ISSN 2278-3091
Volume 8, No.6, November – December 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse77862019.pdf
https://doi.org/10.30534/ijatcse/2019/77862019

Enhancing is Risk Assessment through using Combination Vector Matrix and Octave Methods

[1]Rivo Mahatvira Vijayanto, [2]Devyana, [3]Gunawan Wang
Master of Information Systems Management, Binus Graduate Program,
Bina Nusantara University Jl KH Syahdan 9, Jakarta 11480, Indonesia
[1]rivo.vijayanto@binus.ac.id. [2]devyana@binus.ac.id, [3]gwang@binus.edu.

ABSTRACT

Information System (IS) is an asset for an organization so that its application must be protected properly. It is important in the business environment to work with the internet and where information sent and received has more types of threats and vulnerabilities. This paper wants to discuss two methods for assessing information system security risks in financial technology institutions. The methods to be discussed are the VECTOR Matrix method and the OCTAVE Allegro method. The VECTOR method is a security risk assessment method used to prioritize critical risks. While the method for carrying out a more detailed level of security risk analysis, it is recommended to use the OCTAVE Allegro approach. What IS security practices can learn is the reason for choosing the VECTOR Matrix and OCTAVE Allegro method. That these two methods are complementary during the information security risk assessment process in the business environment.

Key words: Risk Assessment, Information Security, VECTOR Matrix, OCTAVE Allegro, Financial Technology

1. INTRODUCTION

The use of technology in the financial system that produces products, services, technology, and other new business models. This has an impact on monetary stability, financial system stability, efficiency, smoothness, security and reliability of a payment system. With the development of technology in the financial world it has proven to be beneficial for consumers, business people, and the national economy, but on the other hand has a high risk potential if not properly mitigated it will disrupt the running of the financial system.

The increasing dependence of consumers on the products and services offered by financial technology is also a key factor in the rapid development of financial technology to support various financial services in Indonesia. Today many start-up companies are focused on financial technology and are predicted to continue to grow over time. Morgan Stanley's research results, published on February 21, 2019, show the large increase in the number of users and digital transactions in Indonesia. The agency predicts the number of transactions through digital payments will reach US $50 billion by 2027 [1].

As for financial technology organizers registered at OJK as of February 1, 2019, the total number of registered and licensed financial technology operators is 99 companies [2]. In line with the increasing number of players, the services offered by financial technology are also increasingly diverse, ranging from payments, financing / loans, investment in the capital market to more attractive packaged insurance with a touch of financial technology. Knowledge, demands, level of comfort and inclusion of public finance are increasing. However, as a logical consequence of more open access and more options, there is an increased information security risk in transactions. The closer the relationship between technology and financial services, where financial activities can be carried out anytime, so the potential for more sophisticated threats of crime is even greater. There is no sector that is so vulnerable to being exposed to this threat besides the financial services sector - and especially financial technology.

The first action to protect information is to assess the security risk of the equipment and procedures used for processing and storing information. Especially for financial technology institutions where exploitation is vulnerable in information security and can cause loss of reputation or direct financial loss. Therefore, we need a risk measurement in the application of information systems. Information system risk measurement is useful for knowing risk profiles, risks analysis, and responding to risks so that no impact will arise from these risks.

This paper presents two approaches to information security risk assessment. VECTOR Matrix is an information security risk assessment method that is used independently. This method is good for determining the priority of critical risks. OCTAVE Allegro is a more detailed method for assessing information security risks. This method is specifically recommended for assessing the security of information storage. The both methods are used to assess security risks in financial institutions [3].

2. LITERATURE RIVIEW

2.1. Information Security Risk Assessment Standards and Framework

Good and effective management of information security is where an organization takes into account all operational and organizational processes including those related to information security. To date, various standards and framework for

information security have been developed which focus on targets or subjects areas. Various organizations, companies and government use information security standards to improve their security and facilitate them in determining the procedures and forms of security that must be carried out. Some standards and frameworks for information security risk assessment that are often used as reference by companies are:

a. NIST Special Publication 800-30

NIST 800-30 is a standard document developed by the National Institute of Standard and Technology which is a continuation of legal responsibility under the 1987 Computer Security Act and the Information Technology Management Reform Act in 1996. NIST 800-30 there are two important stages namely risk assessment and risk mitigation. Stages of risk assessment based on NIST 800-30, namely [4]

- System Characterization
  At this stage, the boundaries of IT systems must be identified, including resources and information.
- Threat Identification
  Consideration of the possibility of emerging threats such as sources, potential vulnerabilities and controls.
- Vulnerability Identification
  Identification of vulnerabilities is used for the development of a list of system vulnerabilities that can be utilized later.
- Control Analysis
  Analysis of controls that have been implemented or planned for implementation by the organization to minimize or eliminate the possibility of possible development of threats
- Likelihood Determination
  The ranking process for the potential of clusters can be carried out in the environment of the vulnerability. Factor that are taken into consideration are threats (source and ability), nature of vulnerability and the existence and effectiveness of controls if applied.
- Impact Analysis
  This stage is used to determine the negative impacts resulting from the successful application of vulnerability.
- Risk Determination
  Risk level assessment in the IT system is carried out at this step
- Control Recommendations
  This stage assesses controls which can reduce or eliminate the risks that have been identified. Recommended controls should be able to reduce the level of risk in the IT system and data, to an acceptable level of risk.
- Result Documentation
  At this stage, a report on the result of the risk assessment is carried out (source of threat, vulnerability, risk assessed and recommended controls).

b. ISO 27001:2013

To minimize the growing threat, the International Organization for Standardization (ISO) and the International Electrical Technical Commission (IEC) issued guidelines on standards for information security ISO / IEC stated that this guide as an Information Security Management System (ISMS) and explained in a series of ISO / IEC27000 . In ISO 27001: 2013 [5], information security management is based on the Plan Do Check Action (PDCA) model which aims to improve sustainable information security. This standard consists of seven main clauses and some controls available in the APPENDIX section. The items from the main clauses consist of organizational context, leadership, planning, operations support, evaluation and pre-information improvement. There is a statement of applicability (SOA) to control the implementation of ISMS, consists of 114 controls from 14 domains and 35 objectives in ISO/IEC 27001:2013, as illustrated in Table 1.

Table 1: Domains, Objectives and Number of Control in Annex A ISO27001:2013

No Annex	Domain ISO 27007:2013	Number of Objectives	Number of Control
A.5	Information security policies	1	2
A.6	Organization of Information Security	2	7
A.7	Human Resource Security	3	6
A.8	Asset Management	3	10
A.9	Access Control	4	12
A.10	Cryptography	1	2
A.11	Physical and Environmental Security	2	15
A.12	Operations Security	7	14
A.13	Communications Security	2	7
A.14	System Acquisition, Development and Maintenance	3	13
A.15	Supplier Relationship	2	5
A.16	Information Security Incident Management	1	7
A.17	Information Security Aspects of Business Continuity Management	2	4
A.18	Compliance	2	8
Total		35	114

c. COBIT5

COBIT is published by the Information Domain Audit and Control Association (ISACA) IT Government Institute. This framework is used to control the risk of using information technology that is used to support business processes. COBIT is a combination of document and frameworks that are categorized and accepted as a good method for information technology governance. Risk management is specifically discussed in the PO9 process in COBIT. COBIT has the following information technology risk management framework [6]:

- *Objective setting,* COBIT provides information criteria that are used as a basis for defining information technology objects. There are 7 criteria for information, namely effectiveness, reliability, and availability.
- *Risk Identification,* this process is carried out to determine the existence of risks that can originate from processes, people, technology, both from within and from outside the organization, and sourced from disasters, opportunities, and uncertainties.
- *Risk assessment,* this process is used to assess the frequency of occurrence of risk and how much they impact. The impact of risk can be in the form of finance, business activities are stopped, delays in decision making, declining reputation caused by system errors, and assets failures.
- Risk Response, this process is carried out to apply an appropriate objective control in the implementation of risk management. COBIT has several processes that are in accordance with risk management, namely:
  - PO1 (Define a Strategic IT Plan) and PO9 (Assess and Manage Risk)
  - A16 (Manage Change)
  - DS5 (Ensure System and Security)
  - MEI (Monitor and Evaluate IT Performance)
  - Monitor risk, each stage needs to be monitored so that risks and responses are guaranteed to continue.

2.2. Information Security Risk Assessment

The term information security means protecting information and information systems from unauthorized access, user, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability [7] In information security, a risk can be defined as the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information security vulnerability and the resulting impact. Proper contextualized risk assessment is the best way to approach the organization's need for information security. Information security risk assessment is the process (part of Risk Management) that identifies and valuates the risks to information security by determining the probability of occurrence and the resulting impact [8]. It identifies threats, classifies assets and rates system vulnerabilities as it provide key information and guidelines to implement effective controls. [9] The process of the information security risk assessment:

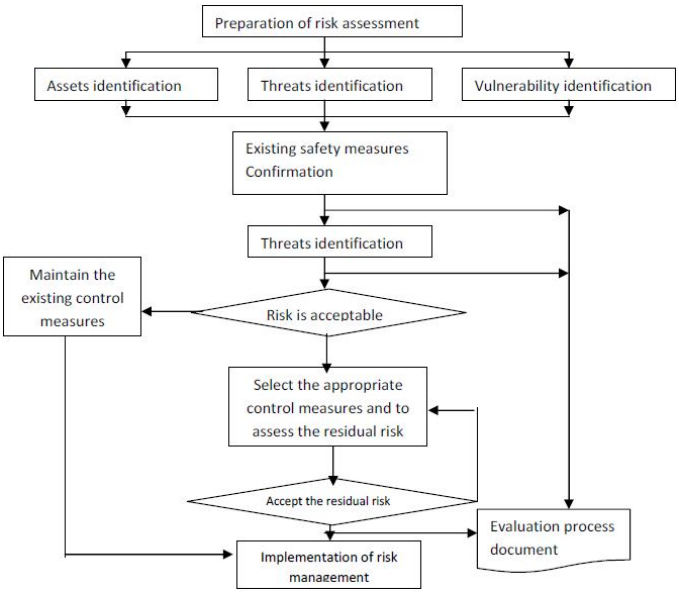

Figure 1: The Process of Information Security Risk Assessment

2.3. Information Security Overview

Security is often achieved by means of several strategies undertaken simultaneously or used in combination with one another. Specialized areas of security include: [10]

- Physical security - Protecting people, physical assets, and the workplace from various threats, including fire, unauthorized access, and natural disasters
- Operation security – Protecting the organization's ability to carry out its operational activities without interruption or compromise.
- Communications security – Protecting the organization's communication media, technology, and content, and its ability to use these tools to achieve the organization objectives
- Network security – Protecting the organization's data networking devices, connections, and contents as well as protecting the ability to use that network to accomplish the organization's data communication functions.

Information security refers to the term that enables to protect the computer system from unauthorized access, use, disclosure, harassment, modification or destruction to provide confidentiality, integrity, and availability [11]. Information security has several important aspects that are known as C.I.A Triad [12], which consists of aspects of Confidentiality, Integrity, and Availability [13]. Confidentiality (C) means that data and information represented by data must be protected in such a way that use is limited only to authorized persons. Integrity (I) means to protect users from unauthorized modification of information. Warranty that data will not be altered without proper authorization. Availability (A) means that protecting users from unauthorized use of denial.

2.4. Information Security Overview

Security is often achieved by means of several strategies undertaken simultaneously or used in combination with one another. Specialized areas of security include: [10]

- Physical security - Protecting people, physical assets, and the workplace from various threats, including fire, unauthorized access, and natural disasters
- Operation security – Protecting the organization's ability to carry out its operational activities without interruption or compromise.
- Communications security – Protecting the organization's communication media, technology, and content, and its ability to use these tools to achieve the organization objectives
- Network security – Protecting the organization's data networking devices, connections, and contents as well as protecting the ability to use that network to accomplish the organization's data communication functions.

Information security refers to the term that enables to protect the computer system from unauthorized access, use, disclosure, harassment, modification or destruction to provide confidentiality, integrity, and availability [11]. Information security has several important aspects that are known as C.I.A Triad [12], which consists of aspects of Confidentiality, Integrity, and Availability [13]. Confidentiality (C) means that data and information represented by data must be protected in such a way that use is limited only to authorized persons. Integrity (I) means to protect users from unauthorized modification of information. Warranty that data will not be altered without proper authorization. Availability (A) means that protecting users from unauthorized use of denial.

2.5. Positioning of VECTOR Matrix and OCTAVE Allegro Methods Against Research Regarding IS Security Risk

We identify several methods used in information security assessments that are oriented towards obtaining product or system certification and involve guidelines and standards from external parties that may not be in accordance with the company's internal circumstances.

In this paper we try to introduce another perspective that suggests the integration of two different approaches method with norms that focus on information system security in considering the organizational and human environment of the organization. In our perspective, the biggest contribution to information security is the development of information security methods that are easily implemented and understood by people in an organization.

The VECTOR Matrix method and the OCTAVE method are both good choices and can be easily understood for information security risk assessment. Although the OCTAVE Allegro method is more complex than the VECTOR Matrix method, and requires more time and effort when applied to the same information security risk assessment for certain assets. Overall the two methods described are complementary and are a good choice for risk assessment in financial institutions.

2.6. VECTOR Matrix

VECTOR matrix is free, open source and quite simple qualitative self-assessment risk method, and was developed to help business systems in defining the priorities of critical risks, including information security risks. The method allows users to easily quantify and visually represent all possible aspects of risk to the business system. VECTOR method is based on universal principles of business risk, scalable for both, small businesses and large enterprise systems, in the domestic and international private sectors [14]. VECTOR method for risk assessment is based on the following formula: RISK= V+E+C+T+O+R: VECTOR is the acronym derived from the following English words:

V = Vulnerability,
E = Ease of Execution,
C = Consequence,
T = Threat,
O = Operational-Importance,
R = Resiliency.

Step 1: Vulnerability (V) – Assess the vulnerability of asset.
V = attributes, characteristics, design flaws, or components of business assets, processes or functions, which make it vulnerable or exposed to exploitation or damage due to cyberattacks, kinetic attacks, or natural disasters. Soft goals (that is, systems or assets that are not protected with widely known weaknesses) increase the vulnerability of an asset while hard targets (that is, systems or assets that are built strongly with additional steps added) reduce the vulnerability of an asset.

Step 2: Ease-of-Execution (E) – Assess ease-of-execution of asset.
E = the level of expertise, advanced training, special tools and equipment needed to successfully complete cyberspace or kinetic attacks. High Ease of Execution implies that an enemy event or disaster requires minimal effort or minimal force to defeat assets (e.g., devices that are not configured with a standard password). While low Ease-of-Execution implies that the enemy requires high-level skills and sophisticated knowledge of system / network architecture to defeat the asset design characteristics and existing security measures (e.g., sophisticated cyberattacks that utilize various exploits for zero days).

Step 3: Consequence (C) – Assess consequence of asset.

C = injuries, loss of life, loss of production, loss of economic value or brand reputation as a result of a successful cyber-attack, kinetic attack, or natural disaster.

Step 4: Threat-Probability (T) – Assess threat-probability of asset.
T = Activities or events that have the potential to disrupt the system and are caused by nation-states, hired hackers, terrorists, hackers, black hats, or natural disasters. To determine the threat of enemy groups, discuss their abilities and history. For the challenges of natural disasters, check the historical floods of storms and seismic data for frequencies and trends. Threat-probability score is the reason the enemy or disaster will succeed for each threat / attack scenario given. The question you can take is the "hint" below, the assessment team can choose several threat / attack scenarios for each asset or can decide on the most likely threat / attack scenario. See the "guide" at the end for additional guidance.

Step 5: Operational-Importance (O) – Assess operational-importance of asset.
O= missions or organizations damaged by successful cyberattacks, kinetic attacks, or natural disasters. Critical assets or key business processes can stop operations throughout the company while less important assets have only a local impact. Redundant, duplicate, and backup systems all reduce Operational-Importance. The top 5% to 20% of the total assets that score high for Operations-Importance must be recognized by management as the organization's most critical assets and special protection and retaliation must be provided to ensure the availability, integrity and confidentiality of assets that are sustained during an attack or natural disaster. Raw ranking sequences that only use Operational-Importance can be used by management to identify and prioritize the organization's most important assets and processes.

Step 6: Resiliency Gap(R) – Asses resiliency gap of asset.
R = is a lack of resilience, a lack of fault tolerance systems (e.g., RAID and SAN) and a lack of planning / readiness by the organization that will enable it to recover, rearrange and reorganize itself to resume operations after a significant cyberattack or natural disaster. Resilience-Gap increases the overall risk of an organization. When an asset is considered to have a low level of resilience, it is inherently risky and results in a high Resiliency-Gap score. Likewise, when an asset is considered to have a high level of resilience, it results in a low Resiliency-Gap score.

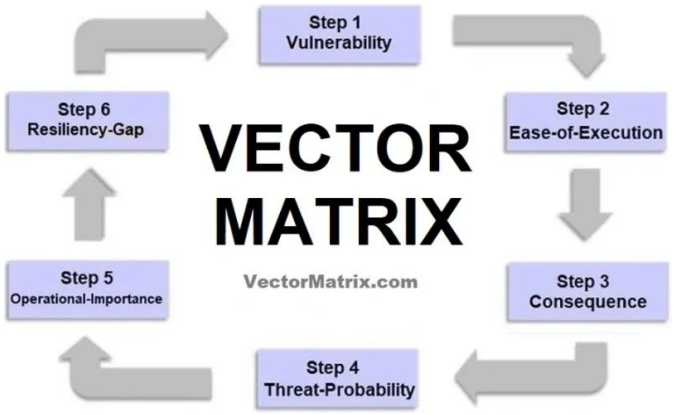

Figure 2: VECTOR Method for Risk Assessment Steps [14]

2.7. OCTAVE Methods

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) enables an organization to sort through the complex web of organizational and technological issues to understand and address its information security risks, OCTAVE defines an approach to information security risk evaluations that is comprehensive, systematic, context driven, and self-directed [15].

At the core of OCTAVE is the concept of self-direction, which means that people from an organization manage and direct the information security risk evaluation for that organization. Information security is the responsibility of everyone in the organization, not just the IT department. The organization's people need to direct the activities and make the decisions about its information security improvement efforts. OCTAVE achieves this by establishing a small, interdisciplinary team drawn from an organization's own personnel, called the analysis team, to lead the organization's evaluation process.

The analysis team includes people from both the business units and the information technology department because information security includes both business and technology related issues. People from the business units of an organization understand what information is important to complete their tasks as well as how they access and use the information. The information technology staff understand issues relates to how the computing infrastructure is configured as well as what is important to keep it running. Both of these perspective are important in understanding the global, organizational view of information security risk.

OCTAVE method is developed at Software Engineering Institute, Carnegie-Mellon University [16]. OCTAVE is a set of tools, techniques and methods for risk assessment and strategic planning of information security. OCTAVE is an acronym of the following English words:

O = Operationally,
C = Critical,
T = Threat,
A = Asset,
VE = Vulnerability Evaluation.

There are three OCTAVE methods:

a. Original OCTAVE method, which is the foundation of all knowledge for OCTAVE
b. OCTAVE-S designed for smaller organizations
c. OCTAVE Allegro a streamlined approach for assessing and ensuring information security, designed for larger organizations.

OCTAVE method is based on the OCTAVE criteria, which are actually standard approach to risk assessment and information security practices. OCTAVE Criteria sets out the basic principles and attributes of risk management using OCTAVE method. Since financial institutions are generally larger organization, the OCTAVE Allegro method is the most appropriate for them.

OCTAVE Allegro is composed of eight step divided into four phases:

- 1st Phase – Participants develop evaluation criteria for measuring risk in accordance with organizational guidelines: the mission of the organization, organizational goals and critical success factors.
- 2nd Phase – Participants prepare profile of any critical information assets with which to establish clear boundaries for the property, identify its security requirements and identify all of its containers.
- 3rd Phase – Participants identify threats to each information asset in the context of container and property.
- 4th Phase – Participants identify and analyse risk information assets and begin to develop approaches for reducing risks.

The eight steps of OCTAVE Allegro methods are:

a. Criteria establishment for measuring risk
b. Development of the information assets profile
c. Identification of containers of information assets
d. Identification of areas of interest (concern)
e. Identification of threats scenarios
f. Risk identification
g. Risk analysis
h. Selection approaches for risk reduction

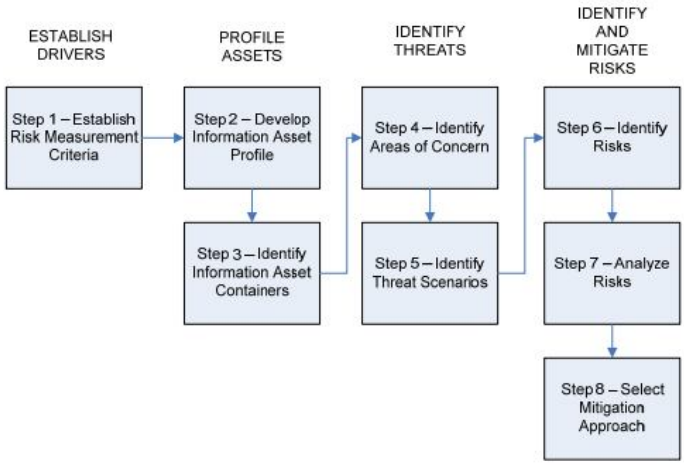

Figure 3: Eight steps and Four Phases Octave Allegro Method [12]

3. COMPARING OF VECTOR AND OCTAVE

The VECTOR Matrix method and the OCTAVE method are both good choices for information security risk assessment but in different implementation steps. As the first step in risk assessment is the recommended VECTOR Matrix method because this method allows users to easily measure and visually represent all possible aspects of business system risk.

When critical risks are determined by the VECTOR Matrix method, a detailed analysis of each identified risk must be carried out. In this step, the VECTOR Matrix method does not provide enough flexibility to describe all aspects correctly. Using the VECTOR Matrix method, each business information or asset is given a score that represents the risk of a potential attack. This risk score does not provide enough information to deal with risk but is used to compare this risk with others to identify critical risks.

Unlike the VECTOR Matrix method, the Allegro OCTAVE method provides a much more detailed and higher analysis and security risk assessment of specific information assets. By using the OCTAVE method it is possible to measure more accurately and consequently better to reduce information security risks for certain properties. However, the Allegro OCTAVE method is more complex than the VECTOR Matrix method and requires more time and effort when applied to the same information security risk assessment for certain assets. Overall the two methods described are complementary and are a good choice for risk assessment in financial institutions.

We can summarize the use of the two approaches to this method as shown below:

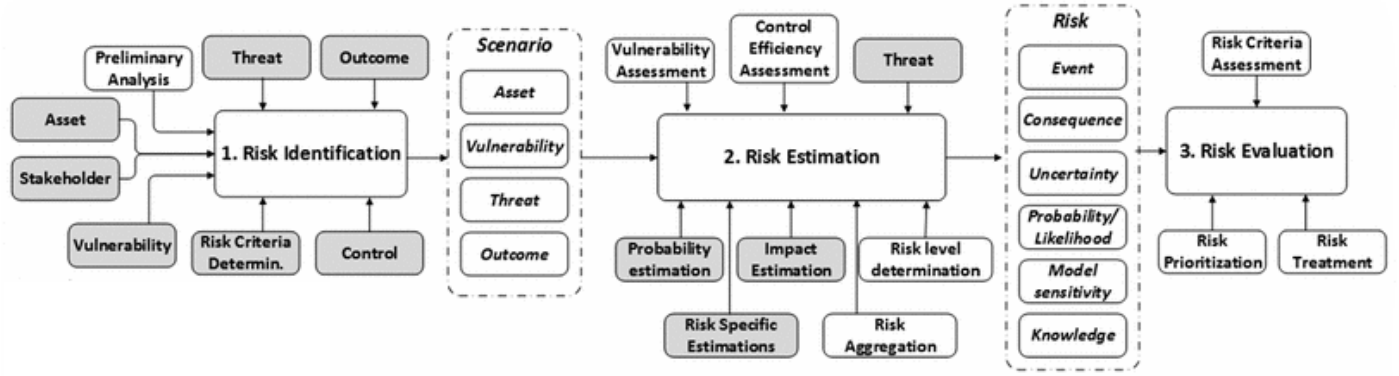

Figure 4: Summary Framework IS Security Assessment Using Two Approach Methods

4. CONCLUSION

Risk management is a critical point in the protection of information assets, especially in the financial industry, therefore it is necessary to use appropriate methods and standards for assessing information security risks. The ultimate goal of the method is to help organizations better manage IT-related risks. Building strict information system security involves continuous improvement, which require additional protection at the operational and organizational levels. With this kind of understanding, we propose an information system security approach that focuses on key attributes: *Adaptive* (flexibility), *Responsiveness* (fast handling), and *Cooperative* (working together between teams based on their needs). The principles of this comprehensive security approach will provide protection at the organizational operational and system level.

What IS Security practitioners can learn is that the reason for choosing the VECTOR Matrix and the Allegro OCTAVE method is that these two methods complement each other well during the information security risk assessment process in the business environment. In the financial sector, the VECTOR Matrix will be the first to be used to prioritize critical risk, which can be made that scales risk scales for each type of information asset. After determining the property with a high level of risk (e.g., operating system firewall), the use of the Allegro OCTAVE risk assessment method is appropriate, which is a far more complex and more accurate method for qualitative analysis and risk assessment of the security of specific information assets. It can be said that the VECTOR Matrix serves as a good basis for the Allegro OCTAVE method for information security risk assessment.

REFERENCES

[1] L. Rahadian, "Industri Pembayaran Digital: Bank dan Fintech Berebut Pasar?," 2019. [Online]. Available: https://finansial.bisnis.com/read/20190225/90/893062/industri-pembayaran-digital-bank-dan-fintech-berebut-pasar. [Accessed: 27-Apr-2019].

[2] OJK, "Penyelenggara Fintech Terdaftar di OJK per 1 Februari 2019," 2019. [Online]. Available: https://www.ojk.go.id/id/berita-dan-kegiatan/publikasi/Pages/Penyelenggara-Fintech-Terdaftar-di-OJK-per-Februari-2019.aspx. [Accessed: 27-Apr-2019].

[3] D. Macek, I. Magdalenic, and N. Ivkovic, "Information Security Risk Assessment in Financial Institutions Using VECTOR Matrix and OCTAVE Methods," in Central European Conference on Information and Intelligent Systems, 2011, p. 133.

[4] G. Stoneburner, A. Y. Goguen, and A. Feringa, "NIST Special Publication 800-30. *Risk Manage. Guide. Inf. Technol. Syst*.," 2002.

[5] I. O. for Standardization, *ISO/IEC 27001: 2013: Information Technology--Security Techniques—Information Security Management Systems—Requirements.* Intenational Organization for Standardization, 2013.

[6] P.Bernard, COBIT® 5-A management guide. Van Haren, 2012.

[7] H. F. Tipton and M. K. Nozaki, Information security management handbook. CRC press, 2007. https://doi.org/10.1201/9781439833032

[8] G. Stoneburner, A. Y. Goguen, and A. Feringa, "Sp 800-30. risk management guide for information technology systems," 2002. https://doi.org/10.6028/NIST.SP.800-30

[9] Fu, Sha, and Y Xiao. "Strengthening the Research of Information Security Risk Assessment." Advances in Biomedical Engineering., vol.9, p.386, 2012.

[10] M. E. Whitman and H. J. Mattord, "Management of Information Security," 2010.

[11] J. T. F. T. Initiative and others, "Guide for conducting risk assessments," 2012.

[12] C. Perrin, "The CIA triad," Dostopno na http//www. techrepublic. com/blog/security/the-cia-triad/488, 2008.

[13] S. Samonas and D. Coss, "THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY.," J. Inf. Syst. Secur., vol. 10, no. 3, 2014.

[14] C. T. Institute, "VECTOR MATRIX ®," 2018. [Online]. Available: https://cyberthreatinstitute.org/vector-matrix. [Accessed: 22-Apr-2019].

[15] C. J. Alberts and A. Dorofee, Managing information security risks: the OCTAVE approach. Addison-Wesley Longman Publishing Co., Inc., 2002.

[16] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing octave allegro: Improving the information security risk assessment process," 2007. https://doi.org/10.21236/ADA470450