p-ISSN: 2655-8807
e-ISSN: 2656-8888

The Octave Allegro Method in Risk Management Assessment of Educational Institutions

Jane Hom[1], Boonsri Anong[2], Kim Beom Rii[3], Lee Kyung Choi[4], Kenita Zelina[5]
Ubon Ratchathani University[1], Sukhothai Thammathirat Open University[2], Jisan College[3], University of Miyazaki[4], Raharja University[5]

e-mail: janehom@yahoo.com [1], boonsri99@yahoo.com [2], kimbeomrii@yahoo.com [3], eekyungchoi@yahoo.com , kenita.zelina@raharja.info[5]

Autor Notifications
23 July 2020
Final Revised
24 August 2020
Published
30 September 2020

Hom, J., Anong, B., Rii, K. B., Choi, L. K., & Zelina, K. (2020). The Octave Allegro Method in Risk Management Assessment of Educational Institutions. Aptisi Transactions on Technopreneurship (ATT), 2(2). 167-179.
https://att.aptisi.or.id/index.php/att/article/view/103

Abstract

Risk management is useful in overcoming various problems such as not optimal business processes, the company's reputation down, financial loss, or bankruptcy of a company. In the application of information systems, most organizations or companies have not noticed the importance of information systems security as well as the assets and impacts that arise. For that, the risk management assessment is used in reducing the errors that occur in the information system of the company's business processes. The risk management assessment is applied to the information system along with its assets in evaluating the possibilities of menaces and vulnerabilities. The Risk management assessment analysis is applied to the academic information system in universities. The result of the risk assessment is the results of recommendations on the stages that need to be done in protecting the assets of information systems and information systems themselves.

Keywords: *Assessment; Risk management; Information Systems*

1. Introduction

Lately, Information technology is often implemented to boost the business strategy in a company, upgrade the business processes and the standard of services. Information technology in its application often carries risks, therefore risk management should be considered. The risk management assessment is used to reduce the damage that occurs in the information system of the company's business processes. In both business and academic processes, information systems are used as supporters to improve the profit, plans, promotion, communication, incorporation, and smooth activities in the academic.[1]. But in fact there are still a few educational institutions that carry out a risk assessment in the ongoing information system, although information systems are important in a business process at educational institutions. If a problem arises in an information system, it will impede the business process that runs within the university[2].

This is the base for conducting a risk assessment at a university using the Allegro OCTAVE method. The research centers on identification, analysis and risk assessment of academic information systems in universities using the OCTAVE Allegro method. The risk management assessment set up is expected to reduce tackling various business issues such as nonoptimal business process, corporate reputation down, financial loss, or bankruptcy of a company.

Below is a formulation of the problem of risk assessment in universities:

1. The implementation of the university's risk management information system has not been implemented yet, so the magnitude of risk impact is difficult to be assessed.
2. The integrity of information systems is lacking, resulting in some departments not fully implementing an information system impacting the lack of coordination in the University.
3. The security of sensitive information technology results in slow action taking in risk prevention and mitigation.
4. The delivery of the value of information assets by management is still difficult due to lack of supporting data or documentation.

The objectives of this risk management Information system assessment are:

1. The risks which influence the security of information assets can be known.
2. Gain design and protection strategy in tackling the risks that arise.
3. Improvement of information system security can be achieved by developing information system security strategy.
4. To identify, analyse and manage the risk of academic information systems at higher education using the OCTAVE Allegro method.
5. The risk management policy is established in supporting mission and organizational priorities to reduce the impact of damage from information systems.

The benefits of this risk management Information system assessment are:

1. Be able to know what is the impact of information system risk, so that it can be taken the right step in tackling the information system risk.
2. Get a protection strategy set up to reduce information system security risks.
3. The value of the importance of information owned assets can be conveyed properly.

2. Research Method

Information system is a system that exists in the organization and has the needs to support daily transactions, support actions, strategic and managerial operations of an organization and provide reports required by certain outside parties. The information system is a collaboration of hardware, software, communication networks, resources, people and a set of policies and procedures used to obtain, process, archive, change and distribute information in an organization[3].

Risk is the potential for disadvantage or destruction due to an action. Managing risk should be well done and structured in detail. It is a systematic procedure in dealing with doubts related to menaces or collection of human activities as well as risk assessment, in improving strategies to process and minimize risk with resource management. The strategy taken, that is to move the risk to the other, get rid of the risk, minimize the negative effects of

p-ISSN: 2655-8807
e-ISSN: 2656-8888

risk, and lastly to provide some or every consequence that the risk has[4].

Risk management is a procedure of recognizing, analyzing and determining actions in order to avoid menaces. The process of risk management is done to address the risks involved in an organization. Risk management is an iterative process regarding the analysis, designing, application, controlling, oversight of strategies and stages to apply security policies[3].

The consequences of financial damage, the decline in the company's reputation, stalled business operations, collapse of assets can be valued and the slow decision-making process can be reduced by the risk management of information technology [5].

Appropriate controls need to be recognized and implemented in the organization to ensure adequate information security is ensured [6]. Organizations are assisted by information security in the providing the required level of security[7].

The information system and its assets are very vulnerable to the risk of physical damage and the risk of logical damage[8]. Can solve this problem because of damage, theft, vandalism, natural disasters, and power surges. Risk of logical damage issued by unauthorized access and intentional or unintentional damage to information and data systems [9] therefore identification of menaces along with risk analysis should be done in order for existing security to increase and risk of damage to the information system can be reduced. Risk Analysis has various benefits, one of which is forming a cost-to-value in security protection. In addition, it also has an impact on decision making with regards to hardware and software system Settings [10].

3. Findings

OCTAVE *(operationally Critical Threat, Asset, and Vulnerability Evaluation)* are methodologies that function in identifying and evaluating information security[11] risks. Organizations can produce information protection with risk decision-making referring to CIA (*Confidentiality, Integrity, Authentication*) to the assets of critical information technology by implementing the OCTAVE method [12]. OCTAVE is applied to assist the company in terms of:

- Development of qualitative risk evaluation criteria that resulted in the company's operational risk tolerance.
- Understand valuable assets for the mission in the company
- Understand Weaknesses and menaces to assets.
- Determination and evaluation of things that may happen for the company if menaces arise.

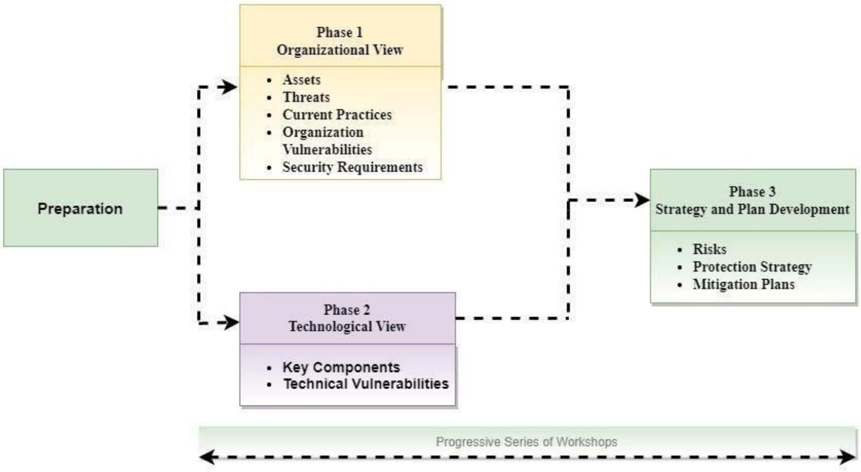

Figure 1. OCTAVE Stages [13]

There is a possible challenge that arises when OCTAVE Allegro is used a

method of risk assessment of information systems[14] The changing mindset, from which the technically-focused turns into a focus on business. Then the structure of the confederacy existed in university. Furthermore, there is a university environment that has openness. And the last one is to make adjustments with the outside or third parties. There are three methods of the OCTAVE that can be applied. These three methods include the OCTAVE, OCTAVE-S, and OCTAVE Allegro methods. These Methods are used to get the specific needs of OCTAVE users in risk assessment[15]. An extensive assessment of the organization's risk environment carried out to obtain better results as with the goal of this OCTAVE Allegro method. The approach is not the same as the OCTAVE approach, because OCTAVE Allegro concentrated on information assets in terms of usage, storage, transfering, processing, response to menaces, vulnerabilities and interferences as a result [16]. The OCTAVE Allegro approach is more specific to the information assets and data of the information. In the OCTAVE Allegro method, there are four main phases:

p-ISSN: 2655-8807
e-ISSN: 2656-8888

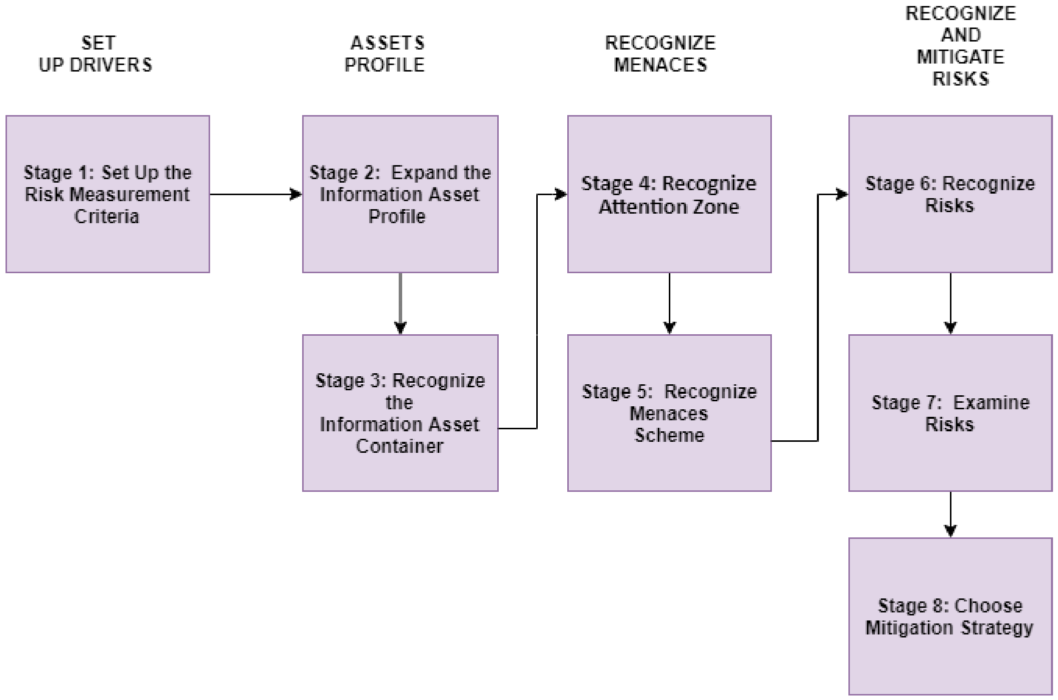
SET UP DRIVERS
ASSETS PROFILE
RECOGNIZE MENACES
RECOGNIZE AND MITIGATE RISKS
Stage 1: Set Up the Risk Measurement Criteria
Stage 2: Expand the Information Asset Profile
Stage 3: Recognize the Information Asset Container
Stage 4: Recognize Attention Zone
Stage 5: Recognize Menaces Scheme
Stage 6: Recognize Risks
Stage 7: Examine Risks
Stage 8: Choose Mitigation Strategy

Figure2. OCTAVE Allegro Steps [16]

The risk management information system assessment activity begins with conducting interviews directly to the head of finance, the head of the Student Academic Administration Bureau and the head of IT, to convey the purpose of holding this Risk Information System Risk Assessment to obtain the required data.

After the preparation is complete and all required data is supported, an information system risk assessment can be done using the OCTAVE Allegro method containing eight stages.

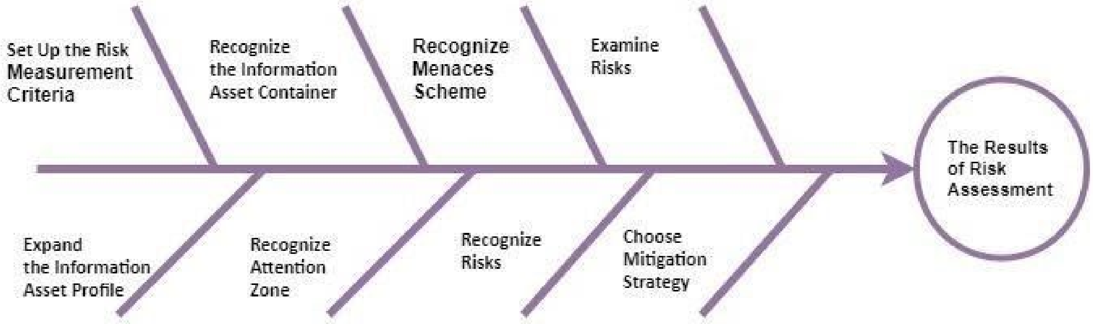
Set Up the Risk Measurement Criteria
Recognize the Information Asset Container
Recognize Menaces Scheme
Examine Risks
The Results of Risk Assessment
Expand the Information Asset Profile
Recognize Attention Zone
Recognize Risks
Choose Mitigation Strategy

Figure. 3. Framework

Stage 1: Set Up the Risk Measurement Criteria

By interviewing the head of the Student Academic Administration Bureau, IT Head, chief of finance staff, and existing staff at the university to determine the criteria for risk assessment. Criteria can be determined by setting the impact area and its priority. Mission and business objectives should also be considered in the determination of the impact area. The result is an area of impact that encompasses the reputation and trust of customers, finance, productivity, safety and health, as well as fines and penalties. The results of the impact Area determination – the reputation and trust of the customer are in table 1 and the priority scale of the impact area is in table 2.

Table 1. Impact Area-Reputation and trust

Impact Area	Low	Are	High
Reputation	Slight influence on reputation; Minimal effort required for improvement	Adverse impacts, on reputation and effort and costs needed for improvement	A devastating impact on reputation is almost irreversible
Customer Trust	Reduction of customers caused by loss of trust is less than 2%	Reduction of customer due to loss of trust from 2% to 10%	Reduction of customer due to loss of trust of more than 10%

Table 2. Impact Field Priorities

Priority	IMPACT AREA
5	Customer Reputation and Trust
3	Financial
4	Productivity
1	Safety and Health
2	Fines and Penalties

Stage 2: Expand the Information Asset Profile

In expanding the profile of an information asset, the asset of the information used is information relating to the core process of that organization, must be determined by the critical information asset based on the core process of that organization, and further written on the Critical Information Asset worksheet in the OCTAVE Allegro method. The items that should be observed in the selection of information assets are:

- Valuable and necessary information assets when doing the daily work.
- An asset of information that if not exist could impede the organization in reaching its objectives and mission.

After the election, it can be determined the important information assets are student profile, lecturer profile, student course schedule, student attendance, lecturer attendance and student grades. Table 3 contains an example of an information asset profile on a lecturer's attendance.

Table 3. Examples of information asset profile-lecturer attendance

Critical assets		Lecturer Attendance
The reason in Election		A prominent lecturer in teaching activities that has been adapted to the study plan of Semester (RPS) in each university. If the lecturer's attendance is not appropriate from the planned RPS target, then the learning achievement in the subject is not maximal.
Explanation		This asset consists of study program, semesters, courses, classes, lecturers, and date of attendance
Holder		IT Division
Secur ity Requi rements	***Confidentiality***	Confidentiality of lecturers attendance information is important for lecturers and academic divisions.
	Integrity	Attendance information should be in line with the real state as it relates to the status of courses that have been adjusted to the Semester Learning Plan (RPS)
	Availability	Lecture attendance information is provided for academic lectures, and academics.
Most important security requirements		**Integrity** Attendance information should be in line with the real state as it relates to the status of courses that have been adjusted to the Semester Learning Plan (RPS)

Stage 3: Recognize the Information Asset Container

The information asset container is the location that stores information assets, transfers or processes information assets. The location of the information asset can be used to identify the container by using a worksheet map of the environment risk Asset information is divided into three categories: technical, physical, and people and each consists of internal and external sections. Table 4 contains examples of information assets risk Map – lecturer Attendance

Table 4. Risk Example
Information assets (technical)-lecturer attendance

Environmental Asset Risk Map Information (Technical)	
Internal	
Description of containers	**Holder(s)**
Web Server & *Database*: Lecturer Attendance In the *database* and can be used through the Web of lecturers attendance	IT Division
Web of lecturer attendance is used to access lecturer attendance to collect data.	Academic administration staff, Study Program
External	
Description of containers	**Holder(s)**
Web accessed to see lecturer attendance data	Lecturer

Stage 4: Recognize Attention Zone

Recognizing of attention zone can be done through the following activities:

1. Monitoring is carried out on each container to review the zones that might be an attention.
2. Each field that has been recognized and become an attention will be recorded in the information asset risk sheet, things to note include the name of the information assets and the attention zone in detail.
3. Enlarge the attention zones to generate menace schemes that can break down menaces characteristics.
4. Write the effect of menaces to the security requirements of information assets. Proceeding to the information Asset Risk worksheet includes all fields that are considered to be more detailed.
5. After that, proceed to another container on the asset risk environment map and write as many zones as you should consider.

Table 5. Example of Attention Zone-lecturer Attendance

No	Attention Zones
1	The staff of the Academic Administration Bureau commits data input errors due to the big amount of data obtained.
2	Access to the lecturers attendance which is disseminated by administrative staff who have access
3	The presence of security flaws from web lecturers can be abused by the parties inside or outside.
4	Errors arising at the time of insert/update/delete of lecturers attendance data conducted jointly

Stage 5: Recognize Menaces Scheme

The observed zones are developed into a menaces scheme that explains more details about the properties of the menaces. The activities are:

1. Accomplishing information asset risk worksheets for each menaces schemes.
2. Create an opportunity within explanation of an existing menace scheme in the information Asset Risk worksheet.

Table 6. Menaces Property Example-Lecturer Attendance

1	**Attention Zones**	**Menaces Property**	
	The staff of the Academic Administration Bureau commits data input errors due to the big amount of data obtained.	***Actor***	Staff of Academic Administration Bureau
		Way	Staff using web of lecturer attendance
		Motif	Happens accidentally
		Results	Disorders
		Securit y Requirements	Improve validation functions, and execute training to minimize errors
2	**Attention Zones**	**Menaces Property**	
	Access to the lecturers attendance which is disseminated by administrative staff who have access	***Actor***	Study Program Staff
		Way	Access to the Web of lecturer attendance
		Motif	Unauthorized access authorizations that result in lecturers ' attendance vulnerable to modification

		Results	Disclosure Modification
		Securit y Requirements	To provide guidance on the importance of maintaining access to authoritative, and to grant sanctions to staff who intentionally disseminate access to authoritative

Stage 6: Recognize Risks

Decide the effect for the company from a menaces scheme in the information Asset Risk worksheet. This stage includes activities such as:

1. Determine how a menace scheme in an asset risk information sheet has an impact on organization.
2. Make notes about the consequences of the information asset Risk worksheet and must be noted specifically. The area of impact of the risk evaluation criteria should be determined when the consequences are considered.

Stage 7: Examine Risks

Risk analysis is done by noticing the criteria that exist in the measurement of risk. Starting from the first risk on high, medium and low impact for the company. It starts with drawing the first worksheet into a review of the interest that it has valued. Then, calculate the relative risk score used to analyze risk to help the organization develop risk strategies.

Step 6 and Step 7 are interconnected, looking at the possibility of consequences that might happen in the attention zone. As a result, the impact area is rated and the score is stated. The score is achieved from doubling the area of impact value with the primary concern. Score calculation is in table 8:

Table 7. Calculating Impact Area Score

Impact Area	**Priority**	**Low (1)**	**Middle (2)**	**High (3)**
Reputation and customer Trust	**5**	**5**	**10**	**15**
Financial	**4**	**4**	**8**	**12**
Productivity	**3**	**3**	**6**	**9**
Security and Health	**2**	**2**	**4**	**6**
Fines and penalties	**1**	**1**	**2**	**3**

Stage 8: Choose Mitigation Strategy

All of the risks that have been determined can be arranged looking at the value of the risk. decision making can be assisted by risk categories in particular arrangements to reduce those risks that happen. After that divide the risks that have been determined looking at the comparative risk score, into :

Table 8. Relative Risk matrix

Relative Risk matrix		
Risk Score		
30 to 45	16 to 29	0 to 15
POND 1	POND 2	POND 3

After dividing the risks, determine the risk mitigation stages. Mitigation stages are divided into :

Table 9. Mitigation Strategies

POND	***Mitigation Strategies***
1	Reduce
2	Snooze/Mitigation
3	Receive

Table 10. Risk mitigation examples based on the Attention Zone

Risk mitigation	
Attention Zones	The staff of the Academic Administration Bureau commits data input errors due to the big amount of data obtained.
Action	Mitigation
Container	Website
Lecturer Attendance Website	Created input validation on certain fields
Staff of department/lecturer	Lecturers or staff can verify the attendance data of lecturers who have been inputted by the administration staff

4. Conclusion

OCTAVE Allegro is one of the OCTAVE methods used in the assessment of Risk management information systems and can be implemented in universities without needing a thorough participation in an organization and centered on critical information assets on the organization in reaching its goals and purposes. The risk assessment results in an overview of potential menaces that arise on important assets and establishes a fixed level of prevention to mitigate potential menaces that may arise. The Risk Management Information System assessment generates strategic planning in the right critical information assets as well as remedial steps if the menace scheme happens. Strategic planning in important information assets can result from the risk management Information system assessment, as well as the countermeasures if menaces occur.

References

[1] P. Hills, “International Journal of Information Management,” *Int. J. Inf. Manag. J. Inf. Prof.*, vol. 26, no. 1, pp. 1–2, 2006.

[2] G. Christakos, *Stochastic Environmental Research and Risk Assessment*. Springer-Verlag, 1999.

[3] J. A. O’Brien and G. M. Marakas, “Introduction to Information Systems (Vol. 13). New York City.” USA: McGraw-Hill/Irwin, 2005.

[4] A. A. Rampini, S. Viswanathan, and G. Vuillemey, “Risk management in financial institutions,” *J. Finance*, vol. 75, no. 2, pp. 591–637, 2020.

[5] K. Mhetre, B. A. Konnur, and A. B. Landage, “Risk management in construction industry,” *Int. J. Eng. Res*, vol. 5, pp. 153–155, 2016.

[6] S. Alhawari, L. Karadsheh, A. N. Talet, and E. Mansour, “Knowledge-based risk management framework for information technology project,” *Int. J. Inf. Manage.*, vol. 32, no. 1, pp. 50–65, 2012.

[7] H. Stewart and J. Jürjens, “Information security management and the human aspect in organizations,” *Inf. Comput. Secur.*, 2017.

[8] B. Ali and A. I. Awad, “Cyber and physical security vulnerability assessment for IoT-based smart homes,” *sensors*, vol. 18, no. 3, p. 817, 2018.

[9] A.-M. Suduc, M. Bîzoi, and F. G. Filip, “Audit for information systems security,” *Inform. Econ.*, vol. 14, no. 1, p. 43, 2010.

[10] R. L. Krutz, R. D. Vines, and E. M. Stroz, *The CISSP Prep Guide: Mastering the ten domains of computer security*. Citeseer, 2001.

[11] C. Anderson, R. L. Baskerville, and M. Kaul, “Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information,” *J. Manag. Inf. Syst.*, vol. 34, no. 4, pp. 1082–1112, 2017.

[12] S. K. Pandey, “A comparative study of risk assessment methodologies for information systems,” *Bull. Electr. Eng. Informatics*, vol. 1, no. 2, pp. 111–122, 2012.

[13] M. T. Jufri, M. Hendayun, and T. Suharto, “Risk-assessment based academic information System security policy using octave Allegro and ISO 27002,” in *2017 Second International Conference on Informatics and Computing (ICIC)*, 2017, pp. 1–6.

[14] E. Goldman, “Challenges and Concerns for Implementing OCTAVE Allegro in a University Environment.” 2013.

[15] T. Aven, “Foundational issues in risk assessment and risk management,” *Risk Anal. An Int. J.*, vol. 32, no. 10, pp. 1647–1656, 2012.

[16] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, “Introducing octave allegro: Improving the information security risk assessment process,” Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, 2007.

[17] S. Santoso, J. Kauf, and N. Aristo, “The Information System Of Name Card

Sales Based On Digital Marketing To Improve Creativepreneur On College E-Commerce Website", *Aptisi Transactions On Technopreneurship (ATT)*, vol. 1, no. 1, pp. 64-72, Mar. 2019.

[18] E. Febriyanto, R. Naufal, and S. Sulistiawati, "Planning of the Web-based E-Raport Assessment System", *Aptisi Transactions On Technopreneurship (ATT)*, vol. 2, no. 1, pp. 48-58, Jan. 2020.

[19] A. Alwiyah, C. Greisy, and A. Afitri, "Implementation Of Information Systems On E-commerce Websites As Media To Deliver Information", *Aptisi Transactions On Technopreneurship (ATT)*, vol. 1, no. 2, pp. 127-133, Aug. 2019.

[20] T. Hariguna, E. Harahap, and S. Salsabila, "Implementation of Business Intelligence Using Highlights in the YII Framework based Attendance Assessment System", *Aptisi Transactions On Technopreneurship (ATT)*, vol. 1, no. 2, pp. 109-116, Aug. 2019.

[21] Hariguna, Taqwa, Muhamad Yusup, and Agung Priyadi. 2019. "The Transaction Optimization Of Color Print Sales Through E-Commerce Website Based On Yii Framework On Higher Education." Aptisi Transactions On Technopreneurship (ATT) 1(1): 1–10.

[22] Santoso, Sugeng, Josch Kauf, and Nabila Cynthia Aristo. 2019. "The Information System of Name Card Sales Based on Digital Marketing to Improve Creativepreneur on College E-Commerce Website." Aptisi Transactions On Technopreneurship (ATT) 1(1): 64–72.

[23] Sunarya, Po Abas, Doucette David Bernard, and Dian Maharani Damanik. 2019. "Viewboard Implementation Based on Javascript Charts as a Media for Submitting Sales Information on a Green E-Commerce Website Light Cafe." Aptisi Transactions On Technopreneurship (ATT) 1(1): 11–19.

[24] Zarlis, Muhammad, Eka Purnama Harahap, and Lina Naelal Husna. 2019. "Test Appraisal System Application Based on YII Framework as Media Input Student Value Final Project and Thesis Session at Higher Education." Aptisi Transactions On Technopreneurship (ATT) 1(1): 73–81.