Technology Safety Audit in Computer Laboratories Using ISO/IEC 17799 : 2005

(Case Study: FTK UIN SUNAN AMPEL SURABAYA)

Muqoffi Khosyatullah[1] , Nurul Fariidhotun Nisaa[2], Ilham[3]
[1,2,3]Faculty of Science and Technology
Sunan Ampel State Islamic University Of Surabaya
[3]Airlangga University Of Surabaya
Jl. A. Yani N0.117, Surabaya, Indonesia
[1]muqoffikhos@gmail.com , [2]rullyfn219@gmail.com[2], [3]ilham@uinsby.ac.id

Abstract

Management audit is very important for assessment of their information technology management to gain efficient and effective business running process. Information technology security as an effort of internal controlling for risk and threat security minimization, is mainly considered due to all learning and lecturing administration activities use information technology. Allso, the implementation of a number of computer labs to facilitate learning processes and access to information in order to support the lectures and personal development of students To find out how secure technology information is, it is then requiring an audit to make sure everything run based on procedure. Management audit is very important for any colleges towards the examination and assessment of their information technology management to gain efficient and effective business running process. Information technology security as an effort of internal controlling for risk and threat security minimization, is mainly considered due to all learning and lecturing administration activities use information technology. To find out how secure technology information is, it is then requiring an audit to make sure everything run based on procedure. Standard used is framework international standardization organization (ISO) 17799:2005

Keyword : Audit, Information security, ISO 17799: 2005

1. Preliminary

Advances in information technology that occur at this time is growing rapidly, in contrast with the greater risk of information security. In an effort to achieve the business goals of a college in utilizing information technology in managing information data to create a quality service to the goals of business processes.

Higher education needs to ensure security and privacy and also the integration of data that is processed, in addition to the performance of information systems also become an important part that must be managed properly so that the use of technology can run optimally [1].

The processing of information technology which is quite complex in tertiary institutions is done by computerization. There is also a well-implemented implementation of information technology security management. However, there are still some data issues that have not been integrated from other systems, for example data or information that is easily accessible by users outside who have access rights as well as lack of human resources in managing information technology security management.

To maintain information technology security management so that it runs smoothly, an audit is needed. There are also standards that must be used in the information technology security audit process that is using a framework or standard that suits your needs.

An audit on information technology security carried out will use the International Standardization Organization (ISO) 17799: 2005. This standard was chosen because it is suitable for use and developed according to the needs of this faculty.

The Faculty of Tarbiyah dan Keguruan (FTK) at UIN Sunan Ampel has several computer laboratories as one of the learning facilities as well as access to information to support lectures and also for self-development for students. Many laboratories have important information that needs to be protected such as lecture material, and so on. In addition, the Tarbiyah dan Keguruan laboratory also has an information system as well as an information system and facilities that are connected in local and internet networks which are widely used for students, lecturers and also the staff of the Faculty of Tarbiyah to support the process of conducting academic and administrative activities.

Computer security is a branch of technology known as information security that is applied to computers. Computer network security as an information system is very important to maintain data validation and integrity, and guarantee the availability of services for its users.

This study uses the framework of ISO / IEC 17799: 2005 Code of Practice for Information Security Management because ISO / IEC 17799: 2005 is widely used as a reference in the information security model environment. ISO / IEC 17799: 2005 is made specifically for the purpose of information security assessment of a system. The ISO / IEC 17799: 2005 framework control clauses measured in this study are communication and operation management, access control and information system acquisition development and maintenance [2]. The three control clauses can answer the problems that occur in. The purpose of an audit of information technology is the value of computer network security in FTK Lab Computer based on ISO / IEC 17799: 2005 to protect existing information in order to support the vision of FTK as a center of information technology excellence [4].

2. STUDY LITERATUR

In previous research with a case study of the Department of Agriculture of the Republic of Indonesia, it was stated that security issues are one of the important aspects of an information system. The aspects studied include aspects of information security policies and procedures (policies) which include the architecture and model of information security, aspects of physical security, technical aspects, personnel aspects, and aspects of information system governance. The recommendation given is the need for making information policy documents and the formation of a unit in the organization responsible for information security in an agency.

The difference between this research and previous research is that this research focuses more on the technical aspects of information security management which consists of communication and operations management, access control, and information system acquisition development and maintenance. In addition, this study uses the ISO / IEC 17799: 2005 standard while previous studies use the ISO / IEC 17799: 2000 standard. Standard differences include the addition and subtraction of ISO / IEC 17799 control clauses, control objectives, and controls security.

According to ISACA, an audit is defined as a systematic, independent and documented process or activity to find evidence (audit evidence) and be evaluated objectively to determine whether it meets the specified audit criteria. The purpose of the audit is to provide a description of certain conditions that take place in the company and reporting on compliance with a set of defined standards [3]. According to Wikipedia, an information technology audit (IT audit) is a form of oversight and control of the overall

information technology infrastructure. Meanwhile, according to Weber, IT audit is the process of gathering and evaluating evidence to determine whether the computer system used has been able to protect the assets of the organization, able to maintain data integrity, can help achieve organizational goals effectively, and use resources owned efficiently. In addition, IT audits are activities similar to SI audits, but the main focus is more on the use of technology including infrastructure related to IT utilization to meet business needs in accordance with applicable management standards and policies and regulations.

Information security consists of protecting against several aspects namely, first is the aspect of confidentiality (confidentiality), namely aspects that guarantee the confidentiality of data or information, ensure that information can only be accessed by authorized people and ensure the confidentiality of data sent, received and stored. Second, the aspect of integrity (integrity), which is an aspect that guarantees that data is not altered without permission from the authorities (authorized), maintaining the accuracy and integrity of information and the method of its process to ensure this aspect of integrity. Third, the availability aspect, namely the aspect that guarantees that data will be available when needed, ensuring that authorized users can use information and related equipment (related assets when needed).

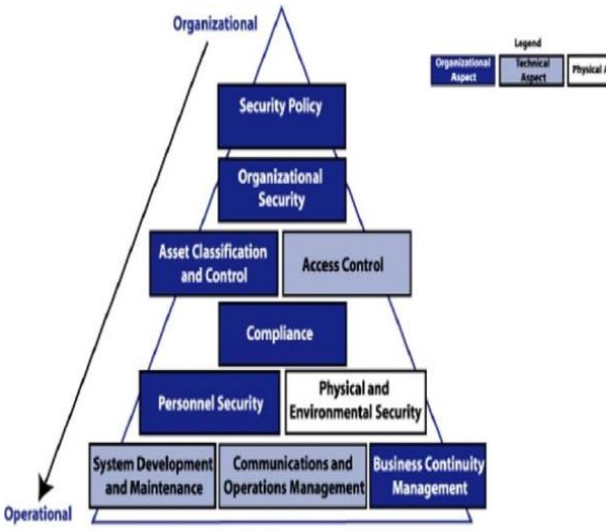
According to ISACA, an audit is defined as a systematic, independent and documented process or activity to find evidence (audit evidence) and be evaluated objectively to determine whether it meets the specified audit criteria. The purpose of the audit is to provide a description of certain conditions that take place in the company and reporting on compliance with a set of defined standards. According to Wikipedia, an information technology audit (IT audit) is a form of

oversight and control of the overall information technology infrastructure. Meanwhile, according to Weber, IT audit is the process of gathering and evaluating evidence to determine whether the computer system used has been able to protect the assets of the organization, able to maintain data integrity, can help achieve organizational goals effectively, and use resources owned efficiently. In addition, IT audits are activities similar to SI audits, but the main focus is more on the use of technology including infrastructure related to IT utilization to meet business needs in accordance with applicable management standards and policies and regulations.

Information security consists of protecting against several aspects namely, first is the aspect of confidentiality (confidentiality), namely aspects that guarantee the confidentiality of data or information, ensure that information can only be accessed by authorized people and ensure the confidentiality of data sent, received and stored. Second, the aspect of integrity (integrity), which is an aspect that guarantees that data is not altered without permission from the authorities (authorized), maintaining the accuracy and integrity of information and the method of its process to ensure this aspect of integrity. Third, the availability aspect, namely the aspect that guarantees that data will be available when needed, ensuring that authorized users can use information and related equipment (related assets when needed) [8].

As mentioned earlier in the background that this research uses the ISO / IEC 17799: 2005 framework. ISO / IEC 17799: 2005 Code of Practice for Information Security Management is an international standard developed for the application of information security in organizations. This framework is directed at developing and maintaining security standards and management practices in organizations to improve the reliability of

information security in relations between organizations.



Gambar 1. Struktur Control clauses ISO/IEC 17799:2005

Figure 1 shows the structure of ISO / IEC 17799: 2005 which consists of 10 control objects (control clauses). The organizational aspect discusses the policies of the company's management regarding information security, the technical aspect discusses the operational aspects supported by various appropriate policies and management procedures, the physical aspect discusses physical access in order to identify the risk and value of each protected asset. In this study only three control clauses were used namely communication and operations management, access control, and information system acquisition development and maintenance. Communications and operations management, aims to develop operational procedures controls, third party service delivery management, system planning, protection against malware, back-up, network security management, media handling, information exchange, e-commerce services and monitoring. Access Control, aims to develop controls on business requirements for user access, user responsibility, network access control, access control of the operating system, application access control, and information access control [5]. Information systems acquisition, development and maintenance, aims to develop controls for correct processing in applications, cryptographic functions, file system security, security of support processes, and vulnerability management [7].

3. RESEARCH METHODS

The research method consists of four parts, namely, the audit planning stage, the audit preparation stage, the audit implementation stage and the audit reporting stage.

a. Audit planning is carried out determining the process and business objectives, determined through literature review, observation and study of literature so that the determination of business processes in accordance with the circumstances and objectives of the information technology security management of tertiary institutions.
b. Audit preparations for the manufacture of an audit instrument for 10 clauses of the ISMS where each question is adjusted to the business objectives and business processes that have been made objectively which are carried out at the audit planning stage. The evaluation of each statement is adjusted to the assessment instrument determined in accordance with the implementation guidelines in the ISO 17799: 2005 standard which is adjusted to the condition of the tertiary institution.
c. The audit used the step of collecting and checking data carried out by means of interviews to the Lecturer, Ka. IT, Ka. Network and Quality Assurance besides the observation at the research site according to the agreed scope.
d. Audit reporting becomes the final stage of making and compiling reports based on the findings of evidence in the field and contains suggestions or

recommendations for improvement at the tertiary institution.

Picture. 2 Stages of research

Picture 2 shows the research stage starting from the data collection, data analysis, and data reporting stages. -Data data collection (data collection) Respondents used in the study are divided into key respondents and supporting respondents. Respondents are administrators and laboratory members (student assistants). Data collection is carried out through several stages including:

1. Questionnaire

The questionnaire used in the study is closed with the answer choices "Yes" and "No". In the questionnaire the respondent can provide the contents or description in accordance with the circumstances and his desire and provide the opportunity for the respondent to provide an explanation of the answers to the questions given. The questionnaire is used to determine the position or level of risk that the organization has achieved in implementing information security management using an ISO / IEC 17799 assessment.

2. Interview

Interviews were conducted with selected respondents to gather information. Selected expert respondents included laboratory coordinators, supervisors and student assistants.

3. Literature review

Literature study is done by reading, studying, and citing various sources including books, theses, journals, and documents of the Faculty of Information Technology related to research so that up-to-date data are obtained that can be used to help the research process.

Analysis of the data obtained was carried out in several stages including:

1. Compilation of data The data obtained are then collected to check whether all the required data has been recorded properly. The process of compiling data is done by selecting data that has to do with research and the authenticity of the data and reviewing the data obtained through interviews and questionnaires. The questionnaire that was filled in by the respondent then checked the completeness of the answer and then arranged according to the respondent's code. The research uses primary data obtained from interviews and questionnaires while secondary data is obtained by collecting data and information through documents or literature studies.
2. Data classification In this stage the answers to each question are arranged by giving the appropriate score with a predetermined weight then made in the form of data tabulation. The equipment used in analyzing these variables is the ISO / IEC 17799 self assessment questionnaire.
3. Data measurement is an analysis of the level of risk in the organization carried out measurements of scoring from ISO / IEC 17799 self assessment questionnaire totaling 36 questions

with answer choices "Yes" and "No". For questions answered "Yes" get a value of 1 and answers "No" get a value of 0. Total questions answered with "Yes" will be identified as the level of risk management in organizations with the following classification: Number of answers "Yes"> 59: Superior Level Number of "Yes" responses 52-59: Fair Level Number of "Yes" answers 43-51: Marginal Level Number of "Yes" answers 34-42: Poor Level Number of "Yes" answers <34: Level At Risk. Interpretation of data assessment results Based on the results of quantitative data processing, the level of risk management in the organization is obtained. The results of the quantitative data are then compared with the results of the interviews conducted in order to obtain recommendations and conclusions.

4. Reporting (reporting) The audit report is prepared based on the evidence that has been found, the results of the analysis, and recommendations based on the ISO / IEC 17799: 2005 framework. The reporting stage is the final stage in the study.

4. DISCUSSION

NO	Indikator ISO/IEC	Responden								
	17799	1	2	3	4	5	6	7	8	9
1	Communications and	18	12	15	13	18	13	10	11	11
2	Access Control	14	28	14	24	8	19	14	14	13
3	Information systems	2	1	2	7	11	1	10	10	11
Rata-Rata		34	41	31	44	37	33	34	35	35
Nilai Rata-Rata		6								

Based on an analysis of the level of risk carried out, it was found that by several factors including communication and operations management, operational objective control procedures and responsibilities, the FTK Infrastructure Facilities section had prepared a Computer Laboratory Standard Operating Procedure (SOP) document to be used as an operational implementation guide that regulates laboratory rules, mechanisms for practicum implementation, mechanism for borrowing tools for practicum and research activities, sanctions, check list of tools, computer service or maintenance, and computer repair However, in its implementation, the existing SOPs are not fully used as a reference in operational activities in the laboratory due to the lack of detailed operational mechanism. In addition, the new SOP only existed in 2012 so operational activities were carried out based on experience and guidance from senior laboratory assistants and supervisors. Control over the implementation of activities is carried out directly by the supervisor of the laboratory assistant (permanent admin).

Changes to information processing facilities and systems are controlled through mechanisms established by the Infrastructure Section where maintenance is carried out every week, software requirements are updated at the beginning of the semester, and the hardware revitalization process. If the request for software installation in a laboratory is submitted when the lecture has started, it will be processed 1 week after submitting the application. Changes to information processing facilities and systems that use the internet network are not made during working days so as not to interfere with network access. There is separation for control of development, testing and operational facilities. This is done as an anticipatory step if the changes made can cause damage. In its implementation there is a division of tasks and responsibilities to reduce opportunities for abuse of authority.

Third Party Service Delivery Management, aims to implement and maintain the level of information security and services in accordance with service agreements with third parties. The third

party that cooperates with managing the network at FTK is the provider, computer service, and electricity. The authority and control over information security management is carried out independently by the FTK. Therefore, it is necessary to conduct audits by third parties on a regular basis.

System planning and acceptance, the use of internet facilities is adjusted to the needs such as the allocation of internet bandwidth and access to access services provided, the allocation of internet bandwidth is 15 MBps where the allocation for faculty offices is 10 Mb, hotspot is 1 Mb, and the laboratory network is 4 Mb. In the laboratory resources, capacity monitoring is carried out at the end of each semester periodically so that lecturing activities in the following semester can run smoothly. Information system testing for systems used from third parties is done before the information system is implemented while for testing the software or application used, adjusted for the capacity of available hardware and software.

Media handling, removable media refers to portable data storage media that can be connected to a computer, and revoked without harming the data in it. As a connection, usually using a USB or drive mounted on a computer such as a flash disk, floppy disk, flash memory, and so forth. In its implementation, the use of removable media is restricted to laboratory computer networks, the use of removable media is only permitted for teaching computers.

Protection against malicious and mobile code, malicious code is a collection of commands that can execute a system to obtain information. Malicious code can spread through viruses, worms, Trojan horses, and others. Therefore, to protect computer networks against harmful software, anti-virus, restriction, and firewall are used. Anti-viruses used are Kaspersky and Microsoft Security Essentials which are placed on the server and closed several ports on the proxy network server. To protect computer networks in laboratories, the use of removable media, internet access is not allowed for users. Internet access in the laboratory is provided for certification subject laboratories while for other laboratories is provided upon request from the instructor. These restrictions are set in the restriction imposed on each domain. Mobile code service is software that is transferred from one computer to another and executes automatically. The mobile code service is not implemented in the FTK computer network because it is not needed in its implementation.

Back-up in the laboratory is done at the end of each lecture semester while back-up of data in the network is done when there is a change. In the back-up laboratory done by clonning. Back-up of data in the laboratory is done based on the permission of the instructor (lecturer and assistant lecturer) but often this has problems due to lack of coordination between the laboratory members and the instructor. Network security management, to ensure data security within the FKI network and protection of services connected from authorized access, use a proxy and firewall. Service providers do not describe security attributes for all services that are used because security attributes are managed and controlled directly by the FTK network administrator.

Information handling procedures, carried out by digitizing documentation using a scanner in the Administration section. Computer media that are no longer needed will be stored in warehouses and used for assembly activities. There are no sensitive data handling procedures to protect data from misuse and there is no protection of system documentation from

unauthorized party access. Data exchange can only be done between instructors and students while between student computers is not permitted. In addition, not all restriction settings in the laboratory are the same, so in their application, there are some computers that do not get restriction. Computer management is the responsibility of each laboratory coordinator. Therefore, intensive control is needed by the laboratory assistant.

Exchanges of information, there is a formal agreement on cooperation regarding policy procedures and formal control to protect the exchange of information. The agreement made by the FTK Infrastructure Facilities Section was carried out and controlled by the Faculty. In its application, not all laboratory members are aware of the agreement. This is in accordance with the specified job description because laboratory members are more directed to the management of laboratory computer networks. In the implementation there are no controls applied to protect the computer media that transmit data, no there is an electronic office system and information exchange through the use of voice, fax and video. There is no control over the service because the FTK does not use the service in the business process that it runs. For electronic messaging services, the FTK uses the Google mail service because it is safer to use. Control over the use of space and documentation of laboratory data is stored in Google services so that it can be accessed by all laboratory assistants. There are no services for electronic commerce activities because the FTK does not use these services in the business processes that are carried out. For public information services, control is carried out directly by users who wish to convey information so that in the implementation there is no input and output validation process.

Monitoring, on the FTK computer network, surveillance logs are carried out on the network server. The laboratory assistant is the operator log for monitoring. For error logs, computer and communication system problems are controlled when complaints are made. There is no procedure to monitor the use of the system that users only carry out processes that have been authorized and there is no clock synchronization used to ensure the accuracy of the time log or time communication device.

Access control, on the basis of observing business requirements for access controls, the FTK business needs have been defined and documented for access control but the documentation does not describe the rights and obligations as well as the authority of each user. The right of access to the laboratory is divided into three levels, namely administrators, instructors (assistant lecturers and lecturers) and students. The right of access to the internet network is divided into three levels namely administrators, lecturers, and students. With access control, it will be easier for administrators to monitor and control information.

User access management, there is no formal user registration procedure for granting access rights for all IT services and there is no deregistration procedure for revoking access rights for all IT services. In its application, all users can still access all IT services when connected to the FTK network as long as the user knows the username and password. Restrictions and controls over the use of IT system features or facilities that enable users to change systems or application controls are based on user access rights. Changes to the system or application control can only be made by an administrator. Giving an Internet Protocol (IP) address to the user is done by DHCP, control is carried out using the user's MAC address. For laboratory computer networks,

user access rights are distinguished from user domains (clients) consisting of lecturers and students, computer administrators, and network administrators (domain administrators). For user access rights as a domain user, password management is left blank because the password is known to all users. For internet services, all users use the same password based on access rights. Reviews are only carried out in accordance with the needs and conditions that occur and in general there is no formal procedure for periodically reviewing user access rights and passwords. Thing this is felt to be insecure because it is often encountered by some users using access rights that are not in accordance with the access rights that they should have so often the internet connection becomes very slow and cannot be used by other users. In addition, in its implementation there are several courses in the laboratory that in access need to use access rights as an administrator, so it is necessary to check the list to check computer systems regularly.

User responsibilities, in using passwords users are not taught about the practice of choosing and using passwords because passwords are set on the server (static). Passwords on the internet network are distinguished based on user access rights while on computer networks in the laboratory do not use passwords. The rules regarding unattended user equipment are conveyed by sticking to each laboratory and given a notification message on the screen after the login process. The FTK has implemented a clear desk and clear screen policy in the laboratory to reduce risk without permission or damage to paper, media, and information processing facilities. The obstacle faced in the laboratory is the lack of awareness of users (students) to maintain cleanliness and safety in the laboratory. Therefore, it is very necessary good cooperation between the laboratory assistant and the instructor. Control by laboratory members (laboratory assistants) who stand guard is done at the end of each lecture. In its development, the FTK is developing the use of computer networks in laboratories based on user identities (Student Id Number) to facilitate monitoring.

Network access control, users can only access services provided based on their access rights. There is no process to ensure that users access the network and computer services from certain places. To limit the route between the user and the computer service used restrictions on the domain on the server. Authentication of remote users' connections through public or non-organizational networks is not permitted to users, users can only access computer networks and services when they are in the FTK (local network) area. Remote user connections over public networks are only allowed for administrators. By using a microtic system a monitoring system has been built that can be used to control access to diagnostic ports. For the information service grouping, the FTK network is divided into several separate domains where each laboratory has its own domain so that it can reduce the risk of unauthorized parties accessing the computer system that uses the network. On the FTK network, routing is done through a router that is connected using a separate user and password by the administrator to ensure that computer connections and information flow according to business unit access policies. Routing is often a problem because looping often occurs and users who use bandwidth exceed the given capacity. This causes the network is often slow so that not all users can enjoy existing internet services.

Operating system access control, there is no automatic terminal identification to authenticate the connection at a certain location. On a computer network laboratory log-on procedures to the computer system

using the laboratory name and user table number while for the internet network there is no log-on procedure. Users do not have a unique identification (user identification) that can be used personally and the appropriate authentication techniques to prove the user's identity. There is no effective password management system for user authentication. There are utility programs that can be used to help control systems and applications, applications used in laboratories are teamviewers. In addition, there is no session limit (session time-out) and connection time (limitation of connection time) provided to prevent unauthorized party access to the computer network.

Application access control, application system data access restrictions are based on user access rights. In the laboratory network, the exchange of data is provided by the directory while for the internet network settings are adjusted to the user's computer settings. According to the identified risks, sensitive application systems operate in an isolated processing environment by separating space and limiting physical access such as separation between laboratory servers and network servers. The application is placed on the server so that access to the application depends on user access rights. Mobile computing and teleworking, there are no formal policies and procedures developed to control the use of mobile computing and teleworking facilities.

Information systems, acquisition, development, and maintenance, on security requirements of information systems, analysis of security requirements is a key requirement for project development. Correct processing in applications, the data input into the application system is validated by the operator to ensure that the data entered is correct and appropriate. Because the data input is done manually by the operator there is no authentication message in the application and the output validation process on the system. Data output validation on the system is done manually by comparing the output with the initial data.

Cryptographic controls, there are no policies regarding the use of cryptographic controls, encryption, digital signatures, and non-repudiation services to protect information deemed at risk. Security of system files, control of operational system software is carried out by means of if there is software to be used then it is adjusted to the hardware capacity and compatibility with the operating system used. There is no protection against data system testing. Access to program source code can only be accessed by administrators to reduce the potential for damage to computer programs.

Security in development and support processes, implementing changes are controlled by using change control procedures. When changes occur, it will be reviewed whether the changes affect the operating system and application.

5. CONCLUSION

Laboratory log-on procedures to the computer system using the laboratory name and user table number while for the internet network there is no log-on procedure. Users do not have a unique identification (user identification) that can be used personally and the appropriate authentication techniques to prove the user's identity. There is no effective password management system for user authentication. There are utility programs that can be used to help control systems and applications, applications used in laboratories are teamviewers. In addition, there is no session limit (session time-out) and connection time (limitation of connection time) provided to prevent unauthorized party access to the computer network.

Application access control, application system data access restrictions are based on user access rights. In the laboratory network, the exchange of data is provided by the directory while for the internet network settings are adjusted to the user's computer settings. According to the identified risks, sensitive application systems operate in an isolated processing environment by separating space and limiting physical access such as separation between laboratory servers and network servers. The application is placed on the server so that access to the application depends on user access rights. Mobile computing and teleworking, there are no formal policies and procedures developed to control the use of mobile computing and teleworking facilities.

Information systems, acquisition, development, and maintenance, on security requirements of information systems, analysis of security requirements is a key requirement for project development. Correct processing in applications, the data input into the application system is validated by the operator to ensure that the data entered is correct and appropriate. Because the data input is done manually by the operator there is no authentication message in the application and the output validation process on the system. Data output validation on the system is done manually by comparing the output with the initial data.

Cryptographic controls, there are no policies regarding the use of cryptographic controls, encryption, digital signatures, and non-repudiation services to protect information deemed at risk. Security of system files, control of operational system software is carried out by means of if there is software to be used then it is adjusted to the hardware capacity and compatibility with the operating system used. There is no protection against data system testing. Access to program source code can only be accessed by administrators to reduce the potential for damage to computer programs.

Security in development and support processes, implementing changes are controlled by using change control procedures. When changes occur, it will be reviewed whether the changes affect the operating system and application.

REFERENCES

[1] Mursito, Danan. 2008. *Evaluasi Kinerja Sistem Manajemen Keamanan Informasi Menggunakan ISO 17799 : Studi Kasus Departemen RI* .Jakarta : Universitas Indonesia.

[2] Aruan,Ferdinand.2003. *Tugas Keamanan Jaringan Informasi (Dosen. Dr. Budi Rahardjo) Tinjauan Terhadap ISO 17799*. Program Magister Teknik Elektro Bidang Khusus Teknologi Informasi ITB.

[3] Mehdi Kazemi, "*Evaluation of information security management system success factors: Case study of Municipal organization*," African J. Bus. Manag., vol. 6, no. 14, 2012

[4] Juliandarini and S. Handayaningsih, "*Audit Sistem Informasi Pada Digilib Universitas Menggunakan Kerangka Kerja Cobit 4.0,*" J. Sarj. Tek. Inform., vol. 1, no. 1, pp. 276–286, 2013.

[5] Syarizal ,Melwin. 2007. *ISO 17799 : Standar Sistem Manajemen Keamanan Informasi.* Seminar Nasional Teknologi 2007.

[6] M. Utomo, A. Holil, N. Ali, and I. Affandi, *"Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC".* ITS

[7] Tom Carlson, Lucent Technologies Worldwide Services. 2001. I*nformation*

Security Management: Understanding ISO 17799.

[8] S. Neumann, A. Kahlert, P. Richter, R. Grimm, M. Volkamer, and A. Roßnagel, "*Holistic and Law Compatible IT Security Evaluation,*" Int. J. Inf. Secur. Priv., vol. 7, no. 3, pp. 16–35, 2013.