User Care Level Audit of Information Data Security at PT XYZ Using Guttman Scale

S Alviana
Departemen Teknik Informatika, Universitas Komputer Indonesia, Indonesia

Email: sopian.alviana@email.unikom.ac.id

Abstract. The purpose of this research is to know the level of care of information technology users on information data security. The utilization of information technology in supporting corporate objectives must be balanced with the level of infrastructure support and user care for data security. The company, more likely to build and develop infrastructure that can support every business process of the company, regardless of the level of care and knowledge of its users. Users play an important role in supporting the security of information data either personally or in the company's information data. So, to be able to assess and improve data security in the company is required not only the increased infrastructure, but the care and knowledge of users in supporting each company's business processes supported by the use of technology Information. The method used was evaluating the user by auditing the user's level of knowledge and concern for the security of information data, so that the level of user care is available. Information security in support of each company's business processes. The results obtained in this study are the overall level of user care is at a level with an average percentage of 75.64% of users concerned about data security. In detail, the company's support level to data security is high enough with 98% of users should follow the procedures set by the company in using information technology. Inversely proportional to the low level of user care, 42% of company users ignore concern about data security demonstrated by behavior not using log in facility. With these results, the company needs to increase the user's level of concern for data security by providing regulations related to the use of information technology, as well as support for increasing user knowledge in order to secure data personal and corporate can be maintained properly.

1. Introduction

Technological developments have made the management of the company always demand solutions from the use of information technology. Information technology is used to encourage and provide business value and increase utilization to increase productivity [1]. In its implementation, information technology has become a necessity for a company. Companies invest heavily in the development of information technology, in order to support every business process of the company. The company’s success, now measured on how far the company manages information technology [2]. The company’s focus on improving performance based on information technology is not balanced with the data security due to both personal data and company data. Companies tend to further improve technology infrastructure with large investment allocation compared to security concerns [3].

In fact, the security of information technology is very important, because security problems can trigger a mechanism to control access to various devices [4]. To improve the efficiency and effectiveness of the use of secure information technology in the company, it is required a mechanism to evaluate each use of information technology, especially related to data security. Quality control of information...
technology can be evaluated using three instruments of application map and infrastructure, risk assessment, and separation of tasks [5]. Risk assessment is one way that can be taken to evaluate the use of information technology, especially in terms of data security through audit mechanisms.

The information technology audits used are typically focused on auditing, indicators, process, and focus on management levels [6]. The results showed that the most common evaluation by auditors was control of application processing, data integrity, privacy, and security control [7]. Any audit or evaluation process of the use of information technology aims to ensure that each system or process fulfils its objectives [8]. The auditing process used during this time focuses on the security of the data from the computer network alone regardless of the user aspect and the level of care. So, for data security is considered both in terms of infrastructure and users, the research aims to determine the level of user care for the security of information data on technology that the company uses.

2. Methods

In this research, there are several phases of audit process including pre-audit, on site audit, and post audit. Pre-audit of the preliminary stages includes the preparation of the initial audit on the scope and preparation of the questionnaire. The phases on site audit are the audit process, including the direct survey process, data collection, and the recording of findings and the questionnaire. The final stage is the post audit study findings and analysis of user survey results. The system user auditing process is shown in Figure 1.

Figure 1 shows each stage and step of the information technology security auditing process consisting of three steps, namely Pre audit, On site audit, and Post audit. Each step has its own stages, including:

2.1. Pre-Audit

Pre-audit phase is an early stage in the data security auditing process which is the information on the determination of audit scope and audit target. In this case the scope of audit related data security information at XYZ company. The audit objective in this case is the user of the information system in the company that amounted to 52 users divided into several parts of the company. The audit process begins with the auditor conducting information collection related to security audits through interviews and document review [9].

2.2. On Site Audit

The process on site audit is a phase of security auditing of information technology by arranging questions and conducting surveys directly to users in using information technology. In this case, the user who is targeted to do surveys is totalled 52 people and covers all the parts that use the information technology in the company XYZ. Here, the number and item of questions provided to the user at table 1:

Table 1. Number and Item questions for the audit process

| No. | Item Questions                                                                 |
|-----|-------------------------------------------------------------------------------|
| 1.  | Does every user login when using a computer?                                  |
| 2.  | Does a user use one computer?                                                  |
| 3.  | Are all employees reminded about the importance of computer security?          |
| 4.  | Are access rights to share data regulated according to employee functions?     |
| 5.  | Does the operating system on the computer being used, often do the latest patch updates? |
| 6.  | Is the computer used antivirus installed and always updated regularly?         |
No. | Item Questions                                                                                                                                 |
---|---------------------------------------------------------------------------------------------------------------------------------------------|
7.  | Does the company use its application?                                                                                                        |
8.  | Are there procedures for employees operating computers following their functions and access rights?                                          |
9.  | Are there procedures for backing up data and applications that are well documented?                                                          |
10. | Does every employee who uses a computer follow the procedures set by the company?                                                             |
11. | Are there standards for prevention, detection of virus disorders?                                                                           |
12. | Are there standard procedures to limit the use of external storage (such as flash drives) in an office computer system?                       |
13. | Is there regular information technology training for employees?                                                                               |
14. | Are there any reporting procedures related to damage or loss of data on either the system or computer equipment?                             |
15. | Are there standard procedures for using computer ethics and access rights for employees or users?                                             |

2.3. Post Audit
The last process in the security auditing phase of information technology is the post audit process which includes the results of analysis and findings. Results of analysis are the end result of the analysis of user data on the security of information data, as well as viewing user behaviour towards maintaining data security.

3. Results and Discussion
This section shows the findings in the information technology security auditing process. Table 2 shows about result of questionnaire responses.

Table 2. Number of user questionnaire responses

| No. | Item Questions                                                                 | Yes | No  |
|-----|-------------------------------------------------------------------------------|-----|-----|
| 1.  | Does every user login when using a computer?                                  | 22  | 30  |
| 2.  | Does a user use one computer?                                                 | 50  | 2   |
| 3.  | Are all employees reminded about the importance of computer security?         | 50  | 2   |
| 4.  | Are access rights to share data regulated according to employee functions?    | 51  | 1   |
| 5.  | Does the operating system on the computer being used, often do the latest patch updates? | 52  | 0   |
| 6.  | Is the computer used antivirus installed and always updated regularly?        | 52  | 0   |
| 7.  | Does the company use its application?                                         | 52  | 0   |
| 8.  | Are there procedures for employees operating computers following their functions and access rights? | 48  | 4   |
| 9.  | Are there procedures for backing up data and applications that are well documented? | 52  | 0   |
| No. | Item Questions                                                                 | Yes | No  |
|-----|-------------------------------------------------------------------------------|-----|-----|
| 10. | Does every employee who uses a computer follow the procedures set by the company? | 51  | 1   |
| 11. | Are there standards for prevention, detection of virus disorders?              | 52  | 0   |
| 12. | Are there standard procedures to limit the use of external storage (such as flash drives) in an office computer system? | 3   | 49  |
| 13. | Is there regular information technology training for employees?                | 4   | 48  |
| 14. | Are there any reporting procedures related to damage or loss of data on either the system or computer equipment? | 50  | 2   |
| 15. | Are there standard procedures for using computer ethics and access rights for employees or users? | 1   | 51  |

Table 2 shows the results of the user’s answer to the given question. These results vary with each question by number of answers yes and the answers are not given by each user to the questions given. Question no 1 relates to a user’s habit of logging in when using the computer. 30 respondents gave a statement that they never did the login facility when using the computer. Question no 2 and 3 have the same number of respondents, with regard to the use of computers by one person and all employees are warned about computer security. In addition, question no 4 has respondents 51 people that each employee uses a computer according to their function. Users are then given questions about the use of device updates, antivirus, and applications. All respondents answered yes that all devices, antivirus, and applications were periodically updated. Question no 8 regarding the user to follow the rules and access rights, 48 respondents answered yes and the rest replied no. Inquiries no 9 through no 11 related data backup procedures, data prevention and data security. More than 50 respondents stated that the procedure has been implemented properly.

The next question regarding the use of external storage media, the training for users states that 48 and 49 people state that there are no restrictions on access to the use of external storage media and training for security to users. From the result of the respondent in Table 1, it was used to calculate the result of the value, percentage, and category of the question to the number of respondents. To calculate the values, percentages, and categories used Guttman scale. Calculations using Guttman scale were used because it provides a non-parametric method that is useful for evaluating quality rating to suit a variety of situations [10]. Here are the calculations for the values, percentages, and categories used. Value is the number of respondents with the answer yes.

\[
\text{Percentage} = \left( \frac{\text{Score}}{\text{Total of Respondent}} \right) \times 100\%
\]

As for the category, the Guttman Scale provides two categories with the following value ranges Table 3:

| Value Range (%) | Category |
|-----------------|----------|
| 0 – 50%         | Low      |
| 50 – 100%       | Middle   |

Table 3. Category Range Questions
Here are the result calculation values, percentages, and question categories (Table 4).

**Table 4.** Calculation of values, percentages, and question categories

| No. | Item Questions                                                                 | Score | Percentage | Category |
|-----|--------------------------------------------------------------------------------|-------|------------|----------|
| 1.  | Does every user login when using a computer?                                  | 22    | 42,31      | Low      |
| 2.  | Does a user use one computer?                                                  | 50    | 96,15      | Middle   |
| 3.  | Are all employees reminded about the importance of computer security?         | 50    | 96,15      | Middle   |
| 4.  | Are access rights to share data regulated according to employee functions?    | 51    | 98,08      | Middle   |
| 5.  | Does the operating system on the computer being used, often do the latest patch updates? | 52    | 100        | Middle   |
| 6.  | Is the computer used antivirus installed and always updated regularly?        | 52    | 100        | Middle   |
| 7.  | Does the company use its application?                                          | 52    | 100        | Middle   |
| 8.  | Are there procedures for employees operating computers following their functions and access rights? | 48    | 92,31      | Middle   |
| 9.  | Are there procedures for backing up data and applications that are well documented? | 52    | 100        | Middle   |
| 10. | Does every employee who uses a computer follow the procedures set by the company? | 51    | 98,08      | Middle   |
| 11. | Are there standards for prevention, detection of virus disorders?             | 52    | 100        | Middle   |
| 12. | Are there standard procedures to limit the use of external storage (such as flash drives) in an office computer system? | 3     | 5,77       | Low      |
| 13. | Is there regular information technology training for employees?               | 4     | 7,69       | Low      |
| 14. | Are there any reporting procedures related to damage or loss of data on either the system or computer equipment? | 50    | 96,15      | Middle   |
| 15. | Are there standard procedures for using computer ethics and access rights for employees or users? | 1     | 1,92       | Low      |

**Count**  590  1134,61  
**Average**  39,34  75,64  Middle
In Table 4 shows the calculation of value, percentage, and question categories. Of the 25 questions given to respondents, the results showed that 21 questions had enough categories, and 4 questions had a low category. 21 categorized questions that are related to computer use, data security warnings, access rights, app updates, antivirus, and data backup procedures have been done entirely by the company and the information technology team. Out of the 4 low-category questions, the questions regarding user habits include the use of login facilities, use of additional storage media, data security-related training activities for users, and computer-use procedures and permissions for the user. With these four low-category questions, it shows that the user's level of concern for data security in the company is low. It is because users do not use the login facility for data security. In addition, users are not provided with data security training by the company. It shows that the level of user care for data security is very low.

4. Conclusion
The results gained in this study are the overall level of user care to be at a level with an average percentage of 75.64% of users concerned with data security. In detail, the company's support level to data security is high enough with 98% of users should follow the procedures set by the company in using information technology. Inversely proportional to the low level of user care, 42% of company users ignore concern about data security demonstrated by behaviour not using log in facility. With these results, the company needs to increase the user's level of concern for data security by providing regulations related to the use of information technology, as well as support for increasing user knowledge in order to secure personal data and corporate can be maintained properly.

Acknowledgment
We acknowledged Department of Informatic Engineering and Directorate AP2SC UNIKOM for research and data as needed.

References
[1] Aprilinda, Y., Puspa, A. K., & Affandy, F. N. 2019. The Use of ISO and COBIT for IT Governance Audit. In Journal of Physics: Conference Series 1381(1) p. 012028. IOP Publishing.
[2] Hendry, P., & Fernandes, A. J. 2019. It Governance at financial Technology company using cobit 4. 1 Framework and balanced scorecard perspective. International Journal of Open Information Technologies, 7(6).
[3] Riki, R. 2018. Implementation of Information Technology Governance Based on CoBIT Framework 5. Case Study: Bureau of Information Systems & Technology-Buddhi Dharma University. Tech-E, 1(2), pp. 43-50.
[4] Kurniawan, E., & Riadi, I. 2018. Security level analysis of academic information systems based on standard iso 27002: 2013 using Sse-Cmm. International Journal of Computer Science and Information Security (IJCSIS), 16(1), pp. 139-147.
[5] Mazza, T., & Azzali, S. 2018. Information technology controls quality and audit fees: Evidence from Italy. Journal of Accounting, Auditing & Finance, 33(1), pp. 123-146.
[6] Bagus, P. D., & Lily, W. 2019. Audit the Implementation of Information Technology Governance in Financial Services Company Using COBIT 4.1 Framework. International Journal of Open Information Technologies, 7(11).
[7] Akinleye, G. T., & Olanipekun, C. T. 2019. Effects of Information Technology (IT) on Internal Audit in Southwest Nigeria Universities. Journal of Economics and Behavioral Studies, 11(1 (J)), pp. 22-26.
[8] HASAN, M. U. 2018. A CONCEPTUAL FRAMEWORK OF INFORMATION SECURITY DATABASE AUDIT AND ASSESSMENT IN UNIVERSITY BASED ORGANIZATION (Doctoral dissertation, Universiti Teknologi Malaysia).
[9] Satoh, N., & Samejima, M. 2019. Risk words suggestion for information security audit by Bayesian inference. *Electronics and Communications in Japan, 102*(1), pp. 42-48.

[10] Wind, S. A. 2018. Using Guttman errors to explore rater fit in rater-mediated performance assessments. *Methodological Innovations, 11*(3), pp. 2059799118814396.