View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Center for Scientific Publication

Information Security Risk Management with Octave Method and ISO/EIC 27001: 2013 (Case Study: Airlangga University)

Indri Sulistyowati[1], R. V. Hari Ginardi[1]

Abstract*—Airlangga University has implemented ISO 27001: 2013 in asset-based information security governance, covering information assets, software assets, hardware assets, and human resources assets. However, many vulnerabilities in university computing systems can not be mitigated properly, as evidenced by the continued hacking of university computing systems. It shows that the results of hacking tests on university computing systems are not identified in more detail and are not included in university risk management. The purpose of this research is to build a university information security risk management framework using OCTAVE method based on ISO / EIC 27001: 2013. This research uses the OCTAVE framework to build a risk management framework model. The measurement method will be done by qualitative method to measure the severity and the likelihood of each asset and quantitative method to measure the potential loss on the cost of each asset. The results of this research are expected to provide an information security risk management framework, so that the vulnerability and financial lost analysis of each asset can be a risk, and risk mitigation plans on each asset may consider vulnerability and return of investment.

Keywords*—Information Risk Management, OCTAVE, Vulnerability, Financial Loss Analysis.

I. Introduction

With increasing development of information technology, the utilization of websites and internet networks has become an important part of the college environment. The Greater access to technology results in a better learning environment, but on the other hand the use of websites and the internet network has a significant vulnerability to information security threats. Almost all colleges have advanced technology by providing service facilities such as extensive Wi-Fi support, online learning using websites, digital libraries, virtualization classes, web conferences, and others[1], [2]. Information security at universities will be different when compared to information security in banks that have private security, while the college is a very large open network[2]. Protecting information security from cyberspace hacking is a big enough challenge for universities that have a wide variety of users, including students, faculty, parents, education personnel, and the public. They have access to college computing systems and the possibility of access being done simultaneously[2]. Each user can have different levels of access. In addition to providing secure access to computing systems, universities should be able to maintain information security from vulnerabilities and security breaches such as hacking.

Airlangga University is a very large open network as shown in Figure 1, has a different network device, a variety of software applications and many servers. Airlangga University has implemented an asset-based information security risk management however the current condition in the Airlangga University assesses the risk of assets based on asset sub-classification so that the analysis of risk on assets cannot be specific to each asset.

II. Method

Vulnerability analysis in college information security can use National Vulnerability Database (NVD)[2]. NVD is a database for security checks, software vulnerabilities related to security, configuration errors, product names, and impact metrics[3], [4]. Vulnerability to information security can be obtained from automated tools such as acunetix, any vulnerability detected at scanning has CVE code[4]. The CVSS risk estimation model estimates the security risk level of vulnerability information as a combination of exploitation period and frequency of occurrence to estimate the impact of CVSS[5], [6], with 4 risk types of low, medium, high, critical[6].

Based on the results of the literature study there are many models of risk assessment management, but the mechanisms to assist universities in determining the best model, which considers the information security challenges in identifying and testing the hacking of college computing systems. The purpose of this study is to create a university information security risk management framework using the OCTAVE method based on ISO/EIC 27001: 2013. Many information security risk management models are available but the college computing environment is different from other organizations because it has a large and open environment and consists of multiple small networks that vary and have a variety of user models. Selection of risk model without analysis only resulted in the implementation of security controls in the wrong place, waste of resources, cost and make the organization vulnerable to unexpected threats.

[1]Indri Sulistyowati is with Magister Management Technology, Institut Teknologi Sepuluh Nopember Surabaya, Indonesia. Email: indri16@mhs.mmt.its.ac.id.

[2]R. V. Hari Ginardi is with Informatic Departement, Institut Teknologi Sepuluh Nopember Surabaya, Indonesia. Email: hari@its.ac.id

The OCTAVE method is used to create a risk management framework[7], [8]. OCTAVE (Operationally Critical Threat, Asset and Vulnerability), developed by CERT is a model for strategic risk assessment and strategic planning based on risk[9], [10]. Risk mitigation is based on vulnerability and must be adjusted to the existing clauses in ISO/IEC 27001:2013[11]–[13] to obtain a risk mitigation plan that fits the information security standard. any risk mitigation should be calculated as loss expectancy to determine the level of expenditure that the college spent in tackling the risk[14], [15]. ROI (return of investment) is the ratio of the value of an investment relative to the amount of value invested. In an information security risk analysis, ROI is used to make a decision whether a risk-handling risk-based risk action is appropriate for execution. The appropriateness is when the ROI has a value of more than or equal to 2: 1[16] [17].

Risk assessment at Airlangga University is based on asset. The main objective in risk assessment is to control the security of information based on the vulnerability contained in the organization's assets, so that security control can be done effectively. The proposed model is based on the most popular risk framework currently used, OCTAVE (Operationally Critical Threat, Asset and Vulnerability), developed at Carnegie Mellon University. The proposed framework undertakes a three phase activity, as shown in Figure 2.

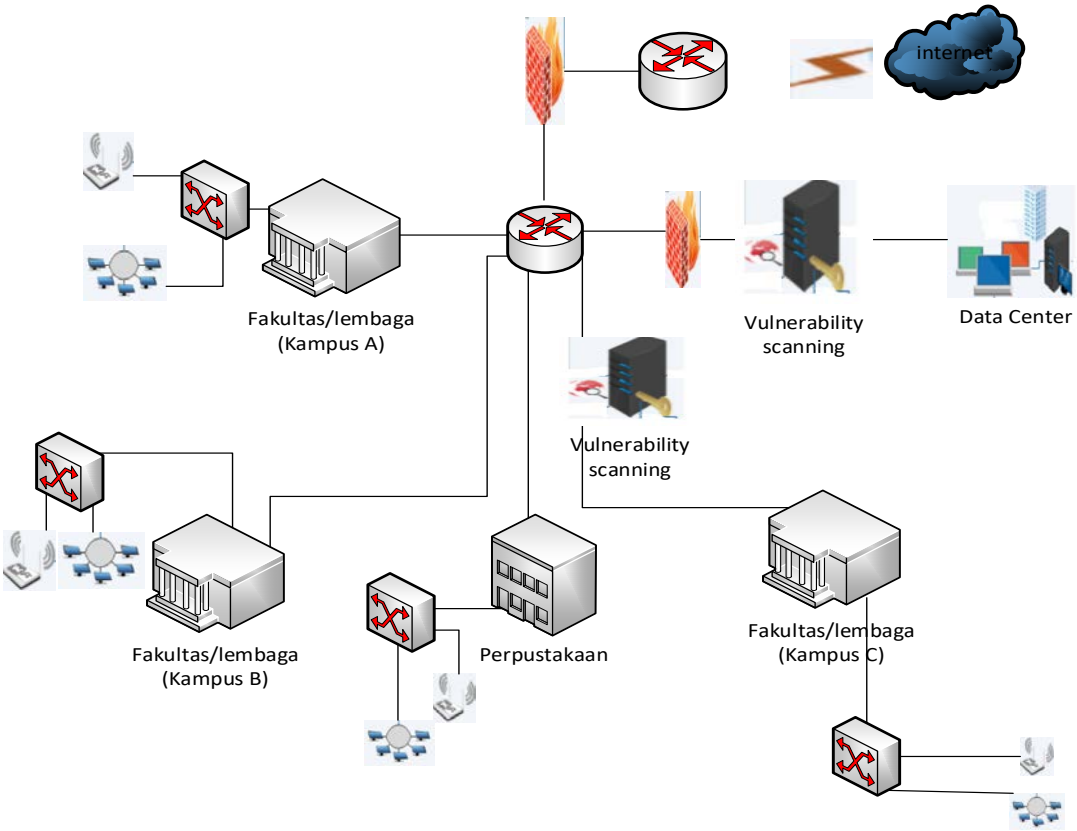

Figure 1. Airlangga University network topology

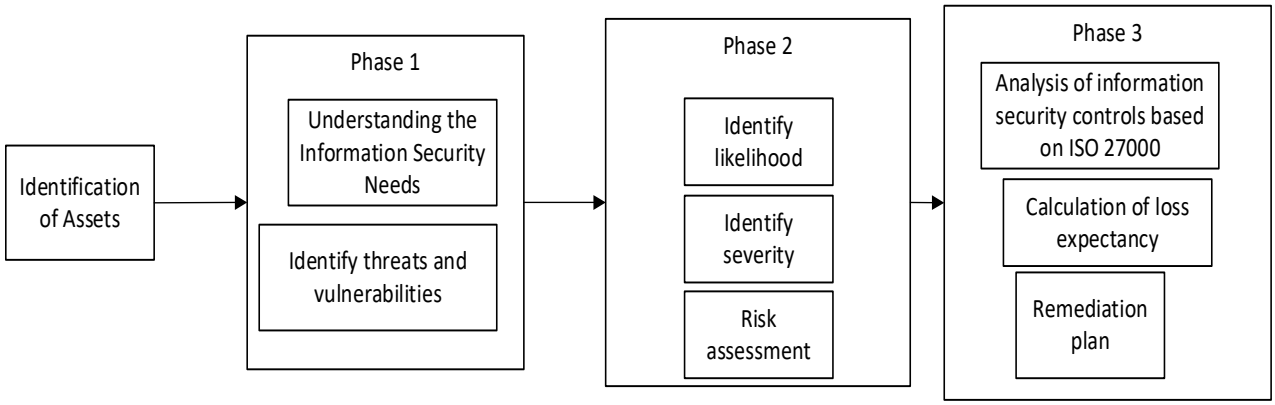

Figure 2. Steps of information security risk assessment

III. Results and Discussion

A. Aset Identification

Assets are everything that has a certain value for the organization. Airlangga University has defined organizational assets covering hardware assets, software assets, human resource assets, and information assets. Hardware e.g. laptops, servers, printers, but also cellular phones or USB memory sticks. Software are not only purchased software, but also freeware and applications. Information are not only in electronic media (databases, files in PDF, Word, Excel, and other formats), but also in paper and other forms, such as contract documents with third parties, logs, databases, procedural guidelines, work instructions. Human Resources are also considered assets because they also have a lot of information in their heads, which is often not available in other form.

Asset identification such as asset id, asset name, custodian, and ect. Asset value calculation is based on CIA (confidentiality, integrity and availability) to find out the important assets of the organization.

The security requirements of information assets will focus on the confidentiality, integrity and availability of information. Information may not be seen by unauthorized personnel (information), information can be modified only by authorized personnel, information must be available whenever requested [18].

Level of confidentiality of information, Note: high (value = 3) = Very confidential information where disclosure of information will illegally threaten business continuity, medium (value =2) = Confidential information but the impact caused by unauthorized disclosure of information is possible to be handled properly without significant impact on business continuity, low (value =1) = Information is not confidential and has no impact due to unauthorized disclosure of the Information.

Integrity and correctness of data, Note: high (value =3) = truth and integrity Information is needed where mistakes and mistakes will have a significant impact on business continuity, medium (value =2) = the truth and integrity of information needed but business impact caused by loss of integrity and truth of information it allows it to be handled well, low (value =1) = the truth and integrity of information does not have a negative impact on business or organization.

Availability of information is when the information is needed by all parties who need it. Note: high (value =3) = Availability of information is needed for the continuity of business, medium (value =2) = Availability of information needed but delay in availability of information within a certain period of time does not have a significant impact on business and organization, low (value =1) = Information is not needed and does not have a negative impact on the business.

Software assets are applications services and software services. Identification of security requirements is not focused on information that is processed, sent, or stored by the application. However, the security requirements parameters are based on: the application may not be used by unauthorized personnel (confidentiality), the application can only be modified by authorized personnel (integrity), the application must be available during normal business hours (availability)[17].

Level of confidentiality of software or application may not be used by unauthorized personnel (confidentiality) Note: high (value =3) = if the Software or application is used illegally by personal will have a negative impact on business continuity, medium (value =2) = if the Software or application is used illegally by the person can handled well so that it does not have a significant impact on business continuity, low (value =1) = if the Software or application is used illegally by personal does not have any impact on the business

Software or applications can only be modified by authorized personnel (integrity) Note: High (value =3) = If the software or application modified by unauthorized personnel can have a significant impact on business continuity, Medium (value =2) = If software or applications modified by unauthorized personnel can be handled properly so that it does not have a significant impact on business continuity, Low (value =1) = If the software or application is modified by unauthorized personnel it does not affect the business and organization

Software or applications should be available during normal business hours (availability). Note: High (value =3) = If the software or application is not available during normal business hours can interfere with business continuity, Medium (value =2) = If the software or application is not available during normal business hours can be delayed in a certain period of time without any impact that is significant for business continuity, Low (value =1) = If the software or application is not available during normal business hours it has no impact on the business and organization

The security requirements of hardware assets are not on information that is processed, sent, or stored by hardware, but on modification of hardware assets that focus on adding or removing hardware (eg, removing disk drives or adding modems). Confidentiality generally does not apply to physical hardware. Availability focuses on whether assets are physically available or accessible. As a guideline for hardware assets, hardware can only be modified by authorized personnel (integrity), hardware must be accessible to authorized personnel during normal business hours (availability)[17].

Hardware can only be modified by authorized personnel (integrity). Note: high (value =3) = If hardware can be modified by unauthorized personnel it will have a significant impact on business continuity, medium (value =2) = If hardware can be modified by unauthorized personnel it will not have a significant impact on business continuity, low (value =1) = If hardware can be modified by unauthorized personnel that have no impact on business continuity.

Hardware should be accessible during normal business hours (availability). Note: high (value =3) = If hardware is not accessible during normal working hours it has a very significant impact on business continuity, medium (value =2) = If hardware is not accessible during normal business hours it does not have a very significant impact on business continuity, low (value =1) = If hardware is not accessible during normal business hours has no impact on the sustainability of business and organization.

Security requirements on people assets are on availability. Asset people are special cases, when people are identified, because of some special skills they have or because of the services provided. Thus, the availability of services or assets is the main requirement. The following are examples of guidelines for people's assets. IT staff must provide continuous and consistent network management systems and services (availability). When identifying people as assets, determine whether there are related assets, for example, identifying the main system used or the type of information that the person knows[17].

Availability of people, Note: high (value =3) = Availability of people is needed and if the unavailability/absence of people will have a significant impact on business continuity, medium (value =2) = Availability of people is needed but unavailability / absence of people in a certain period of time will not significantly affect business continuity, low (value =1) = Availability of not needed and the unavailability/absence of people will not have an impact on business continuity.

Each asset is carried out by asset valuation calculated from the Confidentiality, Integrity and Availability aspects based on this formula:

$$\text{Asset Value} = (\text{Confidentiality} + \text{Integrity} + \text{Availability})/3 \quad (1)$$

The CIA component is needed two, for example integrity and availability, the asset value can be calculated using the formula:

$$\text{Asset value} = (\text{Integrity} + \text{Availability}) / 2 \quad (2)$$

The CIA component is needed only available (for example), the asset value can be calculated using the formula:

$$\text{Asset value} = \text{Availability} / 1 \quad (3)$$

When the asset value 3 is high, value 2 is medium, and value 1 is low. Every asset that has a value of more than or equal to 2 will be identified based on phases 1, 2 and 3.

B. OCTAVE Phase

The first phase of information security risk management is to analyze an organization's information assets to identify current condition, threats and, vulnerabilities, this can be done by vulnerability assessment or penetration testing. The results of the first phase are used as inputs in the second phase.

Identifying current conditions is a process to explain the conditions that cause threats and vulnerabilities can be used by other parties who do not have authentication and authorization to infringe information security on organizational assets. Supporting documents in improving information security risk in universities such as standard operating procedures, work instructions, record, and other legal documents should be explained in the current condition column whether the document already exists and/or is implemented. If these documents do not yet exist and/or have not been implemented, then the remediation plan for the document must be present or executed. Operations, incidents, and problems related to information security risk that occur and/or are likely to occur should be explained in the current condition column so that they can identify the remediation plan needed.

The identification of possible threats in the Airlangga University is as follows: Spam, Ramsomware, Malware: some e-mails of civitas academik at Airlangga University get spam email containing fake bidding letters for financial gain, and there are some personal computer or server affected by malware that impact the disruption of website performance and email civitas academic with domain @unair.ac.id received by the recipient as spam. Virus: computer virus can spread through various media such as storage media, social media like facebook, twitter, etc. Information leakage: leakage of information on employee personal data, server configuration leakage, system log leakage. Reputation: Domain and IP Address of the organization may be included in the organization's blacklist list or security company.

Identification of vulnerability can be done by vulnerability assessment or penetration testing on assets. The scanning process is done on the internal network under the firewall as shown in Figure 1. The scanning results can be known if there is misconfiguration system and other vulnerability, it represents the perception of internet users. The automatic tool used to detect vulnerabilities is acunetix. The result of vulnerability scanning on one of the website of Airlangga University can be seen in table 2. The next is risk priority based on the impact to the system by using CVSS method. Frequency vulnerability is calculated from the date the vulnerability appears in the system. The final CVSS score was obtained from mathematical calculations of CVSS base score, CVSS temporal score, CVSS environmental score [6]. The calculation of the final score score is made by utilizing CVSS calculator [7]. The numerical score for the CVSS V3 [1] [6] risk level is calculated using the range 0-10, and translated into qualitative representations (low, medium, high, and critical) to help organizations correctly assess and prioritize vulnerability management processes, as shown in Table 1. Likelihood is the vulnerability detected by acunetix has the possibility of hacking within a year, then scaled as shown in table 2.

TABLE 1.
SEVERITY RATING SCALE

Rating scale	Risk Category	Description
9.0 to 10.0	Critical	Identified risks can stop the organization's business continuity and can make a bad

		reputation for the organization, should require immediate action to reduce the possibility of occurrence
7.0 to 8.9	High	Identified risks can stop the organization's business continuity, should require a remediation plan to be implemented as soon as possible.
4.0 to 6.9	Medium	The risks identified have the effect of stopping the organization's business over a short period of time, requiring that the remediation plan be carried out to reduce risk.
0.1 to 3.9	Low	The risks that occur have no impact on business continuity, further risk reduction plans should be implemented with other security enhancements

TABLE 2.
LIKELIHOOD RATING SCALE

Value	Quantity
Critical	> 12 Time per Year
High	7 time every year - 11 time per year
Medium	1 time every year - 6 time per year
Low	< 1 time every year

The level of information risk exposure (final risk value) is determined based on the multiplication of Probability with Severity, which is then mapped in the information risk map or guided by table 3. Conclusion of results The final risk value is if low the risk is acceptable, if the medium can be suspended or can accepted on condition, and if high the risk must be mitigated or transferred.

The third phase is a step to analyze information security control based on ISO/IEC 27001:2013 then make remediation plan, calculate lost expectation, and calculate ROI. Based on the vulnerability obtained by scanning one of the websites at Airlanga University there are several vulnerabilities as shown in Figure 3 that are mapped in ISO/IEC 27001:2013 as shown in table 4. In this paper risk mitigation is carried out at all levels of the final risk value to minimize the possibility of information leakage.

TABLE 3.
FINAL RISK VALUE

		Probability			
		Critical (value = 4)	**High (value =3)**	**Med. (value=2)**	**Low (value=1)**
Severity	**Critical (value = 4)**	High	High	High	Medium
	High (value =3)	High	High	Medium	Medium
	Medium (value=2)	High	Medium	Medium	Low
	Low (value=1)	Medium	Medium	Low	Low

The corrective actions on the number 2 and 10 vulnerability described in table 2 are improvements for programming scripts, then the vulnerability number 1,4,5,6,7,8,9 are fix the system configuration on the website server, and the vulnerability number 3 is by to update the current javascript version to the latest version. It is estimated that once in one year there will be hacking due to vulnerability in table 2, this incident will impact on the leakage of information stored on the website server, declining domain reputation and IP Address Airlangga University. Airlangga University website server can be infected by spam and malware.

Each vulnerability in assets should be calculated asset value (AV), then exposure factor (EF), then anualized rate of insurance (ARO), then single lost expectation (SLE), then annual loss expectation (ALE). ALE (current) or pre-control is the annual loss expectation of the risk before the control is implemented. whereas ALE (projected) or post-control is ALE which is checked after the control is implemented

Corrective action needed assistance of expert services with unit cost IDR. 150.000, - per alerts that have been found, and the total repair cost is IDR. 3.750.000, -, so that the ROI (return of investment) obtained by 3: 1 is calculated based on ALE current and ALE projected shown in table 5.

Airlangga University should implement standard operational procedures in the development source code to avoid possible vulnerabilities on the website to reduce risk of information security website. Reduce the risk of server assets, regular server hardening must be done. Reduce the risk of human resource assets, by conducting skills training in making source code in accordance with standard information security. Reducing risk to information assets, is to classify important assets at Airlangga University and how to manage these assets. The identification of classify of information assets such as public categories are categories of assets that can be accessed by the public, internal categories are categories of assets that can be accessed by internal organizations, the restricted category is that which can be accessed by certain people in the organization.

TABLE 4.
VULNERABILITY MAPPING OF ISO/IEC 27001:2013 CONTROL

No	Vulnerability	Severity	Total Alert	Threat Category	Control ISO 27001
1	.htaccess file readable	Medium (2)	2	information leakage, reputation, spam and malware	annex 8.2.3; 9.4.1 ; 12.4.2 ; 12.4.3 ; 12.5.1 ; 18.1.3 ; 18.1.4
2	HTML from without CSRF protection	Medium (2)	1	information leakage	annex 9.2.3
3	Vulnerability Javascript library	Medium (2)	1	information leakage, reputation, spam and malware	annex 12.5.1

4	Possible sensitive directories	Low (1)	11	information leakage	annex 8.2.3; 9.4.1 ; 12.4.2 ; 12.4.3 ; 18.1.3 ; 18.1.4
5	possible sensitive files	Low (1)	4	information leakage	annex 8.2.3; 9.4.1 ; 12.1.4 ; 12.4.2 ; 12.4.3 ; 14.3.1 ; 18.1.3 ; 18.1.4
6	Documentation file	Low (1)	2	information leakage	annex 8.2.3; 9.4.1 ; 12.4.2 ; 12.4.3 ; 18.1.3; 18.1.4
7	Clickjacking : X-frame-Options header missing	Low (1)	1	information leakage, reputation, spam and malware	annex 18.4.1
8	Cookie(s) without HttpOnly flag set	Low (1)	1	information leakage	annex 12.5.1
9	Cookie(s) without Secure flag set	Low (1)	1	information leakage	annex 12.5.1
10	Login page password-guessing attack	Low (1)	1	information leakage	annex 9.2.3 ; 9.3.1 ; 9.4.3 ; 12.5.1

TABEL 5.
ALE CURRENT AND ALE PROJECTED

No	Vulnerability	AV	EF	ARO	SLE	ALE current	ALE projected
1	.htaccess file readable	20,000,000	1	0.1	20,000,000	2,000,000	-
2	HTML from without CSRF protection	20,000,000	1	0.1	20,000,000	2,000,000	400,000
3	Vulnerability Javascript library	20,000,000	1	0.1	20,000,000	2,000,000	400,000
4	Possible sensitive directories	20,000,000	0.5	0.1	10,000,000	1,000,000	-
5	possible sensitive files	20,000,000	0.5	0.1	10,000,000	1,000,000	-
6	Documentation file	20,000,000	0.5	0.1	10,000,000	1,000,000	-
7	Clickjacking : X-frame-Options header missing	20,000,000	0.5	0.1	10,000,000	1,000,000	-
8	Cookie(s) without HttpOnly flag set	20,000,000	0.5	0.1	10,000,000	1,000,000	-
9	Cookie(s) without Secure flag set	20,000,000	0.5	0.1	10,000,000	1,000,000	-
10	Login page password-guessing attack	20,000,000	0.5	0.1	10,000,000	1,000,000	-
	Total Kerugian per tahun					13,000,000	800,000

The OCTAVE method can be used to create information security risk management by combining qualitative assessment obtained from automated tools such as acunetix with risk ranking process using CVSS and quantitative assessment is done with potential lost and return of investment of each vulnerability. The ROI value of the estimation of hacking prevention actions on one of the websites at Airlangga University makes the countermeasures suitable for execution, since the value is equal to 3: 1.

The OCTAVE method can also be used to identify organizational assets, assess and determine important organizational assets, then be able to identify current conditions related to the security of organizational information, threats, and vulnerabilities of each of the organization's important assets. Each of these risks can be assessed as severity and likelihood, which can then be obtained by the value of risk to classify the level of risk, then mapped into ISO / IEC 27001: 2013 to create a risk mitigation plan. The tool used to obtain vulnerabilities in website assets is an automated tool, acunetix.

IV. CONCLUSION

This paper proposes information security risk management for the college environment using OCTAVE and ISO/IEC 27001:2013 methods. This framework makes it possible to accommodate security issues associated with Higher Education Institutions, in a well-structured way, the practical implementation of this framework by defining the use of scanning, assessment and reporting of "support tools" to perform various stages of the process efficiently. The purpose of the proposed model is to reduce the risk of security breaches, the feasibility of the proposed improvement method based on lost expectancy and return of investement. The proposed framework may be applied to higher education or college IT environments; this allows the college to stay one step ahead of security threats and also to get more value from the college security budget, focusing on the really important assets that are really at risk.

REFERENCES

[1] C. Joshi and U. K. Singh, “Information security risks management framework – A step towards mitigating security risks in university network,” *J. Inf. Secur. Appl.*, vol. 35, pp. 128–137, Aug. 2017.

[2] U. K. Singh, C. Joshi, and N. Gaud, “Measurement of security dangers in university network,” *Int. J. Comput. Appl.*, vol. 155, no. 1, pp. 975–8887, 2016.

[3] C. Joshi, K. Singh, and K. Tarey, “A review on taxonomies of attacks and vulnerability in computer and network system,” *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 5, no. 1, pp. 742–747, 2015.

[4] A. Tripathi and U. K. Singh, “Analyzing trends in vulnerability classes across CVSS metrics,” *Int. J. Comput. Appl.*, vol. 36, no. 3, pp. 38–44, 2011.

[5] FIRST, “CVSS v3.0 Specification Document.” [Online]. Available: https://www.first.org/cvss/specification-document.

[6] NIST, "NVD - CVSS v3 Calculator." [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

[7] B. Supradono, "Manajemen risiko keamanan informasi dengan menggunakan metode octave (operationally critical threat, asset, and vulnerability evaluation)," *MEDIA Elektr.*, vol. 2, no. 1, pp. 4–8, 2009.

[8] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," Pittsburgh, Pennsylvania, 2007.

[9] C. Alberts, A. Dorofee, and J. Stevens, "Introduction to the OCTAVE ® Approach," Pittsburgh, Pennsylvania, 2003.

[10] C. J. Alberts and A. J. Dorofee, "OCTAVE SM Criteria, Version 2.0," Pittsburgh, Pennsylvania, 2001.

[11] International Organization for Standardization (ISO), *ISO/IEC 27001 Information technology-Security techniques-Information security management systems-Requirements en*. Geneva: International Organization for Standardization (ISO), 2013.

[12] International Organization for Standardization (ISO), *ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls*. Geneva: International Organization for Standardization (ISO), 2013.

[13] International Organization for Standardization (ISO), *ISO/IEC 27005:2011 - Information technology -- Security techniques -- Information security risk management*. Geneva: International Organization for Standardization (ISO), 2011.

[14] R. Bragg, *CISSP certification : training guide*. Indianapolis: Pearson Education, 2003.

[15] D. Dekhoda, "Combining IRAM2 with Cost-Benefit Analysis for Risk Management Creating a hybrid method with traditional and economic aspects Dorna Dehkhoda," Luleå University of Technology, 2018.

[16] D. W. Sudiharto, "Analisa resiko keamanan informasi (information security). studi kasus: poliklinik XYZ," in *Seminar Nasional Informatika (SEMNASIF)*, 2011, vol. 1, no. 5.

[17] C. Alberts and A. J. Dorofee, *Managing Information Security Risks: The OCTAVESM Approach*. Addison-Wesley Professional, 2002.