E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 04, Desember 2022 : 1058 - 1167

ANALYSIS OF RELIGIOUS COURT INFORMATION SECURITY RISK MANAGEMENT USING THE OCTAVE ALLEGRO METHOD (CASE STUDY OF KEDIRI CITY)

Cintya Risquna Miendarki [1)] , Rahmat Yasirandi [2)] , dan Rio Guntur Utomo [3)]
[1, 2, 3)] Program Studies Technology Information , Faculty Informatics , Telkom University
Jl. Telecommunications No. 1, Sukapura , Kec. Dayeuhkolot , Bandung Regency , West Java 40257
e-mail: cintyarisquna@student.telkomuniversity.ac.id [1)] , batanganhitam@telkomuniversity.ac.id [2)] , riogunturutomo@telkomuniversity.ac.id [3)]

ABSTRAK

Kemudahan akses dapat menjadi pro dan kontra bagi semua orang aplikasi sistem informasi, karena meningkatkan kemungkinan seseorang meretas sistem informasi tersebut. Oleh karena itu, penilaian risiko atau penilaian risiko sistem informasi diperlukan untuk mengidentifikasi dan memahami risiko yang terlibat dalam mengaksesnya. Salah satu metode penilaian risiko yang menganalisis profil risiko aset informasi menggunakan metode OCTAVE Allegro. Tujuan dari penelitian ini adalah untuk mengetahui hasil analisis manajemen risiko keamanan pada sistem informasi di Pengadilan Agama Kota Kediri. Proses rekomendasi adalah tindak lanjut dari penilaian risiko berupa kontrol pada ISO/IEC 27002:2013 yang berfokus pada klausul 9. Access Control. Penelitian ini menggunakan pendekatan studi literatur. Tinjauan pustaka dilakukan dengan mencari referensi analisis manajemen risiko keamanan informasi menggunakan metode OCTAVE Allegro, buku bahan penelitian dan jurnal dari penelitian untuk membantu penyusunan penelitian ini usul. Teori yang diambil dari referensi terutama mengacu pada metode OCTAVE Allegro. Berdasarkan hasil penelitian yang dilakukan maka peneliti mendapatkan 10 area perhatian yang akan diberikan rekomendasi kontrol berdasarkan ISO/IEC 27002:2013.

***Kata Kunci**: Octave, keamanan sistem, manajemen risiko, Octave Allegro, ISO/IEC 27002:2013, Kontrol Akses, Risiko*

ABSTRACT

Ease of access can be pros and cons for all information system applications, because it increases the possibility of someone hacking the information system. Therefore, a risk assessment or risk assessment of information systems is needed to identify and understand the risks involved in accessing them. One of the risk assessment methods that analyzes the risk profile of information assets using the OCTAVE Allegro method. The purpose of this study was to determine the results of the analysis of security risk management on information systems at the Religious Courts of the City of Kediri. The recommendation process is a follow-up to the risk assessment in the form of controls in ISO/IEC 27002:2013 which focuses on clause 9. Access Control. This research uses a literature study approach. The literature review was carried out by looking for references to information security risk management analysis using the OCTAVE Allegro method, research material books and research journals to assist in the preparation of this research proposal. The theory taken from the reference mainly refers to the OCTAVE Allegro method. Based on the results of the research conducted, the researchers got 10 areas of attention that will be given control recommendations based on ISO/IEC 27002:2013.

***Keywords** : Octave, system security, risk management, Octave Allegro, ISO/IEC 27002:2013, Access Control, Risk*

I. INTRODUCTION

THE application of information and communication technology (ICT) management has become a need and demand for every public service provider and the role of ICT is important in improving service quality as one of the benefits of *Good Corporate Governance*. The management of information and communication technology (ICT) has now become a necessity for all government agencies in Indonesia in order to realize *Good Corporate Governance*. ICT management must be supported by information security in order to maintain the *confidentiality*, *integrity*, and availability *of* information against all threats that will endanger the continuity of the organization's performance, especially the application of ICT within the scope of government [1].

The Indonesian government has issued policies related to information security management systems through Minister of Communication and Informatics Regulation No. 4 of 2016 which regulates the Information Security Management System for electronic system operators consisting of state administration institutions, corporations, independent institutions and other legal entities engaged in the realm of public services based on the principle of risk. This regulation also stipulates that the operator of the electronic system that implements the strategic electronic

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 04, Desember 2022 : 1058 - 1167

system must immediately be certified to SNI ISO/IEC 27001. Likewise, the operator that implements the high level electronic system must also immediately implement the standard of SNI ISO/IEC 27001 [2].

The Kediri City Religious Court is a government agency whose services are to fulfill service needs for the community, especially for justice seekers. The Kediri City Religious Court uses an integrated information system to run its business processes, but the Kediri City Religious Court has never carried out risk measurements on its information security and has not implemented risk management to minimize future risks. g. One of the first steps that religious courts can take to balance the impact of risk and cost needed to minimize this risk is to take measures to measure information technology risk (*risk value*).

The Religious Courts in the City of Kediri as one of the Indonesian government agencies are asked to provide the best service to parties who need information, such as employees or other parties. Therefore, religious courts have a special department that serves information management systems and related services. In this case, information becomes an important asset because the information it carries, in addition to confidentiality, risks of unauthorized access, data theft, data theft, human error, hardware and software damage, and the risk of natural disasters [3].

In this study, the method that will be used to assess and analyze risk in information technology is the use of OCTAVE (*Operational Critical Threat, Assets and Vulnerability Evaluation*) Allegro, because compared to other methods the main focus of *OCTAVE Allegro* is on information assets and data that support information.. So the usefulness of this method is how the information is used and how the information is stored, transported, processed, the disruption caused and what the situation will be if exposed to a threat. *Octave Allegro* is suitable for use by individuals who wish to conduct assessments without extensive organizational involvement, expertise, or input [4]. The purpose of this research is to identify and manage *Octave Allegro information system security risk factors*. Furthermore, this study also makes recommendations based on the results of risk assessment using controls in SNI ISO/IEC 27002:2013. The results of the information security risk management analysis of the Religious Courts of the community can be used as guidelines for IT risk mitigation and ISMS implementation.

II. METHODOLOGY

Methodology Study this used for give clear direction and what to do done. Methodology study could seen in Figure 1 below this :

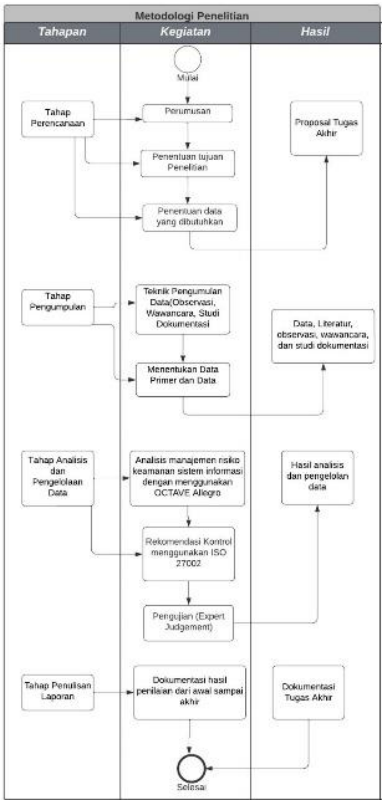

Figure 1.Methodology Study

A. Setting Criteria Measurement Risk

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 04, Desember 2022 : 1058 - 1167

the first step there are 2 activities that is activity first set *organizational drivers* who will used for evaluate effect risk to mission and goals business organization. *organizational drivers* this reflected in a set of criteria measurement risks created and captured _ as part from step beginning this.

Activity two that is make definition criteria measurement risk is set size qualitative with which effect from realized risk _ could evaluated and become base evaluation risk asset information.

B. Develop Profile Asset Information

In Step 2 start the creation process profile for asset information organization. Profile is representation from asset information that describes its unique features , qualities , characteristics and values. Manufacturing process profile methodology ensure that asset explained with clear and consistent , that there is clear definition _ about limit assets , and that requirements security for asset defined by adequate.

C. Identify Receptacle Asset Information

In Step 3 method *OCTAVE Allegro* , everyone receptacle the place asset stored , transported , and processed , both internally and external , identified. In step this , author map asset information to all container , so that define limitations and circumstances must be unique checked the risk.

D. Identify Problem Areas

In Step 4, start the identification process risk with To do *brainstorm* about possibility condition or situations that can threaten asset information organization. With based on documents *information asset risk environment maps* and *information asset risk worksheet* then could noted an *area of 26 concerns.* Based on the document *information asset risk worksheet* do *review* from container for make *area of concern* and document every *areas of concern*.

E. Identify Scenario Threat

Activity one in step five that is To do identification scenario threat addition to activity this could use *appendix c-threat scenarios* questionnaires. Activity two complete *information asset risk worksheets* for any common threat scenarios.

F. Identify Risk

Activity one on step six determine *threat scenarios* that have been documented in the *information asset risk worksheet* could impact for organization.

G. Analysis Risk

In Step 7, start with a review of risk measurement criteria, followed by with counting activities score risk relative that can used for analyze risk and decide the best strategy for resolve risk.

H. Choose Approach Mitigation

In Step 8, step final of the *OCTAVE Allegro process* , organization determine which risks have they identification need mitigation and develop mitigation strategies for risk that. This thing achieved with more formerly prioritize risk based on score risk relative. After risk prioritized , mitigation strategies developed taking into account score assets and requirements safety , container the place asset the being , and the environment operation unique organization.

III. DESIGN

A. Design Studies Case

Subject in study could in the form of individual , group, agency nor society. In the research process , there is a number of steps are made , namely , determine problem , choose design and appropriate instruments , collect data, analyze the data obtained and prepare report results research. Final result from study is something broad and deep picture _ root something phenomenon certain. There is three category studies cases , namely :

1. Studies case exploration (digging)

   Studies case exploration is To do exploration to phenomenon whatever in working data as the place destination for researcher.

2. Studies case descriptive

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 04, Desember 2022 : 1058 - 1167

Studies case descriptive is used for describe phenomenon naturally occurring in the data.

3. Studies case *explanatory* (clarifying)

Studies case *explanatory* (clarifying) is used for explain phenomenon in the data directly clear start from Thing base until depth [8].

Category the study used in processing Duty end this is exploration or excavation. from statement formula problem show that studies case required for destination this. Studies case is for get phenomena that occur and function as base for analysis risk.

B.Subject and Object Study

Study this carried out at the Religious Court of the City of Kediri which is one of the service public related society and technology information. The object to be researched is a service process public based _ technology information managed by the Religious Court of the City of Kediri. Service public based _ technology information will produce document system management security information use method *OCTAVE Allegro* for extracting critical assets and identifying risk. because of that , Service public based technology information in insta the will Becomes more good from previously [9]. For To do study this , author get help from party agency the religious court of the city of Kediri , especially the institutional division computer which is source person main in the process of excavation needs.

C.Design Device Data Mining

In part this is design from device data mining about state organization moment this so that can is known description general based public service technology information in the religious court of the city of Kediri. Data you want to know among others:

1. Asset information owned agency
2. Service public k related technology information managed by the agency.
3. Management security inside information agency

D. Data Mining

Data mining carried out as part from Duty end conducted with using interview technique. Interview conducted on base *interview protocol.* In data mining has 2 stages that is interviews and observations. In writing Duty end this , author using a semi- structured interview technique. This thing because writer use instrument or device however moment interview , writer no only focus on the device. The upcoming interview conducted addressed to resource person who understands about service process public related technology information. For Observation required for obtain data in the form of related documents _ with technology information nor facilities and infra-structure [7]. In every observation , data obtained researcher related with two the important thing , namely information (eg how method researching , appropriate or no the tools used and what happens and the connection (things related around it) [7].

E. Determination Approach Analysis

In study this required method analysis for knowing connection between the processed data. Study this aim for analyze risk on technology information on the agency the religious court of the city of Kediri, get level vulnerability information , and generate recommendation for increase security information on technology information agency the with use eight step in method *OCTAVE Allegro*. *OCTAVE Allegro* make profile asset information important organization , run analysis risk to assets , and define mitigation strategies for every identified risks [4]. So that help organization in analyze risk as well as determine the right strategy for face risk.

IV. RESULTS AND ANALYSIS

This stage explains the implementation of each stage and process process in the research methodology which can be in the form of results, implementation time and related attachments that contain certain records with the implementation of the process. The *OCTAVE Allegro method* consists of eight steps divided into four phases,

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 04, Desember 2022 : 1058 - 1167

namely phase 1 (*establish drivers*), phase 2 (*profile assets*), phase 3 (*identity threads)* phase 4 (*identify and mitigate risks*) [4].

A. Phase 1 (Establish Drivers)

In the first step in the *OCTAVE process Allegro* establishes risk measurement criteria that will be used to evaluate the effect of risk on the organization's mission and business objectives. Risk measurement criteria form the basis for asset risk assessment information and identify the most significant impact areas. In Table I shows score priority on impact areas

TABLE I
IMPACT PRIORITY WORK

Allegro Worksheet 7	Score	Areas of Impact
Priority		Impact Areas
1	5	User Reputation and Trust
2	4	Finance
3	3	Productivity
4	2	Safety and health
5	1	Fines and Penalties

B. Phase 2 (Profile Assets)

In this step using *worksheet 8,* this process when developing an information asset profile is needed to define threats and risks to any assets in the Kediri City Religious Court. This asset is determined and takes into account all aspects of the existing asset risk. At this stage, it is carried out to find out what information assets are the most important in the agency and to know what security requirements must be done by the agency so that the information assets are safe. Could seen in table II explains about profile asset information

TABLE II
PROFILE ASSET INFORMATION

AllegroWorksheet 8	CRITICAL INFORMATION ASSET PROFILE	
Critical Asset What is the critical information asset?	Rationale for Selection Why is this information asset important to the organization?	Description What is the agreed-upon description of this information asset?
Civil Case Information System	Contains information about case cases which are updated every time	Information Center needed by every employee and the public
Cable Phone	Communication tool used for the community with employees or employees with employees. Not all employees in the agency have access rights to operate these tools.	Hardware that is used as a communication liaison between employees and the community or employees and employees
Attendance System	Data that contains information about recording employee attendance related to employee performance, calculating employee salaries and minimizing the occurrence of fraud between employees	Agencies can monitor employee productivity from the number of employee attendance.
CCTV	Data that contains information on existing activities in the agency, overseeing employee performance, and maintaining agency assets	Increase security by preventing crime and criminal acts or acts

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 04, Desember 2022 : 1058 - 1167

	Owner(s)	
	Computer Setup	
	Security Requirements	
	What are the security requirements for this information asset?	
Confidentiality	Information is private and can only be accessed by users and admins	Only computer administration employees can access this asset
Integrity	This information must be filled out correctly, accurately, and always updated so that it can only be filled in or changed by the admin or computer system	Only authorized personnel can correct or change information
Availability	Information must always be available to every user	This asset must be available 24 hours, 7 days/week, 52 weeks/year

Stages Identify Containers in table III of asset information explain about identification of information assets based on the place where information assets are stored, transmitted, and processed both internally and externally external [4]. Identify the information asset container using *Worksheet 9* , namely the *Information Asset Risk Environment Map.*

TABLE III
CONTAINER ASSET INFORMATION

Allegro Worksheet 9c	**ENVIRONMENTAL MAP OF RISK INFORMATION ASSET (PEOPLE)**
In	
Name or Role/ Responsibilities	**Department or Unit**
Computer Administration Staff	Computer Setup
civil servant	Computer Setup
Outside	
Vendor	**Organization/Vendor**
PKL (Practice Work field)	Educational Institutions

C. *Phase 3 (Identity Threads)*

At this stage it is used to describe activities in identifying *areas of concern* based on system use. Identify *areas of concern* by reviewing each *container* to see and select potential *areas of concern* and determine by documenting each *area of concern* which already identified [4]. Identify *areas of concern* in terms of *technical* (TC), *physical* (PS) and *people* (PO). In table IV explains about stages from *areas of concern.*

TABLE IV.
AREAS OF ATTENTION

No	Areas of Attention	Code	Related Assets
1.	Unknowingly, a ransomware application was installed, making a local server used to sync case data to the civil case information system website, the Kediri City Religious Court.	TC,PS ,PO	Web server, database server, Laptop or computer, street vendors
2.	Criminal data processing causes a lot of data input errors by the computer system (*Human* or *Technician error*).	PO	Permanent Employees or PKL Students
3.	Data changed by unauthorized employees	TC & PS	Web Server, Database Server Computer or Laptop, Telephone

On step next use *worksheet 10 information asset risk* then makes the areas that can affect information assets for each container specified in the previous step become more detailed by re-creating the areas that became attention and add *threat properties* for explain threat. This step can be seen in table V.

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 04, Desember 2022 : 1058 - 1167

TABLE V
IDENTIFY SCENARIO THREAT

No.	*Areas of Attention*	*Threat Scenarios*		
1.	Unwittingly, the ransomware application was installed, making a local server used to sync SIPP data to the Kediri City Religious Court website.	1.	*Actors*	Internal staff/users/Bag. Computer Setup
		2.	*Means*	Installing applications that can damage the Information System
		3.	*Motives*	*Human error*
		4.	*Outcome*	*destruction,*
		5.	*Security Requirements*	Perform data backups, evaluate the Civil Case Information System and provide counseling on security awareness to employees who have authority
2.	Criminal data processing causes a lot of data input errors by the computer system (*Human* or *Technician error*).	1.	*Actors*	Internal Staff
		2.	*Means*	Mistakes in case input when there is a special program
		3.	*Motives*	Accidental
		4.	*Outcome*	*Modification*
		5.	*Security Requirements*	Verify before carrying out the case *upload process.*
3.	Data changed by unauthorized employees	1.	*Actors*	Internal
		2.	*Means*	Employees misuse information
		3.	*Motives*	*Malicious*
		4.	*Outcome*	*Modification*
		5.	*Security Requirements*	An increase in security is needed for each information system

D. Phase 4 (Identify and Mitigate Risks)

This phase has 3 steps, namely identifying risks, analyzing risks and choosing a mitigation approach. In the risk identification step , what is done is to determine the impact based on the threat scenario that occurs. Where each scenario that has been formed must determine the impact or consequences that may be caused when the threat occurs. Risk identification aims to determine how the threat scenario give impact or consequence for agency and choose the level. That thing described in table VI as following :

TABLE VI
IMPACT AREA VALUE

Impact Area	**Priority**	**Impact Value**			**Score**
		Low (nL =(1))	Medium (nL =(2))	Height (nL=3))	
Employee Reputation and Trust	1	5	10	15	5
Finance	2	4	8	12	4
Productivity	3	3	6	9	3
Employee Health and Safety	4	2	4	6	2
Fines and Penalties	5	1	2	3	1

Steps to analyze risk it performs risk analysis can identify and calculate risks using consider how to reduce the probability of failure and use consider what are the consequences from risk influence agency. Stages from step analyze could seen in table VII as following :

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 04, Desember 2022 : 1058 - 1167

TABLE VII.
RISK VALUE RELATIVELY

No	Areas of Attention		Risk		
1.	Unknowingly, the ransomware application was installed, making the local server used to sync the SIPP data to the Kediri City Religious Court website,	***Consequences***	Disruption of employee activities resulted in a decrease in the SIPP value of the Kediri City Religious Court which made the agency's performance value decrease.		
		Severity	**Affected Area**	**Score**	**Score**
			Reputation/Customer Confidence	Tall	15
			Financial	Low	4
			Productivity	Tall	9
			Safety and Health	Low	2
			Fines/Legal	Low	1
		Relative Risk Score			31
2.	Criminal data processing causes a lot of data input errors by the computer system (*Human* or *Technician error*).	***Consequences***	It takes additional time to replace the wrong case data		
		Severity	**Affected Area**	**Score**	**Score**
			Reputation/Customer Confidence	Low	5
			Financial	Low	4
			Productivity	Tall	9
			Safety and Health	Low	2
			Fines/Legal	Low	1
		Relative Risk Score			21
3.	Data changed by unauthorized parties	***Consequences***	Employee activities are disrupted or delayed because they need additional time to replace them		
		Severity	**Affected Area**	**Score**	**Score**
			Reputation/Customer Confidence	Tall	15
			Financial	Low	4
			Productivity	Tall	9
			Safety and Health	Low	2
			Fines/Legal	Low	1
		Relative Risk Score			31

On step final determine mitigation approach there are four POOLs in this mitigation approach that are suitable for each impact area based on the table on based on Relatively Risk Matrix from every risk. In table VIII shows that results identification and analysis Risk from all *areas of concern*.

TABLE VIII.
IDENTIFICATION AND ANALYSIS RESULTS RISK FROM ALL AREAS OF CONCERN

No	Areas of Attention	Probability	Risk Score (Impact)	Pool	Mitigation Approach
1.	Unknowingly, the ransomware application was installed, making the local server used to sync the SIPP data to the Kediri City Religious Court website,	Tall	31	POOL 1	*Mitigate*
2.	Criminal data processing causes a lot of data input errors by the computer system (*Human* or *Technician error*).	Currently	21	POOL 2	*Mitigate*
3.	Data changed by unauthorized parties	Tall	31	POOL 1	*Mitigate*

E-ISSN : 2540 - 8984

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Volume 07, Nomor 04, Desember 2022 : 1058 - 1167

E. Recommendation Control

After conducting a risk assessment and mitigating, the next step is to provide control over the risk. Determination of control recommendations on aspects of *people, process,* and *technology.* At *OCTAVE Allegro* does not have a guide in controlling risk. So in this section, control recommendations are developed for areas of concern in POOL 1 and POOL 2. Control recommendations are a form of mitigation of potential analyzed risk _ _ _ use standard ISO/IEC 27002:2013[10]. Recommendation control on the area of attention can be seen in table IX as following :

TABLE IX.
RECOMMENDATION CONTROL

No	Areas of Attention	Identification			Reference
		People	***Process***	***Technology***	
1.	Unwittingly, the ransomware application was installed, making the local server used to sync SIPP data to the Kediri City Religious Court website	Added Policy to provide education on *awareness* , provide action to those who violate information security	Addition of Policy regarding information security breaches for employees who violate		Implementing Controls A.7 Human Resources Security
2.	Criminal data processing causes a lot of data input errors by the computer system (*Human* or *Technician error*).	Addition of Policy to provide education on *awareness*, provide action to those who violate information security	Addition of Policy regarding information security breaches for employees who violate		Implementing Controls A.7 Human Resources Security
3.	Data changed by unauthorized parties		Added protection policy to the *database*, testing the data *backup* in accordance with the specified policy.	Added policies regarding running a *backup policy* , performing regular *backups* , *performing a test restore backup files*, and data retention.	Implementing A.9 *Access Controls* and A.12 Operation Security controls

V. CONCLUSION

From the results of the analysis of potential risks at the Religious Courts of the City of Kediri, a risk profile with 10 areas of concern was obtained , namely:

1. Without aware installed the ransomware application makes a local server that is used for synchronizing Civil Case Information System data to the Kediri City Religious Court *website.*
2. Criminal data processing cause a lot of data input errors by the part of the computer system (*Human* or *Technician error*).
3. Data is changed by unauthorized parties.
4. The use of the information system by other employees or does not have the authority in access rights.
5. *Bugs* or *errors* contained in the Criminal Case Information System.
6. System security can be exploited by outside parties or *hacker attacks.*
7. Errors caused by unforeseen events (lightning, short circuit, or fire)
8. *Servers down.*
9. Error detecting in attendance system
10. Error in system monitoring based CCTV.

In approach mitigation risk using the proposed recommendations to make improvements to controls. The following are the recommended guidelines for Standard Operating Procedures based on ISO / IEC 27002:2013:

1. People : Adding job descriptions, authorities, and competencies to the project and asset divisions
2. Process : A proposal is made in the form of a policy on Standard Operating Procedures and procedures based on the findings obtained at the Religious Court of the City of Kediri.

3. Technology : Perform periodic *backups* , *perform test restore backup files,* data retention and accept permitted user access rights.

Suggestions that can be writer give for study next namely :

1. The need for analyzing and conducting broader research is not only in the division of computer systems regarding information security risks.
2. With the improvement of the risk management system in the organization, it is hoped that in the future there will be no problems in the legal, financial, historical and administrative fields.

REFERENCES

[1] BSN, H. (2017, April 11). Information Security in the Digital Age. Retrieved from Bsn : https://bsn.go.id/main/berita/detail/8331/keamanan-information-dalam-era-digital
[2] daon001. (2016, March 31). Information Security Awareness is Still Weak. Retrieved from Kominfo: https://kominfo.go.id/content/detail/7190/kesadaran-keamanan-nasionalmasih-lemah/0/berita_satker
[3] Information, TD (2011). Guidelines for the Implementation of Information Security Governance for Public Service Providers. Directorate of Information Security, Ministry of Communication and Informatics, RI.
[4] Caralli, RA (2007, May). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. US: Carnegie Mellon University.
[5] Peltier, Thomas E. (2005). *Information Security Risk Analysis (2nd ed.).* Boca Raton, FL., USA: CRC Press, Taylor & Francis Group. Peltier, Thomas E. (2005). *Information Security Risk Analysis (2nd ed.).* Boca Raton, FL., USA: CRC Press, Taylor & Francis Group.
[6] Hughes, G. 2006. *Five Steps to IT Risk Management Best Practices. Risk Management* , Vol 53, Issue 7. 34.
[7] YK R, "Case Study Research Design and Methods Second Edition," International Educational and Professional Publisher, vol. 5.
[8] Z. Z, Case Study As A Research Method," J. Kemanus , Number 9, 2007
[9] KK d. I. RI, Implementation Guide KIPPP Governance , Jakarta, 2011
[10] ISO/IEC:27002, Information Technology - Security Techniques, Geneva, 2013.