Evaluation Of Basic Education Data System (DAPODIK) On UPTD Dinas Pendidikan of District North Sumedang Using The Octave-S Method

Fathoni Mahardika[1], Agun Guntara[2], Asep Saeppani[3], Dani Indra[4], Mulya Suryadi[5]
{fathoni@stmik-sumedang.ac.id[1] , aguntara@stmik-sumedang.ac.id[2], saeppani@stmik-sumedang.ac.id[3], dani@stmik-sumedang.ac.id[4] , mulyasuryadi@stmik-sumedang.ac.id[5]}

Information Technology, STMIK Sumedang, West Java Indonesia[1,2,3,4,5]

Abstract. The development of science and technology is growing very rapidly, it can be seen from individuals who can easily access information without limits of space and time. Every Education Agency certainly hopes to have a system that has good quality and is increasing, especially in the current era of globalization. The UPTD Dinas Pendidikan is one of the government institutions in the field of education that has an Basic Education Data System (DAPODIK) that is important for DAPODIK System Operators. The use of Online Attendance (Attendance of Teachers & Education Personnel) is hampered by the quality of the internet network available, if the internet network is being disrupted, so that access to Online Attendance is not possible. Based on the existing problems, this research was conducted under the title of Evaluation of Basic Education Data System (DAPODIK) at the UPTD Dinas Pendidikan Of District North Sumedang Using the OCTAVE-S Method. The purpose of this study is to help evaluate the DAPODIK System by implementing Risk Management. This study uses the OCTAVE-S Method. This research was carried out through several stages including the preparation stage, the OCTAVE-S stage based on the OCTAVE Method, the evaluation phase, the data processing stage, and the report making stage from the system evaluation results. The results of this study, the DAPODIK System highlighted (Spotlight) to the Green (Green) level which means fulfilling the criteria and 33 of the 40 statements on the Questionnaire were declared valid. From the results of this evaluation, recommendations are formulated to improve system security management in the DAPODIK System.

Keywords: Evaluation, Dapodik Systems, OCTAVE-S, Risk Management.

1 Introduction

Evaluation is a subsystem that is very important and very needed in every education system because evaluation can reflect how far the progress or progress of educational outcomes. With evaluation, then the forward and backwardness of the quality of education can be known, and also by evaluation, we can find out the weaknesses and easily find a way out to change for the better in the future [1]–[5].

According to Hanafi (2006: 1) "Risk is a danger, a consequence or consequence that can occur due to an ongoing process or future event" [6]. The sources of the causes of risk can be distinguished as follows:

1. Internal risk, namely the risk originating from the UPT of the North Sumedang District Education Office.
2. External risk, namely the risk originating from outside the UPT of the North Sumedang District Education Office or the environment outside the UPT of the North Sumedang District Education Office.

3. Financial risk is a risk caused by economic and financial factors.
4. Operational risk is all risks that do not include humans, nature and technology. To manage this risk, management is needed.

Followed by research by Viyanto (2013) "Management is a planning process, organizing resource regulator, communication, leadership, motivation, and use of resources to achieve organizational goals effectively and efficiently [12]".

The management has the purpose of protecting from a significant risk that can hinder the achievement of objectives, provide a consistent management framework for the business processes and functions of each of the Education Offices and increase performance through the provision of risk level information as outlined in useful maps for management in developing strategies and improving management processes that are continuous and continuous. To achieve these goals, a supportive method is needed to assist in solving problems.

Basic Education Data or DAPODIK is an integrated national scale data collection system and is the main data source of national education, 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 plan will be far from the expected goals. To carry out educational planning, as well as to implement educational programs on target, data that is fast, complete, valid, accountable and kept up to date is needed. The availability of data that is fast, complete, valid, accountable and up to date, the process of planning, implementing, reporting, and evaluating the performance of national education programs can be carried out in a more measurable, targeted, effective, efficient and sustainable manner. In this regard, the Ministry of National Education has developed an integrated national scale data collection system called Education Basic Data (DAPODIK).

The problems found in the UPT of North Sumedang District Education Office are:
1. In the DAPODIK System (Basic Education Data), it is difficult to find the location where students live, so that when DAPODIK System Operators need data on student residence, their performance is hampered because the location data needed is not available.
2. Applications from the center are not perfect so that it is difficult to access by users (DAPODIK System Operators) even though 5 (five) links have been provided, the data that the DAPODIK System Operators should have obtained is difficult to obtain.
3. The use of Absent Online (Absent Teacher & Education Personnel) is hampered on the quality of the available internet network if the internet network is being disrupted, so that access to Online Absence cannot be done.
4. Constrained data synchronization when students change schools so that student data cannot be linked to the DAPODIK System database contained in the transfer student's school.
5. There are obstacles to DUPAK (List of Credit Score Proposals) using Microsoft Excel, sometimes the formula does not support the database so that the performance of the Dapodik System Operator is hampered when using Microsoft Excel.

Based on these problems, researchers will use the OCTAVE Method to solve problems found in the UPT North Sumedang District Education Office. The OCTAVE (Operationtionally Critical Threat, Assets and Vulnerability Evaluation) method is one of the methods used to conduct risk research. The OCTAVE method itself has 3 (three) types, namely, OCTAVESM, OCTAVE-Allegro, and OCTAVE-S. OCTAVESM is used to form the knowledge base of OCTAVE, OCTAVE-Allegro is used in effective approaches to information security and guarantees, and OCTAVE-S is used in smaller organizations. The method used in this study is the OCTAVE-S method, where this method is the result of a modification of the OCTAVE method that is adapted to the capacity of the UPT District Education Office in North Sumedang District.

The reason the researchers used the OCTAVE-S method was because the use of the OCTAVE-S method was a variation to develop and analyze risks in the UPT North Sumedang District Education Office which had a comprehensive, systematic, contextual scale with a staff of less than 300 (three hundred) and allows risk analysis activities to be carried out by a small number of teams so that they can be directed by themselves effectively and efficiently.

2 Methods

The research methodology carried out several stages including:

1) Perform preparation stages by conducting a literature study process and literature review. A Literature study is a method used to collect data or sources related to the topic raised in a study. In this study, the literature study that researchers obtained from various sources such as journals, books, and the internet. Literature Review. The literature review is a review of related libraries. In accordance with this meaning, the researcher conducted a review (review) of the literature from the results of the research report on problems related to risk management, evaluation of information systems and the use of the OCTAVE-S method.

2) The second stage is the stages of OCTAVE-S based on the OCTAVE Method.
   a) Building Threat Profile Based Assets
   b) Identifying Infrastructure Vulnerabilities
   c) Developing a Security and Planning Strategy

3) The next stage is the implementation phase of the evaluation, the researcher carries out data collection by conducting interviews, making questionnaires, testing the validity and reliability testing of the data resulting from the distribution of questionnaires and identifying risks from organizational crisis assets.

4) Next step is processing data from the results of data collection (interviews, questionnaires), measuring data (validity test, reliability test) and the results of risk identification from organizational crisis assets.

5) The next stage is to make a report from the results of the system evaluation based on the stages of the OCTAVE-S method and can be used as a reference in determining recommendations in the management of the DAPODIK System.

3 Results and Discussion

3.1 Risk Management

Definition of risk management according to Fahmi (2010: 2) "Risk management is a field of science that discusses how an organization applies measures in mapping various existing problems by placing various management approaches comprehensively and systematically" [7].

Definition of risk management according to Bramantyo (2008: 43) "Risk management is a structured and systematic process in identifying, measuring, mapping, developing risk handling alternatives" [8].

Taken from Research Maryani (2014) citing the opinion of Noshworthy (2000: 600) Risk Management is "Implementation of measures aimed at reducing the threat of occurring and minimizing any damage if they do. Risk analysis and risk control form the basis of risk management where risk control is a balance between security, usability, and cost ". So that it can be interpreted the implementation of measures that aim to reduce the possibility of threats that occur and minimize damage if they do. Risk analysis and control form the basis of a balance between security, usability, and cost [7].

Based on the understanding of risk management above, researchers can conclude that risk management is management carried out to map various existing problems to further overcome the risks that occur.

3.2 OCTAVE-S

The definition of OCTAVE-S according to Alberts and Dorofee (2003: 3) is a variation of the OCTAVE approach developed to find small needs, organizations that do not have hierarchies. So it can be concluded that OCTAVE-S is a variation of the OCTAVE approach that was developed to carry out risk assessments of small-scale organizations that are comprehensive, systematic, contextual, self-directed, able to manage organizational risk by recognizing risks that might occur in the organization and make a plan for mitigation and mitigation of each known risk [9], [10].

3.3 Octave-S Stage and Process

According to Alberts and Dorofee (2003: 5), OCTAVE-S is based on 3 (three) stages described in the OCTAVE criteria, although the numbers and sequence of activities differ from the OCTAVE method used. This section provides a brief overview of the stages, processes, and activities of OCTAVE-S [9].
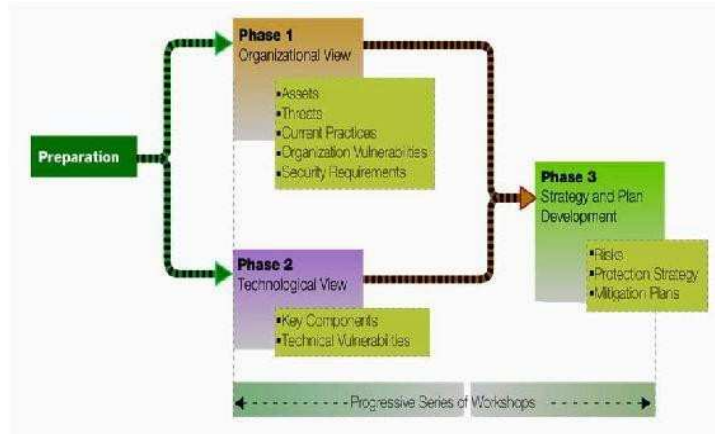
Figure 1. Octave-S

3.4 Results Discussion

This research was conducted to determine the risks that might occur in the DAPODIK System. Data measurement techniques using the SPSS 17.0 program. Based on the results of measurement data, it can be seen that out of the 40 statements in the questionnaire, only 33 statements were valid.

1) Test Validity

The acquisition of questionnaire data was tested for validity by validity test using product moment correlation. This correlation technique is used to find relationships and prove the hypothesis of relationship two if the data of the two variables in the form of intervals or ratios and data sources of two or more variables are the same. In product moment item correlation can be said to be valid if the total values of Correlations are greater than the value of r table. The specified r table value is 0.361 otherwise if the item value is less than 0.361 then the data is invalid. From the tests that have been carried out on 40 item statements produce valid data as many as 33 items and item 7 that are invalid.

Table 1. Result Test Instrument Validation

No	Item Questiion	Corrected Item Statement Total Correlation	r table	Information
1.	P1	0,392	0,361	Valid
2.	P2	0,554	0,361	Valid
3.	P3	0,439	0,361	Valid
4.	P4	0,412	0,361	Valid
5.	P5	0,518	0,361	Valid

No	Item Questiion	Corrected Item Statement Total Correlation	r table	Information
6.	P6	0,418	0,361	Valid
7.	P7	0,434	0,361	Valid
8.	P8	0,445	0,361	Valid
9.	P9	0,474	0,361	Valid
10.	P10	0,38	0,361	Valid
11.	P11	0,104	0,361	Not Valid
12.	P12	0,411	0,361	Valid
13.	P13	0,423	0,361	Valid
14.	P14	0,428	0,361	Valid
15.	P15	0,296	0,361	Not Valid
16.	P16	0,424	0,361	Valid
17.	P17	0,142	0,361	Not Valid
18.	P18	0,423	0,361	Valid
19.	P19	0,533	0,361	Valid
20.	P20	0,367	0,361	Valid
21.	P21	0,388	0,361	Valid
22.	P22	0,283	0,361	Not Valid
23.	P23	0,488	0,361	Valid
24.	P24	0,244	0,361	Not Valid
25.	P25	0,433	0,361	Valid
26.	P26	0,402	0,361	Valid
27.	P27	0,194	0,361	Not Valid
28.	P28	0,409	0,361	Valid
29.	P29	0,084	0,361	Not Valid
30.	P30	0,399	0,361	Valid
31.	P31	0,377	0,361	Valid
32.	P32	0,389	0,361	Valid
33.	P33	0,399	0,361	Valid
34.	P34	0,402	0,361	Valid
35.	P35	0,392	0,361	Valid
36.	P36	0,48	0,361	Valid
37.	P37	0,389	0,361	Valid
38.	P38	0,418	0,361	Valid
39.	P39	0,384	0,361	Valid
40.	P40	0,385	0,361	Valid

From the above tables, it can be seen that 33 of the 40 item statements have r count> from r table (0.361) and are positive. Thus, 33 items of the statement were declared valid.

1) Reliability Test

After testing the validity, the data that has been obtained is tested for its reliability by using a reliability test, this stage is done to determine the extent to which measuring instruments can be relied upon. The item value can be stated as reliability if the result is more than 0.60 otherwise if the item value is less than 0.60 it is stated not reliable.

Table 2. Results Reliability Test

No	Reliabilitas Coefficient	Crobach Alpha	Note
1.	40 Item Question	0,846	Reliable

From the description of the table above, it can be seen that 40 statement items have Crobach Alpha> 0.60. Thus, 40 items of the statement can be said to be reliable.

2) Results Risk Management

In this section, the author will discuss the results of risk management in accordance with the OCTAVE-S Method..

a) Identifying infrastructure vulnerabilities..

1) Analyze processes related to technology
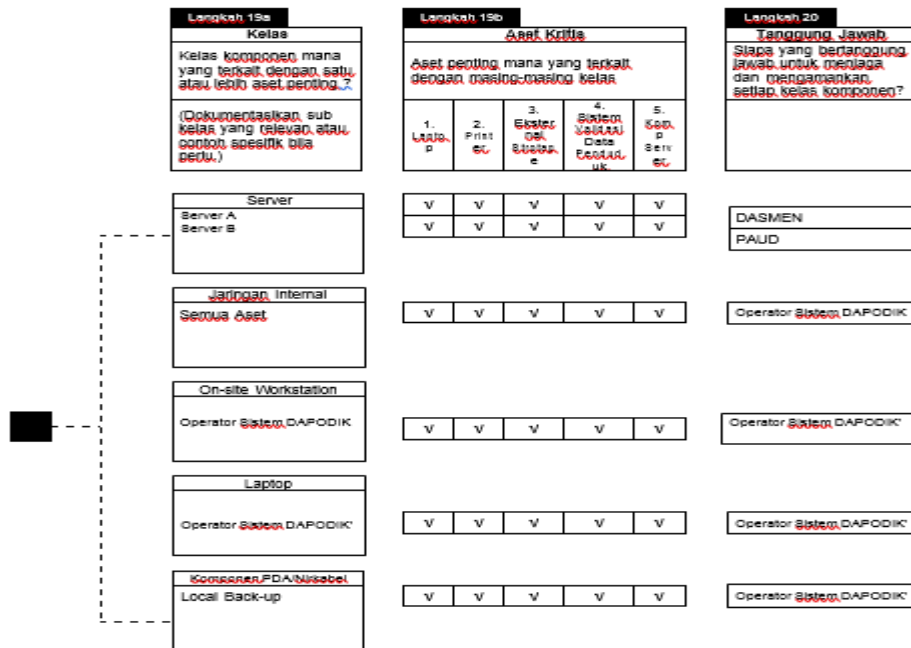
Figure 2. Critical Assets and Responsibility

2) Analyzing processes related to storage

Figure 3. Critical Assets and Responsibility

Figure 4. Level of Protection

b) Organizational Effectiveness in Implementing Risk Management Practices..

Table 3. Spotlight Risk Management

Spootlight Organization On Level	
Red	
Yellow	
Green	
Not Acceptable	

Organizational Effectiveness in Implementing Risk Management Practices. The DAPODIK system found in the Sumedang North District Education Office UPT, highlights (Spotlight) to the Green (Green) level, which means that it fulfills the criteria that the risks in the DAPODIK System are few and 33 of the 40 statements on the Questionnaire are valid.

3) Assessment Stages

At this stage of assessment/design, the researcher made several recommendations for risk mitigation that can be implemented by the UPT North Sumedang District Education Office UPT, especially for DAPODIK System Operators. This recommendation is the result of the processing of the questionnaire which was previously distributed to respondents, namely the DAPODIK System Operator in accordance with the OCTAVE-S Method.

According to the research journal Information Security Risk Management Using the NIST-SP 800-30 Revision 1 Framework (Case Study of STMIK Sumedang) by Fortune Mahardika, in the recommendations of the roles and organizations of the responsibility of the LPSI MU or Chair of the Information Security Unit as the top leadership role in making decisions in giving consideration in establishing documented information security policies, where documentation is built in accordance with standards developed from NIST SO 800-30 Revision 1 and ISO 27002 [11]. According to the research journal Evaluation of the Security of Wireless Hotspot Networks Using the Square Method (Case Study of Medianet Warnet Sumedang) By Yopi Hidayatul Akbar. To improve the security system better, it is expected to routinely check the access control so that data and information relating to legitimate users can be maintained and protected from all forms of threats that may occur unexpectedly [12].

Table 4. Risk Mitigation

No.	Threats	Aspect	Planning	Implementation	Plan Evaluation	Technical Responsibility
1.	Management doesn't accept and act on routine reports that summarize security related information (for example, audits, logs, risks, and vulnerability assessments). The organization does not document, review and test.	Security Management	Management must accept and act on a routine report that summarizes information related to security.	Performed after the system user signs the rules that have been made and socialized.	12 times in one year	Operator Sistem DAPODIK
2.		Contingency Planning / Disaster Recovery	The organization documents, reviews and tests the plans that have been set.	Performed after the system user signs the rules that have been made and	6 times in one year	Operator Sistem DAPODIK

No.	Threats	Aspect	Planning	Implementation	Plan Evaluation	Technical Responsibility
	1) Contingency plans to respond to emergencies, 2) Disaster recovery plans. 3) Business continuity or emergency operation plan.			socialized.		
3.	There are no facility security plans and procedures to safeguard any place, building, and any place, building, and prohibited area documented and tested.	Physical access control	There must be a plan to establish security procedures to maintain important facilities.	Performed after the system user signs a regulation that has been made and socialized.	6 times in one year	Operator Sistem DAPODIK
4.	There is no security plan that is documented and tested to maintain the network system.	System and Network Management	There must be a security plan that is documented and tested to maintain the system and network.	Performed after the system user signs a regulation that has been made and socialized.	4 times in one year	Operator Sistem DAPODIK
5.	Integration of non-installed software is regularly verified.		The software used must be installed regularly and verified.	Performed after the system user signs a regulation that has been made and socialized.	4 times in one year	Operator Sistem DAPODIK
6.	Tools and mechanisms for secure systems and network administration are used and are not routinely reviewed and updated or replaced.		The use of tools and networks must be reviewed regularly reviewed and updated or replaced.	Performed after the system user signs a regulation that has been made and socialized.	4 times in one year	Operator Sistem DAPODIK
7.	There are no documented policies and procedures for establishing and stopping individual or group access rights.	Authentication and Authorization	There must be documented policies and procedures for establishing and stopping individual or group access rights.	Performed after the system user signs the regulations that have been made and have been socialized.	12 time in one year	Operator Sistem DAPODIK

4   Conclusion

Based on the results of the Risk Management evaluation of the DAPODIK System, the UPT North Sumedang District Office can be drawn a number of conclusions including :

1) The stages of the OCTAVE-S method applied to the UPT North Sumedang District Education Office UPT are in the form of risk mitigation recommendations including management must receive and act on a routine report that summarizes security-related information, the organization makes documentation, reviews and tests plans that established, establish security procedures to maintain important facilities, there are documented and tested security plans to safeguard systems and networks, the software used must be regularly installed and verified, the use of tools and networks regularly reviewed and updated or replaced and there are policies and documented procedures for establishing and stopping individual or group access rights..

2) The results of the Risk Management Spotlight at the Green level mean that it fulfills the criteria that the risks in the DAPODIK System found in the Sumedang North District Education Office are few and 33 of the 40 statements on the questionnaire are valid. So the organizations can improve the system and network security in order to reduce the risks that might occur in the DAPODIK System. Although in its activities there is still something that needs to be addressed and implemented as well as documenting security management, Contingency Planning / Disaster Recovery, Physical Access Control, System and Network Management, and Authentication and Authorization.

References

[1]   H. Hendarti and M. Maryani, "Pengukuran Manajemen Risiko Teknologi Informasi dengan Metode Octtave-S," *ComTech Comput. Math. Eng. Appl.*, vol. 5, no. 2, p. 917, 2014, doi: 10.21512/comtech.v5i2.2336.

[2]   S. Selamat, A. Rosidi, and M. R. Arief, "Evaluasi Sistem Informasi Perpustakaan STMIK AMIKOM Yogyakarta," *J. Ilm. DASI*, vol. 17, no. 3, pp. 57–61, 2016.

[3]   Sutarman, *Pengantar Teknologi Informasi*. Jakarta: Bumi Aksara, 2012.

[4]   V. Wahyuni and I. Maita, "Evaluasi Sistem Informasi Manajemen Rumah Sakit Menggunakan Metode Unified Theory of Acceptance and Use of Thechnology," *Ann. Thorac. Surg.*, vol. 1, no. 1, pp. 55–61, 2015, doi: 10.1016/j.athoracsur.2006.03.068.

[5]   A. R. Viyanto, O. S. Latuihamallo, F. M. Tua, A. Gui, and S. Suryanto, "Manajemen Risiko Teknologi Informasi: Studi Kasus pada Perusahaan Jasa," *ComTech Comput. Math. Eng. Appl.*, vol. 4, no. 1, p. 43, Jun. 2013, doi: 10.21512/comtech.v4i1.2682.

[6]   M. Hanafi, *Manajemen Resiko*. Yogyakarta: Unit Penerbit Sekolah Tinggi Ilmu Manajemen YKPN, 2006.

[7]   I. Fahmi, *Manajemen Resiko*. Bandung: Alfabeta, 2010.

[8]   B. Djohanputro, *Manajemen Risiko Korporat*. Jakarta: PPM, 2008.

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

[10] W. Sawyer, *Using Information Technology*. Yogyakarta: Andi, 2007.

[11] F. Mahardika, "Manajemen Risiko Keamanan Informasi Menggunakan Framework NIST SP 800-30 Revisi 1 (Studi Kasus: STMIK Sumedang)," *J. Inform. J. Pengemb. IT*, vol. 2, no. 2, pp. 1–8, 2017, doi: 10.30591/JPIT.V2I2.484.

[12] Y. H. Akbar, "Evaluasi Keamanan Jaringan Wireless Hotspot Menggunakan Metode Square (Studi Kasus Warnet Medianet Sumedang)," *Infoman's J. Ilmu-ilmu Manaj. dan Inform.*, vol. 9, no. 2, pp. 75–90, 2015, doi: 10.33481/INFOMANS.V9I2.60.