© 2018 IJSRST | Volume 4 | Issue 5 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology

Using the Information Security Index to Measure University Information Security Management : Concepts and Strategies

Luqman Hakim*[1], Avinanta Tarigan[2]
*[1]Master of Informatics Engineering, University of Amikom Yogyakarta , Sleman, Yogyakarta, Indonesia
[2]Department of Computer Engineering, University of Gunadarma, Depok, West Java, Indonesia

ABSTRACT

An information security index is an evaluation tool for analyzing the degree of information security preparedness in government agencies. This evaluation tool is not intended to investigate the feasibility or effectiveness of existing forms of security, but rather as a tool to provide a picture of the readiness condition. This study aims to create a concept and evaluation strategy using information security index. The research method used is literature study and interview to generate a proper concept and strategy that matured. The result of this research is information security index will evaluate an organization based on six area that is: ICT Roles, Information Security Governance, Information Security Risk Management, Information Asset Management and Information Technology and Security. In an evaluation using information security index there are nine steps to be taken the first step is planning, second is literature study and interview then six evaluation steps based on the last area is the result of the evaluation, the Estimated time needed to do the assessment is thirteen weeks.

Keywords: Information Security Index, Concept of Information Security Index, Information Security Strategy

I. INTRODUCTION

In the implementation of information and communications technology (ICT) governance, information security elements are a critical aspect to note, given that the performance of ICT governance will be disrupted if information as one of the principal objects of ICT governance experience information security issues related to confidentiality, integrity, and availability.

Information protection is necessary to be taken seriously by all employees, management, and employees of the organization concerned. The information security concerns policies, procedures, execution, and activities to protect information and various types of threats against it to cause harm to the survival of the organization. Higher Education Institution is an organization having multiple types of essential and confidential information or information that should be kept authentic. For example information about the academic implementation of students, asset management colleges, finance, research information, community service, scholarships and so forth.

Maintaining confidentiality, wholeness, and availability of information is confronted with some potential threats. Threats can be intentional (for example, an individual cracker or criminal organization) or by chance (for example, possibly a computer malfunction, or the possibility of a disaster such as an earthquake, fire, or tornado) or situations, skills, actions or events [1]. Information security management becomes very important in the modern era, where current technological developments have made it easier for people to obtain information. This ease is seen with the increasing number of internet visitors from year to year. The number of internet user developments in Indonesia is shown in Figure 1 on Indonesian internet visitor charts from 1998-2012 sourced from the Association of Indonesian Internet Service Providers.

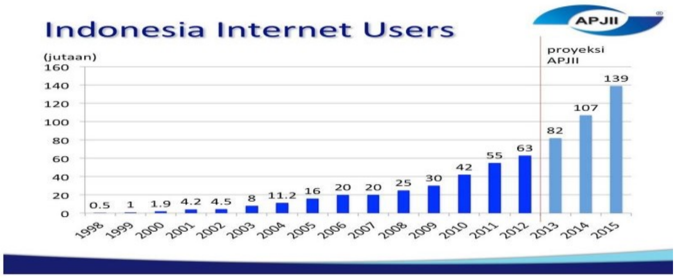


Figure 1. Graphic of Indonesian Internet Visitors during 1998 – 2012

However, until now there are not many higher education institutions that give attention regarding information security, so the level of information security at the college institution is shallow that influence the frequent misuse of information and even damage that can be fatal. Information security is not enough to rely solely on the reliability of information security tools or technologies that are applied, but also a good understanding by the organization about what should be protected and how to accurately determine solutions that can address the situation of information security needs. For that, we need a systemic and comprehensive information security management.

Information systems security still lacks attention in any organization or company that uses ICT in its business processes [2]. Management in the team even prioritizes the utilization and development of ICT services on top of real security is the key to the sustainability of ICT services. Part of the reason is not prioritized information system security, partly because the organization thinks it is not essential, expensive, waste time, slow down work and so on [3].

Information security is an attempt to secure information assets against possible threats. Information security can indirectly ensure business continuity, reduce risks, optimize return on investment. The more information the company keeps, managed and shared, the higher the risk of damage, loss or exposure to unwanted external data [4]. Information security management system that information security is a safeguard against various threats to ensure business sustainability, minimize business risk, and increase investment and business opportunities[5]. The Information System Audit is the process of collecting and evaluating evidence to determine whether the computer system used has been able to protect the organization's assets, be prepared to maintain data integrity, can assist in the achievement of organizational goals efficiently, and use resources efficiently [6].

The Information Security Index is an evaluation tool released by the Indonesian Ministry of Communications and Information which serves to analyze the level of information security readiness. The form of evaluation implemented in the Information security Index is designed to be used by agencies of various levels, sizes, and levels of use of information and communication technology (ICT) in support of the implementation of existing basic tasks and functions [7]. Evaluation parameters The information security index represents the degree of readiness of safeguard implementation following the completeness of control required by ISO / IEC 27001: 2005 standards and the level of maturity of safeguard implementation with categorization referring to the level of maturity used by three COBIT frameworks [7]. This study aims to provide an overview of the concept of information security index and evaluation strategy using information security index at a university.

II. RESEARCH METHODS

The research is a type of descriptive qualitative study that is the research presented in the form of description. In conducting this analysis conducted a leather approach, the existing information security index theory will be discussed concepts and strategies for evaluation of information security management within a university. This study uses the steps as illustrated in Figure 2.

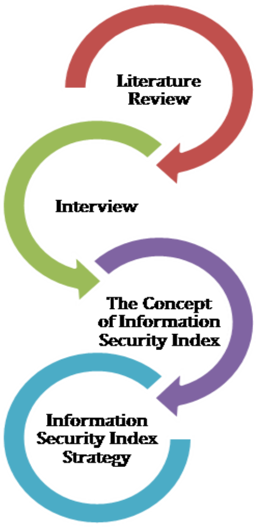

Literature Review
Interview
The Concept of Information Security Index
Information Security Index Strategy

Figure 2. Research Methods

Four steps will be done this research include: Literature Review, Interviews, The Concept of Information Security Index, Information Security Index Strategy

A. Literature Review

Document studies are conducted using existing documents, documents and other written books that become relevant sources of information to gain knowledge of the research and its research objects.

B. Interviews

In this section, the authors conduct interviews to those who have applied the information security index. The author deliberately chooses anyone who has met the requirements as a resource person with the information technology division staff. It aims to get a clearer picture of the business process undertaken in the information technology directorate and know how the information security level exists.

C. The Concept of Information Security Index

The result in this section is the concept of evaluation of information security management at a university using the information security index. In this article will also discuss the questionnaire to be asked, how to assess each questionnaire and measurement results.

D. Information Security Index Strategy

The result in this section is the strategy of applying the information security index to take measurements at a university. The plan to be discussed include a research step if using an information security index, a credible party to be an interview resource and an estimated time of research.

III. DISCUSSION

An information security index is an evaluation tool for analyzing the degree of information security preparedness in government agencies. This evaluation tool is not intended to investigate the feasibility or effectiveness of existing forms of security, but rather as a tool to provide a picture of the readiness condition (completeness and maturity) of the information security framework to the head of the Agency. Evaluations are conducted in the various areas targeted for the implementation of information security with a scope of discussion that also meets all security aspects defined by ISO / IEC 27001: 2005 standards.

The evaluation forms implemented in the information security index are designed to be used by government agencies of varying degrees, sizes, and levels of use of ICTs in support of the implementation of existing Tasks and Functions. The data used in this evaluation will provide a snapshot of the readiness index - from the completeness and maturity aspect - the information security framework is applied and can be used as a comparison to prepare the steps of improvement and prioritization.

This evaluation tool can then be used periodically to get an overview of changes in information security conditions as a result of the work program being carried out, as well as a means of conveying increased preparedness to stakeholders.

The evaluation process is carried out through some questions in each of the areas below:

- The Role of ICT in the organization
- Information Security Governance
- Information Security Risk Management
- Information Security Framework
- Management of Information Assets
- Information Technology and Security

A. The Role of ICT in the organization

This section provides the level of role and importance of ICT in your organization. In this article, the answered questionnaire is divided into five according to the level of concern, among others: Minim; Low; Medium; High; Critical. In the section there are 12 questions to be answered can be seen in table 1

TABLE 1
Questions of ICT Role Areas

No	*Characteristics of the Organization*
1	Total annual budget allocated to ICT
2	Number of staff/users in institutions using ICT infrastructure
3	Level of dependence on ICT services to run the Duties and Functions of your organization
4	The value of intellectual property owned and produced by your organization
5	The impact of significant ICT system failures used by your organization
6	The dependency level of ICT system availability to connect the work location of your organization
7	The impact of your organization's ICT system failure on the performance of other Government agencies or the availability of a national government system
8	Level of sensitivity of ICT system users in your organization
9	Level of compliance with laws and other legal instruments
10	Potential loss or negative impact of incidents penetrated information security ICT system of your organization
11	Degree of dependence on third parties in running/operating ICT systems
12	Level of classification/criticality of ICT systems in your agency, relative to threats of attack effort or information security breach

In question number one the standard used to perform the assessment is as follows:

TABLE 2
Standard Assessment Question Number One

No	Total Spending	Status
1	Less than 1 Billion	Minim
2	1 Billion up to 3 Billion	Low
3	3 Billion up to 8 Billion	Medium
4	8 Billion up to 20 Billion	Height
5	20 Billion or more	Critical

In question number two the standard used to perform the assessment is as follows:

TABLE 3
Standard Assessment Question Number Two

No	*Number of staff*	*Status*
1	Less than 60	Minim
2	60 to 120	Low
3	120 to 240	Medium
4	240 to 600	Height
5	600 or more	Critical

ICT role area assessment standards are as follows

TABLE 3

ICT Role Area Assessment Standards

No	Status	Value
1	Minim	0
2	Low	1
3	Medium	2
4	Height	3
5	Critical	4

B. Information Security Governance

This section evaluates the readiness of information security governance forms as well as the agencies/functions, duties and responsibilities of information security managers. In this article there are 20 questions with the following answer model: Not Performed; In Planning; In Application or Partially Applied; Applied Wholly

TABLE 4

Questions of Information Security Governance Areas

No	Functions / Information Security Agencies
1	Are your agency leaders principally and officially responsible for the implementation of the information security program, including the establishment of related policies?
2	Does your agency have a function or section that has the duty and responsibility explicitly to manage information security and maintain its compliance?
3	Do information security officers have the appropriate authority to implement and ensure compliance with information security programs?
4	Is the person responsible for implementing information security given the appropriate allocation of resources to manage and ensure compliance with the information security program?
5	Is the role of information security implementers covering all the requirements mapped out completely, including internal audit needs and segregation requirements of authorities?
6	Does your agency have defined the requirements/standards of competence and expertise of information security management?
7	Do all implementers of information security in your agency have adequate competence and expertise by applicable requirements/standards?
8	Has your organization implemented a socialization program and increased understanding of information security, including its compliance interests for all concerned?
9	Does your agency implement a program to improve the competence and expertise of information security officers and officers?
10	Does the responsibility for managing information security include coordination with the internal and external information management/usage authorities to identify security requirements/requirements and resolve existing issues?
11	Does the information security manager proactively coordinate with the relevant stake (HR, Legal / Legal, General, Finance, etc.) and the interested external party (security apparatus) to implement and ensure compliance with information security?
12	Is the responsibility for deciding, designing, implementing and managing the continuity of ICT (business continuity and disaster recovery plans) measures defined and allocated?
13	Does the person responsible for managing information security report the condition, performance/effectiveness and compliance of the information security program to the head of the Agency regularly and officially?
14	Are the conditions and issues of information security in your agency being preamble or part of the strategic decision-making process in your agency?
15	Does the head of the work unit in your agency implement a unique program to comply with the objectives and objectives of compliance with information security, specifically covering the information assets under its responsibility?

16	Does your agency have defined parameters, metrics and performance measurement mechanisms for information security management?
17	Has your agency implemented an information security management performance appraisal program for the individual of the executor?
18	Has your agency implemented information security management targets and targets for relevant areas and evaluated its achievements on a regular basis, including its reporting to the head of the Agency?
19	Has your agency identified legislation and other legal instruments related to information security that must be obeyed and analyzed for compliance?
20	Does your agency have defined policies and measures to combat information security incidents that involve legal (criminal and civil) violations?

There are three assessment standards in the information security governance section. The first rule, for questions number 1 through number 8 the minimum value is 0, and the maximum amount is three can be seen in table 5. The second standard for questions number 9 to number 14 values of at least 0 and the maximum value of 6 can be seen in table 6. Standard 3 for questions number 15 to 20 values minimum 0 and maximum value nine can be seen in table 7.

TABLE 5

The First Assessment Standards

No	Status	Value
1	Not Performed	0
2	In Planning	1
3	In Application or Partially Applied	2
4	Applied Wholly	3

TABLE 6

The Second Assessment Standards

No	Status	Value
1	Not Performed	0
2	In Planning	2
3	In Application or Partially Applied	4
4	Applied Wholly	6

TABLE 7

The Third Assessment Standards

No	Status	Value
1	Not Performed	0
2	In Planning	3
3	In Application or Partially Applied	6
4	Applied Wholly	9

In this section, the organization that performs the assessment will get a total value of at least 0 and a maximum value of 114.

C. Information Security Risk Management

This section evaluates the readiness to apply information security risk management as a basis for the implementation of information security strategies. This section consists of 15 questions and can be seen in table 8 with variations of answers are as follows: Not Performed; In Planning; In Application or Partially Applied; Applied Wholly

TABLE 8

Questions of Information Security Risk Assessment Areas

No	Information Security Risk Assessment
1	Does your agency have a documented and officially employed information security risk management program?
2	Does your agency have a documented and officially employed information security risk framework?
3	Does this risk management framework include the definition and relation of the level

	of information asset classification, the level of threat, the likelihood of the occurrence of the threat and the impact of loss on your agency?
4	Has your agency set an acceptable risk level threshold?
5	Does your agency already define ownership and custodian of existing information assets, including critical assets and critical work processes that use the assets?
6	Are the threats and weaknesses associated with information assets, especially for each of the critical assets identified?
7	Is the impact of losses associated with the loss/disruption of the primary asset function established following the existing definition?
8	Has your agency run a structured information security risk assessment initiative/assessment of existing information assets (to be used later in identifying mitigation or mitigation measures that are part of the information security management program)?
9	Has your agency prepared any mitigation and risk mitigation measures?
10	Are risk mitigation measures arranged at the priority level with their completion targets and those responsible for them, ensuring cost-effectiveness that can lower the risk level to acceptable thresholds by minimizing the impact on ICT service operations?
11	Is the status of the completion of the risk mitigation measures regularly monitored, to ensure the end or progress of its work?
12	Has the completion of implemented mitigation measures been evaluated to ensure consistency and effectiveness?
13	Are the risk profiles following their mitigation forms regularly reviewed to ensure their accuracy and validity, including revising the pattern if there are significant changes to the conditions or the need to implement new ways of security?
14	Is the risk management framework regularly reviewed to ensure/improve its effectiveness?
15	Is risk management a part of the criteria of the objective assessment process for the effectiveness of security performance?

This section uses three assessment standards. The first standard for questions 1 through 9 applies a minimum value of 0 and a maximum value of 3, and the first assessment standard can be seen in table 5. The second standard for questions 10 through 13 uses a minimum value of 0 and a maximum value of 6, and the first rating standard can be seen in table 6. The third standard uses a minimum value of 0 and a maximum value of 9 for questions number 14 and number 15, the third assessment standard can be seen in table 7.

In the Information Security Risk Management section, the organization using the information security index will get a minimum value of 0 and a maximum value of 69 that will be used to measure the degree of preparedness in the information security risk management section.

D. Information Security Framework

This section evaluates the completeness and readiness of the information security management framework (policy & procedure) and its implementation strategy. The number of questions in this section is 26 divided into two subsections. Items 1 through 16 exist in the sub-section on the Preparation and Management of Information Security Policies and Procedures, questions 17 through 26 are in the Information Security Strategy and Program Sub-section. There are four grades of assessment in this section are: Not Performed; In Planning; In Application or Partially Applied; Applied Wholly. Table 9 shows a list of questions in this section.

TABLE 9

Questions of Information Security Management Framework Areas

No	Preparation and Management of Information Security Policies and Procedures
1	Have information security policies and

	procedures been developed and written out clearly, with the roles and responsibilities of the parties authorized to apply them?
2	Are information security policies formally established, published to related parties and easily accessible to those who need them?
3	Is there a mechanism for managing information security policy and procedures documents, including the use of master lists, distribution, withdrawal from circulation and storage?
4	Are there mechanisms to communicate the information security policy (and its changes) to all related parties, including third parties?
5	Do overall information security policies and procedures reflect the mitigation needs of the information security risk assessment results?
6	Is the information security aspect that includes incident reporting, maintaining confidentiality, intellectual property rights, rules of use and safeguards of assets contained in contracts with third parties?
7	Are the consequences of an information security policy violation defined, communicated and enforced?
8	Is there an official procedure for administering an exception to the application of information security?
9	Has your organization implemented operational policies and procedures for managing security patch implementations, assigning responsibility for monitoring new security patch releases, ensuring installation and reporting?
10	Has your organization implemented a process to evaluate the risks associated with the purchase plan (or implementation) of the new system and address the emerging issues?
11	If the application of a system leads to new risks or non-compliance with existing policies, is there a process to address this, including the application of new compensating controls and their completion schedules?
12	Is there an unbroken business continuity planning management framework that defines information security requirements/exceptions, including test schedule?
13	Will disaster recovery planning for ICT (disaster recovery plan) services define the composition, roles, authority and responsibilities of the designated team?
14	Is a trial of disaster recovery planning for ICT (disaster recovery plan) services done on schedule?
15	Are the results of disaster recovery plan for disaster recovery planning evaluated to implement the necessary corrective or revamping measures (e.g., if the trial results show that the recovery process can not (meet) the eligible requirements?
16	Are all information security policies and procedures periodically evaluated?
No	Management of Information Security Strategies and Programs
17	Does your organization have an information security implementation strategy as per the risk analysis results that its implementation is undertaken as part of the organization's work plan?
18	Does your organization have a strategy for the use of information security technologies that are implemented and updated according to the needs and changes in the risk profile?
19	Is the information security implementation strategy realized as part of the implementation of your organization's work program?
20	Does your organization own and implement an internal audit program conducted by an independent party with the overall coverage of the information assets, existing security policies, and procedures (or following

	applicable standards)?
21	Does the internal audit evaluate the compliance level, consistency, and effectiveness of the application of information security?
22	Are the results of the internal audit reviewed/evaluated to identify remedial and preventive measures, or information security performance improvement initiatives?
23	Is the result of an internal audit reported to the organization's leadership to establish a corrective action or an information security performance improvement program?
24	If there is a need to revise the applicable policies and procedures, is there an analysis to assess the financial aspects (impact of costs and budgetary needs) or changes to infrastructure and the management of the changes, as a prerequisite to implement them?
25	Does your organization periodically test and evaluate the level/compliance status of existing information security programs to ensure that all initiatives are implemented efficiently?
26	Does your organization have a medium / long term (3-5 year) adequate information security and program improvement plan being realized consistently?

In this section also apply three assessment standards. The first standard uses a value of at least 0 and a maximum value of 3, questions number 1 through number 6 and questions number 17 through number 21 using this rating standard. The second standard uses a value of at least 0 and a maximum of 6, questions 7 through 12 and question 22 and 23. The third standard uses a maximum of 9, questions number 13 through number 16 and question number 24, question number 25 and question number 26.

The organization that evaluates this section will get the smallest value of 0, and the highest value is 144.

E. Management of Information Assets

This section evaluates the completeness of securing the information assets, including the entire cycle of use of those assets. This section uses 34 questions by dividing the two sub-sections, namely the management of information assets and physical security. There are four grades of assessment in this section are: Not Performed; In Planning; In Application or Partially Applied; Applied Wholly. Table 10 shows a list of questions in this section.

TABLE 10

Questions of Management Information Assets Areas

No	Management of Information Assets
1	Is there an accurate and accurate list of information assets inventory available?
2	Is there a process that evaluates and classifies information assets according to the asset importance level for the Agency and its security needs?
3	Are available definitions of different access levels and matrix that record the allocation of such access ?
4	Is there a consistently applied system change management (including configuration change)?
5	Is there a consistently applied configuration management process?
6	Is there a process for releasing a new asset into the operating environment and updating the inventory of information assets?
7	Does your agency own and implement the following tools, as a continuation of the risk mitigation implementation process?
8	The rules of use of computers, email, internet, and intranet
9	Security arrangements and asset usage of Agencies related to intellectual property rights
10	Personal data security rules
11	The management of the electronic identity and authentication process (username &

	password) includes the policy against its violation
12	Requirements and procedures for administration / granting access, authentication and authorization to use information assets
13	Provision of time-related storage for existing data classification and data destruction requirements
14	Provisions relating to data exchange with external parties and their security
15	Investigation/investigation process to resolve incidents related to information security failure
16	Backup procedure for data restore
17	Physical security requirements that are tailored to the zone definition and asset classification contained therein
18	Checking process of HR background
19	Information security incident reporting process to external parties or authorities.
20	Undefined data/asset destruction procedures
21	Access user review procedures and remedial measures in case of non-conformity to the comprehensive policies.
22	Is there a list of data/information to be backed up and a report on compliance analysis of its backup procedures?
23	Is there a list of records of information security practices and forms of safeguards that are appropriate to their classification?
24	Is there a procedure for using third-party information processing devices (including personal and partner/vendor equipment) by ensuring the intellectual property and access security aspects used?
No	**Physical Security**
25	Has the security of physical facilities (work location) following the interests/classification of information assets, layered and can prevent unauthorized access attempts?
26	Is there a process for managing the allocation of entry keys (physical and electronic) to a physical facility?
27	Is the computing infrastructure protected from environmental or fire impact and is in a condition with temperature and humidity following the manufacturer's prerequisites?
28	Is the installed computing infrastructure protected from power supply interruptions or the impact of lightning?
29	Are there any rules for securing the computing device of your agency if used outside of the official work location (office)?
30	Is construction of a central information-processing device storage space using designs and materials that can cope with fire risks and is equipped with appropriate fire-fighting / fire-fighting, fire-fighting, temperature and humidity facilities?
31	Is there a process for inspecting and maintaining: computer equipment, support facilities, and workplace security feasibility to place vital information assets?
32	Are there any security mechanisms in the delivery of information assets (devices and documents) involving third parties?
33	Are there rules to secure essential work locations (server space, archive space) from the risk of a device or material that could compromise the information assets (including information processing facilities) contained therein? (e.g., prohibition of using mobile phone in server room, using camera, etc.)
34	Is there a process for securing the work location of the presence/presence of a third party working for the benefit of your agency?

In this section also apply three assessment standards. The first standard uses a value of at least 0 and a maximum value of 3, questions number 1 through number 16 and questions number 25 through number 29 using this rating standard. The second standard uses a value of at least 0 and a maximum of 6, questions 17 through 21 and question 30 and 33. The third standard uses a maximum of 9, questions number 22 through number 24 and question number 34. The maximum value that can be found in this section is 153

F. Information Technology and Security

This section evaluates the completeness, consistency, and effectiveness of technology use in securing information assets. This section uses 24 Questions to answer, questionnaires can be seen in table 20. There are four types of assessment in this section: Not Performed; In Planning; In Application or Partially Applied; Applied Wholly.

TABLE 11

Questions of Information Technology and Security Areas

No	Security Technology
1	Are ICT services (computer systems) that use the internet already protected with more than one layer of security?
2	Is the communication network segmented according to its importance (sharing of agencies, application needs, unique access points, etc.)?
3	Is there a standard configuration for system security for all computer and network device assets updated as per the developments and needs?
4	Does your agency routinely analyze compliance with existing standard configuration applications?
5	Are routinely used networks, systems and applications scanned to identify potential loopholes or change/configuration integrity?
6	Is the entire infrastructure monitored to ensure the availability of sufficient capacity for existing needs?
7	Are any changes in the information system automatically recorded in the logs?
8	Are unauthorized access attempts automatically recorded in the logs?
9	Are all logs analyzed periodically to ensure the accuracy, validity, and completeness of their contents (for audit and forensic traces)?
10	Does your agency apply encryption to protect critical information assets according to existing management policies?
11	Does your agency have a standard in using encryption?
12	Does your agency apply security to manage the encryption key (including electronic certificates) used, including its usage cycle?
13	Do all systems and applications automatically support and implement automatic password changes, including disabling passwords, setting the complexity/length and reuse of old passwords?
14	Is the access used to manage the system (system administration) using a unique form of layered security?
15	Are the systems and applications used already applying access time restrictions including process timeout automation, lockout after login failure, and access withdrawal?
16	Does your agency apply security to detect and prevent unauthorized use of network access (including wireless networks)?
17	Does your agency apply a unique form of security to protect access from outside the Agency?
18	Is the operating system for every desktop and server device updated to the latest version?
19	Are every desktop and server protected against virus attacks (malware)?
20	Are there recordings and analysis results (audit trail - audit trail) that confirm that antivirus has been updated regularly and systematically?
21	Is there a failed / successful virus-attack report followed up and resolved?

22	Does the whole system (application, computer and network device) already use an accurate time synchronization mechanism, following existing standards?
23	Does each application have verified/validated security specifications at the time of development and testing?
24	Does your agency involve independent parties to review information security reliability on a regular basis?

In this section also apply three assessment standards. The first standard uses a value of at least 0 and a maximum value of 3, questions number 1 through number 10 and questions number 17 through number 19 using this rating standard. The second standard uses a value of at least 0 and a maximum of 6, questions number 11 through number 16 and question 20 and 23. The third standard uses a maximum of 9, questions number 24. The organization that evaluates this section will get the smallest value of 0, and the highest value is 99.

G. Information Security Index Strategy

Before conducting an audit, it should first determine the plan of reviewing how the audit is conducted. The purpose of documenting the work should be sufficiently detailed so that it is enough information for people to be able to understand what is done and get the same conclusion [9]. Planning and documentation of work is the most important thing before an evaluation of an IT system, Also it is also required a strategy how the evaluation system can run by the planning that we do. The following strategy in the evaluation using information security index.

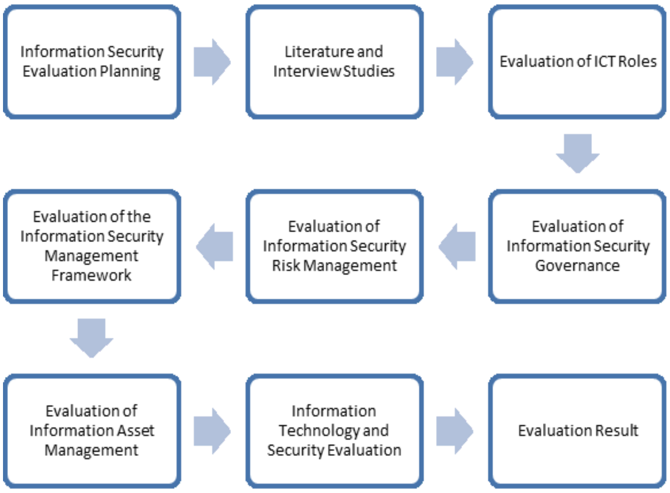

Information Security Evaluation Planning
Literature and Interview Studies
Evaluation of ICT Roles
Evaluation of Information Security Governance
Evaluation of Information Security Risk Management
Evaluation of the Information Security Management Framework
Evaluation of Information Asset Management
Information Technology and Security Evaluation
Evaluation Result

Figure 3. Step Evaluation Of Information Security Index

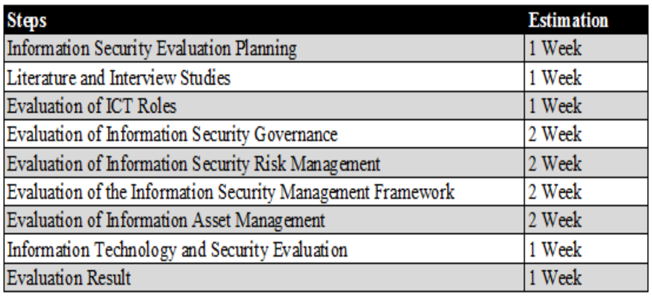
Nine steps can be done to conduct an evaluation using information security index include:

Planning is done at the beginning of the action, this planning process provides preparation, observation, determination of interviews, determination of respondents to the questionnaire.

The Literature and Interview Study is conducted at the same step because the literature study will add to our reference in evaluating and then followed by the interview used to retrieve the preliminary evaluation data.

The next step is an evaluation step of the area on the information security index there are six areas according to the information security index manual. Each area will be evaluated through questionnaires to the respondents who have been specified at the time of planning, for a minimum of respondents depending on the university to be assessed.

The evaluation results using information security index in the form of the dashboard showing the maturity level of information security management.



Steps	Estimation
Information Security Evaluation Planning	1 Week
Literature and Interview Studies	1 Week
Evaluation of ICT Roles	1 Week
Evaluation of Information Security Governance	2 Week
Evaluation of Information Security Risk Management	2 Week
Evaluation of the Information Security Management Framework	2 Week
Evaluation of Information Asset Management	2 Week
Information Technology and Security Evaluation	1 Week
Evaluation Result	1 Week

Figure 4. Estimated Time of Evaluation of Information Security Index

Based on the literature and interviews conducted it can be estimated of the time required to perform an evaluation using information security index. Time estimates are based on the level of difficulty evaluation questionnaire that will be used to estimate the time anyone spent one week there spent two weeks. If the total amount of time required from planning to evaluation result is thirteen week.

IV. CONCLUSION

Based on the description and discussion can be concluded that the concept of information security index can be used to evaluate higher education institutions both private and public. The information security index will determine six areas of ICT Roles, Information Security Governance, Information Security Risk Management, Information Asset Management and Information Technology and Security. In an evaluation using information security index there are nine steps to be taken the first step is planning, second is literature study and interview then six evaluation steps based on the last area is the result of the evaluation, the Estimated time needed to do the assessment is thirteen weeks.

V. REFERENCES

[1] Shirey, R. (2000). Internet Security Glossary: RFC Editor.

[2] Infosecurity. (2011). Elsevier Science Publishers B. V.

[3] Demopoulos, A. (2012). Why do many organizations lack adequate security? Retrieved from http://demop.com/articles/lack-adequate-security.html Davis, C., Schiller, M., & Wheeler, K. (2011). IT Auditing: Using Controls to Protect Information Assets (2 ed.). New York: McGraw Hill.

[4] Sarno, R., & Iffano, I. (2009). Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press.

[5] ISO/IEC. (2005). Information Technology-Security Techniques-Code of Practice for Information Security Management ISO/IEC 17799 (27002):2005. Switzerland.

[6] Wiander, T. (2008). Implementing the ISO/IEC 17799 standard in practice: experiences on audit phases. Paper presented at the Proceedings of the sixth Australasian conference on Information security - Volume 81, Wollongong, NSW, Australia.

[7] Kemenkominfo. (2013). Indeks Keamanan Informasi (KAMI). Retrieved from https://kominfo.go.id/index.php/content/detail/3326/Indeks+Keamanan+Informasi+(KAMI)/0/keamanan_informasi

[8] Isaca. (2012). Cobit 5: ISA.

[9] Davis, C., Schiller, M., & Wheeler, K. (2011). IT Auditing: Using Controls to Protect Information Assets (2 ed.). New York: McGraw Hill.