RISK ANALYSIS IN THE PREPARATION OF A BUSINESS CONTINUITY PLAN (BCP) IN IT SERVICES: A CASE STUDY OF UNIVERSITAS INDONESIA

Akmal Gafar Putra, Betty Purwandari and Farisya Setiadi

Magister of Information Technology, Universitas Indonesia, Depok, Indonesia

ABSTRACT

Based on the Horizons Scan Report 2021 by BSI, the top 6 threats to organizations today are pandemics, health incidents, safety incidents, IT and telecommunications outages, cyber-attacks, and extreme weather. Universitas Indonesia (UI), as a modern, comprehensive, and open campus, strives to become a leading research university globally. As the IT service manager at UI, the Directorate of Information Systems and Technology (DSTI) has the task of strengthening service management by implementing risk management and security management in line with relevant laws and policies. The main problem for DSTI as an IT service at UI is that there are no documents related to risk management and information security management, resulting in IT services' failure. This year, there have been four data center failures due to power and UPS problems. DSTI wants to improve IT services at UI by implementing risk management and Business Continuity Management System (BCMS). This study aims to conduct a risk analysis to design a Business Continuity Plan (BCP) for IT services at the University of Indonesia. The research was conducted using mix method. The OCTAVE qualitative method was carried out in finding a list of risks on critical assets in IT services at UI. A quantitative approach is needed to rank the risk list using a questionnaire and FMEA calculations to get a risk priority number. This study separates the risk of general assets and information system assets. For critical assets, it is generally found that two are at a very high level, one is high, eight risks are at a low level, and 12 are at a very high level, for information system assets found 12 assets with very high risk, three medium and one low.

KEYWORDS

Risk Analysis, OCTAVE, FMEA, ISO 22301:2019, Business Continuity Plan.

1. INTRODUCTION

Universitas Indonesia, abbreviated as UI, is a modern, comprehensive, open, multi-cultural, and humanist university. UI simultaneously and continuously trying to become the world's leading research university. The vision stated in the statutes [1] is: "To become a center of science, technology, and culture" superior and competitive, through efforts to educate the nation's life to improve the welfare of the community, thereby contributing to Indonesian development people and the world. UI has developed three strategic goals that are expected to realize the goals of UI 2024. The three strategic targets in internal business processes are relevant and high-quality education, research-based Tridharma, and effective governance [2]. The Directorate of Information Technology and Systems, abbreviated as DSTI, is a directorate entrusted with being a trusted institution in the management of information technology infrastructure and data

David C. Wyld et al. (Eds): CSTY, SIGI, MaVaS - 2021
pp. 101-111, 2021. CS & IT - CSCP 2021 DOI: 10.5121/csit.2021.112209

processing to support the implementation of the Tridharma of Higher Education and the achievement of the UI development trilogy.

DSTI has a vision "To become an information system management institution with excellent service quality to support the achievement of a world-class UI, which is comparable to the management of information systems at other leading universities in Asia." DSTI has three missions: fostering reliable, integrated, secure, and information-rich information technology infrastructure from, by, and for the entire University of Indonesia academic community; realizing mature IT Governance for the University of Indonesia towards a world-class university; building and ensuring the realization of IT-based application system services and infrastructure that can assist management at UI by UI's strategic plan [2].

Based on a survey conducted by the British Standard Institution [3], the COVID-19 pandemic is the highest disruption compared to other incidents that occur in organizations; this is due to the organization's lack of preparation in dealing with this pandemic. Health incidents, another category considered low risk for 2020, ended the year as the second biggest nuisance. Many of these health incidents are not from pathological causes but from mental health difficulties experienced by staff due to COVID 19. Cyberattacks and IT/telecommunications outages are also causing high levels of disruption in 2020 due to increasing cybercrime. Criminals seek to exploit security loopholes while staff works remotely, and unexpected network outages are caused primarily by issues with internet latency. Based on the list, the first and second ranks are threats caused by COVID-19, followed by work safety incidents, IT and telecommunications blackouts, cyber attacks, and extreme weather in the top 6 positions.

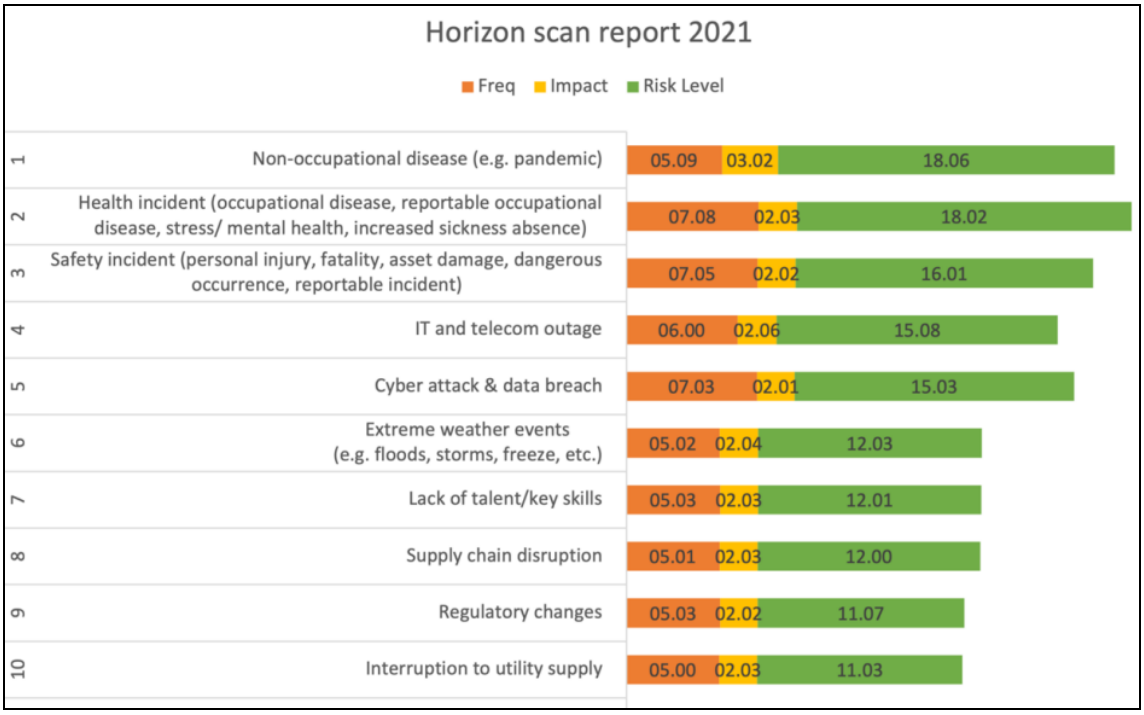

Figure 1. List of Threats to Organizations [3]

In a study conducted by Vasquez and Ortega, the loss of business-critical data and system downtime are two of the most significant risks faced by those in charge of information technology in the IT department [4]. And in other studies, it was found that the design of the Business Continuity Plan (BCP) serves to maintain the continuity of the company's business so

that it continues to run when the company's information technology experiences disruption,, where the research uses an international standard organization framework ISO 22301 [5].

Based on the results of interviews with the Information System Development Manager, there was a problem with the UI data center service, namely the server shutting down caused by damage to the Power Supply Unit and power generator failure for two days. The effect caused by the power failure was the data damage in the Storage Access Network which resulted in the blackout of several information systems for seven days.

From the analysis of the fishbone diagram, five domains affect the continuity of IT services at the University of Indonesia data center, namely: Currently, DSTI does not have a business continuity plan document, DSTI has two SysAdmins and two NetAdmin with levels competencies are in different level so that for disaster recovery DSTI is very dependent on individual staff, In pandemic conditions SysAdmin and NetAdmin often don't be at the data center location when a disaster occurs, so that data center recovery be disturbed, no backup or swap implementation yet to the main applications such as the academic system, financial system, staffing, and others to anticipate failures in the primary system or data center, The loss of the power source and the unavailability of a disaster recovery center are some infrastructure problems, company policy of 25% to 50% presence during a pandemic has a significant impact on disaster management.

This study aims to conduct a risk analysis to prepare a Business Continuity Plan (BCP) on IT services at the University of Indonesia. This research hopes that a list of risks needed to prepare the BCP will be obtained with this research.

2. LITERATURE REVIEW

2.1. Risk

Paul Hopkin defines risk as the possibility of harm, loss, or an accident that may occur [6]. Darril Gibson defines risk as a possible loss of a vulnerability that can threaten an organization [7].

2.2. Risk Management

Risk Management according to Darril Gibson is the practice of identifying, assessing, controlling, and reducing risk [7].

2.3. Business Continuity Management System

Business Continuity Management System or BMCS is the whole process managerial skills that can predict threats and their impacts on the organization if the hazard occurs and provide a framework and blueprint complete set of tools to build organizational resilience with relevant responses to protect key stakeholders, reputation, brand, and business process activities [8]. BCMS emphasizes the importance of understanding the organization's need to conclude policies and objectives, implement controls and estimates for the management of disturbing incidents, observe performance, and carry out sustainability efforts.

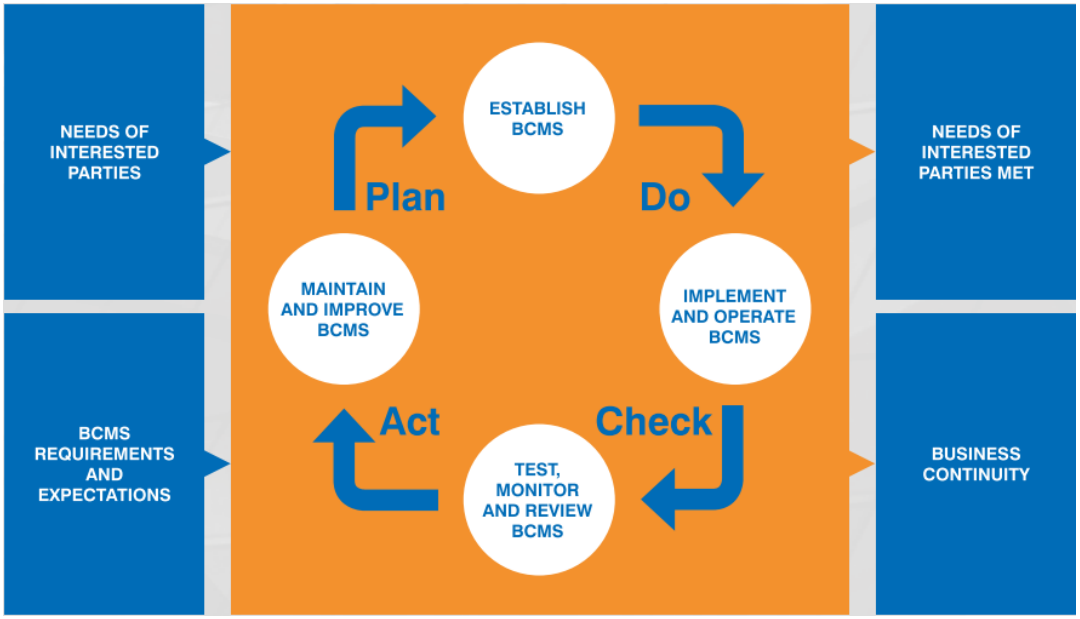

Figure 2. Plan, Do, Check, Act cycle in BCMS process

2.4. Business Continuity Planning

BCP is a document that contains instructions or procedures for how the organization ensures business processes during and after interruptions [9]. BCP is defined as a procedure document of organizational implementation guidelines to restore, repair, and restart basic operations in a state of disturbance [8]. The latest, according to Darril Gibson, BCP is a document used to help a company plan to disaster or emergency. The goal is to ensure that the operation critical organization continues to function. BCP consist of procedures and instructions used to restore operations in the event of a disaster.

2.5. Previous research

2.5.1. Business Continuity Plan in IT Solution Company (PT. ABC) Using ISO 22301:2012 [10]

This study aims to design BCP for companies engaged in solutions IT. This company has two data centers and a DRC. This study conducts a Risk Analysis in designing BCP using a framework work ISO.

2.5.2. Design of a business contingency plan. Case study: Municipality of Cantón Suscal. [4]

This study aims to communicate the results of the BCP design in the technological innovation (DIT) for the City of Cantón Suscal (MCS). This research analyses IT areas where the loss of business-critical data and system downtime are two risks biggest challenges faced by those in charge of information technology in the department of technological innovation (DIT) for the City of Cantón Suscal (MCS) (Vasquez & Ortega, 2020).

2.5.3. Business Continuity Plan Design and Technology Disaster Recovery Plan and Information Systems Using ISO 22301 [5]

This study conducts a risk analysis in the design of BCP with the framework ISO 22301 combined with BS 25999-1 and BS 25999-2.

2.5.4. Risk analysis on the development of a business continuity plan [11]

This research is about designing a business continuity plan that functions to maintain the continuity of the company's business so that it continues to run when technology information on the company is disrupted. This study uses international standard organization framework 22301 (I. Setiawan et al., 2019).

2.6. Risk Analysis Method

2.6.1. OCTAVE Method

OCTAVE (Operationally, Critical Threat, Asset and Vulnerability Evaluation) is a risk-based strategic assessment and planning technique for effective security developed at the Software Engineering Institute (SEI) [12]. OCTAVE is a framework that organizations can use to identify information security risks and help organizations develop risks qualitatively and identify critical assets to the organization's mission. OCTAVE targeted organizational risk and focused on strategic issues related to University of Indonesia practice. OCTAVE is a flexible evaluation that can be adapted to most organizations.

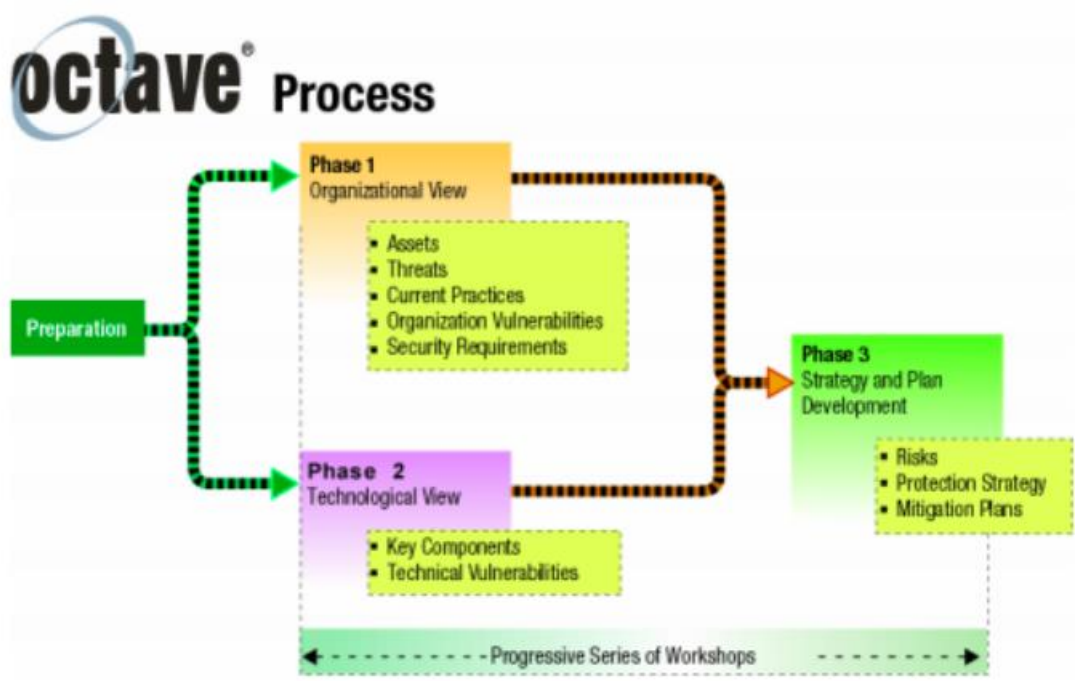

Figure 3. OCTAVE Method Process Flow

2.6.2. FMEA Method

FMEA (Failure Modes and Effects Analysis) is a systematic method used to identify the consequences or consequences of potential failures systems or process and reduce the chance of

failure [13]. FMEA is one of the reliable tools to minimize losses that occurred as a result of this failure. The 10 steps of the FMEA are; Identify the components and their related functions, Identify failure modes, Identify the impact of the failure mode, determine the severity of the failure, Identify the cause of the failure, Determine the frequency value of the occurrence of failure, Identify the necessary controls, Determine the effectiveness of the current control (detection), Calculate the RPN (risk priority number) value, and Determine actions to reduce failure.

In order to produce accurate output of risk analysis using the FMEA method, Firstly there must be some determination of the value of severity, occurrence, and detection. In the FMEA method, the final risk priority number is called the RPN or risk priority number. RPN is a mathematical result of the impact (Severity), the probability of occurrence of the risk that will lead to failure (Occurrence), and the ability to detect failures (Detection). The following equation shows the RPN value:

$$RPN = Severity \times Occurrence \times Detection$$

Table 1. Risk Level

Risk Level	**RPN Value**
Very High	>200
High	<200
Medium	<120
Low	<80
Very Low	<20

2.7. Comparison of Risk Analysis Methods

In this section, the differences in risk analysis methods between OCTAVE and NIST SP 800-30, the OCTAVE method of evaluating organizations, focuses on security practices within the organization, focusing on the organization's strategic issues and Self directions. the following table shows the difference in methods:

Table 2. Comparison of Risk Analysis Method

Method	**OCTAVE**	**NIST SP800-34 Rev.1**
Evaluation Subject	Organization	Information System
Focus	Security Practices	Technology Used
Issue	Organization Strategic	Organization Tactic
Direction	Self-Direction	Expert-Direction

3. ANALYSIS

This section discusses the stages of performing a risk analysis based on the method OCTAVE and FMEA

3.1. Asset Identification

At this stage, asset information is collected, grouped into 4 categories: Hardware, Software, Information, and Personal.

Table 3. Assets

Asset Code	Criteria	Asset Name
H1	Hardware	Server
H2		Firewall
H3		Laptop
H4		Monitor
H5		PC Unit
H6		Router
H7		Switch
H8		CCTV
H9		Electric Generator
H10		UPS
H11		Precise Air Conditioner
H12		Fire Distinguisher
H13		Cabel
I1	Information	Student
I2		Staff
I3		Finance
I4		Vendor
I5		Assets
S1	Software	OS
S2		LDAP
S3		SSO
S4		Ms. Office
S5		Database Tools
S6		App Dev Tools
S7		Academic
S8		Humar Resource
S9		Finance
S10		Logistic and Procurement
S11		Asset and Facilities
S12		Research
P1	Pegawai	Director
P2		Development Manager
P3		Operational Manager
P4		IT Gov Specialist

Asset Code	Criteria	Asset Name
P5		Solution Design Specialist
P6		App Dev Specialist
P7		App Operation Specialist
P8		Infra Dev Specialist
P9		Infra Operation Specialist
P10		Administration

3.2. Risk Assessment

Table 4. General Asset Risk Assessment

Category	**Critical Asset Name**	**Threat**	**S**	**O**	**D**	**RPN**	**Risk Level**	**Risk ID**
Hardware	Server	Hardware Failure	8	2	3	48	Low	1
		Run Out Resources	8	1	2	16	Very Low	2
		configuration crash	8	1	6	48	Low	3
	PC/ Laptop	Hardware Failure	5	1	1	5	Very Low	4
		Virus	5	1	1	5	Very Low	5
		Software Damage	5	1	1	5	Very Low	6
	UPS	Hardware Failure	8	1	1	8	Very Low	7
		Loosing Power	8	6	1	48	Low	8
	Electric Generator	Hardware Failure	8	1	6	48	Low	9
		Run Out of Gas	8	1	1	8	Very Low	10
Networking	Router & Switch	Hardware Failure	5	1	10	50	Low	11
		Configuration crash	5	1	10	50	Low	12
	Cable	Physical Damage	6	1	10	60	Low	13
	Firewall	Hardware Failure	2	1	10	20	Low	14
		Configuration crash	5	1	1	5	Very Low	15
Software	LDAP	Power Down	8	6	5	240	Very High	16
	SSO	Power Down	8	6	5	240	Very High	17
Data	Student	Inconsistencies Data	1	1	1	1	Very Low	18
	Human Resource	Inconsistencies Data	1	1	1	1	Very Low	19
	Finance	Inconsistencies Data	1	1	1	1	Very Low	20
	Research	Inconsistencies Data	1	1	1	1	Very Low	21

Category	Critical Asset Name	Threat	S	O	D	RPN	Risk Level	Risk ID
Human Resource	Staff	Resign	5	1	1	5	Very Low	22
		Work From Home	8	9	2	144	High	23

Table 5. Information System Risk Assessment

No.	Information System Name	Business Categories	S	O	D	RPN	Level RPN
1	emas2.ui.ac.id	Main	9	7	5	315	Very High
2	idols.ui.ac.id	Main	9	6	5	270	Very High
3	rima.ui.ac.id	Main	5	8	6	240	Very High
4	scele.ui.ac.id	Main	7	6	5	210	Very High
5	pra-registrasi.ui.ac.id	Main	5	4	10	200	Very High
6	bp.ui.ac.id	Main	6	3	10	180	High
7	edom.ui.ac.id	Main	7	5	5	175	High
8	evisem.ui.ac.id	Main	7	5	5	175	High
9	emas.ui.ac.id	Main	9	6	3	162	High
10	academic.ui.ac.id	Main	7	2	10	140	High
11	beasiswa.ui.ac.id	Main	5	5	5	125	High
12	pdf.midearth	Main	9	1	10	90	Medium
13	pjj.ui.ac.id	Main	6	5	3	90	Medium
14	ovis.ui.ac.id	Main	6	5	2	60	Low
15	Lontar (Perpustakaan)	Support	7	6	8	336	Very High
16	Remote-Lib	Support	7	6	8	336	Very High
17	Unggah.ui.ac.id	Support	7	6	8	336	Very High
18	Assets and Facilities	Support	5	6	10	300	Very High
19	Mailing	Support	7	7	6	294	Very High
20	Redmine	Support	7	5	8	280	Very High
21	Finance	Support	7	6	5	210	Very High
24	Human Resource	Support	5	5	5	125	High
25	HRIS	Support	5	5	5	125	High
26	UI Archive	Support	5	4	6	120	High
27	Vehicle Loan	Support	5	6	4	120	High
28	Arsip	Support	5	4	5	100	Medium

4. CONCLUSIONS

This study aims to conduct a risk analysis in designing the BCP Business Continuity Plan to be implemented in IT services at the University of Indonesia. The conclusion obtained is as following: At the beginning of 2020, the threat of COVID-19 emerged as a global threat that affect the list of threats and risks to business services in IT services; DSTI UI has not conducted a comprehensive risk assessment related to hardware, software, information, and employees asset; OCTAVE method is suitable for identifying all critical assets, critical asset components, threats, vulnerabilities to key components, practices security, and organizational vulnerabilities; The FMEA method is suitable for measuring the value of risk if it already exists standard measurement methods for the impact, incidence and detection of each risk profile; Found several threats of power source failure such as UPS and Genset have a high and systemic impact on other assets. On system assets information there are 12 SI with very high risk level, 12 high risk, 3 medium and 1 low; the final conclusion is that the risk analysis process in this study has produced a list of risks needed in the preparation of the BCP which contains IT management policies in disaster preparation and management.

ACKNOWLEDGEMENTS

The authors would like to thank everyone, just everyone!

REFERENCES

[1] Statuta UI. Statuta Universitas Indonesia, Pub. L. No. 68 (2013). Indonesia.
[2] Renstra UI. (2017). Rencana Strategis Universitas Indonesia Revisi 2015-2019, 1–90.
[3] Business Continuity Insitute. (2021). BCI Horizon Scan Report 2021. 40, 55.
[4] Vasquez, E. J., & Ortega, J. C. (2020). Design of a business contingency plan. Case study: Municipality of Cantón Suscal. 2020 International Conference on Intelligent Systems and Computer Vision, ISCV 2020. https://doi.org/10.1109/ISCV49265.2020.9204334
[5] Setiawan, I., Waluyo, R., & Pambudi, W. A. (2019). Perancangan Business Continuity Plan dan Disaster Recovery Plan Teknologi dan Sistem Informasi Menggunakan ISO 22301. Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi), 3(2), 148–155
[6] Hopkin, P. (2017). Fundamental of Risk Management Understanding, evaluating and implementing effective risk management. (4th, Ed.). KoganPage.
[7] Gibson, D. (2014). Managing Risk in Information Systems. Retrieved from https://books.google.com/books?id=5lktBAAAQBAJ&pgis=1
[8] ISO 22301 (2012). Social Security – Business Continuity Management Systems Requirement. ISO.
[9] NIST. (2010). NIST Special Publication 800-34 Rev.I: Contingency Planning Guide for FederalIinformation System. Gaithersburg: NIST..
[10] Pramudya, G. W., & Fajar, A. N. (2019). Business continuity plan using ISO 22301:2012 in IT solution company (pt. ABC). International Journal of Mechanical Engineering and Technology, 10(2), 865–872.
[11] Setiawan, A., Wibowo, A., & Susilo, A. H. (2018). Risk analysis on the development of a business continuity plan. Proceedings of the 2017 4th International Conference on Computer Applications and Information Processing Technology, CAIPT 2017, 2018-Janua, 1–4. https://doi.org/10.1109/CAIPT.2017.8320736
[12] Alberts, C., Dorofee, A., Stevens, J., & Carol Woody. (2003). Introduction to the OCTAVE® Approach. August, 121–129. https://doi.org/10.1016/b978-0-7020-3055-0.00004-2
[13] Stamatis, D. H. (1996). Failure Mode and Effect Analysis: FMEA From Theory to Execution. In Technometrics (Vol. 38, Issue 1). https://doi.org/10.1080/00401706.1996.10484424

AUTHORS

I am a master program student at the Faculty of Computer Science, University of Indonesia.