Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 161 (2019) 1206–1215

Procedia Computer Science

www.elsevier.com/locate/procedia

The Fifth Information Systems International Conference 2019

Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency

Muhamad Al Fikri[a], Fandi Aditya Putra[b], Yohan Suryanto[a], Kalamullah Ramli[a,*]

[a]*Universitas Indonesia, Jakarta, Indonesia*
[b]*Badan Siber dan Sandi Negara, Jakarta, Indonesia*

Abstract

Risk management is a practical step in handling risk scenarios in an organization, including in the field of information security. There are many techniques used to carry out information security risk assessments. One of them is a combination technique using ISO 27005 and NIST SP 800-30 revision 1. Previous research proved that the combination technique could be implemented in a non-profit organization (government). However, the detailed risk assessment steps are not explained clearly yet. Thus, raising the question of whether this new approach can be utilized in a common organization or not (not only non-profit but also profit organization). This research focuses on information security risk assessment by implementing the combination technique in a profit organization using semi-quantitative methods. The result, the combination technique can be used in common organizations both profit and non-profit with clear step by step translation.

Keywords: risk assessment; combination technique; information security

1. Introduction

Risk management is a process of identifying, estimating, and identifying steps to reduce risk with an acceptable level [1]. In implementing a risk management process, the organization uses various references and practical standards

* Corresponding author. Tel.: +62-856-125-6367.
E-mail address: kalamullah.ramli@ui.ac.id

10.1016/j.procs.2019.11.234

for the sustainability of its organizational business processes. The most important thing in overcoming issues related to risk is organizations must give close attention on building, improving, and managing the trust level before, during, and after the occurrence of an incident [2]. One focus of current risk management is risk management for information security. ISO 27005 is a widely used standard by organizations in implementing information security risk management.

The latest version of this standard published in 2018. This standard can be implemented on every type of organization, such as government agencies and non-profit/profit organizations regarding information security risk management [3]. ISO 27005 based on compliance with the organizational environment and the conformity with general risk management [4]. In the implementation stage, ISO 27005 can be combined with other standards or guidelines to fulfill the organizational needs regarding information security risk management. Other standards or guidelines are expected to sharpen the risk management process based on information security. NIST SP 800-30 revision 1 can be used as a complement to the risk assessment process and can be applied to the ISO 27005 risk management framework.

In 2017, the issue of combining ISO 27005 and NIST SP 800-30 had been discussed, resulting in a new technique with a detailed and complete document of information security risk assessment [5]. The new technique used in a case study of data communication applications on the XYZ agency, where the XYZ agency itself is a non-profit government agency in Indonesia [5]. However, the detailed risk assessment steps in using the combination techniques are not explained clearly yet. Thus, raising the question of whether this new approach can be utilized in a common organization or not. Even if it is possible, the next question is how the stakeholder can implement the technique? In the year of 2013, Abercrombie, et. al faced the same problem with the raising Risk Assessment Methodology Based on the NISTIR 7628 Guidelines. Abercrombie, et.al. solve the question by detailing the steps and do some experiment by utilizing the new method in a particular workgroup as the case study [6].

This research was conducted to provide detailed explanations and steps regarding how to use the combination technique of ISO 27005 and NIST SP 800-30 revision 1 and to facilitate stakeholders in the field of information security risk management on implementing alternative standard tools by proving whether this new technique is relevant to common organization (profit and non-profit) or not.

2. Literature review

ISO 27005

ISO 27005 is a part of the ISO 27000 family. Based on ISO 27001, the organization can form an information security committee in order to make information security policy [4]. The main focus of information security risk management further discussed on ISO 27005, which has undergone the latest update in 2018. The stages of risk assessment consist of context setting, risk identification, risk analysis, risk evaluation, and risk management [7]. ISO 27005 has a step-by-step process that includes context setting, information security risk assessment, handling information security risk, acceptance of information security risk, communication of information security risk, and monitoring and reviewing information security risk [4].

Context Establishment is the establishment of essential criteria for information security management [4]. The context establishment explained the scope and restriction of risk that are adjusted based on the information security level to be achieved [4]. Information security risk assessment is a stage in measuring and describing the risk qualitatively [4]. The results of risk assessment are essential information for all stakeholders [7]. Risk assessment allows managers to prioritize risks by following perceived seriousness or other criteria set. In the risk assessment process, there are several activities, including identification, analysis, and evaluation [4]. Asset identification has some categories, including information, software, hardware, service assets, human assets, and intangible assets such as reputation and organizational image [8]. In addition to asset identification, risk identification consists of identifying threats, existing controls, and vulnerabilities. In the risk analysis stage, the risk is assessed based on a scale that will be sorted and prioritized based on the produced level of risk. The prioritizing the risk is carried out at the risk evaluation stage.

NIST special publication 800-30 revision 1

One appropriate guideline for risk assessment is NIST Special Publication 800-30 revision 1. NIST SP 800-30 revision 1 is used to provide risk assessment guidelines for organization and government information systems and as a complement to NIST SP 800-39 [9]. Security standards and other guidelines support the approach of NIST SP 800-30 revision 1 risk assessment in order to manage information security risks. The steps in this guideline include identification of threat source, identification of event threats, identification of vulnerability, determining likelihood, determining impact, and determining the level of risk [9]. Table 1 shows a comparison of the use of the original technique in ISO 27005, NIST SP 800-30 revision 1, and the combination between the two.

Table 1. Assessment Scale – Impact of Threat Events.

No.	ISO 27005	NIST SP 800-30 REVISION 1	COMBINATION TECHNIQUE [5]
		CONTEXT ESTABLISHMENT	
1.	Determination of Risk Assessment Criteria and Scale		
		RISK ASSESSMENT	
2.	Risk Identification	1. Threat Source Identification 2. Threat Event Identification 3. Vulnerability Identification	1. Risk Identification: a). Threat Source Identification; b). Threat Event Identification; c). Vulnerability Identification.
3.	Risk Analysis	4. Determining the Likelihood 5. Determining Impact	2. Risk Analysis: a). Determining the likelihood in the risk scenario; b). Determining the impact on the risk scenario.
4.	Risk Evaluation	6. Determine information security risk level	3. Risk Evaluation: a). Determining the level of information security risk; b). Determining Risk Priority.

3. Methodology

Overall, the method used is a qualitative research method with the general flow, as shown in Fig.1.

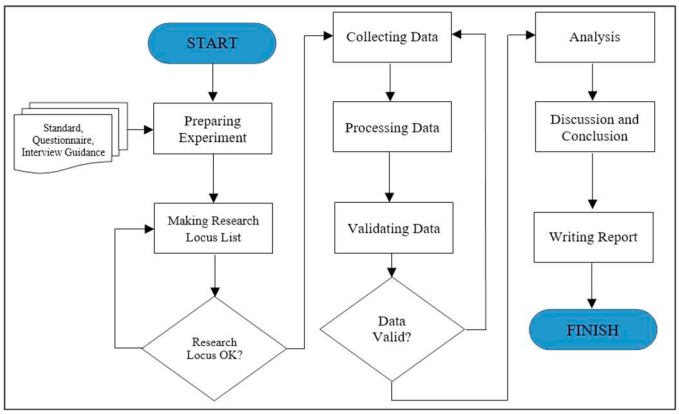

Fig. 1. General Research Flow.

Research object

The location of research for the implementation of this method is the ABC Agency (profit organization), specifically the ZZZ information system application. The consideration is due to ZZZ Information System Applications owned by ABC agency is operated at large scale organizations from the leading organization to the regions.

Data collection technique

In this research, several data collection techniques were used, including:

- **Literature Study**: This data collection is intended to obtain qualitative documents in the form of public documents (i.e., newspapers, papers, and official reports) or private documents (i.e., ABC agency' statutory regulations, diaries, letters, ZZZ information system usage reports, and documents relating to the application).
- **Interviews**: The sources used in the study were determined based on purposive sampling technique [10].
- **Questionnaire**: In this study, a questionnaire was used to identify sources of threats and threat events, assess opportunities for threats, assess the level of impact, and identify vulnerabilities. Respondents in the questionnaire refer to NIST SP 800-30 revision 1.
- **Observation**: The observations are open-ended, where we directly observe the behavior and activities of individuals related to the research object [11]. Following this method, we record or note the activities in the locus in a structured or semi-structured manner.

Data validation technique

The data validation technique from qualitative research is a mean to examine the accuracy and credibility of the research results using specific procedures [11]. The validation technique used in this research is member checking. This method is done by bringing back the final report to participants to check that the research data is accurate.

Data analysis technique

The method used in compiling this alternative information security risk management tool is based on the main framework of ISO 27005 with the technical composition of risk assessment based on NIST SP 800-30 revision 1. The primary consideration in assessing information security risk is based on the owner of the information. Fig. 2 shows the analysis flow.

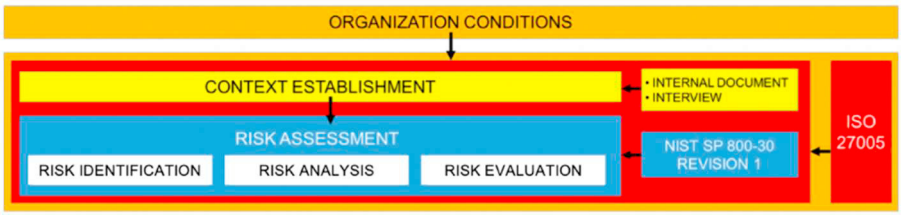

Fig. 2. Analysis Concept.

4. Analysis of the implementation of NIST SP 800-30 revision 1 and ISO 27005 combination technique

Context establishment

In context establishment, several necessary risk assessment arrangements are needed, which consist of a risk management approach, risk evaluation criteria, impact criteria, and risk acceptance criteria. In compiling a risk management approach, the needs of information owners in the scope of information security management are needed. The scope is determined so that the identified assets can be relevant to the central business processes in information security.

Risk evaluation criteria are determined by considering several aspects that focus on confidentiality, integrity, and availability. Criteria that need to be specified in a context establishment are the impact criteria and likelihood criteria. Impact criteria using the level option is based on the level description on NIST SP 800-30 revision 1. Likelihood criteria use consideration of the impact that allows the threat to occur, as well as the likelihood that is initiated/occurs. Based on the two likelihood assessments, the overall likelihood result is obtained, which describes the level of

likelihood in the risk scenario. The table below will explain the criteria of impact and likelihood based on NIST SP 800-30 revision 1.

The following in Table 2 describes the impact of threat events based on criteria and scale on the NIST SP 800-30 revision 1. Table 3 and Table 4 together explain about likelihood, with the focus of the likelihood of threat event initiation/occurrence and the likelihood of threat event, resulting in adverse impact. Then, using the information and considerations in Table 3 and Table 4, the overall likelihood can be determined using the criteria in Table 5. The results of the impact assessment in Table 2 and the overall likelihood in Table 5 are then used as considerations in Table 9 to determine the risk appetite.

Table 2. Assessment Scale – Impact of Threat Events.

Scale	Criteria		
	NIST SP 800-30 Rev.1	Description	Value
Very High	Multiple Severe or Catastrophic	The threat event could be expected to have **multiple severe** or **catastrophic adverse** effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.	10
High	Major		8
Moderate	Serious	.....	5
Low	Limited		2
Very Low	Negligible	The threat event could be expected to have a **negligible adverse** effect on organizational operations, organizational assets, individuals' other organizations, or the Nation.	0

Table 3. Assessment Scale – Likelihood of Threat Event Initiation/ Occurrence.

Scale	Criteria		
	NIST SP 800-30 Rev.1	Description	Value
Very High	Almost Certain	Error, accident, or act of nature is almost certain to occur more than 100 times a year / Adversary is almost certain to initiate the threat event	10
High	Highly Likely		8
Moderate	Somewhat Likely	.....	5
Low	Unlikely		2
Very Low	Highly Unlikely	Error, accident, or act of nature is highly unlikely to occur, or occur less than once every ten years / Adversary is highly unlikely to initiate the threat event	0

Table 4. Assessment Scale – Likelihood of Threat Event, Resulting in Adverse Impacts.

Scale	Criteria		
	NIST SP 800-30 Rev.1	Description	Value
Very High	Almost Certain	Threat events are initiated or occur; it is **almost sure** to have adverse impacts	10
High	Highly Likely		8
Moderate	Somewhat Likely	.....	5
Low	Unlikely		2
Very Low	Highly Unlikely	Threat events are initiated or occur; it is **highly unlikely** to have adverse impacts	0

Table 5. Assessment Scale – Overall Likelihood.

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Event Result in Adverse Impacts				
	Very Low (0)	Low (2)	Moderate (5)	High (8)	Very High (10)
Very High (10)	Very Low	Moderate	High	Very High	Very High
High (8)	Very Low	Moderate	Moderate	High	Very High
Moderate (5)	Very Low	Low	Moderate	Moderate	High
Low (2)	Very Low	Low	Low	Moderate	Moderate
Very Low (0)	Very Low	Very Low	Very Low	Low	Low

Risk assessment

4.2.1. Risk identification

- *Identification of Assets*

Asset identification is the first step in conducting a risk assessment. The risk assessment process begins with the compilation of a list of assets related to the business process information that is used as the primary source of security. Each asset has the location and owner. Assets are clustered based on its type, which consists of hardware, software, network, passive or active relay, personnel, site, and organization. There are two types of assets, secondary assets, and primary assets. The example given in this study is the identified assets of 16 types with the code A1 – A16.

Table 6. List of Assets.

Code	Type	Asset	Kinds of Asset	Owner	Location
A1	Technology	ZZZ Information System Application	Secondary	Infrastructure Protection Division	Operation Room
A2	Technology	Database	Primary	Infrastructure Protection Division	Data Center
A3	Network	PSTN	Primary	Infrastructure Protection Division	Operation Room
A...	.....				
A16	Personnel	Security Officers	Secondary	Infrastructure Protection Division	Operation Room

Table 6 explains that the scope implementation focus of information security is the Infrastructure Protection Division (IPD) that owns the assets. This case example is obtained in the context of infrastructure protection business processes which have information that must be protected. The table also shows that the information business process scope does not only originate from one location, but it is found in several locations, which is a critical risk point for information security. From some of these locations, asset managers may not be from the Infrastructure Protection Division, but other work units.

- *Identification of threats*

The focus is on the identification of threat sources and events. The identification of threat sources was divided into two, namely the identification of adversarial and non-adversarial threat sources. In this case, we obtained some adversarial threat sources as follows: internal personnel (S1), programmers (S3), technician networks (S4), application operators (S5), hackers and crackers (S7), computer criminal (S9), and network vendors (S10). Some non-Adversarial threat sources are as follows: human error (personnel) (S11), human error (privileged user) (S12), power supply availability (S13), IT Equipment Failure (S14), software aging (S16), and fire disaster (S18).

Threat events are based on assets that allow it to be exploited by the threat source. Relevance is obtained based on NIST SP 800-30 revision 1. The relevance is shown as the linkages between threats and assets (See Table 7).

Table 7. Threat Events.

	Assets Code	Threat Event	Threat Sources	Relevance
1	A1	Abuse of rights (T1)	S1, S5, S7, S9, S10	Confirmed
2	A1	Software malfunction (T2)	S7, S9, S10, S11, S12, S13, S14, S16, S18	Anticipated
3	A1	Forging of rights (T3)	S3, S11, S12, S14	Anticipated
4	A2	Forging of rights (T3)	S1, S7, S9	Anticipated
....				
42	A16	Breach of personnel availability (T27)	S4	Possible

Table 7 explained that ZZZ Information System Application (A1) has three threats, namely abuse of rights (T1), software malfunction (T2), and Forging of Right (T3). Each threat event has its threat sources. The linkages between threat sources and threat events are made based on ISO 27005. This relation has relevance based on NIST SP 800-30 revision 1.

- *Identification of existing controls*

In identifying risks, there must be an existing control for information sources. Sources of information may come from information owners or information managers. Example of existing control in case of control in ZZZ Information System Application (A1), namely access control leveling with login page (C1), a hash function for output login (C2), and log implementation system (C3) that has been implemented by the Infrastructure Protection Division (IPD). Other existing controls are the existence of a database and storage server shelter (C10), the application of database security with encryption (C11), the application of a log system on the database (C12), UPS in electricity handling (C13), Network Management System (C16), monitoring and troubleshooting functions by administrators (C17), application of filtering functions and security policy using firewall (C37), procedures for limiting information on passwords (C38), training (C39), security awareness understanding (C40), emphasis on administration and procedures (C42), and routine operational reports (C43).

- *Identification of vulnerabilities*

Vulnerability identification focuses on the results of the extent to which controls have been implemented to protect assets from threats. The description of vulnerability is obtained from the factors of user behavior or location of the asset in maintaining information security. Vulnerability is a result of deficiencies that exist in the existing controls. Vulnerability measurement is based on the NIST SP 800-30 revision 1, which is known as the vulnerability severity. Table 8 shows asset vulnerabilities based on the applied existing control.

Table 8. Vulnerabilities.

Assets	Existing Control	Vulnerability	Vulnerability Severity
ZZZ Information System Application (A1)	C1, C2, C3	Poor password management (V1)	High
ZZZ Information System Application (A1)	C1, C2, C3	Unprotected password tables (V2)	Moderate
Database (A2)	C10, C11, C12, C13	Lack of identification and authentication mechanisms like user authentication (V3)	Moderate
PSTN (A3)	C15, C16, C37, C17	Unprotected communication lines (V4)	Moderate

Assets	Existing Control	Vulnerability	Vulnerability Severity
.....			
Security Officers (A16)	C38, C39, C40, C42, C43	Absence of personnel (V46)	Low

4.2.2. Risk analysis

Risk analysis is the core stage of risk assessment. The results of risk handling are based on output risk analysis prioritized on risk evaluation. In determining the risk level, it is necessary to have a matrix which then will be used by the information owner. Table 9 shows risk appetite based on the semiquantitative based risk level guidance in NIST SP 800-30 revision 1 with two risk handling criteria (overall likelihood and level of impact). Risk appetite is obtained based on agreement on respondents who are directly involved in the ZZZ information system application in the ABC agency.

Table 9. Risk Appetite.

Overall Likelihood	Level of Impact				
	Very Low (0)	Low (2)	Moderate (5)	High (8)	Very High (10)
Very Low (0)	Accept	Mitigation	Mitigation	Mitigation	Mitigation
Low (2)	Accept	Mitigation	Mitigation	Mitigation	Mitigation
Moderate (5)	Accept	Mitigation	Mitigation	Mitigation	Mitigation
High (8)	Accept	Accept	Mitigation	Mitigation	Mitigation
Very High (10)	Accept	Accept	Accept	Mitigation	Mitigation

Based on the risk appetite in Table 9, the assessment is carried out in Table 10. Table 10 shows the risk analysis table, which describes the linkages between assets, threat events, threat sources, and likelihood with the impact resulting in a level of risk. From the table, we obtained coherence between ISO 27005 and NIST SP 800-30 revision 1 in determining the level of risk.

Table 10. Risk Analysis.

	Asset	Threat Event	Threat Source	Likelihood of Attack Initiation	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Level of Risk
1	A1	T1	S1, S5, S7, S9, S10	Moderate	Moderate	Moderate	Very High	High (Mitigation)
2	A1	T2	S7, S9, S10, S11, S12, S13, S14, S16, S18	Moderate	Moderate	Moderate	Moderate	Moderate (Mitigation)
3	A1	T3	S3, S11, S12, S14	Low	Moderate	Low	Moderate	Moderate (Mitigation)
4	A2	T3	S1, S7, S9	Moderate	Moderate	Moderate	High	Moderate (Mitigation)
.....								
42	A16	T27	S4	Low	Low	Low	Low	Low (Retention)

4.2.3. Risk evaluation

Risk determination is the initial stage before risk prioritizing. The risk priority matrix is classified based on the NIST SP 800-30 revision 1 and is a matrix of the relationship between assets and threats. From the matrix, we obtained

result examples as follows: 4 high (priority), 20 moderate (second priority), 15 low (last priority), and 3 very low (no priority) risk scenarios. Fig. 3 explains the priority of these risks.

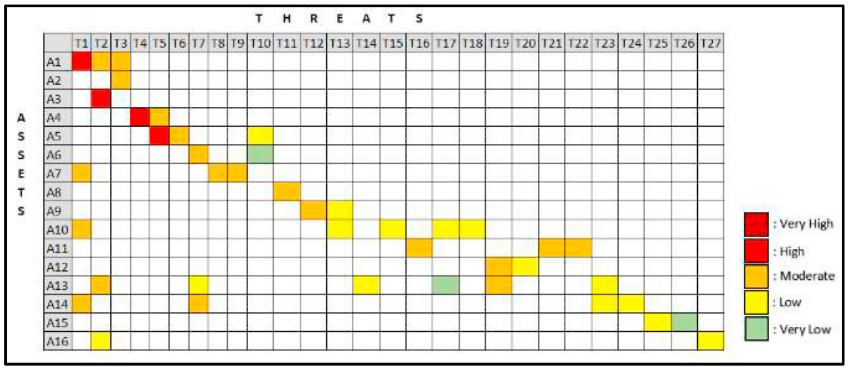

Fig. 3. Risk Priority.

5. Discussion and conclusion

In the analysis, the type of asset is identified based on the asset category in ISO 27005. The information business process has a risk scenario which must then be assessed. Assessment can be done based on perceptions of the information owner or based on the technical side of the system.

The mapping of NIST SP 800-30 revision 1 at ISO 27005 focused on information security risk assessment. The mapping-based analysis resulted in a comprehensive risk assessment by following the ISO 27005 standard. Comprehension was obtained from the threat source details based on adversary and non-adversary at the threat identification stage. The combination technique above can be done on applications as a tool to simplify the information security risk management process for information owners. The semi-quantitative technique at NIST SP 800-30 revision 1 is also instrumental in supporting risk analysis at ISO 27005. This process can be developed in applications up to the stage of handling risks by giving control recommendations.

In order for the stakeholders to handle information security risks, stakeholders can implement CBA method. CBA can be applied to profit organizations by calculating material/profit losses and benefits in implementing risk control recommendations. In the case of government agencies or non-profit organizations, CBA can be used to determine losses and benefits based on the availability of budget and long-term investment of the organization. The capability of actors to carry out risk communication is divided into several sectors consisting of monitoring, analysis, warning, and response [12]. Risk treatment and risk acceptance are not included in the research.

By following the research result, this new approach was proved to be able to be applied in a common organization (profit and non-profit). Following this research methodology, stakeholders can directly implement this new technique as an alternative tool for information security risk assessment.

Acknowledgments

The article publication is partly supported by the Ministry of Research and Higher Education of The Republic of Indonesia through INSINAS grant number NKB0004/UN2.R3.1/HKP.05.00/2019 and the United States Agency for International Development (USAID) through the Sustainable Higher Education Research Alliance (SHERA) Program for the Universitas Indonesia's Scientific Modeling, Application, Research, and Training for City-centered Innovation and Technology (SMART CITY) Project, Grant #AID-497-A-1600004, Sub-grant #IIE-00000078-UI-1. We also would like to thank all parties involved, especially the reviewers for their feedback and suggestions.

References

[1] Stoneburner, G., A. Goguen, and A. Feringa. (2002) "NIST SP 800-30: Risk Management Guide for Information Technology Systems." **1 (1)**: 1-56.

[2] Akhgar, Babak and Simeon Yates. (2013) *Strategic Intelligence Management. National Security Imperatives and Information and Communications Technologies*, Oxford, Elsevier Inc.

[3] Chazar, C. (2015) "Information Security Management System Based on ISO/IEC 27001: 2005," in *Information Journal* **8 (2)**: 48–57, IEEE.

[4] ISO/IEC. (2011) "International Standard ISO/IEC 27005: 2011." **1 (2)**: 1–68.

[5] Putra, Fandi A., S. Hermawan, and R.P. Anggi. (2017) "Design of Information Security Risk Management using ISO/IEC 27005 and NIST SP 800-30 Revision 1: A Case Study at Communication Data Applications of XYZ Institute," in *2017 International Conference on Information Technology Systems and Innovation (ICITSI)* **8 (4)**: 251-256.

[6] Abercrombie, R.K., et.al. (2013) "Risk Assessment Methodology Based on the NISTIR 7628 Guidelines," in *2013 46th Hawaii International Conference on System Science.*

[7] Refsdall et. al. (2015) *Cyber-Risk Management*, New York, Springer.

[8] Sarno, R., and I. Iffano. (2009) *Information Security Management System Based on ISO 27001*, Surabaya, ITSpress.

[9] National Institute of Standards and Technology. (2012) *NIST SP 800-30 Revision 1: Guide for Conducting Risk Assessments* **1 (2)**: 1-95.

[10] Sugiyono. (2014) *Metode Penelitian Manajemen* [Title in English: *Research Method in Management*], Bandung, Alfabeta.

[11] Creswell, J. W. (2016) Research Design: Pendekatan Metode Kualitatif, Kuantitatif, dan Campuran [Title in English: *Research Design: Quantitative, Qualitative Method*], 4th Ed., SAGE Publication, Yogyakarta, Pustaka Pelajar.

[12] Norwood, Herry T., and P. Sandra. Catwell. (2009) *Cybersecurity, Cyber analysis and Warning,* New York, Nova Science Publisher, Inc.