered carefully [6]. IT governance is a part that is integrated with corporate governance and contains leadership and organizational structures and processes that guarantee that IT organizations contain and support business strategies and objectives [7].

Currently there are various tools for auditing data security and different valuation methods for measuring security in the IT field in an organization or company, one of which is IT Baseline Manual Protection [8]. Information technology audit methods called IT Baseline Protection were created by the German government under the Federal Agency for Security in Information Technology which provides a collection of security protections and appropriate methodologies for selecting and adapting safeguards that are suitable for handling information that is safe for application in diverse environments [1]. In this study the audit method will be applied to conduct an audit of the application of information technology to employees working in the Communication and Information Department of Badung Regency.

II. Literature Review

A. IT Baseline Protection

IT Baseline Protection is a method created by BSI (Bundesamt für Sicherheit in der Informationstechnik) or the Federal Agency for Security in Information Technology in Germany. BSI offers a simple method to protect all organizational information appropriately. With a combination of the IT-Grundschutz approach in the BSI 100-2 standard and IT-Grundschutz Catalogs, BSI provides both a collection of security protections and an appropriate methodology for selecting and adapting safeguards that are suitable for handling information that is safe for application in diverse environments. [1]

B. IT Baseline Protection Layer

In order to map a generally complex information system to the modules in the IT-Grundschutz Catalogues, it makes sense to consider the security aspects grouped according to certain topics: [1]

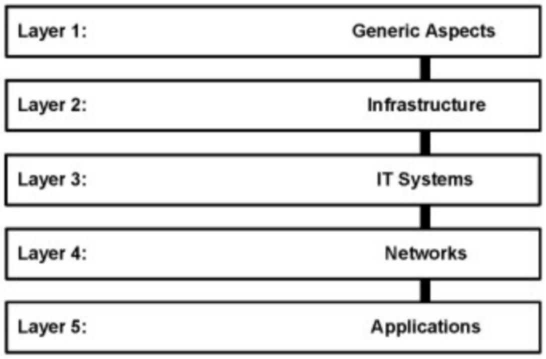

Figure 1. The Layers of the IT baseline protection model

The security aspect of an information system is assigned to each layer as follows: [1]

- Layer 1 covers the same comprehensive security aspects that apply to all or most information systems. This is especially true for comprehensive concepts and regulations originating from such. Typical layer 1 modules include security, organization, data backup policy, and protection against malware, among other things.
- Layer 2 covers physical and technical conditions. At this level, various aspects of infrastructure security are combined. For example, this refers to the Building module, Server Room, Computer Center, and Workplace Home.
- Layer 3 discusses individual IT systems from an information system that might have been divided into several groups. This layer discusses security aspects for clients, servers and stand-alone systems. This layer includes the Telecommunications, Laptop, and Client system modules under Windows Vista, for example.
- Layer 4 examines aspects of the network that are not directly related to a particular IT system, but to network and communication connections. These include modules for network management, WLAN, VoIP, and VPN, for example.
- Layer 5 finally discusses applications that are actually used in information systems. Among other things, the Groupware module, Web server, Fax server, and database can be used for modeling in this layer.

C. IT Baseline Protection Domain

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

a. Threats Catalog

Threat Catalog consists of 5 categories:

1. T 1 Threats Catalogue - Force Majeure
2. T 2 Threats Catalogue Organisational Shortcoming
3. T 3 Threats Catalogue Human Failure
4. T 4 Threats Catalogue Technical Failure
5. T 5 Threats Catalogue Deliberate Acts

b. Safeguard Catalog

Safeguard Catalog consists of 5 categories:

1. S 1 Safeguard Catalogue Infrastructure
2. S 2 Safeguard Catalogue - Organisation
3. S 3 Safeguard Catalogue - Personnel
4. S 4 Safeguard Catalogue - Hardware & Software
5. S 5 Safeguard Catalogue - Communications
6. S 6 Safeguard Catalogue: Contingency Planning

D. IT Baseline Protection Personnel Module

The Personnel module or employee module in the IT Baseline method is part of the common aspect layer. This module describes the generic IT-Grundschutz security that must be implemented as a standard in the field of personnel. A number of safeguards are needed starting from the time employees are hired and continue until they leave the organization. Adequate security must also be carried out to deal with external personnel such as visitors or maintenance technicians. [2]

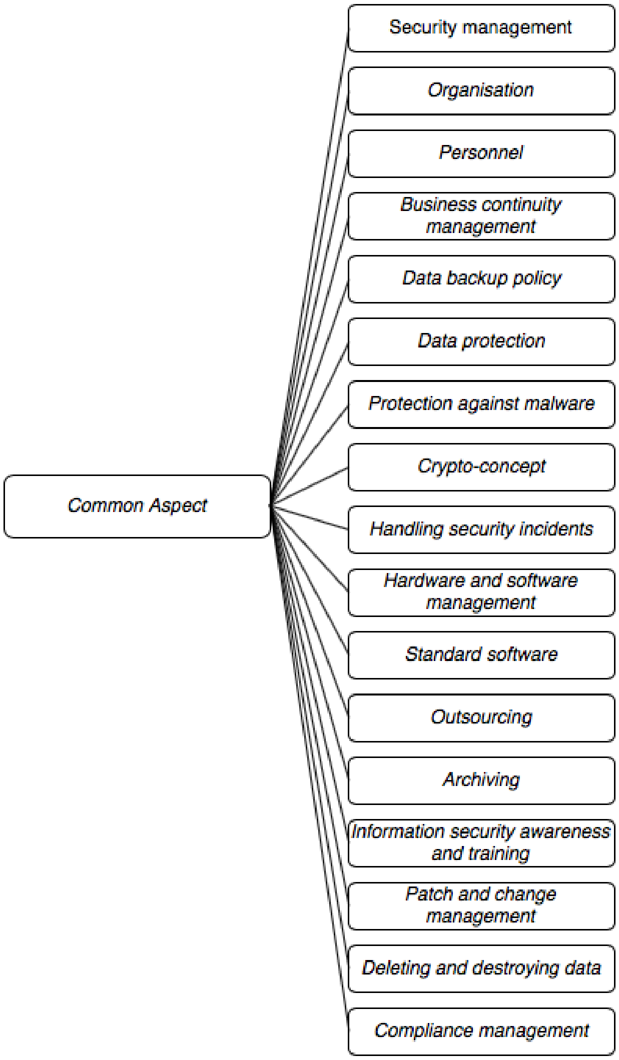
Common Aspect
Security management
Organisation
Personnel
Business continuity management
Data backup policy
Data protection
Protection against malware
Crypto-concept
Handling security incidents
Hardware and software management
Standard software
Outsourcing
Archiving
Information security awareness and training
Patch and change management
Deleting and destroying data
Compliance management

Figure 2. Modules in common aspect layer

Following are the domains for IT baseline protection that are examined in this module: [2]

Force Mejure

T 1.1 Loss of personnel

T 1.2 Failure of the IT system

Organisational Shortcomings

T 2.2 Insufficient knowledge of rules and procedures

T 2.7 Unauthorised use of rights

Human Error

T 3.1 Loss of data confidentiality or integrity as a result of user error

T 3.2 Negligent destruction of equipment or data

T 3.3 Non-compliance with IT security measures

T 3.37 Unproductive search

T 3.44 Carelessness in handling information

Deliberate Acts

T 5.2 Manipulation of information or software

T 5.20 Misuse of administrator rights

T 5.23 Malicious software

E. Maturity Model

Maturity model is a maturity model to control Information Technology processes by using scoring methods [9]. There are six levels of process capability that can be achieved, ranging from Non-existent (level 0) to Optimized (level 5). A description of the Maturity Model at each level as follows: [10]

1. Level 0 : Non-Existent
   There is no understanding of risks, vulnerabilities, and threats for IT operations or the impact of losing IT services for businesses. Continuity of service is not considered as requiring management attention.
2. Level 1 : Initial
   Responsibility for sustainable services is informal, with limited authority. Management begins to be aware of the risks associated with and the need for sustainable services.
3. Level 2 : Repeatable
   There is an emerging understanding that IT risk is important and needs to be considered. Several approaches to risk assessment exist, but the process is still immature and developing.
4. Level 3 : Defined
   Security awareness exists and is promoted by management. Security awareness notices have been standardized and formalized. IT security procedures are defined and entered into the structure for security policies and procedures. Responsibility for IT security is assigned, but is not consistently enforced. An IT security plan exists, encouraging risk analysis and security solutions.
5. Level 4 : Managed and Measurable
   The responsibility for IT security is clearly defined, managed and enforced. IT security risks and impact analysis are consistently carried out. Security policies and practices are equipped with certain security baselines. Security awareness briefing has become mandatory. Standardized identification, authentication, and user authorization, staff security certifications set.
6. Level 5 : Optimized
   IT security is a shared responsibility of business and IT management and is integrated with the objectives of the company's security business. IT security requirements are clearly defined, optimized and included in a verified security plan. Security functions are integrated with applications at the design stage and end users are increasingly responsible for managing security. IT security reports provide early warning of changes and risks that arise, using an automatic active monitoring approach for critical systems. The incident is immediately handled by a formal incident response procedure that is supported by automatic tools. Security assessments regularly evaluate the effectiveness of implementing security plans. Information about threats and new vulnerabilities is systematically collected and analyzed, and adequate mitigation controls are immediately communicated and implemented. Intrusion

testing, root cause analysis of security incidents and identification of proactive risks are the basis for continuous improvement. Security and technology processes are integrated throughout the organization.

III. Research Methods

The subject of this study was an audit analysis of the application of information technology to employees in the communication and computer department of Badung regency. Maturity levels are measured from the results of a questionnaire distributed to 12 employees at Badung communication and computer department with a minimum of bachelor degree education. Questions from questionnaires are based on points relevant to the application of information technology to employees based on the IT Baseline Protection Manual domains.

Observation Details	0	1	2	3	4	5	Total	Capability Level
T.1 Force Maejure								
Handling work if one or more of your coworkers is unable to handle the work			2	5	5		39	3,25
Handling if one of the supporting components of the work (such as: electricity, internet) is not available for some of time			3	8	1		34	2,83
Average value								3,04
T.2 Organitational Shortcomings								
The application of work rules within the employee's workplace			1	5	6		41	3,42
Data security of each field whether data can be accessed by employees from other fields			2	4	6		40	3,33
Average value								3,37
T.3 Human Error								
Data security on the agency computer used by employees is protected by keywords or other security measures				1	6	5	52	4,33
Computer security is protected from water spills or food that can damage the computer and eliminate data in it					3	9	57	4,75
Prevention of loss of data on the computer by making backups for certain periods			2	5	5		39	3,25
Prevention of employees discussing important matters in work in public places				1	7	4	51	4,25
Average value								4,145
T.4 Deliberate Acts								
Checking the software used to avoid fake software that can retrieve information			2	4	6		40	3,33
Security uses authentication on a computer to avoid theft of valuable files			1	5	6		41	3,42
Security by doing a routine scan to optimize computer performance that can be disrupted by computer viruses			2	7	2		33	2,75
Average value								3,167
The average maturity level of application of information technology by employees	(3,04 + 3,37 + 4,145 + 3,167) / 4							3,43

Table 1. Questionnaire Results

IV. Analysis Of Results And Discussion

The results of the questionnaire can be seen in table 1. For the results of the questionnaire obtained from the average total score of all questionnaire questions that exist in the IT Baseline Manual Protection in accordance with the topics analyzed. The results of the 3.43 maturity score state that the application of information technology by employees at the communication and information services department has been good enough but can still be improved to achieve optimal standards. The following is an analysis of the maturity level of each domain.

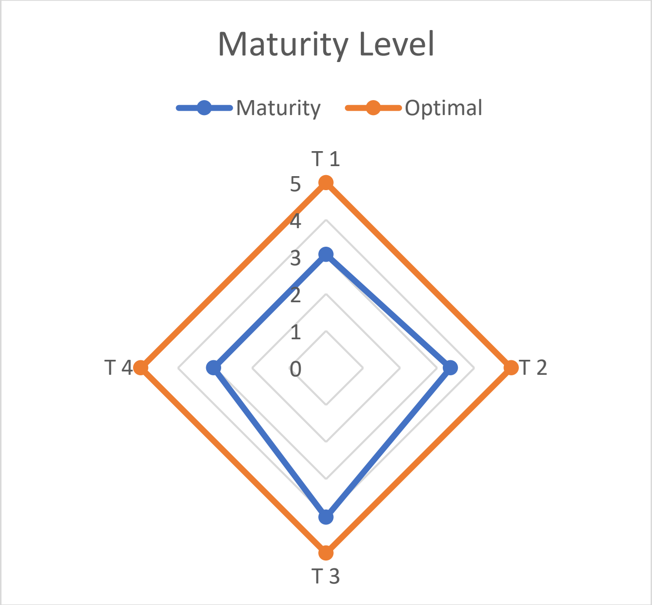

Figure 3. Maturity Level Chart

V. Conclusion

Based on the results of the audit analysis in the application of information technology to employees of communication and information department of Badung. Then the conclusions are as follows:

1. The results obtained using the Maturity Level assessment with the IT Baseline protection Manual method show that the maturity level of the application of information technology by employees produces a Maturity Level score at Level 3 obtained from the results of the questionnaire.
2. The average level of Maturity Level 3.43 obtained shows the level of application of information technology by employees at the communication and information service has been running well in accordance with the standards but can still be

improved in order to obtain optimal performance results.

REFERENCES

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

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

[3] Amnah -, “Analisa Proses Audit Sistem Informasi Biro Manajemen Asset Dan Logistik Menggunakan Framework Cobit 4.1. Pada Institut Informatika Dan Bisnis Darmajaya Bandar Lampung,” J. Inform., vol. 14, no. 1, pp. 72–83, Dec. 2015.

[4] J. F. Andry, “Audit Tata Kelola Ti Menggunakan Kerangka Kerja Cobit Pada Domain Ds Dan Me Di Perusahaan Kreavi Informatika Solusindo,” p. 8, 2016.

[5] R. K. Candra, I. Atastina, and Y. Firdaus, “Audit Teknologi Informasi menggunakan Framework COBIT 5 Pada Domain DSS (Delivery, Service, and Support) (Studi Kasus : iGracias Telkom University),” p. 16.

[6] Surendro, Kridanto. Implementasi Tata Kelola Teknologi Informasi. Bandung: Informatika, 2009.

[7] C. W. Iswara And I. Asror, “Audit Penerapan Teknologi Informasi Berbasis Risiko Dengan Framework Cobit Versi 4.1 Di Perguruan Tinggi Xyz,” Vol. 1, P. 8, 2014.

[8] Bhaskara, I Made Adi; Putri Suardani, Luh Gede; Wijaya, Wayan Artha. Data And Information Security Audit Using It Baseline Protection Manual At Pt. Xyz. International Journal Of Engineering And Emerging Technology, [S.L.], V. 2, N. 2, P. 78-82, Mar. 2018. Issn 2579-597x.

[9] S. Wardani and M. Puspitasari, “Audit Tata Kelola Teknologi Informasi Mengunakan Framework Cobit Dengan Model Maturity Level (Studi Kasus Fakultas Abc),” J. Teknol., vol. 7, p. 9, 2014.

[10] Information security governance: guidance for boards of directors and executive management. Illinois: IT Governance Institute, 2001.