IJCCS (Indonesian Journal of Computing and Cybernetics Systems)
Vol.13, No.3, July 2019, pp. 231~240
ISSN (print): 1978-1520, ISSN (online): 2460-7258
DOI: https://doi.org/10.22146/ijccs.43922

System Security Awareness Planning Model Using The Octave Method Approach

Zaied Shouran*[1], Nur Rokhman[2], Tri Kuntoro Priyambodo[3]
[1]Computer and Electronics Science, Department, UGM, Yogyakarta, Indonesia
[2]Department of Computer Science and Electronics, FMIPA UGM, Yogyakarta, Indonesia
*[1]**Shouran.zaied@mail.ugm.ac.id** , [2] nurrokhman@ugm.ac.id , [3] mastri@ugm.ac.id

Abstrak

Kesadaran akan keamanan sistem informasi adalah hal penting untuk diperhatikan. Pada penelitian ini akan dibahas mengenai model perencanaan kesadaran tentang keamanan sistem informasi menggunakan model atau metode Octave. Metode analisis yang digunakan adalah analisis deskriptif kualitatif. Hasil penelitian menunjukkan dengan model Octave dapat meningkatkan kesadaran tentang pentingnya keamanan dalam sebuah sistem informasi dan perusahaan yang menerapkannya akan dapat meningkatkan kinerjanya di masa mendatang.

Kata kunci*— kesadaran, keamanan, motode Octave*

Abstract

Awareness of the security of information systems is an important thing to note. In this study, we will discuss planning models of awareness about information system security using Octave models or methods. The analytical method used is qualitative descriptive analysis. The results of the study show that the Octave model can increase awareness about the importance of security in an information system and companies that implement it will be able to improve their performance in the future.

Keywords— *awareness, security, Octave method*

1. INTRODUCTION

The use of Information Technology has now developed for support all activities in the organization. Information is the result of processing data obtained from Information System (IS) and Information Technology (IT). Information is an asset which is very valuable for survival commercial organization (company), college, government institutions that must be maintained availability, accuracy, and integrity [1]. Therefore the ability to provide information fast and accurate are essential for the organization [2]. The emergence of IT and SI innovations useful to support the size of the need for information. Along with its development, technology often used by several parties irresponsible that can cause the emergence of threats and risks from use technology [3].

Information system security issues often less attention from stakeholders and manager of information systems [4]. Sometimes security issues are often ignored. If disrupt the performance of the system, often security is reduced or eliminated [5]. On its application, often information system security starts to get attention when the threat already happens. Risk of loss and damage to information is a critical thing for the organization because information is an important asset

Received March 3rd,2019; Revised May 8th, 2019; Accepted July 11th, 2019

in the organization which needs to be kept intact. Therefore Information system security is necessary carefully planned when designing the system. An ounce of prevention is worth a pound of cure (prevention is better than cure). Every organization has a variety of information related to the vision, mission, strategy, management, finance, procurement, assets, and information other support. Where is the majority confidential. Effectiveness and efficiency of IT usage also cause a level of risk of high information system security. Importance planning Security Management Standards Well structured information can be a reference and can be applied to protect information of various kinds of the threat of damage.

In this research will develop a new model using Octave methods in making better planning and implementation of security awareness in system information and technology in a company or organization.

2. METHODS

The threat is an action or event can harm the organization [6]. System security information aims to protect information and information systems from various risk threats. According to G. J. Simons [7], information system security is how we can prevent fraud (cheating) or, at least, detect it a fraud on an information-based system, where the information itself does not have physical meaning [8]. According to John D. Howard, system security information is a preventive measure from attack computer users or network accesses irresponsible [9].

Figure 1. Information System Security Aspects

Therefore, information system security is something that needs to be considered from the start of SI planning. Information is an asset important for the company. Information security contains several important aspects. The following is an explanation of the aspects of information system security, namely [1]:

1. Confidentiality
   Aspects that guarantee data confidentiality or information, ensuring that information only accessible to people who authorized and guarantees data confidentiality sent, received, and saved.
2. Integrity
   Aspects that guarantee that data is not changed without permission from the authorities (authorized), maintain accuracy and information integrity and process method to guarantee this integrity aspect.
3. Availability

Aspects that guarantee that the data will available when needed, ensuring the user the right to be able to use information and related devices (assets that are relating when needed).

Operational Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methods are a system approach to security risk evaluation comprehensive, systematic, directed, and information can be done alone [10]. The OCTAVE method can be used to identify risks related to aspects of confidentiality, integrity, and availability of valuable assets and establish disaster mitigation to deal with risk. The OCTAVE method uses three phases approach in examining organizational problems and technology, gives a picture comprehensive information security needs for organizations [11]. Stages in the OCTAVE method in the figure in Figure 1 below:

The OCTAVE method includes the following stages: (1) Build Asset-Based Threat Profiles. In this phase evaluation of the organization. (2) Identify Infrastructure Vulnerabilities. In this phase evaluation of the infrastructure of information. (3) Develop Security Strategy and Plans. In the phase will produce identification risk and design disaster mitigation to handle these risks.

OCTAVE method Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) defines important components in a comprehensive, systematic, context-driven evaluation of information security risk. Using the OCTAVE method, organizations can make protection against CIA-based risk decision-based information (Confidentiality, Integrity, Authentication) for critical information technology assets [12]. OCTAVE is a methodology for identifying and evaluating information system security risks. The use of OCTAVE is intended to assist organizations in terms of: (a) Developing qualitative risk evaluation criteria that describe the organization's operational risk tolerance; (b) Identifying important assets to achieve the organization's mission; (c) Identifying vulnerabilities and threats to these assets; (d) Determine and conduct evaluations to deal with the consequences that occur to the organization if the threat occurs. The OCTAVE method has three variants namely OCTAVE, OCTAVE-S and OCTAVE Allegro. OCTAVE is a set of tools, techniques and methods for risk-based information system security planning and planning. OCTAVE Allegro is a simplified method that focuses on information assets. OCTAVE Allegro can be done by workshop-style and collaborative methods. OCTAVE Allegro consists of eight steps divided into four phases [13].

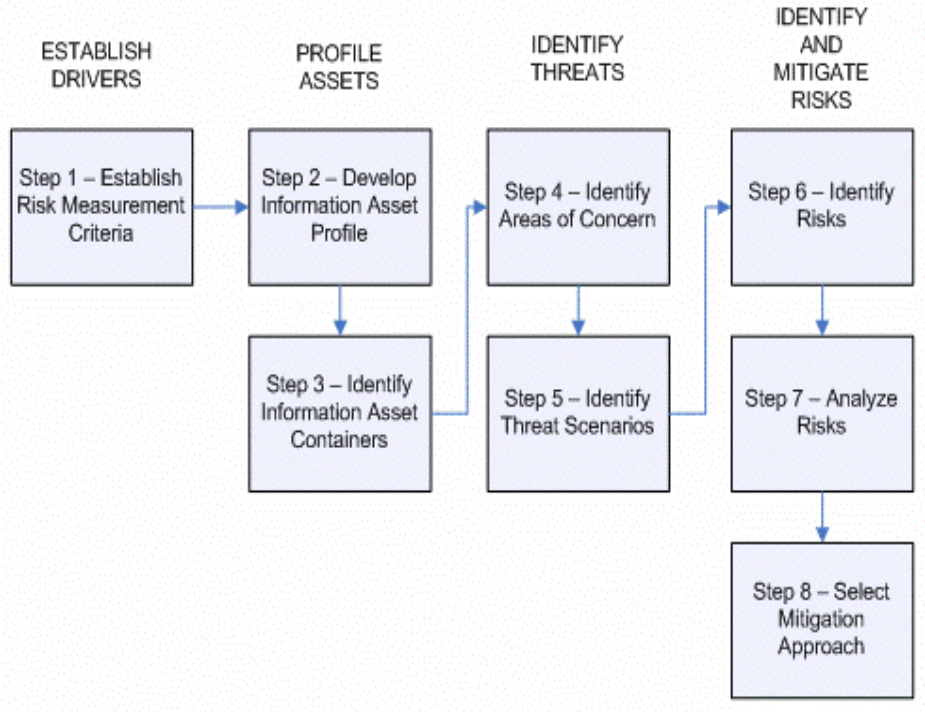

Figure 2. Steps of OCTAVE Allegro [13]

Risk Assessment Stage

Step 1 - Build Risk Measurement Criteria

This step has two activities, beginning with building organizational drivers used to evaluate the impact of risks on business mission and objectives, and recognizing the most important impact areas. Activity 1 is to make qualitative size definitions documented in the Risk Measurement Criteria Worksheets. Activity two gives priority impact area values using the Impact Area Ranking Worksheet.

Step 2 - Develop an Information Asset Profile

Consisting of eight activities, beginning with the identification of information assets, then a structured risk assessment is carried out on critical assets. The activities of three and four gather information about important information assets followed by documenting the reasons for choosing critical information assets. Activities five and six make a description of critical information assets and then identify ownership of these critical information assets. Seven activities filled security needs for confidentiality, integrity and availability. Activity eight identifies the most important security needs for information assets

Step 3 - Identifying Containers from Information Assets

There is only one activity in step three, note the three important points related to the security and concepts of information asset containers, namely the way information assets are protected, the level of protection or security of information assets and vulnerabilities and threats to containers from information assets.

Step 4 - Identify the Problem Area

Activities in step four are initiated by developing a risk profile of information assets by exchanging ideas to find components of threats from situations that might threaten information assets. Based on the Information Asset Risk Environment Maps and Information Asset Risk Worksheet documents, area of concern can be recorded. Guided by the Information Asset Risk Worksheet document, do a review of containers to make an Area of Concern and document each Area of Concern.

Step 5 - Identifying Threat Scenarios

One activity in step five which is identifying additional threat scenarios in this activity can use Activity two complements Information Asset Risk Worksheets for each common threat scenario.

Step 6 - Identifying Risks Activity one in step 6 determines the threat scenario that has been documented in the Information Asset Risk Worksheet can have an impact on the organization

Step 7 - Analyzing Risk

Activities must be carried out referring to the documentation contained in the Information Asset Risk Worksheet. One activity starts with reviewing risk measurement criteria followed by a second activity calculating the value of relative risk that can be used to analyze risks and decide on the best strategy in dealing with risk.

Step 8 - Select the Reduction Approach

The one activity in step eight is to rank each identified risk based on the risk value. This is done to assist in making risk mitigation status decisions. Activity two carries out a mitigation approach for each risk based on conditions unique to the organization.

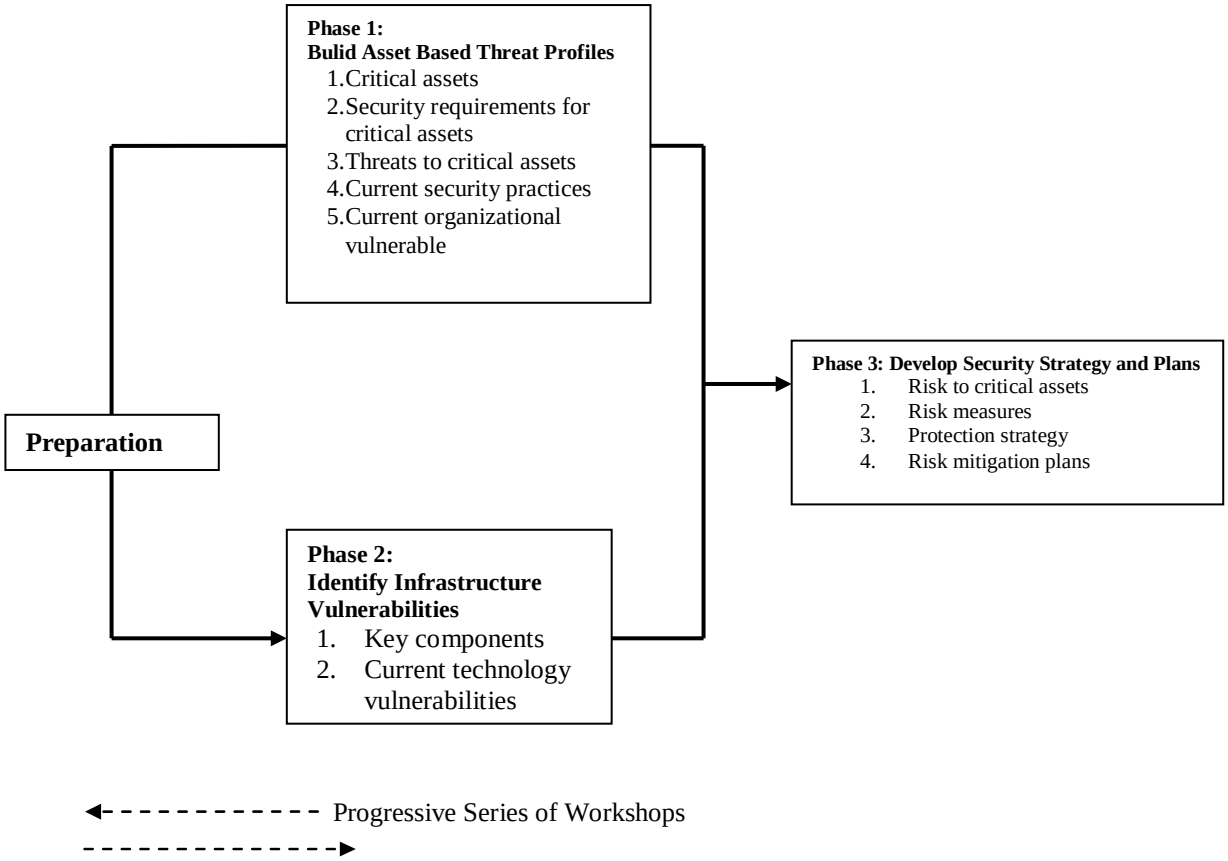

Figure 3. OCTAVE Methods [14]

3. RESULTS AND DISCUSSION

The stages of analysis and design carried out in developing a system security design information model are illustrated in Figure 4.

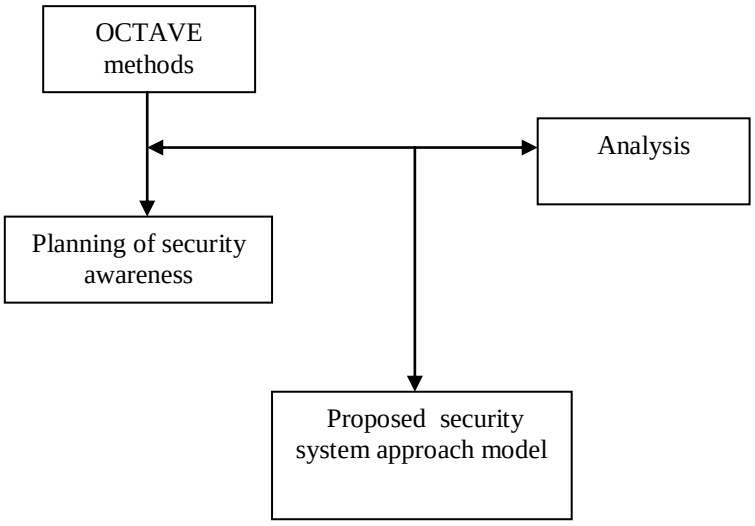

Figure 4. Model Design and Development Stages [15]

The standard that can be used to design guidelines for security policy documents in the form and scope of procedures for implementing the ISMS. An overview of the structure of documentation based on ISMS documentation shown in Figure 5.

Figure 5. Structure of the ISMS Documentation [16]

The ISMS documentation generally consists of 3 levels, namely:

1. Level 1: Policies and Standards
   Is a document with the highest hierarchy, which is strategic in the form of policies, standards, targets, and plans related to the development, application, and improvement of the ISMS.
2. Level 2: Procedures, Guidelines, Implementation Guidelines
   It is a document that contains procedures and guidelines developed by the organization and includes how to implement policies and the person in charge of implementing SMK
3. Level 3: Technical Instructions, Work Instructions, Forms
   Is a document that contains technical instructions, work instructions, and forms used to support the implementation of certain procedures to the technical level

The results of the analysis of the document are illustrated in table 1. [17]

Table 1. Document analysis

Stage	No	Document
Stage 1	**1-1**	Information Security Policy
	1-2	Organization, Role, and Responsibility
	1-3	Information Security
	1-4	Information Classification Guide
	1-5	ICT Risk Management Policy
	1-6	Business Continuity Management Framework
Stage 2	**2-1**	Identifying components
	2-2	the key to information infrastructure
	2-3	Document Control
	2-4	Record Control
	2-5	Internal Audit
	2-6	Corrective & Preventive Measures
	2-7	Labeling, Safeguards, Exchange & Information Disposal
	2-8	Management of Removable Media & Media Disposal
	2-9	Monitoring the Use of ICT Facilities
	2-10	User Access Management
	2-11	Teleworking
	2-12	Software Installation Control & Intellectual Property Rights
Stage 3	**3-1**	Management of ICT Changes
	3-2	Security Incident Management & Reporting
	3-3	Technical Procedure

From the results of the analysis carried out, a model of information system security design proposals obtained using the OCTAVE and the standard method approaches is illustrated in the following figure 6:

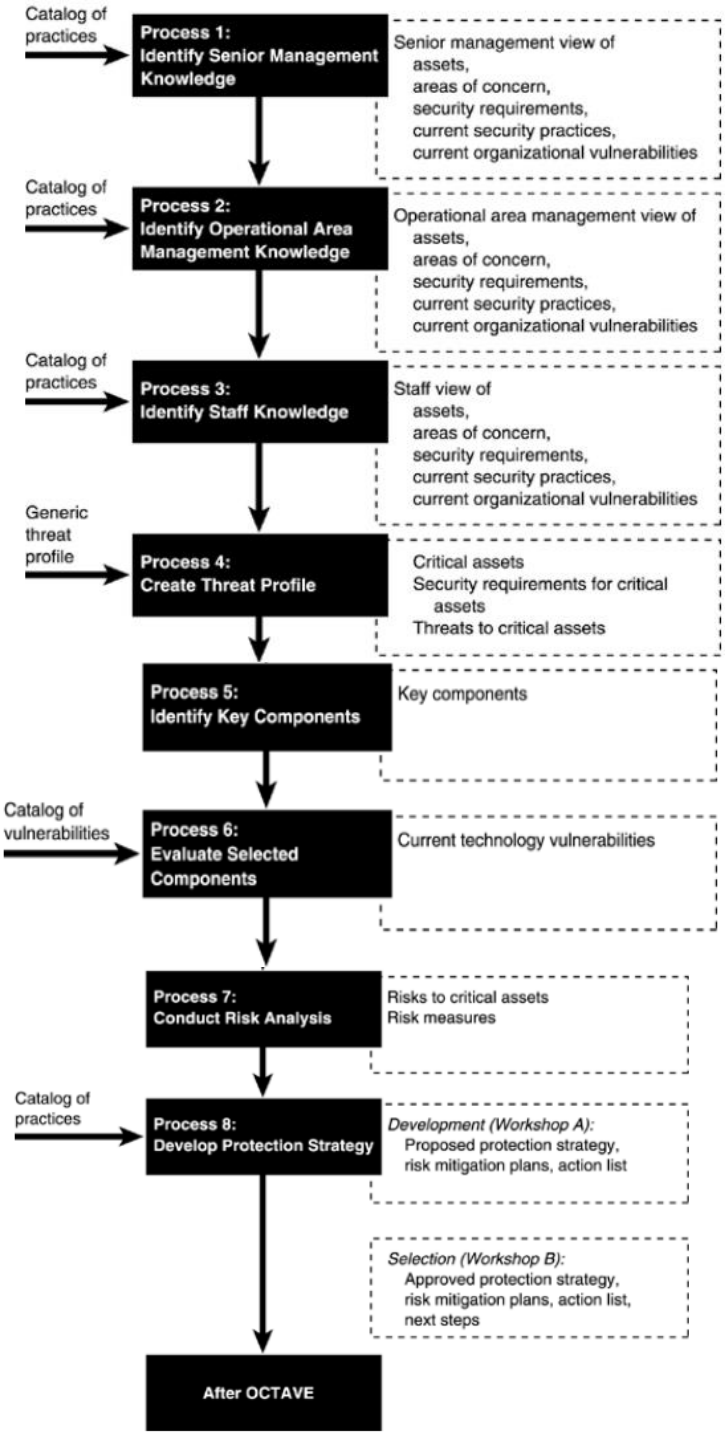

Figure 6. Information System Security Planning Model Using the OCTAVE Method Approach

The following is an explanation of the steps in the information system security design proposal model using the OCTAVE method approaches [18]:

1. Stage 1: Performed through 2 stages based on the OCTAVE method. First, identify important assets and identify threats to assets. Second, identify the weaknesses of infrastructure from information technology.
2. Stage 2: Information system security planning is carried out based on the results in stage 1 with adjustments based on the ISO

3. Stage 3: Based on the results in stage 2, an information system security planning document will be obtained based on 3 levels of documentation.

The information system security planning model by combining two methods, namely the OCTAVE method as the initial stage to identify risks based on the threats and weaknesses of information assets standards can be used as a reference framework in developing guidelines for producing more detailed management information plans for risk of threats and weaknesses of information assets of a company [19].

4. CONCLUSIONS

Based on the results of the research conducted, the OCTAVE method can be used as an initial tool to classify assets, risks, and design risk mitigation. Based on the results of the classification carried out, the next step is planning a security strategy. Where in its design, conformity with the ISMS document is based on ISO 27001: 2005. So as to produce an ISMS document that is directed towards the need to secure important company assets. For recommendations for further research, the proposed model produced can be directly implemented in an organization as a reference framework in information system security planning.

REFERENCES

[1] Chazar, C. (2015). Management Standards for Information Systems Security Based on ISO / IEC 27001. Information Journal Volume VII No.2 / November / 2015. Bandung.

[2] M. Thierry and T. K. Priyambodo, "SMS and Web-Based e-Government Model Case Study: Citizens Complaints Management System at District of Gihosha –Burundi," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 11, no. 1, p. 67, Jan. 2017 [Online]. Available: https://journal.ugm.ac.id/ijccs/article/view/17167.

[3] T. Wachowicz and P. Błaszczyk, "TOPSIS Based Approach to Scoring Negotiating Offer in Negotiation Support Systems," *Gr. Decis. Negot.*, vol. 22, no. 6, pp. 1021–1050, Nov. 2014 [Online]. Available: http://link.springer.com/10.1007/s10726-012-9299-1

[4] H. Núñez, M. Sànchez-Marrè, U. Cortés, J. Comas, M. Martínez, I. Rodríguez-Roda, and M. Poch, "A comparative study on the use of similarity measures in case-based reasoning to improve the classification of environmental system situations," *Environ. Model. Softw.*, vol. 19, no. 9, pp. 809–819, 2016.

[5] Sembiring, S. & Lubis, S. A. (2015). Application of ISO 27001 Based Information Security Index to Measure the Level of Information Security Readiness in Higher Education Institutions. 2014 SNASTIKOM Proceeding Vol-2.

[6] Cheristian, I., Fatoni., Negara, E. S.: ISO 27001: 2016 Planning and Implementation of Standards at PT. Sinar Sosro Palembang. From http://digilib.binadarma.ac.id/files/disk1/139/123-123- imamcheris-6945-1-journal-n.pdf.

[7] Rahardjo, B. (2015). Internet-based Information System Security. Bandung.

[8] P. S. Ardiantara, R. Sumiharto, and S. B. Wibowo, "Prototype of Control of Stable Position and Attitude on Unmanned Aircraft Using IMU and the Kalman Filter Fusion Sensor Algorithm," *IJEIS (Indonesian J. Electron. Instrum. Syst.*, vol. 4, no. 1, pp. 25–34, 2014 [Online]. Available: https://jurnal.ugm.ac.id/ijeis/article/view/4219.

[9] I. Dwicahyo Pratomo, A. Rouf, and T. Wahyu Supardi, "Hole Distance Measurement in Solid Objects Using Ultrasonic Sensors," *IJEIS (Indonesian J. Electron. Instrum. Syst.*, vol. 6, no. 1, p. 81, Apr. 2016 [Online]. Available: https://jurnal.ugm.ac.id/ijeis/article/view/10774.

[10] T. Nur Syahril Sidiq, A. Rouf, and T. Wahyu Supardi, "Solid Object Disability Detection System Using Ultrasonic Angle Variation Techniques," *IJEIS (Indonesian J. Electron. Instrum. Syst.*, vol. 6, no. 1, p. 69, Apr. 2016 [Online]. Available: https://jurnal.ugm.ac.id/ijeis/article/view/10773.
[11] Richard. A. Caralli. (2017). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. http://www.sei.cmu.edu/pub/documents/07.reports/07tr012.pdf.
[12] S. K. Pandey dan K. Mustafa. (2015). A Comparative Study of Risk Assessment Methodologies for Information Systems. Buletin Teknik Elektro dan Informatika, 1(2),111-122.
[13] A. M. Suduc, M. Bîzoi dan F. G. Filip. (2016). Audit for Information Systems Security. Journal Informatica Economică, 14(1),43-48.
[14] Christopher Alberts, Audrey Dorofee. 2016). Managing Information Security Risks: The OCTAVESM Approach. Publisher: Addison Wesley. ISBN : 0-321-11886-3.
[15] J. Simons. (2015). Information Security & ISO 27001. IT Governance Green Paper. The United Kingdom.
[16] S. K. Pandey dan K. Mustafa. (2012). A Comparative Study of Risk Assessment Methodologies for Information Systems. Buletin Teknik Elektro dan Informatika, 1(2),111-122.
[17] Joint Task Force Transformation Initiative (2011). Managing Information Security Risk: Organization, Mission, and Information System View. NIST Special Publication 800-39.
[18] A. M. Suduc, M. Bîzoi dan F. G. Filip. (2010). Audit for Information Systems Security. Journal Informatica Economică, 14(1),43-48.
[19] Technical Department of ENISA Section Risk Management (2006). Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools. ENISA.