FRAMEWORK FOR COMMUNITY OF PRACTICE FOR BLOOD CENTER

K. S. Prasasti,
Telkom University,
Industrial Engineering Faculty
E-mail:kinanthisp@gmail.com

L. Andrawina,
Telkom University,
Industrial Engineering Faculty
E-mail:luciana@telkomuniversity.ac.id

A. F. Rizana,
Telkom University,
Industrial Engineering Faculty
E-mail:afrinfauzya@telkomuniversity.ac.id

ABSTRACT

Community of Practices plays many roles within the society. The interconnection of various entities in CoP enables the problem to be resolved and even anticipated. The Indonesian Red Cross, as an Institution, needs the support of many parties or entities in achieving its mission. Knowledge management will help to ensure the availability of knowledge in a timely and accurate manner so that it can be fully realized. This requires a continuous activity. Through each step in the knowledge management cycle, each entity in the community can contribute to collaborate and synergize by becoming a part of knowledge worker within the Community of Practices for blood donation center.

Key Words: *Community of practices, knowledge management cycle, knowledge worker* ***JEL Classification:*** *I18, I19*

1. INTRODUCTION

Knowledge plays important roles since it is regarded as a highly valuable asset that is sited in a community, an institution, or even both. According to Kusuma and Devie (2013), the faster and the more precise the availability of knowledge possessed by organization, the better the performance of the organization will be. Therefore, knowledge sharing that is connected in a network is necessary to obtain better organization performance. Making connections through networking is one of important component in building social capital since connectivity between entities makes knowledge becomes more meaningful (Lesser and Storck, 2001). Knowledge possessed by community member can be in the form of expertise and experience. When knowledge is connected with other community entities, it would be helpful to solve problems or create new ideas so that problems can proactively be prevented before even exist.

One of the problems expected to be solved through the utilization of knowledge is humanity problem. One of problem regarding humanity that still exists in big cities is the availability of blood needed by hospitals for transfusing purposes which may result the condition that causes human victims, such as accidents or disasters. That problem might occur in big city in Indonesia including Bandung city. The city of Bandung is considered as a city that quite prone to natural disasters. Bandung has 2.490.662 population, 40 units of hospital, 75 units of community health centers, a local government effort to establish social security administer program—under the authority of department of health, and also Indonesian Red Cross. The role of Indonesian Red Cross is to assist the government in social humanity, especially handling tasks as they are required in the provisions of the Geneva Conventions of 1949. These provisions have been ratified by the government of Republic of Indonesia in 1958 through Law No. 59. Moreover, There is a National SAR Department—a

nongovernmental institution in which the Indonesian ministries is in charge of carrying out government duties in search and rescue. National SAR Department has a role in dealing with cruise and aviation calamity, as well as other disasters that are related to search and rescue effort. Handling of the calamity in question includes 2 main things which are search and rescue. The main task of the Department of Health is to execute some regional government affairs in health sector based on the regulation and principal of autonomy and assistance.

The problem of blood supply is critical to be solved since it could become a fatal thing for one's life. This makes a proactive engagement of all entities in a comprehensive way is important. The process of educating to encourage a humanitarian empathy, donation time, communication system, distribution, the involvement of personal or community to donate blood is important in order to prevent the unavailability of blood stock. Community of Practices in the field of health, especially in Bandung, is needed to improve the performance of the following entities namely, The Indonesian Red Cross, The National SAR Department, hospitals, Department of Health. A harmonious and solid interconnection between entities will affect the performance so that it has a high value.

Community of Practices is a group whose members regularly engage in sharing and learning, based on their common interests (Lesser and Storck, 2001). There are several communities in Bandung (can be categorized as NGO, student council, and University) such as '*Aleut*' Community, '*Aksara Kuna Nusantara*' Community, '*Reptil Bandung*' Community, *Bandung Liteter* Community, student council from across 136 Senior High School and 158 Universities. This group can be considered as potential resource for PMI. Empowerment needs to be done by linking these informal entities with existing formal entities (hospital, Red Cross Indonesia, and National SAR Department)

According to Lin (2007), knowledge sharing is an activity of transferring or disseminating knowledge from a person, group or organization to another person, group, or organization. Knowledge sharing can be interpreted as a way to live up CoP activity, with the existence of knowledge worker in every entity. The existence of knowledge worker becomes absolute. Knowledge worker is an individual who has a level of education and special abilities combined with skills in identifying and solving problems (Drucker, 1993). Every community and institution has knowledge workers who play a role in identifying and solving problems. Based on the number of communities and hospitals in Bandung as well as the roles of Indonesian Red Cross, National SAR Department, and Department of health, the health sector in Bandung needs to have a framework to ensure knowledge management cycle has been implemented well. This framework is created by the SECI method that can be used as a guide for implementing knowledge management. Knowledge management itself has a purpose for organizations. To be able to achieve business value, there must be a group of people who have a role in ensuring the existing cycle in KM cycle work.

2. LITERATURE REVIEW

2.1 KNOWLEDGE

Knowledge cannot be interpreted as knowledge alone, instead, it is a complex thing. Knowledge is a function of particular perspectives, goals, or positions held by individuals, and therefore different from information, knowledge relating to beliefs and commitments (Nonaka and Takeuchi, 1995). Knowledge is a combination of experience, value, contextual information, expert views and intuition that provides an environment and framework for evaluating new experiences and information (Tiwana, 1999).

Based on the opinions of some experts, it can be concluded that knowledge is a combination of data, information, and experience that can be used to improve the performance of an organization by evaluating experiences, decision-making tools, and learning tools. Knowledge is closely related to data and information that a person has to be able to express an opinion and a policy.

2.2 KNOWLEDGE MANAGEMENT

Knowledge management plays a role in the process of managing and maintaining the knowledge used for decision-making processes and learning tools. Knowledge management is also an important part that an organization has because the effective use of knowledge management of assets and knowledge is able to assist organizations in innovating and responding to changing desires of customers (Dachler and Sandhawalia, 2010).

Organizations often find it difficult to get sufficient information to support the decisionmaking process so that it impacts the policies taken by the organization. Steps that organization must take in managing information and employee skills are a big challenge. Knowledge management has a share in creating added value for the organization by giving a big influence on employee performance. Documenting knowledge as a means of learning and decision making has a significant impact on organization performance.

2.3 KNOWLEDGE MANAGEMENT CYCLE

Knowledge Management Cycle (KMC) is a process that forms a spiral and gets bigger when knowledge is being managed from time to time (Parikh, 2001). The continuous process can broadly be divided into 4 parts, namely knowledge acquisition, knowledge organization, knowledge dissemination, knowledge application. The research undertaken by Evans, Dalkir, and Bidian (2014) has largely covered the overall development of KMC that starts from a non-sequential cycle into successive cycles and has feedback loops. Figure 1 shows KMC based on research conducted by Evans, Dalkir, and Bidian (2014).

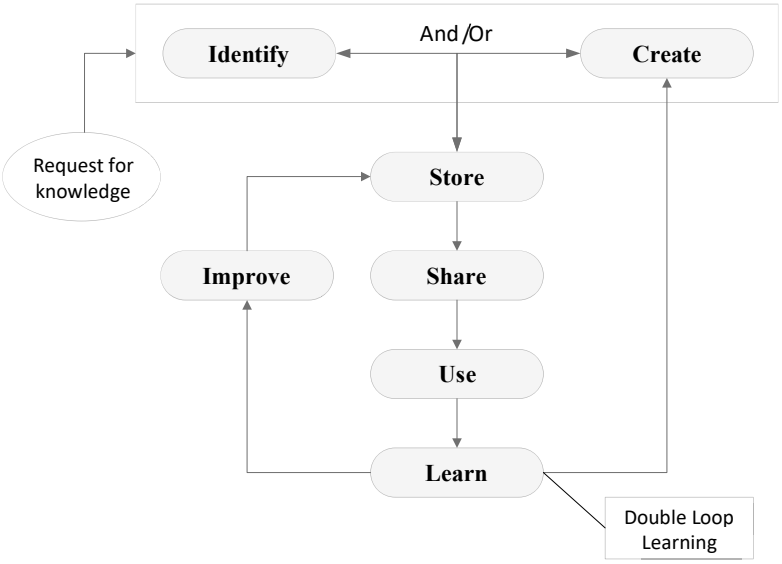

Fig 1. Knowledge Management Cycle Model (Source: Evans, Dalkir, and Bidian, 2014)

The KMC stage of Evans, Dalkir, and Bidian (2014) accommodates continuous improvement. KMC consists of 7 stages of identifying, creating, store, share, use, learn, and improve. The nature of the cycle is sequential and cyclical. This KMS model is sufficient to represent the KMC stage. However, there are two stages that are non-existent which are knowledge acquisition and knowledge retrieval. Knowledge acquisition is defined as a process for capturing or acquiring knowledge to add value to previous knowledge (Kurniawati, Samadhi, & Wiratmadja, 2016). Knowledge retrieval is defined as a process for managing, classifying, storing, positioning knowledge that has been obtained and can be accessed to optimize knowledge organization (Kurniawati, Samadhi, & Wiratmadja, 2016).

2.4 SECI

The SECI method is one of the methods of Knowledge Conversion that can be used to transform Tacit Knowledge into Explicit Knowledge or vice versa. SECI consists of several processes namely Socialization, Externalization, Combination, and Internalization. The following is a SECI cycle process developed by Nonaka and Takeuchi (1995).

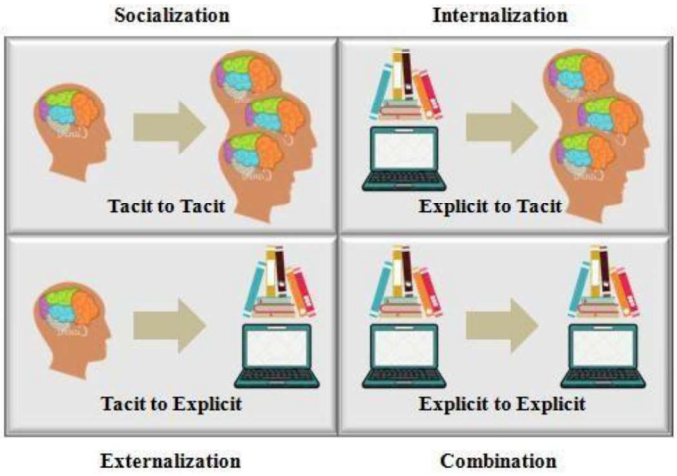

Fig 2. SECI Model (Source: Nonaka and Takeuchi, 1995)

Based on Figure 2 there are 4 knowledge conversion processes which are: Socialization, Externalization, Combination, and Internalization. Socialization is the process of converting knowledge from tacit knowledge to tacit knowledge. The process of knowledge sharing that happens in socialization is the experience or knowledge (tacit knowledge) owned by someone that is being distributed to others through socialization such as discussions, seminars, and interviews. Externalization is the process of converting knowledge from tacit knowledge to explicit knowledge. In externalization documentation of tacit knowledge that has been obtained from the process of socialization happens. Combination is the process of converting knowledge from explicit knowledge to new explicit knowledge. Combination is the process of collecting, uniting, and integrating the knowledge of each individual into the knowledge system (Nonaka, 1995). Internalization is the process of converting knowledge from explicit knowledge to tacit knowledge. In the internalization, the distribution of new knowledge to people happens.

2.5 COMMUNITY OF PRACTICE

Community of Practice (CoP) is a community of people who share a common desire for what they do and interact regularly to learn together in order to help their work (Wenger, 2004). This community is growing significantly because the transfer of knowledge between one individual and the other is considered to be effective in solving complex problems in their work. Through the existence of Community of Practice, the process of knowledge transfer can occur easily and impact the emergence of a number of benefits from the knowledge transfer process and allows entities in an organization to maximize the assets of the organization in order to have a positive impact on the development of the organization.

3. METHODOLOGY

3.1 RESEARCH QUESTIONS

Every community and institution has knowledge workers who play a role in identifying and solving problems. The problems that often arise in the field of humanity and health is the unavailability of blood bags in the hospital when patients seem to need them most. This can be caused by the lack of knowledge worker or there is no interaction between knowledge worker from an entity to another

entity in spreading knowledge and knowledge management cycle that is not implemented. Whereas utilizing the interaction between existing entities can be a way to prevent this from happening. This research has main objective that is to design a framework that can be used as a guide for implementing knowledge management. As indicated in the introduction, we have three major research questions. The first research question is how to encourage interaction between knowledge workers from an entity to another entity in spreading knowledge. The second one is how to make knowledge management cycle well implemented, and the last question is how is the framework to ensure knowledge management cycle has been implemented well.

3.2 RESEARCH MODEL

Figure 3 illustrates the illustration of this research regarding how to make entities in CoP connected to each other through the PIC of each entity to make the knowledge has a bigger meaning by using the concept of KM cycle and KM SECI. The entities are consist of Indonesian Red Cross, NGO, Hospital, National SAR Department, Department of Health, and University. PIC of University is Ministry of Research, Technology, and Higher Education of

Republic Indonesia, PIC of Department of Health is Ministry of Health of Republic of Indonesia, PIC of National SAR Department is Ministry of Transportation of Republic of Indonesia, PIC of Indonesian Red Cross is International Federation of Red Cross and RedCrescent Societies, PIC of Hospital is Hospital Association Indonesia, and PIC of NGO is Local Government.

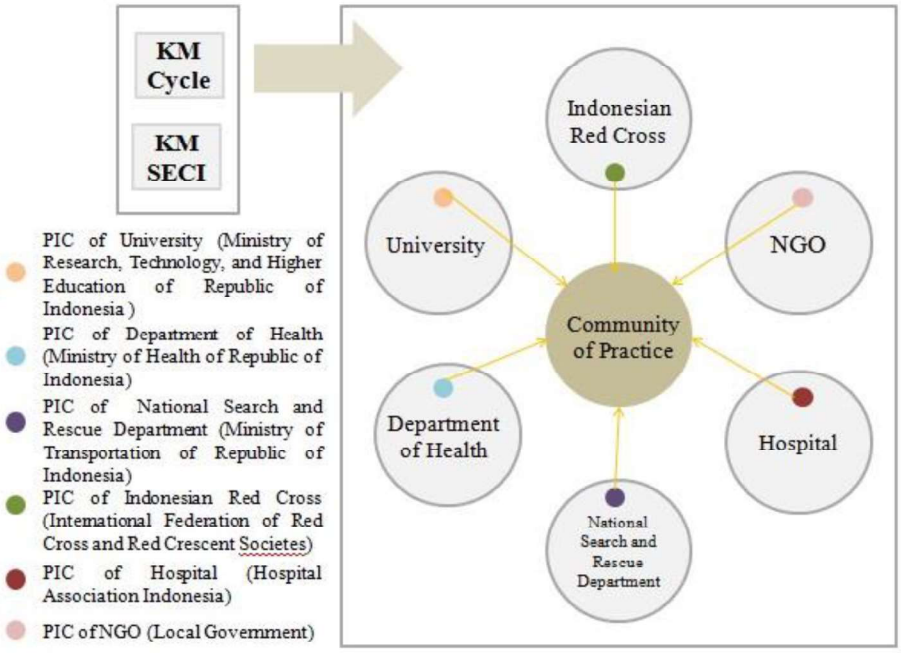

Fig 3. Conceptual Model

4. RESULTS AND DISCUSSION

A new community consists of various entities that require governance in order to streamline the collaboration of work. Table II shows the interaction between KM cycles and KM role. According to Dalkir (2005), KM roles are composed by several categories which are:

- Senior and middle management roles–Chief Knowledge Officer, Knowledge Manager
- Knowledge leaders, also reffered to as KM champions, who are responsible for promoting KM within the organization
- Knowledge managers, responsible for the acquisition and management of internal and external knowledge
- Knowledge navigators, responsible for knowing where knowledge can be located, also called knowledge brokers
- Knowledge synthesizer, responsible for facilitating the recording of significant knowledge to organizational memory, also called knowledge stewards
- Content editors, responsible for codifying and structuring content, also called content managers; roles involving capturing and capturing and documenting knowledge–researchers, writers, editors
- Web developers, electronic publishers, intranet managers, content managers
- Learning-oriented roles such as trainers, facilitators, mentors, and coaches–including those with responsibility for developing information and knowledge skills
- Human resources roles with specific responsibility for developing programs and processes that encourage knowledge-oriented cultures and behaviors
- Knowledge publishers, responsible for internal publishing functions, usually on an intranet, also called Webmasters, knowledge architects, and knowledge editors
- Coaches and mentors, responsible for assisting individuals throughout the business unit or practice to develop and learn KM activities and diciplines
- Help desk activities, including the delivery of KM and information related to training, also called KSO (Knowledge Support Office)

Table I. Interaction Between KM Cycle and KM Role

Step	Category	Entity
Identify	Knowledge Leader	Department of Health (West Java)
		Indonesian Red Cross
		National Search and Rescue Department
		Hospital
Create	Knowledge Manager	Indonesian Red Cross
Store	Knowledge Navigator Knowledge Synthesizer Electronic Publisher	IT Expert

Share	Content Editors Managing Web Developers	Department of Health (West Java)
		Indonesian Red Cross
		National Search and Rescue Department
		Hospital
Use	Facilitators PIC	School
		University
		NGO/CoP
Learn Improvement	Mentors	Knowledge Worker or Knowledge Evaluator

Table 1 shows the interaction between KM cycle and KM role according to Dalkir (2005). In Knowledge Leader category there are several entities like Department of Health (West Java), Indonesian Red Cross, National Search and Rescue Department, and Hospital. Knowledge

Manager category has one entity that is Indonesian Red Cross. Knowledge Navigator, Knowledge Synthesizer, and Electronic Publisher are in one category and have one entity that is IT Expert. Content Editors Managing and Web Developers are in one category and have several entities like Department of Health (West Java), Indonesian Red Cross, National Search and Rescue Department, and Hospital. Facilitators and PIC are in one category and have several entities like School, University, and NGO or CoP. And the last category is Mentors which has one entity that is Knowledge Worker or Knowledge Evaluator. The interconnection of various entities in CoP enables the blood center in the future easier to get information from all entities and all the problems to be resolved and even anticipated.

5. CONCLUSIONS AND RECOMMENDATIONS

The research provides a CoP framework for various entities formally or informally in The City of Bandung. The application of KM roles can make knowledge workers interact with each other in spreading knowledge of blood center. Blood center has several entities there are University, Indonesian Red Cross, NGO, Hospital, National Search and Rescue Department, and Department of Health. Each entity has a Person In Charge that will join in a Community of Parctice. This condition indicates that KM roles and KM cycle are well implemented. The combination of KM roles and KM cycles that are well implemented can create a framework for community of practice for blood centers which can be seen in Table I. The framework consists of KM Cycle steps, KM Roles roles, and entities from each step and category. All entities have their own roles and support each other's roles.

Further research will be focused on identifying or recognizing the characteristics of each community to get detailed description of each knowledge worker that should exist in each step of the knowledge management cycle. Furthermore, research be done by exploring every existing entity to build a Community of Practices scheme in the ease of access to data, information, and knowledge especially related to humanitarian concern.

References

Dalkir, K. (2005). *Knowledge Management in Theory and Practice*. London: The MIT Press.

Dalkir, K., Bidian, C. & Evans, M. (2014) A Holistic View of the Knowledge Life Cycle: the

Knowledge Management Cycle (KMC) Mode. *The Electronic Journal of Knowledge Management*. p. 85-97.

Drucker, P. F. (1993) Knowledge Worker Productivity: The Bisggest Challenge. *California Management Review*. p. 79-94.

Kusuma, F.S.D., & Devie. (2013) Analyzing the role of knowledge management towards organization's competitive advantage and performance [Analisa Pengaruh Knowledge Management Terhadap Keunggulan Bersaing dan Kinerja Perusahaan]. *Business Accounting Review*. Vol. 1. No. 2.

Lin H. (2007) Knowledge Sharing and Firm Innovation Capability. *International Journal of Manpower*. p. 315-332.

Parikh, M. (2001) Knowledge Management Framework for High-Tech Research and Development. *Engineering Management Journal*. p. 27-34.

Rice, J. L. & Rice, B. S. (2005) The applicability of the SECI model to multi-organisational endeavours: an integrative review. *International Journal of Organisational Behaviour*. Vol. 9, No. 8. p. 671-682.

Samadhi, T., Wiratmadja, I. & Kurniawati, A. (2016) Indicators of Knowledge Management Cycle in Small and Medium Enterprises. *2016 IEEE International Conference on Management of Innovation and Technology (ICMIT)*. p. 198-202.

Sandhawalia, B. S. & Dalcher, D. (2010) Developing Knowledge Management Capabilities: A Structured Approach. *Journal of Knowledge Management*. p. 313-328.

Soesanto, R. P., Samadhi, T. A., Wiratmadja, I. I., Sunaryo, I. & Kurniawati, A. (2017) Development of Knowledge Management Cycle Model: A Literature Review. *SNTI and SATELIT*. p. F28-33.

Storck, J. & Lesser E. L. (2001) Communities of Practice and Organizational Performance. *IBM Systems Journal*. p. 831-841.

Takeuchi, H. & Nonaka, I. (1995) The Knowledge-Creating Organization. *Oxford University Press*. p. 70-73.

Tiwana, A. (1999). *The Knowledge Management Toolkit*. Chicago: Prentice Hall PTR.

Wenger, E. (2004). *Cultivating Communities of Practice.* Boston: Harvard Business Press.

RISK-MANAGEMENT BASED GOVERNMENT INFORMATION SYSTEM SECURITY USING OCTAVE ALLEGRO FRAMEWORK

Surya Tri Atmaja Ramadhani,
Gadjah Mada University,
Departement of Electrical Engineering and Information Technology, Yogyakarta, Indonesia.
E-mail: surya.tri.atmaja.cio15@mail.ugm.ac.id

Rudy Hartanto,
Gadjah Mada University,
Departement of Electrical Engineering and Information Technology, Yogyakarta, Indonesia.
E-mail: rudy@ugm.ac.id

Eko Nugroho,
Gadjah Mada University,
Departement of Electrical Engineering and Information Technology, Yogyakarta, Indonesia.
E-mail: nugroho@ugm.ac.id

ABSTRACT

Maintaining information security by protecting confidential and sensitive electronic information assets from unauthorized access, misuse, disclosure, destruction, and modification. Kulonprogo Regency Government needs the protection of its information assets, which mostly manage confidential information services for the purpose of implementing e-government. This research implements OCTAVE Allegro framework to perform a risk assessment on information assets supporting information technology services at Kulonprogo Regency Government. The end result is the policy recommended by this study can lead the organization to consider Human resources and information technology services used.

Key Words: *Information Services, Risk Assessment, OCTAVE Allegro, Information Security*

JEL Classification*: G32, D81, G32*

1. INTRODUCTION

Information technology is no longer viewed as a separate tool from organizational tools, but is already considered one of the resources that have an equally important role with other resources such as finance, assets, and human resources(Kurniawan, 2012). Today many organizations have used information technology as a means to serve their business processes. The nature of information technology that is easily accessible and used is the main reason some organizations choose it to support their business processes.

Information is an important asset for organizations in their information technology services(Supradono, 2009b), this information security cannot be based solely on information security tools or technologies, but rather an understanding of the organization about what should be protected and determine the

exact solution that can address the problem of what information security needs(Alberts C. J., Behrens, S. G., Pethia, R. D. & Wilson, 1999). Therefore, information security must be well managed and structured.

Information security cannot only rely on tools or technologies, but it requires awareness in organizations on what needs to be protected and correct selection of solutions to deal with problems in information security needs. For this, a systematic and comprehensive information security management is essential. The need for information security must contain 3 important elements: confidentiality, integrity, and availability(Supradono, 2009b).

This research will observe information security based on application services in one of the government agencies. This study focused on the identification, analysis and risk assessment of Information Security based on application services at Kulonprogo Regency Government using OCTAVE Allegro method.

Kulonprogo regency government was chosen as the object of this study based on the regulation of Regent of Kulonprogo number 65 year 2012 about the implementation of risk management to local government that pursuant to the provision of Article 13 paragraph (1) Government Regulation Number 60 Year 2008 concerning Government Internal Control System, The Leader of Government Institution must conduct risk assessment of the application of information technology today as one of the supporting elements of the vision and mission of the organization, as well as the number of vulnerabilities present in its information security system. Such vulnerabilities include the risk of attacks on critical information assets related to local and online networks as a consequence of utilizing information technology. There is also the risk of theft and fire hazard to their physical assets because their electronic equipment is vulnerable to fire hazards due to the excess of unattended voltages; so they need surveillance cameras, heat sensors, fire extinguishers, and outdoor water sprayers, especially inside server rooms that store information assets.

From these observations, the initial conclusion is that the Kulonprogo Regency Government has not implemented an optimal information security policy and risk assessment on its critical information assets. To conduct a risk assessment, terms of reference are required. The OCTAVE method stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation. The methods used are: confidentiality, integrity, availability. OCTAVE Allegro is a development of the OCTAVE method to evaluate information security risks that are comprehensive, systematic, directed, and self-directed(Farida, 2015). Keating (Keating, 2014) states the OCTAVE Allegro risk assessment method created by the Carnegie Mellon University Software Engineering Institute (SEI) has the ability to deliver robust risk assessment results, with relatively small investment in time and resources, even for organizations which do not have extensive risk management skills.

Information technology services Kulonprogo Regency Government is provided by the Communications and Informations Departments which fulfills its needs relies on information systems on each service that contains information assets. To know the process of applying the information security risk management of this Communications and Informations Departments, it is necessary to investigate how far the implementation of risk management of information system using OCTAVE Allegro method in Kulonprogo Regency Government. The results of this study are constructive recommendations to be used as a basis for decision-making in protecting government information security as well as its information assets.

2. LITERATURE REVIEW

2.1 Previous Researches

In 2009, B. Supradono(Supradono, 2009a) use first version of OCTAVE that has been developed by Software Engineering Institute, Carnegie Mellon University to evaluate information security risks that are comprehensive, systematic, directed, and self-directed. His approach is organized into a set of criteria that define the essential elements of an information security risk assessment. As a result, the OCTAVE Method provides a systemic and comprehensive guidance on information security risk management. This method further emphasizes the risk-based management of threats and vulnerabilities to organizational information assets including hardware, software, systems, information and people.

In 2015, Rosini Rachmaniah et al. (Rosini, Rachmaniah and Mustafa, 2015), assessed the risk of information vulnerability by using OCTAVE Allegro method against X library. OCTAVE method stands for Operationally Critical Threat, Asset, and Vulnerability Evaluation. The OCTAVE method performs risk assessment based on three basic principles of security administration, namely: confidentiality, integrity, availability. From the results of this risk assessment, what can be done is reducing or eliminating the risk (mitigate) as much as 21 areas of concern, transferring risk or mitigate as much as 16 areas of concern, defer the risk as much as 12 areas of concern, and accept the risk or delaying as much as 3 areas of concern.

2.2 Risk Management

An information system asset is anything of value an organisation needs to utilise in order to accomplish its mission (Klinger, 2009). An asset can either be tangible or intangible (Theoharidou et al., 2005). Tangible assets include software, hardware and data while intangible assets include reputation, operations, trust and morale (Theoharidou et al., 2005). Information systems assets can be critical or non-critical depending on the importance of the operations each asset is supporting(Fallis, 2013), and these vary from organisation to organisation (Theoharidou et al., 2005). Information systems assets can be at risk, compromising information integrity, confidentiality and availability. A risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the asset (Klinger, 2009). In this regard, a risk is the potential for an unwanted event to occur and is a function of the likelihood of that unwanted event occurring and its consequences(Fallis, 2013). A risk arises from three conditions called risk factors (contextual problems), namely the existence of a threat (hazard), exposure of an asset to that threat and the vulnerability of the asset(Fallis, 2013). A threat is a natural or man- made occurrence, individual, entity, or action that has or indicates the potential to harm information, operations, the environment, and/or property(Karabacak and Sogukpinar, 2005). The existence of a threat implies that there exists the capability and intention of an adversary to undertake actions that could be detrimental to an organisation’s interests(Karabacak and Sogukpinar, 2005). An information security exposure may be a system configuration issue, mistake in software or a problem according to some reasonable security policy that allows access to information or capabilities that can be used by an attacker as a stepping stone into the system or network(Rainer, Snyder and Carr, 1991). Vulnerability is a combination of the attractiveness of a facility as a target and the level of deterrence and (or) protection provided by the existing countermeasures(Fallis, 2013). Therefore, vulnerability is the degree to which the exposed elements of an information system will suffer a loss from the impact of a threat. All assets are exposed to some degree of risks which the owners of assets may be unaware of.

Risk management is a basic management activity that helps an organisation to meet its objectives through the allocation of resources to undertake planning, make decisions, and carry out productive activities(Fallis, 2013). Risk management differs from other management activities because it deals with uncertainties that an organisation faces. The uncertainties include the occurrence of harmful events and the value to the organisation of consequences of such events(Fallis, 2013).

The two major activities of risk management are risk assessment and analysis(Karabacak and Sogukpinar, 2005). Risk assessment is the process of identifying, characterising, and understanding risk; that is, studying, analysing, and describing the set of outcomes and likelihoods for a given endeavor(Shortreed, Hicks and Craig, 2003). Risk analysis involves further identification of security risks, determining their magnitude and identifying the corresponding areas that need safeguards (Klinger, 2009).

2.3 OCTAVE Allegro

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) define the critical components in a comprehensive, systematic, context-driven manner of information security risk evaluation. Using the OCTAVE method, organizations can create risk-based information protection based on CIA (Confidentiality, Integrity, Authentication) for critical information technology assets(Jakaria and Informatika, 2013). OCTAVE is a methodology for identifying and evaluating information systems security risks. The use of OCTAVE is intended to assist organizations in the areas of (a) Developing qualitative risk evaluation criteria that describe the operational risk tolerance of an organization; (b) Identify key assets to achieve the organization's mission; (c) Identify the vulnerability and threats to the asset; (d) Determine and evaluate to deal with the consequences that occur in the organization if such threats occur(Jakaria and Informatika, 2013).

The OCTAVE method has three variants: OCTAVE, OCTAVE-S and OCTAVE Allegro. OCTAVE is a suite of tools, techniques, and methods for the assessment and planning of risk-based information systems security. OCTAVE Allegro is a simplified method with a focus on information assets. OCTAVE Allegro can be done with workshop-style and collaborative methods. OCTAVE Allegro consists of eight steps divided into four phases (Caralli et al., 2007).

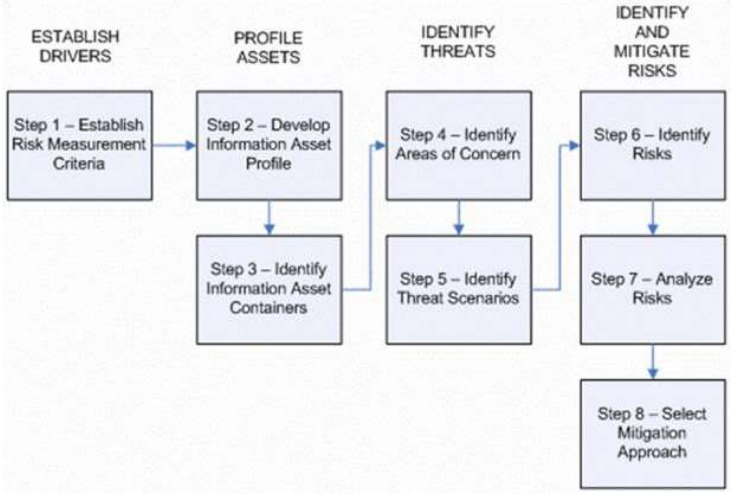

Figure 1 OCTAVE Allegro phases

3. METHODOLOGY

This study attempts to describe the results of the study of each stage adopted from the OCTAVE Allegro method in assessing potential vulnerabilities in Kulonprogo Regency Government through the Communications and Informations Departments. This research was conducted in accordance with the Figure 2 below.

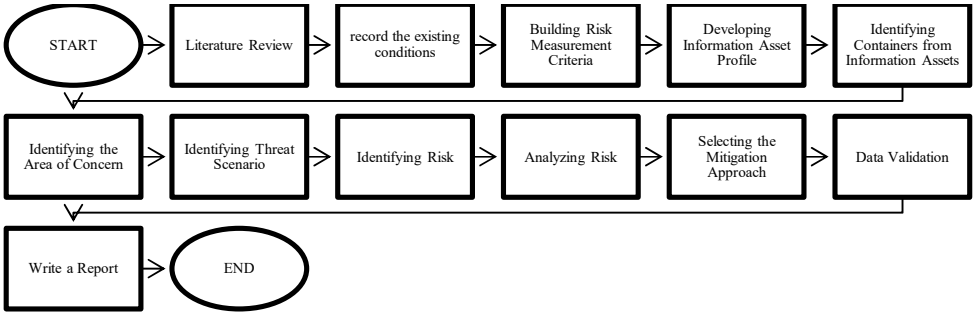

Figure 2 Research methodology

The measures taken in this research are mentioned below:

Literature Review

This measure was performed by reading and studying papers related to this research. The objective of this measure was to seek for references and also understanding the stages in risk management evaluation and implementation of OCTAVE Allegro.

Record The Existing Conditions

This measure was performed by discussion with the Head of Department KOMINFO to determine the condition of current IT services that have been done, the data can be obtained by interviewing and studying documents related to applicable policies. In addition, it is also necessary to know about the current state of information security IT governance in the Office KOMINFO. After this phase will proceed with collecting all data related IT services based on information security with OCTAVE Allegro method.

Building Risk Measurement Criteria

Beginning with building organizational drivers used to evaluate the impact of risk on mission and business objectives, as well as identifying the most important impact areas. There are two activities, Activity one is to create a qualitative size definition that is documented in the Risk Measurement Criteria Worksheets. Activity two performs the priority assignment of the impact area using Impact Area Ranking Worksheet.

Developing Information Asset Profile

Identification of information asset then doing a structured risk assessment to the critical asset. This activity is collecting information on critical information asset then continued by making documentation of the reasons for the selection of critical information assets. This stage make the description of critical information asset then identify the ownership of the critical information assets, fills security needs for confidentiality, integrity, and availability, and identifies the most important security needs for information assets.

Identifying Containers from Information Assets

There is only one activity in step three, note three important points related to the security and concept of the information asset container that is how the information assets are protected, the level of protection or the safeguard of information assets and the vulnerability as well as threats to the container of the information assets.

Identifying the Area of Concern

This measure begins with developing a risk profile of information assets by exchanging ideas to locate threat components from situations that may threaten information assets. By referring to Information Asset Risk Environment Maps and Information Asset Risk Worksheet documents then the area of concern can be recorded. Guided by the Information Asset Risk Worksheet document do a review of the container to create an Area of Concern and document every Area of Concern.

Identifying Threat Scenario

In this step, this documented areas of concern that could affect Thisr information asset. Area of concern are expanded into threat scenarios that further detail the properties of threat. To expand areas of concern into threat scenarios, This must first understand the basic components of a threat.

Identifying Risk

Activity in this step is to determining the documented threat scenario in the Information Asset Risk Worksheet so it can have an impact on the organization. This determine how the threat scenarios that This have recorded on each Information Asset Risk Worksheet could impact This organization.

Analyzing Risk

This activity should be referring to the documentation contained in the Information Asset Risk Worksheet. Activity one begins by reviewing the risk measurement criteria followed by the second activity by calculating the relative risk value that can be used to analyze the risk and decide the best strategy for dealing with risk.

Selecting the Mitigation Approach

Activity one in step eight is to sort every risk that has been identified based on the value of the risk. This is done to assist in the decision making of risk mitigation status. Activity two takes a mitigation approach for each risk based on conditions unique to the organization.

Validating Data

At this stage the validation/checking of the documentation of interviews and workshops is performed in information security risk management using OCTAVE Allegro. Checks are intended to determine whether the data obtained from interviews and workshops is complete and in accordance with OCTAVE Allegro framework or not.

Write a Report

The last stage is research report writing. At this stage the conclusions are drawn based on the results of research that has been done. The recommendations proposed based on research results are described at this stage.

4. RESULTS AND DISCUSSION

Prior to initiating risk assessment, researchers have contacted key persons associated with risk management at the KOMINFO Office of Kulonprogo District. These individuals are: department head, staff in the IT division, and head of the administration division. These people are contacted to get the required data. The next step is to conduct interviews to obtain information about existing conditions and operational assets that are considered important for the organization. Data is presented in the appendix.

In this research we use the method of interview and data collection as well as the prevailing policy. Data collection is based on the OCTAVE Allegro Process Assessment Model by following the guidelines on activities to determine the level of ability. This survey is used to determine the level of risk management capability with a question form.

The team of analysts performs initial identification with current security practices. From the result, it is found that Kulonprogo Regency did not have awareness to operational practices / standard operating procedure (SOP) in maintaining documented security. While the results of the evaluation of current security practices are still focused on technical factors that are undocumented and focused on authentication: i.e., user and password to log on access to information systems, there is no firewall, encryption, IDS / IPS (intrusion detection system / intrusion protection system) and manageable switch device.

Identification of areas of concern has been obtained by reviewing each container to see and determine potential areas of concern. Areas of concern are extended to get a threat scenarios and then documented to see if they affect security requirements. Areas of Concern obtained are listed in Table I below:

Table I Areas of Concern

No	Area of Concern
1	A Leak of access password transaction information service by the operator who have access.
2	Easy access to the server room can lead to unauthorized access to the server.
3	Security holes in management information system portals can be exploited by outsiders.
4	Halt of service occurs when the power outages because it does not have backup power to the server room.

Based on the results of the existing data collection we distribute, we can obtain and analyze the risks that exist in the information security of the district government of kulonprogo by calculating the level of capability in the form of Relative Risk Score for each area of concern based on the governance / management practices and the resulting output.

OCTAVE Allegro has focused on risk management related of information security within the organization. This information security is related to the business process that runs in Kulonprogo District Government. Summary of achievement of relative risk score based on area of concern for OCLAVE Allegro Framework can be seen in Table I.

Table II Summary of Risk Analysis Assessment

Area of Concern	**Risk**			
A Leak of access password transaction information service by the operator who have access	Consequences	Halt of services due to irresponsible parties may unauthorized access to application services.		
	Severity	Impact Area	Value	Score
		Reputation and customer trust	Moderate	8
		Financial	Low	3
		Productivity	Moderate	4
		Security and Health	High	15
		Fine and Penalty	Low	1
		Relative Risk Score		31

The calculation result of relative risk score is obtained from calculating the score of each concern of area mentioned in the above table. In the case of a leak of access password transaction information service by the operator who have access, have value relative risk score 31, therefore need to do Mitigation.

Based on the results of the assessment, The mitigation approach is how Communications and Informations Department will decide to address its risks. OCTAVE Allegro provides a selection of mitigations that can be selected: accept, mitigate, and defer. Table III shows an grouping mitigation steps based on Relative Risk Matrix, in table IV is a grouping of mitigation steps, table V is an risk mitigation by area of concern.

Table III Relative Risk Matrix

Risk Score		
30 to 45	16 to 29	0 to 15
Pool 1	Pool 2	Pool 3

Table IV Mitigation Approach

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

Table V Mitigation by Area of Concern

Risk Mitigation	
Area of Concern	A Leak of access password transaction information service by the operator who have access

Action	Mitigate
Container	Control
Database Module information service	Using encryption, digital certificates, web secure / SSL / https when going to web portal login application.
Application Operator and Communications and Informations Department (KOMINFO)	Good Password Management: (Changes every 30/60/90 days, made minimum standard of characters and unique for password, admin using password generator, prohibits use of admin login as login demo etc).

5. CONCLUSIONS AND RECOMMENDATIONS

This study has produced an analysis of the risks that can occur in the Information Service database system within the server which consists of applications used by SKPD. Applying OCTAVE Allegro method has resulted in impact system mapping with the result of Mitigation Approach for Information Service database system in the server at pool 1 that is mitigated. These results can recommend top-level management to change the work patterns of service operators to further raise awareness of data confidentiality.

The study offers the following recommendations :

Security Awareness and Training. Safety concerns and training are conducted periodically. Understanding of staff documented and compliance with documents that have been made periodically verified.

Security Strategy. Create a master plan / strategic plan for security development and risk management of information security and conduct a security audit once every year.

Security Management. Kominfo Pemkab Kulonprogo establishes policies and appropriate procedures to prevent, detect and identify risks to the confidentiality, integrity and availability of information services.

Security Policies and Regulations. Kulonprogo regency should have process documents for evaluation and ensuring compliance with information security policies, laws and rules and insurance requirements and Establish uniform rules of enforcement on security policies.

REFERENCES

Alberts C. J., Behrens, S. G., Pethia, R. D. & Wilson, W. R. (1999) 'Operationally Critical Threat, Asset, and Vulnerability Evaluations (OCTAVE(SM)) Framework, Version 1.0. Carnegie Mellon Software Engineering Institute', (June). Available at: http://www.sei.cmu.edu/publications/pubweb.html.

Caralli, R. a R. a. C. et al. (2007) 'Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process', Young, (May), pp. 1–113.

Fallis, A. . (2013) 'Information Security Risk Management in Small- Scale Organisations: A Case Study of Secondary Schools Computerised Information Systems', Journal of Chemical Information and Modeling, 53(9), pp. 1689–1699. doi: 10.1017/CBO9781107415324.004.

Farida, U. (2015) 'Penerapan manajemen risiko sistem informasi perpustakaan uin sunan kalijaga yogyakarta', p. 356337.

Jakaria, D. A. and Informatika, J. T. (2013) 'Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro', pp. 37–42.

Karabacak, B. and Sogukpinar, I. (2005) 'ISRAM: Information security risk analysis method', Computers and Security, 24(2), pp. 147–159. doi: 10.1016/j.cose.2004.07.004.

Keating, C. G. (2014) 'Validating the OCTAVE Allegro Information Systems Risk Assessment Methodology : A Case Study by', (192).

Klinger, K. (2009) Encyclopedia of Multimedia Technology and Networking, Second Edition. doi: 10.4018/978-1-60566-014-1.

Kurniawan, J. (2012) PENGEMBANGAN SISTEM EVALUASI KINERJA GURU BERDASARKAN KOMPETENSI : Studi Kasus SMK 45 Kota Bima. Universitas Gadjah Mada.

Rainer, R. K., Snyder, C. A. and Carr, H. H. (1991) 'Risk Analysis for Information Technology', Journal of Management Information Systems. Routledge, 8(1), pp. 129–147. doi: 10.1080/07421222.1991.11517914.

Rosini, Rachmaniah, M. and Mustafa, B. (2015) 'Penilaian Risiko Kerawanan Informasi Dengan Menggunakan Metode OCTAVE Allegro', Jurnal Pustakawan Indonesia, 14(1), pp. 14–22.

Shortreed, J., Hicks, J. and Craig, L. (2003) 'Basic Framework for Risk Management - Final Report'. Available at: http://www.sobanebrasil.org/adm/fotos/6bad672342f38b0776512b211433a994.pdf.

Supradono, B. (2009a) 'Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode Octave (Operationally Critical Threat , Asset , and Vulnerability Evaluation)', 2(1), pp. 4–8.

Supradono, B. (2009b) 'PENERAPAN FRAMEWORK OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION) UNTUK MANAJEMEN RESIKO KEAMANAN INFORMASI DI INSTITUSI PERGURUAN TINGGI DALAM MENDUKUNG KEBERLANJUTAN PROSES BISNIS (Studi Kasus : Kemanan Informasi Proses Bi'.

Theoharidou, M. et al. (2005) 'The insider threat to information systems and the effectiveness of ISO17799', Computers and Security, 24(6), pp. 472–484. doi: 10.1016/j.cose.2005.05.002.