Analysis Risk Assessment on Village Information System using OCTAVE Allegro Framework

Agung Nur Maghribi
Department of Information System
UniversitasAhmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
UniversitasAhmad Dahlan
Yogyakarta of Indonesia

ABSTRACT

The Village Information System or commonly known as SID is an application used to manage village government data, can be interpreted as IT-based applications and processes to manage information related to the village office, support the duties and functions of the village office. SID allows for risks that can interfere with information assets and organizational goals. This study uses the OCTAVE Allegro framework with the aim of analyzing risk assessment and choosing a mitigation approach to the risks that may occur. The OCTAVE Allegro risk assessment method is divided into eight steps, namely establishing risk measurement criteria; developing information asset profiles; identify containers of information assets; identify areas of concern (problem areas) on technical, physical, and people container aspects; identify threat scenarios; identify risks; analyze risk; choose a mitigation and control approach that is adjusted to the results of the relative risk score calculation. Based on the test results on the Village Information System (SID), the results of the mitigated approach are 4, accept is 2, and defer is 2, with a relatively high risk value found in Physical Container with a risk value of 29, namely due to natural disasters that caused SID services (Village Information System) stops. While the relatively low risk value is found in Technical Containers with a total of 15, which is caused by interference with internet connectivity so that the SID (Village Information System) service stops temporarily.

Keywords

Village Information System, Risk Assessment, OCTAVE Allegro, Mitigation.

1. INTRODUCTION

The development of information technology has undergone significant changes which have begun to become the main support for the success of an organization. This also affects the existing processes in the Government where services to the community must be provided more optimally by utilizing information technology. Kalurahan is the spearhead of government that is very close to the community which directly handles services to the community, the village has the task of regulating, managing resources in government at the village level and has an obligation to carry out population administration as a form of service to the community.

In carrying out public services, the Baturetno village district utilizes the Empowered Village Information System application. The Village Information System can be defined as a computer-based application and process for managing information related to the village office, supporting the duties and functions of the village office, related to population administration, reporting, planning, asset management, public services, budget management, and so on. Through the Village Information System, village offices become more effective and efficient in carrying out their duties and functions properly. Considering the main task of the village office itself is to provide services to the community, so that this function can work better. The use of the system widely must be realized the importance of information system security which aims to protect confidential data, personal information, misuse of data, and interference with the system.[9]

One of the methods used for information technology risk management and analysis is OCTAVE (Operationally Critical Threat, Assets and Vulnerability Evaluation). OCTAVE was developed by the Software Engineering Institute (SEI) of Carnegie Mellon University. OCTAVE is a set of tools, techniques and methods for risk-based information system security assessment and planning. OCTAVE has three variants, namely OCTAVE, OCTAVE-S and OCTAVE Allegro. The method that is used as a reference in this research is the OCTAVE Allegro framework. OCTAVE Allegro is a simplified method with a focus on information assets, it can be done with a workshop-style and collaborative method. OCTAVE Allegro is slightly different from other Octave approaches, because this framework focuses on information assets owned by an organization or company in the context of how these assets are used, their storage, movement, processing and how (threats), vulnerabilities and disruptions can occur in assets. that

2. LITERATURE STUDY

2.1 Definition of Information System

Systems are technically a set of five interrelated components that have the function of collecting (retrieving), processing, storing, and distributing information to support decision making and as control within the organization. In addition to supporting decision making, coordination and control, information systems can also help managers and workers analyze problems, visualize complex subjects and create new products.[4]

2.2 Types of Information Systems

There are several types of information systems including:[8]

a. Executive information system, an information system designed to provide information that is easily understood by executives and managers to make strategic plans, monitor business and economic conditions, identify business opportunity issues and make various decisions.
b. Decision support systems, namely information systems that are built to help users make decisions in an unstructured environment where the degree of uncertainty is high.

c. Expert system, this system contains the knowledge and expertise of experts in their respective disciplines.
d. End user systems are information systems built by users to meet their own information needs.

2.3 Characteristics Information System

systems have three general characteristics, namely:[22]

a. Communication networks, information systems are similar to a communication network because they both provide information for various parties, inside and outside the company.
b. Having stages and data conversion, information systems convert inputs into outputs. There are three stages in this change or transformation, namely the input stage, the processing stage or processing stage and the power stage
c. Data input and information output, various data are entered for processing during the input stage while information is presented during the output stage.

2.4 Village Information System

The Village Information System or commonly referred to as SID is an application used to manage data in the village can be interpreted as a computer-based application and process to manage information related to the village office, support the duties and functions of the village office, related to population administration, reporting, planning, asset management, public services, budget management, and so on.[17]

2.5 Information System Security

Information Security is safeguarding information from all threats that may occur in an effort to ensure or guarantee business continuity, minimize business risk (reduce business risk) and maximize or accelerate investment returns and business opportunities. [7]

In designing a good information security system, there are aspects of information security that must be considered. As for the information security aspect, there are three things described by the CIA Triad as Figure 1.[7]

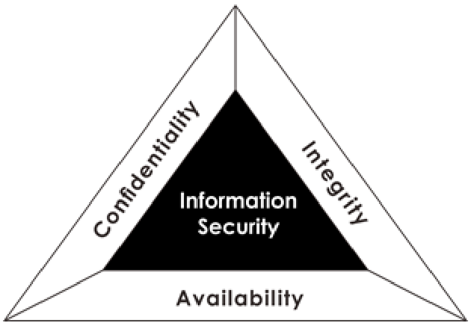

Figure 1.CIA Triad

2.6 Definition of Risk Management

Risk management is defined as a practical activity of identifying, assessing, controlling, and mitigating risks. Implementation of risk management is an organizational stage in identifying and viewing risk sources, risk vulnerabilities in a comprehensive and controlled manner by carrying out continuous process evaluations [12] Risk management is basically carried out through a process of risk identification, risk evaluation and measurement and risk management. Organizations often deliberately optimize risks because they see the potential benefits of these risks, on the other hand, if the organization cannot take risks, it is certain that the organization cannot develop.[13]

2.7 OCTAVE Allegro

Method The OCTAVE method, which stands for the Operationally Critical Threat, Asset, and Vulnerability Evaluation, is a set of tools, techniques, and methods for assessing risk-based information security strategies and planning. The OCTAVE method consists of three basic principles of security administration, namely: confidentiality, integrity, and availability (Pandey & Mustafa, 2012). The OCTAVE Allegro assessment method conducted by Carnegie Mellon University Software Engineering Institute (SEI) which has the ability to provide robust risk assessment results, with a relatively small investment in time and resources, even for organizations that do not have adequate risk management expertise. area (Keating. 2014). There are eight steps contained in the OCTAVE Allegro method as shown in Figure 2 [6]

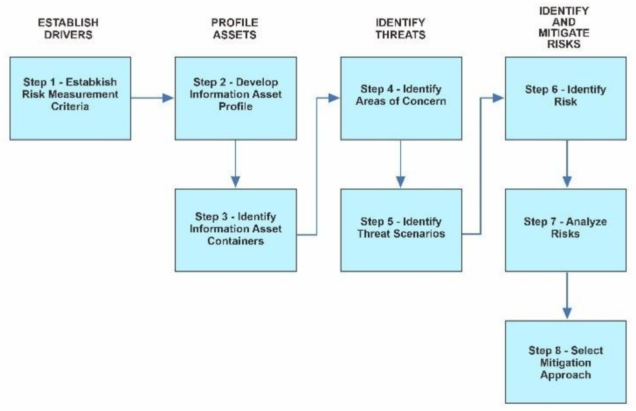
ESTABLISH DRIVERS
PROFILE ASSETS
IDENTIFY THREATS
IDENTIFY AND MITIGATE RISKS
Step 1 - Estabkish Risk Measurement Criteria
Step 2 - Develop Information Asset Profile
Step 3 - Identify Information Asset Containers
Step 4 - Identify Areas of Concern
Step 5 - Identify Threat Scenarios
Step 6 - Identify Risk
Step 7 - Analyze Risks
Step 8 - Select Mitigation Approach

Figure 2.OCTAVE Allegro steps

3. METHODOLOGY

In this research, several stages of the research process were used to collect the required data. The stages are divided into the following sub-chapters:

1. Observation
   The observation method is a way of collecting data by direct observation and recording by making direct visits to the Village Office of Baturetno Village. Doing questions to the IT department regarding the information system process at the Baturetno Village Office. One of the information systems used is the Village Information System (SID), so observations are made regarding the information system used.
2. Interview
   data collection technique by communicating with related parties on information or information obtained previously by asking direct questions to related parties at the village office of Baturetno Village. The interview process was carried out to obtain information on the preliminary study and collect data from respondents for each step to be taken.
3. Literature Study
   Searching for various written sources or looking for theoretical references that are relevant to the cases or problems found. These references can be found from books, journals, research report articles and websites on the internet. In this study, the literature study used is

related to references related to research, namely risk management and the risk assessment method used is theframework OCTAVE Allegro.

4. Questionnaire
   Do some questions given to respondents to be filled in and then developed to the researcher. The questionnaire that will be used in the study uses a reference based on the OCTAVE Allegro method.

4. RESULTS AND DISCUSSION

The stages of risk assessment that will be carried out in the Village Information System will refer to the 4 stages and 8 stages that exist in Octave Allegro, namely:

1. **Step 1 Determine the Risk Assessment Criteria**

This step is to build organizational drivers reflected in a series of risk measurement criteria. In this step, there are two activities, as follows:

In activity 1.1, establish a series of qualitative measures (risk measurement criteria) that are used to evaluate the impact of significant risks on the organization. Determine the impact area to identify the extent of the risk impact. The selected impact areas are:

a. The impact of risks posed by citizens on the reputation and trust of institutions is related to risk.
b. The impact of risk on operational costs that must be incurred from the institution is related to risk.
c. The impact of risks posed on the productivity of services in the Baturetno sub-district. This is also related to technicians ensuring the services provided run well.
d. Impact on the area of safety and health on users when there is a risk.
e. Sanctions will be given if there is a risk of violation or fraud committed by user administrators or employees

In the second activity, the priority value is given to each impact area on a scale of 1-5, starting from the most important, the highest scale is 5 and the least important will be get the lowest scale, namely 1. Then the determination of the impact area affected can be concluded as table 1

Table 1Impact Area Prioritization

Allegro Worksheet 7	Priority Score Worksheet Impact Area
Priority Score	***Impact Areas***
4	Reputation and Trust Customers
3	Finance
5	Productivity
1	Security and Health
2	Fines and penalties

The first priority is productivity with a priority score of 5 because it involves services to employees and the community. How can admins or village officials ensure that SID services can run well and without any disturbance, because productivity can affect the comfort and satisfaction of employees and the community as users. The second priority is the reputation and trust of the customer user with a priority score of 4, because it is related to the reputation and trust of the customer. If reputation and trust are reduced, the intensity of using SID can decrease, and it will have an unfavorable impact on SID. The third priority with a score of 3 is financial because it relates to the cost of maintaining the system and replacing the equipment when needed to ensure the equipment can run properly according to its function. The fourth priority is fines and legal sanctions, but this happens so rarely or never happens that there are almost no rules regarding fines and legal sanctions. The fifth priority is safety and health with the last priority because there has never been a risk that affects security and health that can affect SID so far.

2. **Step 2 Identifying Information Asset Profiles**

At this stage, identification is carried out by identifying a collection of important information assets, identification is obtained from the identification of Village Information System service business processes. The information assets that can be found in this study can be seen in the critical asset profile in table 2.

Table2.Critical Information Asset Profile

Allegro Worksheet 8	CRITICAL INFORMATION ASSET PROFILE	
(1) Critical Asset What is information asset aset critical?	**(2) Rationale for Selection** Why areassets information important in organizations?	**(3) Description** What is the description of theasset information that?
Population Data andservices licensing correspondencewhich in there are (Name, NIK, KK) of residents	Population data is very important because the data contains the name, NIK, KK of residents and letters. Therefore, if the data is lost or damaged, it will disrupt the business processes in the Village Information System (SID)	Population data is individual or aggregate data that is structured as a result ofregistration populationand civil registration activities
(4) Owner (s) Who owns the assets that information?		
Communication and Information Office of Bantul Regency and Baturetno Village		
(5) Security Requirements What are the security requirements for information assets?		
Confidentiality	Maintain the confidentiality of data access rights from unauthorized parties and maintain the confidentiality of data information. Only registered users can access the entire data.	
Integrity	Maintain data so that it remains integrated so as not to experience changes or modifications to data from any party, unless you receive instructions to make changes from the person concerned if you experience problems.	
Availability	Data can only be accessed within the Baturetno sub-district office	

(6) Most Important Security Requirement What are the most important security requirements for the information asset?		
Confidentiality	✓**Integrity**	Availability

Based on the results of the process of identifying and profiling against critical information systems in Table 2 which explains that requipment security of information systems assets at layananan Village Information System (SID) of the most important is the integrity (integrity). Population data is critical data in the village information system because it contains various important information related to population data, the information in question starts from (name, address and age), for that it is very important to have integrity so that data is not easily lost or modified by unauthorized parties. to be responsible. However, other security needs are equally important to maintain functionality and prevent security from being compromised.

3. Step 3 Identifying Information Asset Containers

The third step in this research is to identify information assets through the interview stage, the process of identifying information asset containers has 3 containers namely, technical, physical, and people, each identified container has internal and external sides. . The results of the interview, it can be seen that the summary of the technical forum focuses on the server network and infrastructure managed by the Baturetno district. Then the physical container focuses on the physical assets in the Baturetno sub-district that are used to manage services, then the people forum focuses on the people in the Baturetno sub-district, both internally and externally.

4. Step 4 Identifying Areas of Concern

The fourth step is to identify related areas of concern, which is divided into three parts, namely technical (TC), physical (Phc) and people (PC). In this step, it then describes a descriptive statement in detail about the conditions in related agencies that can affect assets in the Village Information System (SID) as shown in table 3:

Table3.Area of concern

No	Area of concern	Code	Security Requirments
Technical Container			
1	Discontinuation of Baturetno SID service due to disruption of Internet connectivity	TC-1	1) Avaibility
2	Disruption of Baturetno SID service due to system equipment being updated/repaired	TC-2	1) Avaibility
3	Disruption of SID (Village Information System) serviceBaturetno's because the server is down	TC-3	1) Avaibility
4	There is a gap in system security that can be accessed by unauthorized parties	TC-4	1) Confidentiality 2) Integrity
5	disruption Servicedue to a crash on the service system or operating system.	TC-5	1) Avaibility
Physical Container			
6	The occurrence of natural disasters or environmental threats causes services to stop	PhC-1	1) Avaibility
People Containers			
7	Errors in data input by employees oradministrators	PC-1	1) Confidentiality 2) Integrity 3) Avaibility
8	Distributed access rights (username and password) administrator as a result ofsocial engineering	PC-2	1) Integrity

5. Step 5 Identifying Threat Scenarios

The fifth step will clarify threats that occur in each area of concern by identifying threat scenarios to determine the effect of risk on information assets, the identification process is carried out using several scenarios of questionary questions as referred to in "Appendix C Threat Scenarios Questionaries 1 - 3" which consists of 3 types of containers, namely technical, physical, and people.

Technical service containers can cause software damage, then system crashes can occur, either way g the cause is known or not so that it causes interference, hardware damage occurs which causes disruption of the service process, there is malicious code such as (virus, Trojan horse, or back door) that can cause damage or loss of information assets will cause disruption and disruption to the process services due to problems related to telecommunications (network). Furthermore, in technical facilities, attacks can occur by irresponsible parties and cause the disclosure of usernames and passwords and can lead to disasters, both caused by nature and by humans (such as floods, fires, earthquakes, explosions, etc.) . Further in the physical container there are no situations that could cause the service infrastructure to be damaged or lost. Then there is social engineering obtained from internal agencies by outside parties so that usernames and passwords can be revealed that can be misused. So it can be concluded that the container that contains the most threats is the technical container.

6. Step ke-6 Identifying Risks

In this step, we start by calculating the number of impact area scores by looking back at the risk measurement criteria that have been obtained in Step 1. How to calculate totalscore for each impact area is multiplied by the impact area value obtained in table 4.8.

The way to calculate the score for each impact area is as follows:

a. If the value or value in the impact area is low, then the value of the value of priority is multiplied by the number 1.

b. If the value or value in the impact area is of medium value, then the value of the value of priority is multiplied by number 2.

c. If the value or value in the impact area is high, then the value of the value of priority is multiplied by number 3.

Furthermore, the results of the calculation of the score for each impact area can be seen in table 4

Table4.Skor Impact Area

Impact Areas	**Value Of Priority**	**Impact Score**		
		Low (1)	**Medium (2)**	**High (3)**
Productivity	5	5	10	15
Reputation and Trust	4	4	8	12
Financial	3	3	6	9
Fines and Penalties	2	2	4	6
Safety and Health	1	1	2	3

7. Step-7 Analyzing Risks

This step analyzes the total risk from the results of steps 4, 5, and 6. Perform a simple quantitative calculation of the extent to which the organization is affected by threats. This relative risk score is obtained by considering the consequences of risk impacting the organization. This is done by quantifying the risk assessment criteria of stage 1. The results of this quantification is called relative risk score that is obtained by calculating a score for each area of impact by multiplying the value area of impact with the impact area priority value obtained from the order of priority is made in step 1.

Next analyze the total number of risks in all areas of concern which are the result of identifying threats previously by creating profiles and then determining the pool in each risk profile in the risk areas of concern using Allegro Worksheet 10 as shown in table 5.

Table 5. Order of Risk-Based on Total Risk Score

Code	***Areasof Concern***	**Reputation and Trust *User***	**Financial**	**Productivity**	**Safety and health**	**of fines and legal sanctions**	**Total Risk Score**	**Probes**	**Mitigation Approach**
TC-1	SID (Village Information System) service Termination of Baturetno'sdue to interference with Internet connectivity	Low (4)	Low (3)	Low (5)	Low (1)	Low (2)	15	**Low**	*Accept*
TC-2	Disruption of SID (Village Information System) service) Baturetno because the system equipment is being updated/repaired	Low (4)	Low (3)	Low (5)	Low (1)	Low (2)	15	**Low**	*Accept*
TC-3	Disruption ofSID (Village Information System) service Baturetno'sbecause the server is down	Low (4)	Low (3)	High(15)	Low (1)	Low (2)	25	***High***	*Defer*
TC-4	There is a gap in system security that can be accessed by unauthorized parties	*Medium(8)*	Low (3)	Low (5)	Low (1)	Low (2)	19	***Medium***	*Mitigate*
TC-5	Servicedue to a crash on the service system or operating system.	*Low (4)*	*Low (3)*	High (10)	Low (1)	Low (2)	20	**Medium**	*Defer*
PhC-1	natural disaster or environmental threat causes the service to stop	*Medium(8)*	*Low (3)*	High (15)	Low (1)	Low (2)	29	***High***	*Mitigate*
PC-1	Error inputting data by the employee or Administrator	*Medium(8)*	Low (3)	Low (5)	Low (1)	Low (2)	19	***Medium***	*Mitigate*
PC-2	Distribution ofaccess rights administrator(username and password) as a result of social engineering	*Medium(8)*	Low (3)	Low (5)	Low (1)	Low (2)	19	***Medium***	*Mitigate*

After the risks are arranged based on the total risk score, the next step is to group the number of threats in each container which serves to make it easier to carry out mitigation which can be seen in table 6.

Table 6. Grouping Number of Threats

Mitigation Approach	Technical Container (TC)	Physical Container (PhC)	People Container (PC)
Mitigate	1	1	2
Defer	2	0	0
Accept	2	0	0
Total	**5**	**1**	**2**

The results in the table of grouping the number of threats above show that technical containers have the most threat risk with a total threat risk of 5. While physical containers have 1 threat risk and 2 people containers

8. Step-8 Choosing an Approach Mitigation

Step 8 in OCTAVE Allegro is choosing a mitigation approach. The mitigation approach can be done bygrouping each identified area of concern based on the relative risk score in the previous table. The results of the recommendations for the mitigation plan are reducing the threat risk based on the areas of concern which can be seen in table 7

Table 7. Grouping based on the Mitigation Approach Mitigation

Mitigation Approach	Kode	*Area of Concern*	Rekomendasi
Mitigate	TC-4	There is a gap on security system that can accessed by party who does not Authorized	Use features block if it happens error enter username and repeated passwords times, as well as encrypt password so as not exposed in aringan
	PhC-1	Occurrence natural disasters or threats environment cause service stopped	Performing backup data periodically so that the data is saved safely and when it happens natural disaster data that lost or damaged can be recovered
	PC-1	Error data input by party employee or administrator	Efforts that recommended for To do recheck before doing submit to system so that it doesn't happen input error which will result to data population
	PC-2	Spread of rights access (username and passwords) administrator as a result of happening	Suggested attempt to solve this problem is to add 2-step verification which requires password and verification code to login system.
Defer	TC-3	Disruption of theSIDBaturetno(Village Information System) service because the server is down	Server down often occurs due to a sudden power outage, the recommended effort, the Baturetno village party provides or uses backup power backup (genset)
	TC-5	Disruption of services due crashes on the service system or operating system.	Efforts to control and check computers or networks on a regular basis.
Accept	TC-1	SID Termination of Baturetno's (Village Information System) service due to Internet connectivity disruption	Selection of a network provider that can ensure smooth internet connectivity in the SID service process.
	TC-2	Disruption of SID Baturetno's(Village Information System) service due to system equipment being updated/repaired	Control and periodically check the computer or system outside of working hours so that the service process is not disrupted.

Based on the results from table 7 it can be seen that the mitigate approach is carried out in the area of concern with codes TC-4, PhC-1, PC-1 and PC-2, defer approach is carried out in the area of concern with code TC- 3, and TC-5 and the accept approach is carried out in the area of concern with codes TC-1, and TC-2.

5. CONCLUSION

1. The risk assessment of the SID (Village Information System) service in Baturetno Village is carried out by following the steps contained in the Octave Allegro method guide, starting with determining and defining the impact area in the information asset, then determining the critical assets of the information asset, identifying container of information assets consisting of Technical Container (TC), Physical Container (PhC) and People Container (PC), determine the threat of each container and determine the severity of the risk and make recommendations for mitigation of each threat that occurs.

2. Based on the results of the tests carried out on the Village Information System (SID) service in Baturetno Village, it was found that theapproach was mitigated 4,

defer was 2, and accepted was 2. Therisk value is relatively highin Physical Container (PhC) with a total risk value of 29, namely due to a natural disaster that caused the SID service to stop. Therisk value is relatively lowin the Technical Container (TC) with a total risk value of 15, namely due to internet connectivity disruptions so that SID services are disrupted or temporarily stopped

6. REFERENCES

[1] Australian Government Publishing Service. 1994. Style manual for authors, editors and printers (5th ed.). Canberra: Writer.

[2] Azhari, I., & Rahman, A. May 2005. Detection of circles in digital images using Sobel filter and Hough transform. Expert, 6(1), 25-32.

[3] Aristasari, P. and Riadi, I. (2011) 'Risk Management in Learning Management System Using OCTAVE Allegro Framework', pp. 1–15.

[4] Bohrer, S., Zielke, T., & Freiburg, V. 1995. Integrated obstacle detection framework for intelligent cruise control on motorways. Presentation paper at the IEEE Intelligent Vehicles Symposium. Detroit, MI: Piscataway.

[5] Brookshear, JG 2003. Computer science: An introduction (7th ed.), Trans. Computer science: An overview (7th ed.), I. Hardiansyah (Pen.), HW Hardiani (Ed.). Jakarta: Erlangga.

[6] Caralli, RA, Steven, JF, Young, LR, & Wilson, RW 2007. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. USA: Software Engineering Institute Carnegie Mellon University Alberts, Christopher, &Dorofee, A. 2005. OCTAVE Method Implementation Guide. PA: Software Engineering Institute, Carnegie Mellon University.

[7] DeHart, GB, Alan SL, & Cooper, RG 1995. Child development: Its nature and course (4th ed.). Boston: McGraw-Hill.

[8] Effendi, BD 2007. Application of object-oriented programming methods to build a lecturer activity agenda system using PHP 4. Informatics Dynamics, 1 (1), 53-67.

[9] Finnegan, D., M. 2006. E-Learning success: Readability versus reading skill [Electronic version]. International Journal of Instructional Technology and Distance Learning, 3 (10), 37-47.

[10] Friedman, SL, &Wachs, TD (Ed.). 1999. Measuring environment across the life span: Emerging methods and concepts. Washington, DC: American Psychological Association.

[11] Kristanto, A. 2003. Data structure with C++. Yogyakarta: GrahaIlmu. Prajanti, AD, &Krisnadi, I. 2016. Project Management Review on Implementation of Electronic Service Manuscripts in Indonesian Government Towards Bureaucratic Reform. Thesis. Faculty of Electrical Engineering. University of Indonesia: Jakarta.

[12] Kurniawan, Y. April 2007. KOffice: Alternative Office Tools on Linux. Computer Info, p. 142-143.

[13] Security Holes in Firefox. April 2007. Computer Info, p. 84.

[14] Merceron, A., &Yacef, K. May 2005. TADA-Ed for educational data mining. Interactive Multimedia Electronic Journal of Computer-Enhanced Learning, 7 (1). Retrieved April 30, 2007, from http://imej.wfu.edu/articles/2005/1/03/index.asp

[15] NAACP. April 29, 2005. NAACP supports Congressional fight to end predatory lending. Retrieved August 19, 2005, from http://www.naacp.org/inc/docs/washington/109/109_aa-2005-04-28.pdf

[16] Nielsen, J., & Loranger, H. 2006. Prioritizing the Web Usability. Berkeley, CA: New Riders.

[17] Oxford learner's pocket dictionary. 2003. New York: Oxford University Press.

[18] Purwadi, E., &Istiyanto, J., E. 2005. SMS-based remote temperature monitoring device. In Ardiansyah, E. Aribowo, &Hasanudin (Ed.), Proceedings of the 2005 National Informatics Seminar (pp. 317-320). Yogyakarta: Informatics Study Program, Ahmad Dahlan University.

[19] Ramadiani. 2005. Measuring the success of information systems using information user satisfaction indicator variables and structural equation model in LISREL (Case study at UPT Library ITB). Thesis, Computer Science, Gadjah Mada University, Yogyakarta.

[20] Wareham, J., Zheng, JG, & Straub, D. February 2005. Critical themes in electronic commerce research: A meta-analysis. Journal of Information Technology, 20(1), 1-19.

[21] Wibowo, HS 2006. Modeling analysis and design of object-oriented systems using UML (Case study of lecture scheduling information system FMIPA-UAD). Thesis, Computer Science, Ahmad Dahlan University, Yogyakarta.

[22] Winograd, T. 1997a. From computing machinery to interaction design. In P. Denning & R. Metcalfe (Ed.), Beyond calculation: The next fifty years of Computing (pp. 149-162). Amsterdam: Springer-Verlag.

[23] Winograd, T. 1997b. Understanding computers and cognition. Norwood, NJ: Addison-Wesley. Kang, Y., & Liu, R. (2016). Development of a rail-breaking risk management information system. 3rd International Conference on Systems and Informatics (ICSAI) (pp.492-496). Shanghai China: IEEE.

[24] Ikhsan, Hidayatul and Nanda Jarti. 2018. Information Technology Security Risk Analysis Using Octave Allegro. Responsive Journal, 2(1), 31-41.