International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Implementing IT Risk in ITSM Tools using Octave Allegro Method Based at ITSMProject

R. Arga Tristian, Antoni Wibowo

Abstract*:The purpose of this research is to identify and conduct risk analysis a Analyze risk on IT Service Management Information System Tools vulnerabilities at IT Service Management project, To obtain the level of vulnerability or weakness of information and to produce a strategic recommendation to overcome the vulnerability of information in the Project, OCTAVE Allegro was used as the method. Awareness of the importance of information system security and its assets to an organization and the impact that may arise from the destruction of the information system and its assets does not seem to be getting attention for most organizations and resulting low performance on Service Management while the evaluation and analysis process is more focused on the management of critical assets owned by the Project. Conclusion of the risk assessment is recommendations on the steps to be taken protect and manage the IT Service information system critical assets at IT Service management Project and also for a better service and achieve Service Level Agreement.

***Keywords* :Information Asset, Information Vulnerability, OCTAVE Allegro, Risk Management, threat**

I. INTRODUCTION

The use of information technology in organizations is a company need to help and support business activities. Information technology can produce an effective and efficient process so that it can generate greater profits for the company. With the information that can be distributed well, complete, relevant and accurate, the company will be able to compete in the business it is running. However, not all companies that have an information system think about the weaknesses of the infrastructure or assets of the system they have even Security of the Information Systems is one of the biggest challenges faces by almost all the organizations in today's world [1].

PT. MBK is one of the many national scale System Integrator (SI) companies, PT. MBK provides a variety of IT solutions specifically for business customers, and also as a "Business Partner" of several leading global and local IT products, PT. MBK also provides solutions for infrastructure, information systems, IT security, and management solutions for all IT-related devices.

PT. MBK has 147 Service Partner, 115.000 under maintenance service, 500 Costumer List and more than 200 employees. To support business processes, of course, Information systems are also used to enhance not only value, promotion, strategy, communication, integration, but also smooth management solutions.

One aspect that must be safeguarded in securing information is the presence of vulnerabilities. PT. MBK as an IT Service Management (Business partner) company that is sure to store a lot of information and needs to know immediately the potential vulnerabilities that arise in PT. MBK, currently, Management and information technology risk assessment at PT. MBK has not been done for ongoing projects in a telecommunication's company. When there is information that does not reach the helpdesk due to an application or hardware side problem, it will cause SLA to often not reach the target. Therefore, risk management is needed for current project, it is necessary to identify the potential vulnerability of information available so that the information available in the company is always up-to-date, ready and easily accessible when needed according to needs and that SLAs in IT Service projects are always achieved.

II. LITERATURE REVIEW

Information systems (IS) involve a variety of information technologies (IT) such as computers, software, databases, communication systems, the Internet, mobile devices and much more, to perform specific tasks, interact with and inform various actors in different organizational or social contexts [2].Information as a key asset in organizations has been given especial attention in the literature [3]. Information is a perennially significant business asset in all organizations. Therefore, it must be protected as any other valuable asset [4].

IT security risk assessment is discussed with respect to asset identification, lifecycle clarification, system model definition, and conceptual frameworks for risk assessment [5]. A risk is a critical vulnerability that leads to discrepancies in the application of information technology. The System's risk exposure was reviewed with respect to the confidentiality, integrity, and availability [6] [7].

In the Analysis of Information System Data Security Risk Management during the use and implementation of information technology, various risks can arise which can threaten the sustainability of business processes in the other hand Risk analysis is the basis of information protection, risk management, and risk in the process of information protection [8] [9].

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
R. Arga Tristian*, Computer Science, Bina Nusantara University, Jakarta, Indonesia. Email: rizky.tristian@binus.ac.id
Antoni Wibowo, Lecturer of Magister TeknologiInformasi,Bina Nusantara University, Jakarta, Indonesia. Email: anwibowo@binus.edu

Therefore, it is critical to establish reliable information security risk assessment and treatment frameworks to guide organizations during the risk management process [10].

Risk assessments provided a mechanism for reaching a consensus on which risks were the greatest and what steps were appropriate for mitigating them.

The processes used encouraged discussion and generally required that disagreements be resolved and risk assessment and identification and selection of countermeasures. It is applicable to all kinds of information systems and can be used in all stages of the life cycle [11] [12].

For future work, there is need of development of an operation-based Information Security Risks Management framework that should be simple and clearly defined the security risks management process [13].

TABLE I. RELATED WORKS

Reference	Type of Problem/company	Research Suggestion	Output
Information System Risk Assessment at the Ministry of Disadvantaged Areas Using the Octave Allegro Method By Mochamad Ilham Akbar at Binus University in 2015.	This study aims to minimize and manage the impact of potential risks. The scope is only limited to the application of SISPA-PDT (Geo spatial Information System for Development of Disadvantaged Regions) and SISPDT (Disadvantaged Regional Statistical Information System). This study produced several recommendations.	Providing counseling to employees regarding responsibility for the importance of information asset integrity.	Enforce a sanction system if data input errors occur repeatedly. Add server testing and QA to the source code produced by IT staff. Enact regulations on system password changes regularly. And the new password cannot be the same as the previous password.
Assessment of Information System Risk Management with Octave Allegro at Education Institution By Jarot S. Suroso& Muhammad A. Fakhrozi at Binus University in 2018.	This study uses the OCTAVE Allegro method to assess risk in information systems at Educational Institutions such as MH. Thamrin University, where this study produced 8 important information assets with 51 areas of concern, 34 of which had to be reduced and 17 others could be postponed/postponed	Mitigation measures are determined and then collected and collated, into 12 statements in the form of questionnaires and distributed to the team or parties who use the use of information systems to get input regarding the implementation of these steps.	The results of the questionnaire stated that all parties involved agreed and appreciated the mitigation measures resulting from the risk assessment, as seen from no answers that strongly disagreed or disagreed from the 12 statements in the questionnaire
Information Systems Risk Analysis Using Octave Allegro Method Based at Deutsche Bank By Wahyu Sardjono& Muhamad Ilham Cholik at Binus University in 2018	This study aims to conduct a risk analysis on company information systems using factor analysis. The results of the risk assessment are recommendations on steps to take to protect information systems and their assets.	level of ability of five factors to evaluate information system governance in companies that are done using factor analysis conducted in this study, can be explained in the following model. **Y = 3.405 + 0.251 X1 + 0.691 X2 + 1.003 X3 + 0.265 X4 + 0.255 X5**	concluded that the management of the information system on the Core Banking System is now quite good. The results of the evaluation of information system governance use exploratory factor analysis with factors and indicators taken from the domain and process in OCTAVE ALLEGRO.
Evaluation of Information Security Risk Assessment for Internet Banking Among Commercial Banks in Kenya By Collins Odhiambo NdaloJowi& Elisha Abade at University of Nairobi in 2016	this research reveals that achieving high-level business information integrity and addressing user security concerns requires more attention. this research also clearly explains that management strategies not only address technological changes, risk management strategies must address issues related to the ethical and social fields.	This study recommends that the Bank of Kenya recommends not only address technological changes, risk management strategies in Kenyan banks, but must address issues related to ethics and the social field.	This study recommends that strategic compatibility and suitable information security solutions can be adapted in a sustainable manner where it is to overcome various social, ethical and technological issues that will later create a positive and safe environment that will welcome information security in the Kenyan banking sector.

A. Octave Allegro Risk Assessment

This Research using Octave Allegro Risk Assessment Method. The OCTAVE method stands for the Operational Critical Threat, Assets, and Vulnerability Evaluation. OCTAVE has two variants, namely OCTAVE-S and OCTAVE Allegro. The word allegro: (al-leg-ro) means in a fast and agile tempo. This illustrates the quick and fast performance of OCTAVE Allegro.

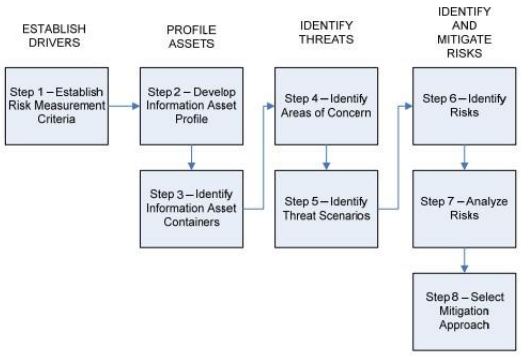
IT service provider organizations that have implemented a Quality Management System (QMS) according to ISO 9001 can take advantage of all the efforts made when implementing an IT Service Management System (ITSMS) [14]. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a methodology used to identify and evaluate information security risks [15].

The OCTAVE Allegro method consists of eight stages which are grouped into four categories or phases. The four categories are as follows:

- Category 1, Phase "Establish Drivers" aims to justify and priorities the measurement criteria for risk for a specific organization.
- Category 2, Phase "Profile Assets" is designed to identify and document logical, technical, physical and people assets.
- Category 3, Phase "Identify Threats" focuses on the identification of threats against the identified assets.

- Category 4, Phase "Identify and Mitigate Risk" supports the valuation of the risks posed against the critical information assets. Finally, after this step, the mitigation strategy for each of the identified risks is defined [16].

Fig 1. Allegro Road Map [16]



B. IT Service Information System (ITSM Tools)

IT service management (ITSM) is an activity in which all activities are directed by policies, organized and structured in supporting processes and procedures - carried out by organizations to design, plan, provide services, operate, and control information technology (IT) services offered to customers.

III. RESEARCH METHDOLOGY

The methodology that used in this research are OCTAVE Allegro method, purpose of this research is to describe each stage or worksheet that has been provided by the OCTAVE Allegro method in conducting risk management processes in the IT Service information system at IT Service Management Project. Each stage in Figure 1 will be divided into several risk assessment activities. The data collection method used was to conduct a literature study conducted by studying scientific books, Journals and literature relating to the scope of research and conducting interviews and observations with several team in a project.

IV. RESULT AND DISCUSSION

To begin the risk assessment, by conducting interviews with Project Managers and the MBK IT team, operational division managers, and several division heads, and direct observation to obtain the required data. Interviews with some of these people not only aim to collect the data that the author needs, but also the author provides an understanding of the importance of risk assessment of information technology Service in the Project. Interviews with IT managers and IT teams were carried out in more depth to obtain information about critical assets in the ITSM Tools Project. The following are eight steps for analyze and evaluating ITSM Tools Information system using Octave Allegro Method, which is use on IT Service Management Project.

A. Step 1 - Establish Risk Measurement Criteria

In the first step, two activities will be carried out, namely determining the impact area, and determining the scale of priorities in the determined impact area. At this stage, discussions were held with IT Project Managers, Heads of operational divisions and several division heads so that risk measurement criteria would be determined later. The chosen impact areas are reputation and customer satisfaction, financials, project completion, productivity, and penalties.

TABLE II. Octave Allegro first worksheet, Risk Measurement Criteria

Allegro Worksheet 1	REPUTATION AND COSTUMER CONFIDANCE		
Impacted Area	***LOW***	***MODERATE***	***HIGH***
Reputation	Reputation are slightly affected; no effort or there is no special handling.	Reputation is badly affected and need special treatment to improve.	The reputation is affected so badly that it is damaged and cannot be repaired.
Customer Loss	Less than 2% of customers who don'trenew their contracts are due to a loss of trust.	2% to 10% Customers who do not renew their contracts are due to loss of trust.	More than 10% of customers who do not renew their contracts are due to a loss of trust.

TABLE III. Allegro Worksheet 7, Impact Area Prioritization Worksheet [17]

Allegro Worksheet 7	**REPUTATION AND COSTUMER CONFIDANCE**
Priority	**Impact Area**
5	Reputation and Customer Confidence
4	Financial
3	Productivity
2	Safety and Health
1	Fines and Legal Penalties

B. Steps 2 - Develop Information Asset Profile

In developing critical information assets in ITSM Tools, the assessment is done by focusing on the core process of ITSM Tools itself, including user profiles, service requests and complaints, information related to requests and complaints, technicians or the handling team, and report history.

Based on the activities that have been carried out it can be concluded that ITSM Tools is the most important asset because these assets must always be available, cannot be accessed without permission, and can only be modified by certain employees. Following is an overview of ITSM Tools information assets that are explained using the Allegro Worksheet.

TABLE IV. Allegro Worksheet 8, Critical Information Asset Profile – ITSM Tools Profile

(1) **Critical Asset** What is the critical information asset?	(2) **Rationale for Selection** Why is this information asset important to the organization?	(3) **Description** What is the agreed-upon description of this information asset?

Application Server on Redhat (ITSM Tools)	This asset is the most important asset because this asset runs the BMC Remedy application system that is used by all customers of ITSM Project	Application Server is a server based on a Virtual Machine whose job is to run data processing and display information.

(4) Owner(s) Who owns this information asset?			
Project Operation Unit			
(5) Security Requirements What are the security requirements for this information asset?			
Confidentiality	Only authorized personnel can view this information asset, as follows:	**CTO, IT Project Manager, dan IT Infrastructure Specialist and Analyst, IT Security Analyst, and Support team (Helpdesk, End User Computing)**	
Integrity	Only authorized personnel can modify this information asset, as follows:	**CTO, IT Project Manager, dan IT Infrastructure Specialist and Analyst, IT Security Analyst, and Support team (Helpdesk, End User Computing)**	
Availability	This asset must be available for these personnel to do their jobs, as follows:	Server Monitoring CPU load, network load, potential failure system	
	This asset must be available for **24** hours, **7** days/week, **52** weeks/year.	Application servers still have to operate because most customers operate 24 hours, and Helpdesk working time also 24/7.	
Other	This asset has special regulatory compliance protection requirements, as follows:	Applications that run on Application Server are protected by copyright	
(6) Most Important Security Requirement What is the most important security requirement for this information asset?			
□ Confidentiality	□ Integrity	√ **Availability**	□ Other

C. Step 3 - Identify Information Assets Containers

At this stage, we identify information asset containers where information will be collected relating to the location of information assets that are stored and managed both internally and externally. Information asset containers are containers where information assets are stored, transferred or processed. Using the Information Asset Risk Environment Map worksheet, the team identified the container where the information assets were located. The storage place for this information asset can be technical, physical, and human. At this stage there is only 1 activity that needs to be carried out, namely identifying and documenting how information assets are stored, transferred or processed.

TABLE V. Allegro Worksheet 9a, Information Asset Risk Environment Map (Technical) - ITSM Tools Profile

INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. BMC Remedy (ITSM Tools) is an administration system that is used to carry out the Reporting & administration input process which is useful for managing customer Report data registered on the IT Service Management Project.	IT Department
2. Remedy Database is a console application that operates continuously in charge of processing report data received by the server in real-time as well as report data from users.	IT Department
3. Employee Identity Manager is a Web Application whose job is to display the user's access status of data that has been processed or requested.	IT Department
4. Internal Server which is used as a File Server. This file server is used to store internal files, such as application source code used for the development of the IT Service Management Platform.	IT Department
EXTERNAL	
1. Red hat Enterprise Linux is a Virtual Machine based IT infrastructure that provides services and places where BMC Remedy (ITSM Tools) works.	IT Department Provided by Red Hat as a Virtual Machine vendor.

TABLE VI. Allegro Worksheet 9b, Information Asset Risk Environment Map (Physical) - ITSM Tools Profile

INTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Application documentation such as Flow Charts, System Design, User Manual Guides, Application Technical Documents are stored as documentation to be studied.	**Project and Analyst Team**
EXTERNAL	
CONTAINER DESCRIPTION	**OWNER(S)**
1. Application documentation such as flow charts, system designs, User Manual Guides, Application Technical Documents can be provided to customers if needed as a documentation package provided.	**Project and Analyst Team**

TABLE VII. Allegro Worksheet 9c, Information Asset Risk Environment Map (People) - ITSM Tools Profile

INTERNAL PERSONNEL	
NAME OR ROLE/RESPONSIBILITY	**DEPARTMENT OR UNIT**
1. Developer Staff, Compile the program code that is used as the basis for building IT Service Management Tools	IT Department Developer
2. Project and Analyst Staff. Manage projects being undertaken such as developing new features and managing the required documentation	IT Department Project and Analyst

Retrieval Number: E6766018520/2020©BEIESP
DOI:10.35940/ijrte.E6766.038620
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

3.	IT Infrastructure and Support Staff. Manage and monitor the Virtual Machine infrastructure that runs IT Service Management Tools	IT Department IT Infrastructure
EXTERNAL PERSONNEL		
CONTAINER DESCRIPTION		**DEPARTMENT OR UNIT**
1.	There is no external staff to manage ITSM Tools information assets	

D. Step 4 - Identify Areas of Concern

At this stage, an information asset risk profile will be created which will later be made a statement describing the real situation that will be faced and affecting the information asset. At this stage, there is only 1 activity that requires information from the Information Asset Risk Environment Map that was carried out in Step 3 Identify Information Asset Containers that will be used as a reference for filling in the Information Asset Risk Worksheet (Worksheet 10).

TABLE VIII. Area of Concern - ITSM Tools Profile

AREA OF CONCERN
ITSM Tools suddenly stopped working and interrupted the service process used by EUC's & Service Desk Team.
Application Server and ITSM Tools is accessed without permission by others without the knowledge of the Project Manager.
Notebook device is not functioning, not connected to the network so it cannot create reports sent by End Users.
Application Server and ITSM Tools experienced Not responding, Crash or could not be accessed. and had to be force restarted and needed an EUC support team.

E. Step 5 - Identify Threat Scenarios

The area of concern is expanded into a threat scenario that details more about the property. In the previous stages, documentation of areas of concern or areas of concern has been made. Identification of threat scenario that provides a Description of the properties of the threat, including actors, means, motives, outcomes and security requirements. Complete Information Asset Risk Worksheets for each common threat scenario.

TABLE IX. Properties of Threat - ITSM Tools Profile

Area of Concern	Threat of Properties	
Due to the large number of User reporting, ITSM Tools suddenly stopped working and interrupted the service process used by EUC's & Service Desk Team.	Actors	IT Department
	Means	Staff is using ITSM Tools
	Motives	An error occurred due to a human error and system failure
	Outcome	Modification interunion
	Security Requirement	Addition of daily checking and dual control process between staff and supervisors in carrying out information / update process of the ITSM Tools
	Motives	Deliberate
	Outcomes	Disclosure, Modification, Interruption and Loss
	Security Requirement	Application security testing related to the ITSM Tools VM and module.

F. Step 6 – Identify Risk

This step later determines the threat scenarios that have been recorded in each Work Information Asset Risk Worksheet can have an impact on the company. There is 1 activity at this stage which is to complete the threat scenario with the consequences that can be caused to complete the risk profile.

A. TABLE X. Guidelines for calculating the relative risk score (Identifying Risks) *[17]*

Impact Areas	Priority Value	Low (1)	Moderate (2)	High (3)
User Reputation and Trust	5	5	10	15
Financial	4	4	8	12
Productivity	3	3	6	9
Law and Regulation	2	2	4	6
Finance or Operational Costs	1	1	2	3

G. Step 7 – Analyze Risk

At this stage, an analysis of risks to the risks that can occur in the IT Service Management Project's information system assets will be analyzed. The first activity at this stage will be assessed, this activity will review the risk measurement criteria created in step 1. The threat and consequence scenarios that focus on how the definition of high, medium, and low impact for the company. Then the second activity of the predetermined influence will be assessed based on the risk criteria and their level. If the effect of high or high risk will be given a value of 3, medium or moderate will be given a value of 2 and a low or low will be given a value of 1. This number will be multiplied by the level of risk criteria that exist in stage 1. The level of risk criteria that have been set in value at stage 1 will be used as a multiplier for the effect value. The results of the multiplication will be added to the total value for each risk.

TABLE XI. Risk Analysis ITSM Tools Profile

No.	Area of Concern	Risk			
1.	Due to the large number of User reporting, ITSM Tools suddenly stopped working and interrupted the service process used by EUC's &Service Desk Team.	Consequences	Impacting on creating report or process report that already create by user itself. The result make SLA not achieve and require additional time to record/create report when tools is up.		
		Severity	Impact Area	Value	Score
			User Reputation and Trust	***Moderate (2)***	***10***
			Financial	***Moderate (2)***	***8***
			Productivity	***High (3)***	***9***
			Law and Regulation	***Low (1)***	***1***
			Finance or Operational Costs	***Moderate (2)***	***4***
			Relative Risk Score		32

H. Step 8 – Select Mitigation Approach

At this stage, it will determine how companies choose the right risk mitigation approach. Grouping risks into a specific order can help in making decisions in the status of mitigating these risks.

there are many ways to categorize risks. One direct method is to start by sorting all the risks in sequence from highest to lowest risk. Then the risk is separated into four groups with the same amount of risk.

The risk with the highest score must be in the first (Group 1), the risk with the next highest score range in the second group (Group 2), the next highest in the third rank (Group 3), and the lowest score in the fourth group (Group 4).

TABLE XII. Relative Risk Matrix

RELATIVE RISK MATRIX			
PROBABILITY	**RISK SCORE**		
	30 TO 40	**16 TO 29**	**0 TO 15**
HIGH	GROUP 1	GROUP 2	GROUP 2
MEDIUM	GROUP 2	GROUP 2	GROUP 3
LOW	GROUP 3	GROUP 3	GROUP 4

TABLE XIII. Mitigation Approach

Pool	Mitigation Approach
GROUP 1	Mitigate
GROUP 2	Mitigate or Defer
GROUP 3	Defer or Accept
GROUP 4	Accept

TABLE XIV. Risk Mitigation of Area of Concern

Scenario/Action	Pool 1 Mitigate	Pool 2 Mitigate /Defer	Pool 3 Defer/Accept	Pool 4 Accept
ITSM Tools suddenly stopped working and interrupted the service process used by EUC's & Service Desk Team.	✓			
Application Server and ITSM Tools is accessed without permission by others without the knowledge of the Project Manager.	✓			
Notebook device is not functioning, not connected to the network so it cannot create reports sent by End Users.	✓	✓		
Application Server and ITSM Tools experienced Not responding, Crash or could not be accessed. and had to be force restarted and needed an EUC support team.	✓			

V. CONCLUSION

Risk assessment is the process of identifying information assets, threats and vulnerabilities and the OCTAVE Allegro method is one method that can be used by IT Service Management Project in conducting information system risk management. By implementing good risk management that focuses on the threat and vulnerability of each critical asset owned, the ITSM Project can find out the threats, vulnerabilities and their impact on each of the critical assets that exist. From the results of the risk assessment, Project can prepare further policies in managing critical information assets appropriately and can be used for ITSM Project out there.

Based on 16 areas of concern, the threat that has the highest relative score is Malware in User email attachments with a score of 39, while for threats with the lowest relative score is the process of email backup during operating hours with a score of 15.

ACKNOWLEDGMENT

First, I would like to thank to Bina Nusantara University and my Mentor Dr. Eng. Antoni Wibowo, S.Si., M.Kom., M.Eng for his guidance and advice. I would specially thank my family who has supported me. through the ups and downs in completing this study. Without helps of the person mentioned above, I couldn't be succeeded in this research.

REFERENCES

1. D. M. Alghazzawi, S. H. Hasan and M. S. Trigui, "Information Systems Threats and Vulnerabilities," International Journal of Computer Applications, pp. Vol 89 No.3. 25-29, 2014.

2. S. K. Boell and D. Cecez-Kecmanovic, "What is an Information System?," in 2015 48th Hawaii International Conference on System Sciences (HICSS), 2015.
3. M. Padyab, T. Paivarinta and D. Harnesk, "Genre-Based Assessment of Information and Knowledge Security Risks," in 2014 47th Hawaii International Conference on System Sciences (HICSS), 2014.
4. Shameli-Sendi, R. Aghababaei-Barzegar and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," computers & security, p. 14–30, 2016.
5. Y. Kawanishi, H. Nishihara, D. Souma, H. Yoshida and Y. Hata, "A Comparative Study of JASO TP15002-Based Security Risk Assessment Methods for Connected Vehicle System Design," Security and Communication Networks, vol. 2019, 2019.
6. Ali and A. I. Awad, "Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes," 2018.
7. 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), Jayapura, 2017.
8. M.-C. Lee , "Information Security Risk Analysis Methods and Research Trends: AHP and Fuzzy Comprehensive Method," International Journal of Computer Science & Information Technology (IJCSIT), vol. 6, 2014.
9. M. Nurhafifah, I. N. Isnainiyah and A. Muliawatic, "Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ)," Jurnal Rekayasa Sistem dan Teknologi Informasi, p. 282–287, 2018.
10. W. Al-Ahmad and B. Mohammad, "Addressing Information Security Risks by Adopting Standards," International Journal of Information Security Science, pp. 28-43, 2013.
11. O. N. Jowi and E. Abade, "Evaluation of Information Security Risk Assessment for Internet Banking Among Commercial Banks in Kenya," American Journal of Networks and Communications, pp. 51-59, 2016.
12. P. Shamala, R. Ahmad and M. Yusoff, "A conceptual framework of info structure for information security risk assessment (ISRA)," journal of information security and applications, vol. 18, pp. 45-52, 2013.
13. U. K. Singh and C. Joshi, "Comparative Study of Information Security Risk Assessment Frameworks," International Journal of Computer Application, vol. 2, no. 8, pp. 2250-1797, 2018.
14. A.-L. Mesquida and A. Mas, "Integrating IT service management requirements into the organizational management system," Computer Standards & Interfaces, 2015.
15. Amini and N. Jamil, "A Comprehensive Review of Existing Risk Assessment Models," in 1st International Conference on Big Data and Cloud Computing, 2018.
16. Brunschwiler, "Compass Security Blog," 2013. [Online]. Available: https://blog.compass-security.com/2013/04/lean-risk-assessment-based-on-octave-allegro/. [Accessed 25 March 2019].
17. 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 Institute, 2007.

AUTHORS PROFILE

R. Arga Tristianis currently working in a project partner withmobile telecommunications services company working as IT Service Supervisor. Now, he is completing his Master's of Computer Science at BINUS University, Jakarta, Indonesia

Dr. Eng. Antoni Wibowo, S.Si., M.Kom., M.Engis currently working at Binus Graduate Program (Master in Computer Science) in Bina Nusantara University-Indonesia as a Specialist Lecturer and continues his research activities in machine learning, optimization, operations research, multivariate data analysis, data mining, computational intelligence and artificial intelligence.