ISSN PRINT : 2407-4322
ISSN ONLINE : 2503-2933

The Modeling of Information Security Classification With Risk Value Assesment Factor to Good Information Governance on The Indonesia Higher Education Sector

IGN Mantra
Perbanas Institute; Jl. Perbanas, Karet Kuningan, Setiabudi, 021-5252533
Teknik Informatika, Fakultas Teknologi Informasi, Perbanas Institute Jakarta
e-mail: ign.mantra@perbanas.id, ignmantra@gmail.com

Abstract

Digital information is currently dominating the turnover or circulation of information in any institution, whether in government, private sector, universities, Social, Defense and Security, Economy, Politics etc. Almost certainly the information is spearheading the movement of the economy, "who holds the information then he will win the war". Today's Internet era, which is highly sought after by the hackers or crackers and intruders is information, the heart of the information in the database, computer and laptop is not worth more in the eyes of hackers or crackers, hackers either individual or team will try to break through the defense and security information in server , they are vying to be able to obtain important information, and even the most sensitive secrets though. The purpose of the security classification of information is made rating models on levels of sensitivity of the information, with the security classification of information would make the control of the security protection of data and information, the classification will do with risk value assessment factor so that information can be saved away from the hands of scavengers information especially in Indonesia higher education sector.

Keyword : *information security classification; information governance; information security policy; IT security risk management, risk value assessment factor*

Abstrak

Informasi digital saat ini mendominasi pertukaran atau peredaran informasi di institusi manapun, baik di sector Pemerintahan, Swasta, Pendidikan/Perguruan Tinggi, Sosial, Pertahanan dan Keamanan, Ekonomi, Politik dll. Hampir pasti informasi merupakan ujung tombak pergerakan ekonomi, "yang memegang informasi maka ia akan memenangkan perang ". Di era internet saat ini, yang sangat dicari oleh hacker atau cracker dan penyusup adalah informasi, jantung informasi dalam database, komputer dan laptop tidak bernilai lebih di mata hacker atau cracker, hacker baik individu atau tim akan mencoba untuk menerobos informasi pertahanan dan keamanan pada server, mereka berlomba-lomba untuk dapat memperoleh informasi penting, dan bahkan rahasia paling sensitif sekalipun. Penelitian ini bertujuan untuk klasifikasi keamanan informasi dengan dibuat model rating pada tingkat sensitivitas informasi, dengan klasifikasi keamanan informasi akan dapat mengontrol perlindungan keamanan data dan informasi, klasifikasi dihitung dengan dengan faktro penilaian risiko sehingga informasi dapat disimpan jauh dari tangan pemulung informasi terutama di sektor pendidikan tinggi Indonesia.

Keyword : *information security classification; information governance; information security policy; IT security risk management, risk value assessment factor*

1. INTRODUCTION

In the context of information security, information security classification based on the level of sensitivity of the information and the impact if the information is revealed/opened by people who do not have legal authorization so that information can be categorized been a leak of information[6].

There are several approaches to classify the security of informations depends on the country and the institutions do, classification of information on military and security industry is very different from the Banking and Finance Industry including other institutions such as education and health.

Information is necessary to be classified, there are several important reasons behind the classification is as follows:

1. To protect the Personal Information, whoever and wherever citizen to get protection in the law of Information Technology and Electronics, personal information such as Medical Record, Data Banks, detailed data clerks, students are well guarded by the owner of the information system. Moreover, the personal database state officials may not be republished without permission.
2. To protect the information from unauthorized access is allowed, classification restricts information to everyone and not to access parts information indiscriminately, accesses to the database are arranged so that should only be accessible to any interested operator, for example, telephone customer service, banking , hospitals can only access such information with the consent of the customer in front of their screens, and even then only to the extent necessary information, such as saving savings entry, customer database load being complain, customer data load Hospital etc.
3. To protect the intellectual property rights, at the time the information has been generated by the institution, the information relating to the work of individual and institutional copyright must be maintained properly, because copyrighted works is an asset of the company, before it gained recognition as a right of a copyright work, the work of the government should be saved and properly supervised in order not to fall to the competitors and the edges are each claim to the copyright work[2].
4. To protect the leakage of information and dissemination of such information, the information can leak or transfer from one place to another without realizing it and want, at any institution should be able to do well because the classification information is not confidential information carelessly placed and can be stolen by others as well as employees, information has a very high value and can be leaked accidentally or intentionally, recklessly not copy important information into Flash Disk personal and brought to and fro, the probability of lost and forgotten plugged into the computer in general very harmful information in in the flash disk.
5. To provide the facilitation for internal information exchange and integrated services at the time the information is sent / received, information that has been produced by each department should to be interchangeable between departments, with the rules of classification of information is not just information can be sent / received , must go through strict procedures, classification of information is helpful in order not to move information to unauthorized and ends is leaking information to the other party.
6. To protect the information in the form of support for public security and law enforcement, the classification of the information would put the information on the actual place so that the necessary safeguards on who will have access to such information, if there is a violation of misuse of the information classification should be imposed for violations of the law enforcement has been done , such as the classification of information "top secret", should not be just anyone to know that information, it could be nuclear pin, pin cruise missiles, pin chemical bombs, guns and force development

ISSN PRINT : 2407-4322
ISSN ONLINE : 2503-2933

plans, plans transfer of combat equipment, broken equipment and maintenance, the amount of organic weapons and non-organic, document new discoveries, investment, human resources involved etc. must be very concealed its existence.

2. METHODOLOGY

Methodology to be used for this research is a model of constructive research, analysis of important information and sensitive owned by the education sector, making the rating sensitivity of the information security and information security ultimately make a classification of all asset information held by the higher education sector.

The method used in this study is constructive research, conduct studies and calculations that IT risk management has been owned by Higher Education institutions, and then create a security classification of the information in the information security governance.

Analysis of the IT risk management will acquire high risk, moderate and low for information security classification can be made applicable in many institutions university.
Security classification information obtained will clarify which information will be placed on information security classification model conditions suitable for the university.

3. RESULTS AND DISCUSSIONS

The risk assessment is the first phase of the risk management process. The risk assessment aims to determine the threats from the outside that could potentially disrupt the organization's information security and potential weaknesses that may have information on the organization.
Methods of risk assessment consists of six stages:

1. Identification of informations
2. Identification of threats
3. Identify the weaknesses
4. Determine the possible threats
5. The impact assessment
6. The determine of risk value

Information Security classification at Universities in Indonesia did not like with the classification in the Military, so in the University was simplified into four levels namely : **SECRET, CONFIDENTIAL, RESTRICTED dan UNCLASSIFIED,** the framework shows in the fig.1.

Meanwhile, to make information security classification and placement the information in the proper category in the universities should be calculated the informations using Information Technology Risk Management, it has already done in many organizations[1]. Approach to IT Risk Management calculate using methods Qualitative and Quantitative methods, for Qualitative, Risk value is usually determined by the range :

LOW RISK = Risk received minor (0)
MEDIUM RISK = Risk received medium (1)
HIGH RISK = High-risk accepted (2)
SUPER HIGH RISK = Super High-risk accepted (3)

The quantitative methods of risk assessment methods with a mathematical approach. With this method the value of the risk can be calculated using the following formula.
Calculation of the risk with a mathematical approach (1).

Risk value = *NA x BIA x NT* (1)

where:

Asset value	=	*NA (Nilai Asset)*
	=	*NC + NI + NV*
Business Impact Analysis	=	*BIA*
Threat Value	=	*NT*

Calculation :

1. The kind of qualitative information so classification of information security classification is Honor credits per each faculty (Lecturers are not fixed)/file → so, the asset value is LOW RISK (0).
2. The kind of quantitative information so classification of information security classification is ***Mail Server***, *calculation :*

Nilai Ancaman (NT, threats value),
Confidentiality : Internal user only (NC=1)
Integrity : Mayor disturbance (NI=3)
Availability : Very high availability (NV=4)

Nilai Asset (NA, asset value)	*= NC + NI + NV*
	= 1 + 3 + 4
	= 8
Nilai Ancaman (NT)	*= Σ PO x Σ Ancaman*
NT (mail server)	*= Σ PO / Σ Ancaman*
	= 2.1 /6
	= 0.35

Nilai Resiko (NR, risk value),

Asset value (NA)	*= 8*
BIAvalue (BIA)	*= 60*
Threat values (NT)	*= 0.58*

The obtained value of the risk for MailServer:

Risk value (Mail Server)	*=NAxBIAXNT*
	= 8x60x0.58
	= 278.4

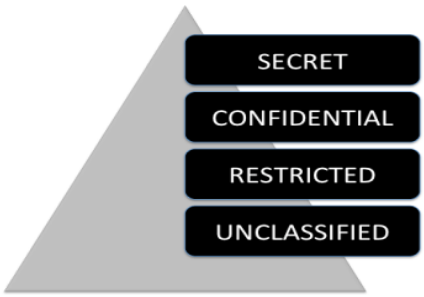

Fig. 1. Information Security Classification Framework for Indonesia Higher Education Sector.

In higher education[7] needs to be compiled first asset owned information such as in list :

a. Diploma Certificate/file
b. Transcript values (values that have been processed)/file
c. Value of raw (unprocessed value) / original value of the lecturer/file
d. Professors Data archive (especially tenured faculty)/file
e. Operating licenses and permits establishment Studies Colleges/file

ISSN PRINT : 2407-4322
ISSN ONLINE : 2503-2933

f. Basic salaries of tenured faculty (energy e.functional) and support personnel/file
g. Honor credits per each faculty (Lecturers are not fixed)/file
h. Computer Laboratory/file
i. Laptop or PC computer structural employees (Rector, Vice Rector, Director, Chairman of the department, BAAK, and finance)/file
j. Computer Server as Web Server, Database Server, Email Server etc.
k. Academic guidelines, final project, and so forth.
l. LCD Projector/file
m. Student and grades database
n. Library books database
o. Books Catalogs
p. Subjects per semester (the curriculum) database
q. Alumni database
r. Student financial database
s. Office inventory database
t. Data extracurricular activities of students database
u. Certificate lecturer in performing community service/file
v. Research Data lecturers/file publications
w. Certificate of accreditation from the BAN PT/file
x. Marketing Information
y. Academic Calender Information
z. ISO 9001:2008 Documentations
aa. Lecturer and Student presence
bb. Employee presence
cc. Project Research
dd. Institution Budgeting

The implementation of the security classification of the information depends on the individual institution, following the author decrypt reset in accordance with the references used in several countries[4], so it can be used as reference material in the Indonesia classification information.
Implementation is divided into several sections such as doing:

1. Labeling
2. Storage
3. Transmission
4. Destruction that has not been used
5. Protecting the integrity
6. Licensing limited access and disclosure
7. Establish accountability

To be able to place the exact position of the critical information necessary to rating based Risk owned by each such information, the risks can be computed qualitative (can not be calculated the value of an information / assets) and quantitative (can be calculated price of an information / assets)[5].
Results perform information security classification of the various asset information in the higher education sector as follows (Table 1).

Table 1 Information Security Classification

Classifications	Asset Description of Information	Information Detail
UNCLASSIFIED	The informations are open to the public, to all university employees and non-employees, to university contractors and subcontractors, agents, etc.	Marketing Information, Lecturer and Student presence Academic Calender Information
RESTRICTED	The informations are limited just to name personnel / team designated course to be open information. Provide limited access for contractors and subcontractors, agents, suppliers, etc.	Books Catalogs Diploma Certificate/file Transcript values (values that have been processed)/file Value of raw (unprocessed value) / original value of the lecturer/file Professors Data archive (especially tenured faculty)/file Operating licenses and permits establishment Studies Colleges/file Computer Server as Web Server, Database Server, Email Server etc. LCD Projector/file ISO 9001:2008 Documentations
CONFIDENTIAL	The informations are very limited to personnel and teams involved only in the access and functionality such information.	Basic salaries of tenured faculty (energy functional) and support personnel/file Honor credits per each faculty (Lecturers are not fixed)/file Computer Laboratory/file Laptop or PC computer structural employees (Rector, Vice Rector, Director, Chairman of the department, BAAK, and finance)/file Data extracurricular activities of students database Certificate lecturer in performing community service/file Library books database Project Research Institution Budgeting Research Data lecturers/file publications Employee presence
SECRET	The informations are very limited only to a few personnel are allowed access to such information.	Student and grades database Student financial database Office inventory database

The Information security classification for the type qualitative classification as follows :

UNCLASSIFIED = LOW RISK (0)
RESTRICTED = MEDIUM RISK (1)
CONFIDENTIAL = HIGH RISK (2)
SECRET = SUPER HIGH RISK (3)

ISSN PRINT : 2407-4322
ISSN ONLINE : 2503-2933

After the making of the information security classification we can make a classification matrix based on categories and the planning application to be made to follow the standard Information Security clasification agreed and defined by each institution[7].

Table 2 Risk Value Factor Calculation

No.	Descriptions	NA	BIA	NT	NR
		Asset Value		Threat Value	Risk Value
1	Diploma Certificate/file	6	40	0.30	72.00
2	Transcript values (values that have been processed)/file	9	30	0.40	108.00
3	Value of raw (unprocessed value) / original value of the lecturer/file	3	6	0.32	5.70
4	Professors Data archive (especially tenured faculty)/file	4	6	0.35	8.40
5	Operating licenses and permits establishment Studies Colleges/file	2	4	0.27	2.13
6	Basic salaries of tenured faculty (energy functional) and support personnel/file	4	20	0.35	28.00
7	Honor credits per each faculty (Lecturers are not fixed)/file	4	20	0.35	28.00
8	Computer Laboratory/file	3	6	0.32	5.70
9	Laptop or PC computer structural employees (Rector, Vice Rector, Director, Chairman of the department, BAAK, and finance)/file	7	60	0.45	189.00
10	Mail Server	8	60	0.58	280.00
11	Academic guidelines, final project, and so forth.	3	6	0.27	4.80
12	LCD Projector/file	2	4	0.25	2.00
13	Student and grades database	12	100	0.65	780.00
14	Library books database	4	20	0.35	28.00
15	Books Catalogs	4	10	0.35	14.00
16	Subjects per semester (the curriculum) database	6	40	0.37	88.00
17	Alumni database	6	40	0.37	88.00
18	Student financial database	11	80	0.62	542.67
19	Office inventory database	6	30	0.38	69.00
20	Data extracurricular activities of students database	5	30	0.37	55.00
21	Certificate lecturer in performing community service/file	5	20	0.37	36.67
22	Research Data lecturers/file publications	9	60	0.40	216.00
23	Certificate of accreditation from the BAN PT/file	5	8	0.37	14.67
24	Marketing Information	1	4	0.17	0.67
25	Academic Calender Information	3	4	0.25	3.00
26	ISO 9001:2008 Documentations	6	20	0.37	44.00
27	Lecturer and Student presence	3	6	0.25	4.50
28	Employee presence	3	6	0.25	4.50
29	Project Research	10	60	0.58	350.00
30	Institution Budgeting	10	60	0.58	350.00

Protecting the integrity of information

The integrity of information is protected so that information remains current, complete and unchanged (as original), information is accessed and stored in the system information with the principle of "right", so the extent to which user rights to perform "modify" (edit, insert, delete) or "read only". Significant threats to the integrity of that file are stored in a "read only", to modify the file can only be done by the creator of the course, control access rights to the file is set based on user accounts and workgroups as well as physical access to special equipment, while file/ document transfer its integrity must be maintained because it could be a document intercepted by others who are not entitled. To maintain the integrity of many enterprise do encryted to files/ documents are "restricted" when it is transmitted to the other party or stored somewhere.[5]

The most important thing is the integrity of access control to files/documents to be opened/read, track logs anybody who has opened and transmits the file to the other party, of course file "encrypted" is much safer than clear text transmission. Here is the implementation of Integrity protects information as (Table 3) :

Table 3 Information Security Classification and Audit Works

Classifications	Access Restrictions	Audit Works
UNCLASSIFIED	Access to informations are open to the public, to all university employees and non-employees, to university contractors and subcontractors, agents, etc.	No audit file
RESTRICTED	Access to informations are limited just to name personnel / team designated course to be open information. Provide limited access for contractors and subcontractors, agents, suppliers, etc.	Files/documents audit periodically monthly or per 4 months. Read log files/documents that have been accessed by personnel/teams.
CONFIDENTIAL	Access to informations are very limited to personnel and teams involved only in the access and functionality such information.	Files/documents audit periodically per day / per week to make sure the files maintained confidential. Read access log file, who and what authorize to opening.
SECRET	Access to informations are very limited only to a few personnel are allowed access to such information.	Files/documents periodically per day / per week to file make sure awake "secret". Read access log file anyone who has access. Replace the passwords and periodically conduct to encrypt the file/documents.

ISSN PRINT : 2407-4322
ISSN ONLINE : 2503-2933

Classification of Information Security Logic Flow Chart (Fig. 2)

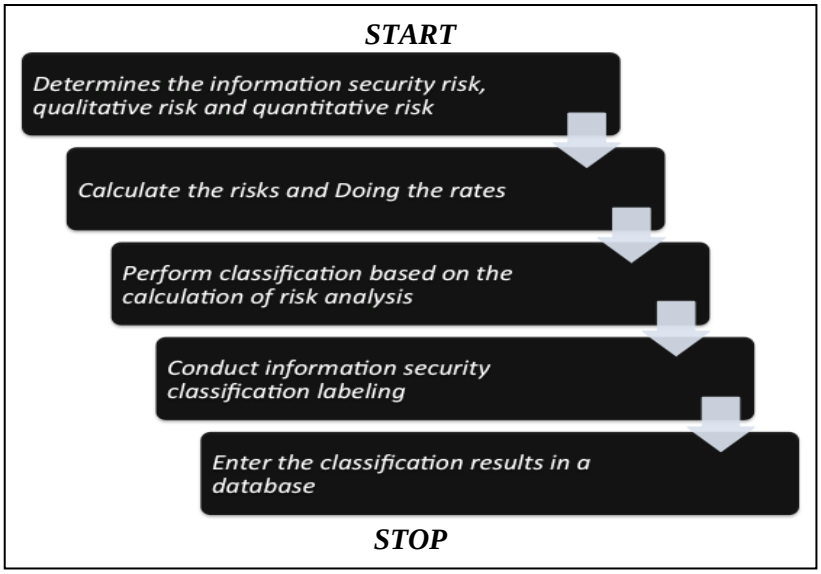

Fig. 2. Classification of Information Security Logic Flow Chart

This flow chart (Fig. 2) to determine the risk of information security, calculate the risks and doing the rating results of the risk analysis. After that perform the security classification of information security risk analysis, and then conduct a security classification labeling and enter this information in a database[8].

Handling and Processing the Information

Important to have a good set of procedures to determine the marking and handling of information in accordance with the classification scheme used by the organization. This procedure should include both physical assets and information in electronic format. For each classification, handling procedures should be established, including the following types of information processing operations like, labeling, storage, delivery, archieve and destruction.

Output from systems containing information classified as confidential or important classification should be marked. Flagging generally shaped mark physical. However, some information assets such as documents in electronic format, can not be marked as physical and electronic tagging should be used.

4. CONCLUSIONS

Classification of Information Security, especially in higher education are needed to secure the information itself and makes it easier to access later in the file / document that has been classified. So much vital of information assets as confidential and highly valuable to be protected. The most important of the classification information is anyone who should not open anything, not just anyone should open up and reveal confidential information. In any country in the world there must be a file / document "State Secrets" and no documents to "Public", of course, confidential documents and must not be disclosed to the public and it is not a secret document. The latter is the shared commitment to save the security classification of the information, if there is no commitment and the rule of law there is no point in doing and protect the informations.

5. SUGGESTION

This research is still preliminary research, to continue this research required list / register asset information that much more can be collected by the university, and then save the first asset information to be calculated the value of its risks, low, medium, high risk and super high risk more detail again, and the next is made application that can automatically classify the security classification of information by the system, member labels and can be stored on server. Without a good application it will be impossible to do this manually classification.

THANK YOU

The author would like to thank the institution where I work and shelter for nearly 20 years, Perbanas Institute. Thanks to the Rector and Dean that provide strong support to the author in terms of funding. Thanks also to colleagues who have helped and provide references to the improvement of this publication. There is no ivory that is not cracked, for their mistakes will make us learn again to correct the error. Hopefully, this publication can help to improve national information security in the Homeland and can be upgraded according to the science of information security, in order to increase knowledge to further the advancement of knowledge among fellow educators both in Jakarta and in the entire country of Indonesia. Thus this publication may be beneficial to all.

REFERENCES

[1] AlBone, A. 2010, PEMBUATAN RENCANA KEAMANAN INFORMASI BERDASARKAN ANALISIS DAN MITIGASI RISIKO TEKNOLOGI INFORMASI. *Jurnal Informatika*, *10*(1), 44-52.

[2] Calder, A. 2011, *Implementing Information Security based on ISO 27001/ISO 27002*. Van Haren.

[3] Clark, D. D., & Wilson, D. R. 1987, April, A comparison of commercial and military computer security policies. In *Security and Privacy, 1987 IEEE Symposium on* (pp. 184-184). IEEE.

[4] Dewi, I. K., Fitroh, F., & Ratnawati, S. 2015, USULAN MANAJEMEN RISIKO BERDASARKAN STANDAR SNI ISO/IEC 27001: 2009 MENGGUNAKAN INDEKS KAMI (KEAMANAN INFORMASI) STUDI KASUS: BADAN NASIONAL PENEMPATAN DAN PERLINDUNGAN TENAGA KERJA INDONESIA (BNP2TKI). *SISTEM INFORMASI*, *8*(1).

[5] Eloff, J. H., & Eloff, M. 2003, September, Information security management: a new paradigm. In *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology* (pp. 130-136). South African Institute for Computer Scientists and Information Technologists.

[6] Mohammadian, M., & Hatzinakos, D. 2009, Data classification process for security and privacy based on a fuzzy logic classifier. *International Journal of Electronic Finance*, *3*(4), 374-386.

ISSN PRINT : 2407-4322
ISSN ONLINE : 2503-2933

[7] Rozas, Indri Sudanawati, Rozas, Sarno, Riyanarto Sarno. 7 Agustus 2010, "Bayesian Probabilistik Sebagai Pendekatan Heuristic Untuk Manajemen Resiko Teknologi Informasi", Prosiding Seminar Nasional Manajemen Teknologi XII, Program Studi MMT-ITS, Surabaya, pp. c-9-2—c-9-8.

[8] Ryana, H., & Rahardjo, B. Kajian ISO/IEC 17799: 2005 Sebagai Kerangka Dasar Pengendalian Keamanan Informasi.