Analysis of Risk Management on DAPODIK System Services using OCTAVE Allegro Framework

Nadia Cahya Kartika
Department of Information System Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT

Dapodik is a comprehensive national-scale data collection system that is the main source of national education data for national education planning programs. As a result, schools must actively participate in DAPODIK activities to collect data. This study discusses risk management analysis in the DAPODIK system at SD Negeri Karangtalun 03 Cilacap with a qualitative approach using the OCTAVE Allegro method to reduce the occurrence of risks in the DAPODIC system. The OCTAVE Allegro method focuses on information assets owned by an organization or company in the contex t of how they are used, their storage, movement, processing, how threats, vulnerabilities, and disruptions occur in those assets. The OCTAVE Allegro method is divided into eight steps, namely building risk measurement criteria; developing information asset profiles; identifying containers of information assets; identifying areas of concern (problem areas) in technical, physical, and people container aspects; identifying threat scenarios; identify risks; analyze risks; Choose mitigation and control approaches that are adjusted to the results of the calculation of the relative risk score. Based on the results of testing on the DAPODIK system at SD Negeri Karangtalun 03 Cilacap, 4 mitigate approaches, 2 defers, and 2 accept. The relatively high-risk value is found in the Physical Container (PhC) with a total risk value of 29, due to a natural disaster that causes DAPODIK system services to stop. The risk value is relatively low in the Technical Container (TC) with a total risk value of 15, due to internet connectivity disruptions so DAPODIK system services are interrupted or temporarily stopped.

Keywords

DAPODIC System, Risk Assessment, OCTAVE Allegro, Mitigation.

1. INTRODUCTION

The process of implementing strategic plans on national education development aimed at improving access, quality, governance, and accountability of national education is highly dependent on national education planning programs.

Dapodik is a system that contains information on students, educators, and education, as well as provides direct information about educational materials that are always updated online and sourced from schools. This system is managed directly under the direction of the Ministry of Education, Culture, Research, and Technology. Dapodik is a national standard and comprehensive data collection system that is the main source of national education data for planning national education programs that have the aim of Indonesia producing smart and highly competitive human resources.

School facilities and infrastructure which include educators and education personnel (PTK), students, and also the process of speakers in the learning group (Rombel) is an entity from primary data. Thus, it is very important in education planning to be mature and quality in the education system, there is something called DAPODIK. All programs resulting from educational planning will be far from expected if not mature. Fast, complete, valid, accountable, and always up-to-date data is needed to implement education programs and appropriate planning, it will facilitate the entire process from planning, implementation, and reporting to evaluation of the performance of national education programs. This can be done more structured, effectively, efficiently, and on target, and can also be connected quickly, validly, accountably, completely, and also up to date with the latest data.

By utilizing data from the DAPODIK application as a reference for student data, schools are requested to participate in DAPODIK activities to collect data for the Ministry of Education and Culture program for primary and secondary education for the provision of National Examinations, National Student Identification Number (NISN), School Operational Assistance (BOS), Unique Number of Educators and Education Personnel (NUPTK), Poor Student Assistance (BSM), and also teacher allowance As a result, schools must actively participate in Dapodik activities to collect data. One of the methods used for information technology risk management and analysis is OCTAVE (Operationally Critical Threat, Assets, and Vulnerability Evaluation). OCTAVE was developed by Carnegie Mellon University's Software Engineering Institute (SEI). OCTAVE is a set of tools, techniques, and methods for risk-based information systems security assessment and planning. OCTAVE has three variants, namely OCTAVE, OCTAVE-S, and OCTAVE Allegro. The method that is a reference in this study is the OCTAVE Allegro framework. OCTAVE Allegro is a simplified method with a focus on information assets, which can be done in a workshop-style and collaborative method. OCTAVE Allegro is slightly different from other Octave approaches because this framework focuses on information assets owned by organizations or companies in the context of how they are used, stored, moved, processed and how threats, vulnerabilities, and disruptions occur in these assets.

2. LITERATURE STUDY

2.1 Understanding of Information Systems

An information system is a system that uses hardware and software to convey useful information and relates between data and methods. [4]

Information systems can facilitate decision-making, coordination, and control as well as assist workers and managers in analyzing problems, visualizing complex subjects, and developing new products. [30]

2.2 Understanding of Management

Management is the process of planning, organizing, directing, and controlling an organization's resources to achieve predetermined goals. [25]

Management is the process of using human, financial, and physical resources to help an organization achieve its goals through planning, organizing, leadership, and controlling. [9]

2.3 Elements of Management

The elements of management consist of human resources, finance, materials or raw materials, machines, methods, and markets [5] with the following explanation:

1. Human Resources (HR)
   When the company has competent human resources, the company will have effective management because individuals set goals and do it to achieve goals.
2. Finance
   All planned activities can be carried out effectively with finances so that the company can carry out all its activities easily.
3. Material or Raw Material
   The products to be produced are of high quality if the materials used are good and function effectively.
4. Machine
   Machine components are necessary to make it easier for workers to complete them to work efficiently and effectively.
5. Method
   The method can be interpreted as the approach taken to carry out work. A good method always considers various things.
6. Pass
   Products that have been produced will be marketed to customers. If the product has good quality, then the sales rate will increase and affect profits.

2.4 Risk Definition

Risiko is a condition that arises due to the uncertainty associated with existing consequences, which can lead to unfavorable conditions. [26]

The Big Indonesian Dictionary (KBBI) defines risk as the possibility of events that can harm the company. Thus, it can be seen that risk is an uncertain condition in which some elements can be detrimental as a result of a series of processes that are being carried out now and in the future.

Uncertainty leads to the emergence of risks. Uncertainty itself has many levels with characteristics that can be seen in Table 1:

Table 1. Uncertainty Levels

Uncertainty Levels	Characteristic	Example
None (Definitely)	Results can be predicted with certainty	Natural law
Objective Uncertainty	Results can be identified and probabilities known	Dice games, cards
Subjective Uncertainty	Results can be identified but probabilities are unknown	Fire, car accident, investment
Very uncertain	Results cannot be identified but probabilities are unknown	Space exploration

2.5 Risk Factors

Factors affecting risk management: [13]

1. Disasters are the cause of the actual deviation of events from the expected. Disasters (perils) can be defined as the direct cause of loss. Common disasters are fires, typhoons, explosions, accidents, dying young, disease, carelessness, and dishonesty.
2. Hazard is a condition that is behind the occurrence of the chance of loss (possible loss) from certain disasters. The danger increases the risk of possible loss.

Meanwhile, the classification of hazards can be divided into several types, namely:

1. Physical hazards, for example, are related to the building facilities of a company.
2. A moral hazard such as dishonesty or indiscipline.
3. Moral hazards (moral hazard) such as carelessness or lack of attention from parties involved in a company.
4. Danger due to law or regulation (legal hazard) for example due to ignoring laws or regulations that have been set.

2.6 OCTAVE Allegro Method

OCTAVE Allegro can be done in the form of workshops, co-settings supported by guides, worksheets, and questionnaires, contained in the appendix of OCTAVE Allegro. One of the advantages of OCTAVE Allegro is that it is suitable for use by individuals who want to conduct a comprehensive risk assessment without extensive involvement from existing organizations, experts, or resources. The OCTAVE Allegro method consists of eight stages grouped into four categories or phases. The four categories are as follows: [7]

1. Category 1, establishes what the organization is directing.
2. Category 2, create a profile of assets owned by the organization.
3. Category 3, identifies threats to each information asset in the context of its container.
4. Category 4, identifying and mitigating risks to information assets and developing mitigation approaches.

The four categories can be seen in Figure 1.

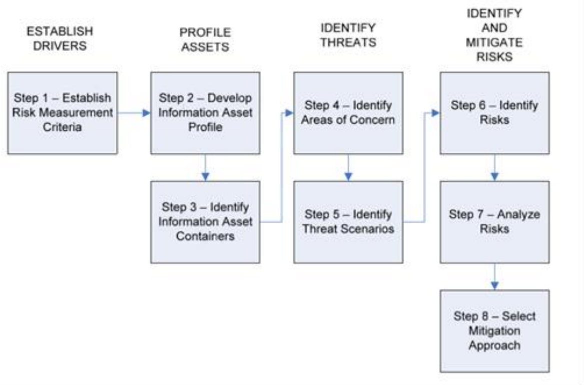
ESTABLISH DRIVERS
PROFILE ASSETS
IDENTIFY THREATS
IDENTIFY AND MITIGATE RISKS
Step 1 – Establish Risk Measurement Criteria
Step 2 – Develop Information Asset Profile
Step 3 – Identify Information Asset Containers
Step 4 – Identify Areas of Concern
Step 5 – Identify Threat Scenarios
Step 6 – Identify Risks
Step 7 – Analyze Risks
Step 8 – Select Mitigation Approach

Figure 1. OCTAVE Allegro Steps

Figure 1 describes the 4 categories and 8 steps on Octave Allegro that correspond to the book guide "Improving The Information Security Risk Assessment Process".

2.7 DAPODIC System

DAPODIK is an integrated national-scale data collection system and the main source of national education data, which is part of the national education planning program in realizing smart and competitive Indonesian people because, without careful education planning, all programs formed from the planning will be far from the expected goals. To carry out educational planning, as well as to implement educational programs in a measurable, targeted, effective, efficient, and sustainable manner, fast, complete, valid, accountable, and up-to-date data is needed. In this regard, the Ministry of National Education has developed an integrated national-scale data collection system called Basic Education Data (DAPODIK). [23]

3. METHODOLOGY

This study will use the OCTAVE Allegro method. This research stage is by making observations, interviews, and filling out questionnaires on internal sources from the DAPODIK system of SD Negeri Karangtalun 03 Cilacap. The stages include:

1. Observation
   Observation is a way of collecting data by observing and reviewing an object that you want to study based on the method to be used. Observation aims to obtain the basic information needed, then identify the problems to be studied in the study.
2. Interview
   The interview is a data collection technique conducted face-to-face and asks several direct questions with related parties between the author and Mrs. Rosalia Muliana, S.Pd as a resource person or DAPODIK system operator at SD Negeri Karangtalun 03 Cilacap. This is done to gather information from reliable sources and better understand the identity of the object.
3. Questionnaire
   A questionnaire is a list of questions made by the author and then distributed to respondents to fill out and will later be returned to the author again. This is part of the collection of data or information. Questionnaires are conducted to see the level of risk in the objects analyzed.

4. RESULTS AND DISCUSSION

The risk assessment stages in the DAPODIK System refer to 4 phases consisting of 8 OCTAVE Allegro work steps. This research was conducted by interviewing the DAPODIK system operator of SD Negeri Karangtalun 03 Cilacap as the school's IT. Every step completion will be displayed discussion based on the data obtained. The risk assessment steps and their discussion will be shown in the following subchapters:

1. **Step 1: Determining Risk Assessment Criteria**

This step is done by building organizational drivers that are reflected in a series of risk measurement criteria. In this step there are two activities, which are as follows:

The first activity establishes a series of qualitative actions (risk measurement criteria) that are used as an evaluation of the organization by determining the impact area to recognize how widespread the impact of risk is. The selected impact areas are:

1. The impact of risk posed by citizens on the reputation and trust of the institution is related to risk.
2. The impact of risk on operational costs that must be incurred by the institution is related to risk.
3. The impact of risks posed on productivity on services related to ensuring the services provided run well.
4. Impact on safety and health areas on users when there is a risk.
5. Sanctions will be given if there is a risk of violation or fraud committed by the user administrator or employee

The second activity is giving priority to each impact area with a scale of 1-5, starting with the most important will get the highest scale which is 5 and the less important will get the lowest scale which is 1. Therefore, the determination of the affected impact area can be concluded in Table 2.

Table 2. *Impact Area Prioritization*

Allegro Worksheet 7	**Worksheet Skor Prioritas *Impact Area***
Priority Score	***Impact Areas***
4	Reputation and Customer Trust
3	Financial
5	Productivity
1	Safety and Health
2	Fines and Legal Penalties

In Table 2 the first priority is on productivity with a priority score of 5 because it concerns service to employees and the community. How do admins or district employees ensure that DAPODIK System services can run well and without any disruption, productivity can affect the comfort and satisfaction of employees and the community as users.

The second priority is the reputation and trust of customer users with a priority score of 4 because it relates to customer reputation and trust. If reputation and trust are reduced, the intensity of using the DAPODIC System can decrease and have an adverse impact on the DAPODIC System.

The third priority with a score of 3 is financial because it relates to the cost of maintaining the system and replacing devices when needed to ensure that the devices can run properly according to their functions.

The fourth priority is fines and legal sanctions, but this is so rare that there are almost no rules on fines and legal sanctions.

The fifth priority is safety and health by occupying the last priority because there has never been a risk that affects security and health that can affect the DAPODIC System so far.

2. Step 2: Identifying information Asset Profiles

This stage identifies a collection of critical information assets. Critical information assets profile obtained from the identification of interviews in the business process service DAPODIK system SD Negeri Karangtalun 03 Cilacap. The critical identification results in the DAPODIK System are information assets that are used every day. The most important information asset is student data, because the school does not store student data manually, so school operators cannot input data which can be hampered.

The results of asset identification information will be documented by asset profiling using Allegro Worksheet-8 as in Table 3 below:

Table 3. Critical Information Asset Profile

Allegro Worksheet 8	**Critical Informatio Asset Profile**	
(1) Critical Asset What are critical information assets?	**(2) Rationale for Selection** Why are these information assets important in organizations?	**(3) Description** What is the description of the information asset?
Student data (Name, NISN, NIK, grade level, study group, and date of birth)	Student data is important because data contains name, NISN, NIK, grade level, study group, and date of birth. Therefore, if the data is lost or damaged, it will disrupt the running of business processes in the DAPODIK System	Student data is individual data that is structured as a result of student registration activities for school
(4) Owner (s) Who owns the information asset?		
DAPODIK belongs to the Ministry of Education, Culture, Research, and Technology of the Republic of Indonesia.		
(5) Security Requirements What are the security needs for information assets?		
Confidentiality	Maintain the confidentiality of data access rights from unauthorized parties and maintain the confidentiality of information data. Only registered users can access the entire data.	
Integrity	Maintain data so that it remains integrity so as not to experience changes or modifications to data from any parties unless getting instructions to make changes from the person concerned if experiencing problems.	
Availability	Data can only be accessed on one school operator's laptop, SD Negeri Karangtalun 03 Cilacap.	
(6) Most Important Security Requirement What are the most important security needs for those information assets?		
Confidentiality	✓ **Integrity**	Availability

Based on the results of the identification process in Table 3, it is explained that the most important asset in DAPODIK services is integrity. Student data is critical data in the DAPODIK system the information in question starts from (Name, NISN, NIK, grade level, study group, and place of birth) it is very important integrity so that data is not easily lost or modified by irresponsible parties. But other security needs are also no less important to maintain functionality and prevent compromised security.

3. Step 3: Identifying Information Asset Containers

The third step is to identify information assets through the interview stage, the process of identifying information assets has 3 parts, namely, technical (TC), physical (Phc), and people (PC). Each identified container has internal and external sides. From the results of the interview, it can be seen that the technical container summary focuses on the server network and infrastructure managed by SD Negeri Karangtalun 03 Cilacap. Then the physical container focuses on physical assets in SD Negeri Karangtalun 03 Cilacap which are used to manage services, then the people container focuses on people in SD Negeri Karangtalun 03 Cilacap, both internal and external.

4. Step 4: Identifying Areas of Concern

The fourth step is to identify areas of concern which are divided into three parts, namely technical (TC), physical (Phc), and people (PC). This step describes a detailed descriptive statement about the conditions in the agency related to matters that can affect assets in the DAPODIK system, which can be seen in Table 4.

Table 4. Area of concern

No	**Area of concern**	**Code**	**Security Requirements**
Technical Container			
1	The cessation of DAPODIK System (Basic Education Data) services at SD Negeri Karangtalun 03 Cilacap due to Internet connectivity disruptions.	TC-1	1) Availability

2	Disruption of DAPODIK System (Basic Education Data) services at SD Negeri Karangtalun 03 Cilacap due to system devices that are being updated/repaired.	TC-2	1) Availability
3	Disruption of DAPODIK System (Basic Education Data) services at SD Negeri Karangtalun 03 Cilacap due to server down.	TC-3	1) Availability
4	There are loopholes in system security that can be accessed by unauthorized parties.	TC-4	1) Confidentiality 2) Integrity
5	Service disruption due to crashes on the service system or operating system.	TC-5	1) Availability
Physical Container			
6	The occurrence of natural disasters or environmental threats causes services to stop.	PhC-1	1) Availability
People Containers			
7	Data input errors by employees or administrators.	PC-1	1) Confidentiality 2) Integrity 3) Availability
8	The spread of administrator access rights (usernames and passwords) due to social engineering.	PC-2	1) Integrity

5. Step 5: Identifying Threat Scenario

The fifth step in the OCTAVE Alegro is to identify additional areas of concern to complement the areas of concern in the previous table. This step is carried out documentation of DAPODIK system information assets by asking several questions using questionnaires to determine the effect of risk on the DAPODIK SYSTEM using a questionnaire, there are three parts, namely technical, physical, and people containers. In technical containers, software damage can occur, there is a crash on the system both known and unknown, there is malicious code such as (viruses, Trojan horses, or back doors) that will cause disruption of the service process, and disasters caused by nature and humans (such as floods, fires, earthquakes, etc) that can cause disruption or loss. In a physical container, no situations that can cause the service infrastructure to be damaged or lost. There is social engineering obtained internally so that usernames and passwords can be misused. So it can be concluded that the container that contains the most threats is the technical container.

6. Step 6: Identifying Risk

This step starts by calculating the number of impact area scores by looking back at the risk measurement criteria that have been obtained in Step 1. The way to calculate the number of scores for each impact area is to multiply the value of the impact area obtained in Table 5

. The way to calculate the score in each impact area is as follows:

1. If the value in the impact area is low, then the value of priority is multiplied by 1.
2. If the value in the impact area is medium, then the value of priority is multiplied by 2.
3. If the value in the impact area is high, then the value of priority is multiplied by 3.

Furthermore, the results of calculating the score in each impact area can be seen in Table 5.

Table 5. *Impact Area Score*

Impact Areas	Value Of Priority	Impact Score		
		Low (1)	Medium (2)	High (3)
Productivity	5	5	10	15
Reputation and Customer Trust	4	4	8	12
Financial	3	3	6	9
Fines and Legal Penalties	2	2	4	6
Safety and Health	1	1	2	3

7. Step 7: Analyze the Risk

This step analyzes the total risk from the results of steps 4, 5, and 6 by performing a simple quantitative calculation of the extent to which the organization is affected by the threat. This relative risk score is obtained by considering the consequences of risk impact on the organization. This is done by quantifying the risk measurement criteria from stage 1. The result of this quantification is called the relative risk score obtained by calculating the score for each impact area by multiplying the impact area value by the impact area priority value obtained from the priority sequence created in stage 1. Next, analyze the total amount of risk in all areas of concern that are the result of identifying threats previously by profiling, then determine the pool in each risk profile in the risk area of concern using Allegro Worksheet 10 as in Table 6.

Table 6. Order of Risk-Based on Total Risk Score

Code	***Areas of Concern***	**Reputation and Customer Trust**	**Financial**	**Productivity**	**Safety and health**	**Fines and Legal Penalties**	**Total Risk Score**	**Probes**	**Mitigation Approach**
TC-1	The cessation of DAPODIK System (Basic Education Data) services at SD Negeri Karangtalun 03 Cilacap due to Internet connectivity disruptions.	Low (4)	Low (3)	Low (5)	Low (1)	Low (2)	15	**Low**	*Accept*

TC-2	Disruption of DAPODIK System (Basic Education Data) services at SD Negeri Karangtalun 03 Cilacap due to system devices that are being updated/repaired.	Low (4)	Low (3)	Low (5)	Low (1)	Low (2)	15	**Low**	*Accept*
TC-3	Disruption of DAPODIK System (Basic Education Data) services at SD Negeri Karangtalun 03 Cilacap due to server down.	Low (4)	Low (3)	High(15)	Low (1)	Low (2)	25	***High***	*Defer*
TC-4	There are loopholes in system security that can be accessed by unauthorized parties.	*Medium (8)*	Low (3)	Low (5)	Low (1)	Low (2)	19	***Medium***	*Mitigate*
TC-5	Service disruption due to crashes on the service system or operating system.	*Low (4)*	*Low (3)*	High (10)	Low (1)	Low (2)	20	**Medium**	*Defer*
PhC-1	The occurrence of natural disasters or environmental threats causes services to stop.	*Medium (8)*	*Low (3)*	High (15)	Low (1)	Low (2)	29	***High***	*Mitigate*
PC-1	Data input errors by employees or administrators.	*Medium (8)*	Low (3)	Low (5)	Low (1)	Low (2)	19	***Medium***	*Mitigate*
PC-2	The spread of administrator access rights (usernames and passwords) due to social engineering.	*Medium (8)*	Low (3)	Low (5)	Low (1)	Low (2)	19	***Medium***	*Mitigate*

The next step is to group the number of threats in each container that serves to facilitate mitigation which can be seen in Table 7.

Table 7. Grouping Number of Threats

Mitigation Approach	Technical Container (TC)	Physical Container (PhC)	People Container (PC)
Mitigate	1	1	2
Defer	2	0	0
Accept	2	0	0
Total	**5**	**1**	**2**

The results contained in the number of threats grouping table above show that technical containers have the most threat risk with the number of threat risks 5. While physical containers have a threat risk of 1 and people containers number 2.

8. Step 8: Choosing a Mitigation Approach

Step 8 on OCTAVE Allegro is to choose a mitigation approach. A mitigation approach can be taken by grouping each identified area of concern based on the relative risk score in the previous table. The result of the recommendation for the mitigation plan is to reduce the risk of threats based on areas of concern which can be seen in Table 8.

Table 8. Grouping based on the Mitigation Approach Mitigation

Mitigation Approach	Code	*Area of Concern*	Recommendation
Mitigate	TC-4	There are loopholes in system security that can be accessed by unauthorized parties	Use the blocking feature if there is an error entering the username and password repeatedly, and encrypt the password so that it is not exposed on the network
	PhC-1	The occurrence of natural disasters or threats caused services to stop	Back up data regularly so that data is stored safely and in the event of a natural disaster the data lost or damaged can be recovered.
	PC-1	Data input errors by employees or administrators	The recommended effort is to double-check before submitting to the system so that there are no input errors that will result in student data
	PC-2	The spread of administrator access rights (usernames and passwords) due to social engineering	A recommended effort to resolve the issue is to add a 2-step verification that requires a password and verification code to log into the system.

Defer	TC-3	Disruption of DAPODIK System (Basic Education Data) services at SD Negeri Karangtalun 03 Cilacap due to server down	Server downs often occur due to sudden power outages, and recommended efforts, the school provides or uses backup power backup (generator)
	TC-5	Service disruption due to crashes in the service system or operating system.	Attempts to exercise control and Check the computer or network regularly.
Accept	TC-1	The cessation of the DAPODIK System (Basic Education Data) at SD Negeri Karangtalun 03 Cilacap due to Internet connectivity disruptions	Selection of network providers that can ensure smooth internet connectivity in the process of DAPODIK System service.
	TC-2	Disruption of DAPODIK System (Basic Education Data) services at SD Negeri Karangtalun 03 Cilacap due to system devices that are being updated/repaired	Control and periodically check the computer or system outside working hours so that the service process is not interrupted.

Based on the results of Table 8 it can be seen that the mitigate approach is carried out in the area of concern with the codes TC-4, PhC-1, PC-1, and PC-2, the deferred approach is carried out in the area of concern with the TC-3 code, and TC-5 and the accept approach is carried out in the area of concern with the TC-1 and TC-2 codes.

5. CONCLUSION

Conclusions obtained as a result of the DAPODIK System service risk management analysis research conducted using the OCTAVE Allegro method: 1. Risk assessment on the DAPODIK System service at SD Negeri Karangtalun 03 Cilacap is carried out by following the steps contained in the Octave Allegro method guide, starting with determining and defining the impact area in information assets, then determining critical assets from information assets, identifying containers of information assets consisting of Technical Containers (TC), Physical Container (PhC) and People Container (PC), determine the threat of each container and determine the severity of the risk and make mitigation recommendations of each threat that occurs. 2. Based on the results of tests conducted on the DAPODIK System service at SD Negeri Karangtalun 03 Cilacap, mitigate approaches were obtained in number 4, defer in number 2, and accept in number 2. The relatively high-risk value is found in the Physical Container (PhC) with a total risk value of 29, namely due to a natural disaster that causes DAPODIK system services to stop. The risk value is relatively low in the Technical Container (TC) with a total risk value of 15, namely due to internet connectivity disruptions so DAPODIK system services are interrupted or temporarily stopped.

mitigate approaches were obtained in number 4, defer in number 2, and accept in number 2. The relatively high-risk value is found in the Physical Container (PhC) with a total risk value of 29, namely due to a natural disaster that causes DAPODIK system services to stop. The risk value is relatively low in the Technical Container (TC) with a total risk value of 15, namely due to internet connectivity disruptions so DAPODIK system services are interrupted or temporarily stopped.

6. REFERENCES

[1] Australian Government Publishing Service. 1994. *Style manual for authors, editors and printers* (5th ed.). Canberra: Penulis.

[2] Al Fatta, Hanif. 2007. Analisis dan Perancangan Sistem Informasi untuk Keunggulan Bersaing Perusahaan dan Organisasi Modern. Yogyakarta: Andi.

[3] Andrianof, H. (2018). Rancang Bangun Sistem Informasi Promosi dan Penjualan pada Toko Ruminansia Berbasis Web. Jurnal Pendidikan Dan Teknologi Informasi, 5(1), 11–19.lppm.upiyptk.ac.id/ojs3/index.php/PTI/article/download/52/22/%0A

[4] Anjelita, P., & Rosiska, E. (2019). E- Learning Pada Smk Negeri 3 Batam. http://ejournal.upbatam.ac.id/index.php/comasiejournal/article/view/1572

[5] Aristasari, P. and Riadi, I. (2011) 'Manajemen Risiko Pada Learning Management System Menggunakan Kerangka Kerja OCTAVE Allegro', pp. 1–15.

[6] Asari, S. O. 2020. Analisis Penilaian Risiko pada Layanan Pos Corporate Menggunakan Framework OCTAVE Allegro. Skripsi Sistem Informasi, Universitas Ahmad Dahlan, Yogyakarta, hlm. 17 - 19.

[7] Caralli, R.A., Steven, J. F., Young, L.R., & Wilson, R. W. 2007. Introducing OCTAVE Allegro: Improving the Information Security Risk Assesment Process. USA: Software Engineeering Institute Carnegie Mellon UniversityAlberts, Christopher, & Dorofee, A. 2005. OCTAVE Method Implementation Guide. PA: Software Engineering Institute, Carnegie Mellon University.

[8] C. Callahan and J. Soileau. 2017. "Does Enterprise risk management enhance operating performance?". Adv. Account., vol. 37, pp. 122–139.

[9] Deva, B. S., & Jayadi, R. (2022). Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro. Jurnal Teknologi Dan Informasi, 12(2), 106–117. https://doi.org/10.34010/jati.v12i2.6829

[10] Erawati, W. (2019). Perancangan Sistem Informasi Penjualan Dengan Pendekatan Metode Waterfall. Jurnal Media Informatika Budidarma, 3(1), 1. https://doi.org/10.30865/mib.v3i1.987

[11] Friedman, S. L., & Wachs, T. D. (Ed.). 1999. Measuring environment across the life span: Emerging methods and concepts. Washington, DC: American Psychological Association.

[12] Hanafi, M.M. 2009. Manajemen Risiko. Unit Penerbit dan Percetakan Sekolah Tinggi Ilmu Manajemen YKPN: Yogyakarta.

[13] Hutagalung, L. E. (2022). Analisa Manajemen Risiko Sistem Informasi Manajemen Rumah Sakit (Simrs) Pada Rumah Sakit Xyz Menggunakan Iso 31000. TeIKa, 12(01), 23–33. https://doi.org/10.36342/teika.v12i01.2820

[14] Ikhsan, Hidayatul dan Nanda Jarti. 2018. Information Technology Security Risk Analysis Using Octave Allegro. *Jurnal Responsive,* 2(1), 31-41.

[15] Instruksi Menteri Pendidikan No.2 Tahun 2011 penggunaan sistem pendataan DAPODIK.

[16] Kuntari, N. L., Chrisnanto, Y. H., & Hadiana, A. I. (2018). Manajemen Risiko Sistem Informasi di Universitas Jenderal Achmad Yani Menggunakan Metoda Octave Allegro. Seminar Nasional Teknologi Informasi Universitas Ibn Khaldun Bogor, 552–559. http://prosiding.uika-bogor.ac.id/index.php/semnati/article/view/106

[17] Laudon. Kenneth C., dan Laudon. Jane P., "Management Information System", 10th ed, Jakarta: Selemba empat,2007.

[18] Lokobal, A. 2014. Manajemen Risiko pada Perusahaan Jasa Pelaksana Konstruksi di Propinsi Papua. Modul 1, pp, hlm. 109 - 118.

[19] Martin Halomoan Lumbangaol, M. R. R. (2020). Rancang Bangun Sistem Informasi Penjualan dan Penyewaan Properti Berbasis WEB Di Kota Batam. Jurnal Comasie, 01(03), 83–92.

[20] Maydianto, & Ridho, M. R. (2021). Rancang Bangun Sistem Informasi Point of Sale Dengan Framework Codeigniter Pada Cv Powershop. Jurnal Comasie, 02, 50–59.

[21] Moleong, Lexy J. 2016. Metodologi Penelitian Kualitatif. Bandung: Remaja Rosdakarya.

[22] Pai, P., Tanjung, S. M. P. N., & Sumatera, R. (2022). Kata Kunci: Manajemen, Resiko, Pembelajaran, PAI. 7(3), 240–250.

[23] Peraturan Menteri Pendidikan Dan Kebudayaan Nomor 79 Tahun 2015 Tentang Data Pokok Pendidikan.

[24] Richard F. Neuschel,1960. "*Management By System*". McGraw Hill, New York.

[25] Sandy, S., & Solihin, H. H. (2021). Audit Keamanan dan Manajemen Risiko pada e-Learning Universitas Sangga Buana. Jurnal Manajemen Informatika (JAMIKA), 11(1), 1–14. https://doi.org/10.34010/jamika.v11i1.3641

[26] Syariah, P. B., Rahmayanti, D., Fadillah, D., & Syifa, I. F. (2020). Studi Literatur Manajemen dan Risiko Kepatuhan. 17(01), 38–41.

[27] Tukino. (2020). Rancang Bangun Sistem Informasi E-Marketing Pada Pt Pulau Cahaya Terang. Computer Based Information System Journal, 08(01), 25–33.

[28] Viyanto.R.A, L. T. 2013. Manajemen Risiko Teknologi Informasi (Studi Kasus Pada Perusahaan Jasa). Binus University.

[29] Waidah, D. F., & Tarika, L. (2018). Analisis Dan Pengembangan Sistem Informasi Data E-Raport Dapodik Di Sd Swasta 001 Pt. Kg Meral Barat. Angewandte Chemie International Edition, 6(11), 951–952., 3(1), 10–27.

[30] Wahyudi, M. D., & Ridho, M. R. (2019). Sistem informasi penjualan mobil bekas berbasis web pada cv phutu oil club di kota batam. http://ejournal.upbatam.ac.id/index.php/comasiejournal/article/view/1565