Information Security Risk Management for BIDUK System

Kristianto, Natanael Alamas, Jarot S. Suroso

Abstract*: The use of digital technology nowadays makes data and information become vital part of any organization. Non-profit organization, such as Archdiocese of Jakarta, also relies on system to do their work and services for Catholic people under their jurisdiction. BIDUK system is used by Archdiocese of Jakarta as information system to administrate and provide service to people. Its information also used as tools for decision making. Currently, there is no proper information security risk management method used for BIDUK system, which is important system for Archdiocese of Jakarta. This study's objective is to propose a IS risk management method that can be used to manage risks for BIDUK system. This study proposes OCTAVE Allegro method because of its simplicity and suitable for small organization. After following every IS risk management phases of OCTAVE Allegro, we found that this method is suitable to be used to manage risks of BIDUK system.

Keywords: information security, information system, risk management

I. INTRODUCTION

In recent years, most organization already use information technology for their activities. Information become vital part of organization. Almost everything in daily works involves the use of information [1]. Non-profit organization, such as Archdiocese of Jakarta is no exception. Archdiocese of Jakarta was founded in 1807 and have around 499.000 Catholic people under their supervision in 2016 [2]. To administrate these people accurately and support their needs, Archdiocese of Jakarta establish system called Basis Integrasi Data Umat Keuskupan (BIDUK) in 2015. BIDUK system is used as integrated information system which collect people's data for consolidation and to provide better services [3]. Accurate data is crucial for Archdiocese of Jakarta to make a decision. This data is obtained from a collection of data or reports submitted by the small church/parish which is located at the level of the subdistrict or kelurahan.

Manuscript published on November 30, 2019.
* Correspondence Author

Kristianto*, Master's degree student of Information Systems Department in Binus University
Natanael Alamas, Master's degree student, Information Systems Management Department in Binus, University.
Jarot S. Suroso, Senior lecturer, Information Systems Management Department in Binus University.

Catholic people's data in the BIDUK system until now has reached 96% of all and used to take policy and pastoral decision. Archdiocese of Jakarta as the leading sector that regulates the survival of Catholic has the responsibility to provide useful data services in planning Pastoral and social activities in the Archdiocese of Jakarta. Availablity of data and information are expected to serve as Pastoral intelligence. Data and information used as Pastoral intelligence is very useful in criticizing a decision, as guidance in decision making, make the interpretation of a phenomenon in detail and in depth as well as to alert and remind welfare issues of Catholic or society in general. To realize the Pastoral intelligence at the city level needed the integration of data and information from all the parish churches within the subdistrict so as not to have difficulties in obtaining complete, accurate, and short-term information. Based on previous explanation, a unified database in form of BIDUK System is needed to assist Archdiocese of Jakarta to provide social assistance for poor citizen and specifically provide complete and accurate information to develop a worthy and prosperous community life.

BIDUK system certainly faces many threats like any other information systems. For example, there are several attacks through internet that tries to access forcefully into BIDUK system. Another risk comes from external partners of Archdiocese. These partners want to have access into BIDUK system's data. These two examples proves that information inside BIDUK system need to be secured properly. Currently, any threats are handled case by case and there is no proper information security (IS) risk management yet for BIDUK system. Therefore, this study is performed to propose IS risk management method which can be adopted by BIDUK system.

This paper is organized as following: First section share about background of the study and the problems that want to be resolved. Second section explores related articles and researches which can be used to support the study. Third section inform about methodology used for the study. Fourth section share the results of the study. And fifth section will summarize the conclusion.

II. LITERATURE REVIEW

IS risk management is all activities to identify, analyze, and mitigate possible risks to reduce their negative impact [4]. The initial step to define IS risk management work is understanding organization view of business risks. Business risks can cause financial loss, reputational damage, and even harm to the customers [5].

IS risk management should not be viewed as merely legal necessity, because it can add values to define business strategy and help to make business decision [6]. IS risk management needs to be viewed as investment of business because its cost is pale compared to financial loss caused by the risks [7].

The importance of IS risk management in organization is increasing every year as the business growth because of the new technology applied [8].

There are various IS risk management methods which can be used organization, such as CRAMM, MEHARI, EBIOS, and OCTAVE [9]. These methods usually consists of some steps to identify risk, analyze risk, evaluate risk, mitigate risk, implement control, and re-evaluation [10]. Based on the use of historical data, IS risk management methods can be categorized into two: quantitative and qualitative. Qualitative methods is more preferable because they are easy to deploy and lower cost of implementation [11]. Study [12] focus on OCTAVE, one of qualitative method, which they found suitable for small team of IT and business people because of its simplicity. OCTAVE can be used to identify important organizational assets, and determine risks of those assets. It became one of the most popular IS risk management method [13]. There are other variant called OCTAVE Allegro. OCTAVE Allegro is more focused on information asset on how it is used, stored, and processed [14].

Several studies has been performed to explore IS risk management in organization. Study [15] explores IS risk management for some hospitals in Iran. They found that only eight hospitals have framework for IS risk management, but lacks in systematic approach. Study [16] proposes a quantitative IS risk assessment model for the digital environment of university. It consists of three phases: identify network weak point, measure risk level, and enhance the security. Study [17] proposes combination of socio-technical security requirements STS and risk analysis method CORAS. The method consists of two phases: modeling (social, asset, authorization, and threat model) and automated analysis. Study [18] use OCTAVE-S method on a construction company in Indonesia which consists of three phases: build asset-based threat profiles, identify infrastructure vulnerabilities, and develop security strategy and plans. Study [19] use OCTAVE Allegro method for debtor information system in a bank. This study conclude that OCTAVE Allegro can be used by banks to conduct a good IS risk management.

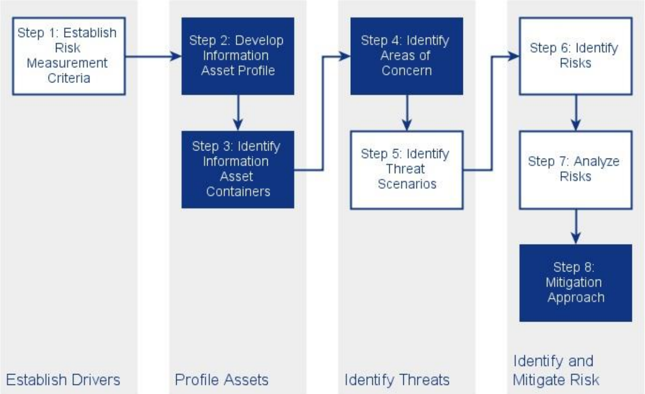
Step 1: Establish Risk Measurement Criteria
Step 2: Develop Information Asset Profile
Step 3: Identify Information Asset Containers
Step 4: Identify Areas of Concern
Step 5: Identify Threat Scenarios
Step 6: Identify Risks
Step 7: Analyze Risks
Step 8: Mitigation Approach
Establish Drivers
Profile Assets
Identify Threats
Identify and Mitigate Risk

Fig. 1. OCTAVE Allegro's steps [20]

III. METHODOLOGY

This study is performed by identifying, evaluating, and combining information from several other studies which relevant with the study's objective. First, we discuss about background of the study, which are: history and current condition of Archdiocese of Jakarta, BIDUK system used by them, and the problems of BIDUK system. Second, we review various literature to understand about IS risk management, such as: the functions, methods of IS risk management, examples of IS risk management implementation in several industries, and results of IS risk management in organization. After all information collected, we start creating the proposed IS risk management for BIDUK system using our preferred method.

IV. RESULTS AND DISCUSSION

A. Current Situation

BIDUK has several functions inside its system. User management function is used to maintain user id & profile, and control access rights. Master data management function is used to manage all master data such as church, liturgy, catechism, etc. Form management function is used by moderator of neighborhood to input their people's data. Message function is used to send message between BIDUK users. Dashboard function is used for data analytics and reporting.

Beside its function, the most important thing in BIDUK is the data. BIDUK system stores important and sensitive data about Church's people, such as their gender, date of birth, address, occupation, etc. Because these data are important, there are menu access restriction to secure this information. Parish's bishop is only given access to information about their own parish. Moderator of neighborhood is only given access when they must enter data. After their task is done, then the moderator of neighborhood's access is revoked.

Since its launch in 2015, BIDUK system has been used by six dioceses in Indonesia. Five more dioceses will join soon to adopt BIDUK system. They are currently in progress of building system infrastructure. In total there are 27 dioceses left in Indonesia which is not using BIDUK system yet.

We propose to use OCTAVE Allegro as IS risk management method for BIDUK system because it is simplified version of OCTAVE which is suitable for small organization. Additionally, OCTAVE itself is widely used IS risk management method in various industries. OCTAVE Allegro consists of eight steps which grouped into four phases. We will go through each step one by one.

B. Establish Drivers

First step is to establish risk measurement criteria. To do this step, we need to look the objective of BIDUK system. The objective is to establish integrated data management for all dioceses in Indonesia. By having integrated data management, information can be shared quickly and accurately even to the remote location. Based on this objective, we analyze that the highest priority impact area is safety and then lawsuits.

Table-I: Impact Area

Impact Area	Low	Moderate	High
Safety	Minimal impact to people's safety	People's safety is threatened. But they will recover after some period of time	People's safety is highly threatened, such as high financial loss, or losing lives
Lawsuits	People can make lawsuit less than 10 million IDR due to damage to them	People can make lawsuit between 10 million and 100 million IDR due to damage to them	People can make lawsuit more than 100 million IDR due to damage to them
Reputation	Minimal impact to reputation	Reputation is damaged. Need expense and effort to recover	Reputation is badly damaged
Investigation	No queries from government of other regulators	Government or other regulators conduct low profile investigation	Government or other regulators conduct high profile, in-depth investigation
One-time financial loss	One-time financial loss of less than 10 million IDR	One-time financial loss of 10 million to 100 million IDR	One-time financial loss greater than 100 million IDR

Table-II: Priority Scale of Impact Area

Priority	Impact Area
5	Safety
4	Lawsuit
3	Reputation
2	Investigation
1	One-time financial loss

C. Profile Assets

There are two steps in this phase: develop information asset profile and identify information asset containers. During develop information asset profile, we must identify information asset that is important and is often used in the system. If this information asset is lost then it will cause high impact to organization's objective.

Table-III: Information Asset Profile

Critical Asset	People's data
Rational	Catholic's people data is important asset for BIDUK system because it is used by Archdiocese for analytics and decision making
Description	People's data contains data such as: name, date of birth, gender, address, phone number, and identity number
Owner	Church/parish
Security Requirements	-Confidentiality: Each church/parish can only view people's data under their jurisdiction. -Confidentiality: Only authorized bishop of church/parish that have access to insert and view people's data. -Integrity: Bishop can't update data directly. It needs administrator permission.
Most Important Security Requirements	Confidentiality

Next step is to identify information asset container. That is consists of three types: people, technical, and physical. The container is described in following tables.

Table-IV: Information Asset Risk Environment (Technical)

Container Description	Owner(s)
Internal:	
BIDUK interface: People's data can be viewed through BIDUK system's interface	IT section
Database: People's data is stored in database server	IT section
External:	
Database's server: Database server is managed by vendor	Vendor

Table-V: Information Asset Risk Environment (Physical)

Container Description	Owner(s)
Internal:	
Form: People's data is filled in form which is given to bishop of the parish	Bishop
Report: Bishop can print report contain people's data	Bishop
External:	

Form: People's data is filled in form which is collected by moderator of neighborhood	Moderator of neighborhood

Table-VI: Information Asset Risk Environment (People)

Container Description	Department or Unit
Internal:	
Church/parish staff	Bishop
Archdiocese staff	Archdiocese
External:	
Regulator	Government

D. Identify Threats

There are two steps in this phase: identify area of concern and identify threat scenarios. Area of concern is any situation or condition that can affect information asset in the organization. Threat scenarios is expanded from area of concerns with addition of detailed information such as actor, means, motive and outcome. In actuality, we need to identify area of concern and threat scenarios for all information asset containers. Below table shows example of information asset risk worksheet already filled with area of concern and threat scenarios.

Table-VII: Area of Concern & Threat Scenario

Information Asset	BIDUK interface
Area of Concern	External partners want to be able to have access into BIDUK system and able to view people's data
Threat Properties	
Actor	External partners (bank, hospital, etc.)
Means	External partners can access BIDUK system from anywhere through internet
Motive	Want to gain benefit from using people's data
Outcome	Modification
Security Requirement	Restrict only limited information that can be shared to external partners

E. Identify and Mitigate Risks

In this phase, all possible threat scenarios from previous phase are further analyzed to understand about their impact for the organization. First thing to do, we need to give impact score for impact area from the first phase. We find that Safety is the highest impact area so it will have highest impact score. Below table lists impact score for all impact areas.

Table-VIII: Impact Score

Impact Area	Priority	Low	Medium	High
Safety	5	5	10	15
Lawsuits	4	4	8	12
Reputation	3	3	6	9
Investigation	2	2	4	6
One-time financial loss	1	1	2	3

After we have impact score ready, we start analyzing all possible threat scenarios into risks. Risks is defined by adding consequences and severity to threat scenarios in information asset risk worksheet. Consequences is what will happen to the organization as a result of outcome of threat scenario. Severity is the impact of consequences quantitated using impact score. Below table shows example of risk in the information asset risk worksheet.

Table-IX: Risk Analysis

Information Asset	BIDUK interface		
Area of Concern	External partners want to be able to have access into BIDUK system and able to view people's data		
Threat Properties			
Actor	External partners (bank, hospital, etc.)		
Means	External partners can access BIDUK system from anywhere through internet		
Motive	Want to gain benefit from using people's data		
Outcome	Modification		
Security Requirement	Restrict only limited information that can be shared to external partners		
Consequences	**Severity**		
If external partners have access to sensitive people's data, they can use that data to do some harm to those people financially, physically, or mentally	**Impact Area**	**Value**	**Score**
	Safety	High	15
	Lawsuits	Medium	8
	Reputation	Low	3
	Investigation	Medium	4
	One-time financial loss	Low	1
	Relative Risk Score	**31**	

All impact scores in Severity is calculated into relative risk score. Relative risk score will be used to determine risk mitigation. There are four action for risk mitigation, which are Accept, Defer, Mitigate, and Transfer. To help determine which risk mitigation, there is tool called relative risk matrix. This tool help to map relative risk score and probability to get risk mitigation. For example: area of concern "external partners want to have access to BIDUK system" have relative risk score = 31.

We predict the probability of this case is Medium. Using table below, we find that it mapped to Pool 2. The mitigation approach for Pool 2 is Mitigate/Defer.

Table-X: Relative Risk Matrix

	Risk Score		
Probability	**30 to 45**	**16 to 29**	**0 to 15**
High	Pool 1: Mitigate	Pool 2: Mitigate/Defer	Pool 2: Mitigate/Defer
Medium	Pool 2: Mitigate/Defer	Pool 2: Mitigate/Defer	Pool 3: Defer/Accept
Low	Pool 3: Defer/Accept	Pool 3: Defer/Accept	Pool 4: Accept

After we know which mitigation action to follow, we can create more detailed strategy to mitigate the risk. The mitigation strategy is created based on each related information asset container. Below is the example for

Table-XI: Mitigation Action

Area of Concern	External partners want to be able to have access into BIDUK system and able to view people's data
Action	Mitigate
Action for related containers	
Biduk interface	- Restrict user access permission for external partners - Hide sensitive people's data such as name, birth date, and ID number - Logging every action/menu accessed by external partners.

V. CONCLUSION

IS risk management is important thing to do in any organization. Information is vital for business's life being. Implementing information security should be considered as investment, because it can actually help organization save money from potential loss. Information security is also important in non-profit organization, such as Archdiocese of Jakarta. If the information that they have is not properly secured, it can be stolen or misused. BIDUK system, the central information of Archdiocese of Jakarta, must be secured due to its importance. Especially with current situation that risks can come anytime unexpectedly, any risks need to be properly managed. Through this study, we found that OCTAVE Allegro can be used to perform IS risk management properly for BIDUK system. OCTAVE Allegro is easy to understand and easy to do. This method cover most important aspects around BIDUK system, and not only touching technical aspect, but also physical and people aspects. Using this method, Archdiocese of Jakarta can prepare further security policy and procedure to manage critical information assets and mitigate risks that may happen in the future.

REFERENCES

1. J. Webb, S. Maynard, A. Ahmad, and G. Shanks, "Information Security Risk Management: An Intelligence-Driven Approach", Áustralasian Journal of Information Systems, Vol. 18, No. 3, 2014, pp. 391-404.
2. Catholic-Hierarchy, (2019, Oct 20). Archdiocese of Jakarta. Available: http://www.catholic-hierarchy.org/diocese/djaka.html
3. HidupKatolik, (2019, Oct 20). BIDUK Berbasis Web-Online. Available: https://majalah.hidupkatolik.com/2016/11/11/1888/biduk-berbasis-web-online/
4. A. Yan, and V. Sauter, "Risk Management in Information Systems Development in Distributed Environment", Proceedings of Nineteenth Americas Conference in Information Systems, 2013.
5. E.Y.Yildirim, "The Importance of Risk Management in Information Security", International Journal of Advances in Electronics and Computer Science, Vol. 4, No. 1, 2017, pp. 18-21.
6. Prof.Dr. Olaf Passenheim, "Enterprise Risk Management", 2010.
7. J. Boyce and D. Jennings, "Information Assurance: A Practical Guide". Butterworth-Heinemann, 2002.
8. 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, No. 1, 2013, pp. 45-52.
9. W. Abbass, A. Baina, and M. Bellafkih, "Improvement of Information System Security Risk Management", 4th IEEE International Colloquium on Information Science and Technology, 2016, pp. 182-187.
10. N. Mathur, H. Mathur, and T. Pandya, "Risk Management in Information System of Organisation: A Conceptual Framework", International Journal of Novel Research in Computer Science and Software Engineering, Vol. 2, No. 1, 2015, pp. 82-88.
11. U. Saluja, and Dr. N.B. Idris, "Information Risk Management: Qualitative or Quantitative? Cross Industry Lessons from Medical and Financial Fields", Systemics, Cybernetics and Informatics, Vol. 10, No. 3, 2012, pp. 54-59.
12. M.A. Khan, "Efficacy of OCTAVE Risk Assessment Methodology in Information Systems Organizations", International Journal of Computer Applications Technology and Research, Vol. 6, No. 6, 2017, pp. 242-244.
13. I. Sulistyowati, and R.V.H. Ginardi, "Information Security Risk Management with Octave Method and ISO/EIC 27001: 2013 (Case Study: Airlangga University)", The 4th International Seminar on Science and Technology, 2018, pp. 32-38.
14. Jarot. S. Suroso, and M.A. Fakhrozi, "Assessment of Information Security Risk Management with Octave Allegro at Education Institution", Procedia Computer Science, 135, 2018, pp. 202-213.
15. J. Zarei, and F. Sadoughi, "Information Security Risk Management for Computerized Health Information Systems in Hospitals: a case study of Iran", Risk Management and Healthcare Policy, 2016, pp. 75-85.
16. U.K. Singh, and C. Joshi, "Information Security Risk Management Framework for University Computing Environment", International Journal of Network Security, Vol. 19, No. 5, 2017, pp. 742-751.
17. S. Dashti, P. Giorgini, and E. Paja, "Information Security Risk Management", 2017.
18. B. Gunawan, Merry, and Nelly, "Information Technology Risk Assessment: Octave-S Approach", CommIT, Vol. 5, No. 1, 2011.
19. A. Januanto, D.Z. Febria, and Jarot. S. Suroso, "Risk Management of Debtor Information System (At Bank XYZ Using OCTAVE Allegro Method)", 2018.
20. 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 University, 2007.

AUTHORS PROFILE

Kristianto is Priest at Pejompongan's Parish. He is assigned by Archdiocese of Jakarta to study as master's degree student of Information Systems Department in Binus University.

Natanael Alamas is master's degree student of Information Systems Management Department in Binus University. After graduated from Binus University's Computer Science Department in 2011, he has been working in various multinational insurance companies. His current job is Business Analyst at Allianz Life.

Dr. Ir. Jarot S. Suroso, M.Eng is senior lecturer at Information Systems Management Department in Binus University. jsembodo@binus.edu