Risk Analysis of IT Applications Using FMEA and AHP SAW Method With COBIT 5

Amrina Friska Apriliana¹, Riyanarto Sarno², Yutika Amelia Effendi³ ¹Department of Information Technology Management, ^{2,3}Department of Informatics Institut Teknologi Sepuluh Nopember Surabaya, Indonesia

e-mail: apriliana.17092@mhs.its.ac.id, riyanarto@if.its.ac.id, yutika.effendi@gmail.com

Abstract—Nowadays, the rapid technological developments have impact in several aspects, including the development of technology in government companies, such as PT. PLN Persero. PT. PLN Persero - East Java Distribution is one of the government companies which is supported by the role of technology to help their business processes implementation. To improve the quality of information technology which is known as Operational Technology, Support, Strategic, High Potential can be done by using the technology continuously. But continuous usage can provide potential threats that can impact risks during implementation. Therefore, a company needs to pay attention to risk management. Risk management is an important element in running a business because the company is growing and the complexity of corporate activities in it. The main objective of the implementation of risk management is to anticipate the hazards that can occur within the company, especially in the application of technology and can bring losses to the company. This research propose the method to analyze the risk Analysis using FMEA and AHP SAW Methods with COBIT 5. The results of this study shows the most affect the course of business processes.

Keywords—Risk mitigation; AHP SAW; FMEA; COBIT 5

I. INTRODUCTION

The development of information technology gives its own impact to several aspects and sectors in daily activities [1]. It also includes the rapid technological developments in providing services for the public, one of them PT. PLN Persero. PT. PLN Persero - East Java Distribution located in Surabaya, is a central electricity supply and management company for East Java. For daily business processes, the company is supported by the role of technology to help maintenance of their business processes implementation in order to achieve the effectiveness and efficiency. So that business process activities in PT. PLN Persero can not be separated from technology support for information transmission that integrates company performance.

As the main support, technology also has value. Both the importance and the added value that affect the company's business processes [2]. Value in the field of Information technology is one of them included in the application of technology for the provision of network or network for business processes company. The technology for network providers is the implementation of IT Network network technology that has been implemented for more than 20 years.

During the implementation of IT network technology implementation will produce an impact for the company, especially in terms of information transmission [3]. As we know that Information and Communication Technology serves as the Key of Operations, Support, Strategic, High Potential. So this technology is useful to support internal business process activities. In addition, as an effort to maintain the existence of the company in providing electricity management services to the community.

However, continuous use in the implementation of IT network implementation may also pose a potential threat that may cause risks during implementation [4]. Risk is the positive or negative influence of uncertainty about a goal. Risks can come from uncertainty, uncertainty of standard operating procedures, or lack of care. It is therefore necessary to identify potential risk analysis as a form of anticipation or mitigation with risk management process.

Risk management as one of the important elements in running the company's business processes due to the development of the corporate world and the increasing complexity of the company's activities resulted in an increased level of risk facing the company. The main purpose of the implementation of risk management is to protect the company especially in the application of IT network technology against the possibility of loss [5]. So, this research will be discussed about risk management by balancing between business strategy and risk management. This is expected to help companies get optimal results from business process activities. The output of this research is the obtaining of risk management document in the form of Registry. Its contents include a list of risks, levels of risk, impact, and risk management.

Many measurement methods can be used to solve this problem, but the data is sometimes not good, and this can cause problems. Existing data are sometimes inadequate to address real-life problems, as human calculations that include preferences are often unpredictable according to their preferences with exact numerical values. A new model for measurement is required. In this research use SAW logic model in decision making of structured preference maker [6]. SAW theory helps to measure the subjective concepts of humanrelated uncertainty. Using two methods of calculation i.e. AHP to determine weight criteria, SAW for decision making and FMEA to identify any risk. The results of these three methods as a reference to make standard operating procedures so as to minimize risk and prevent failure, this is what makes the excess of this research because it uses 3 methods in data processing. So the results obtained will be more valid.

This paper consists of five sections. In Section II, it contains preliminaries. We explain the methodology of this research in Section III. The results and analysis are explained in Section IV. Last, this paper is concluded with conclusions in Section V.

II. PRELIMINARIES

This section will explain about AHP (Analytic Hierarchy Process), SAW (Simple Additive Weighting), FMEA (Failure Mode Effect Analysis) and COBIT 5 as the basis of this research.

1. AHP (Analytic Hierarchy Process)

AHP (Analytic Hierarchy Process) is the criterion weight calculated in four steps in pairs with the comparison matrix:

- 1) Forming an assessment
- 2) Making a calculation set ratings
- 3) Preparing normalized normal-pair comparisons matrix
- 4) Calculating the weight

Ranking is based on expert opinion and compared to matrix pair comparison. Comparative analysis of couples helps decision makers to establish importance levels with different criteria related to priority. A priority ranking analysis study has been established [6].

2. SAW (Simple Additive Weighting)

Multi-attribute procedure based on the concept of a weighted summation is the definition of SAW (Simple Additive Weighting). The number of weighted performance assessments of each alternative on all alternative criteria with the highest overall value will be sought and obtained by this method. The best alternative of all available alternatives will be used. The steps are explained in [7]:

- 1. Determine the alternative, A_i.
- 2. Determine the criteria C_j . This criteria will be used as a reference for the decision. It then identifies the type of criteria, whether the benefit criterion or cost criteria. If C_j is a benefit criterion, the greater the value the better the alternative the determination criterion. If C_j for the cost attribute, the smaller the value the better the alternative determination criteria.
- 3. Provide a rating which will refer to the value for each alternative on each criterion.
- 4. Determine the weight of the level of preference or importance level (W) for each criterion. $W = [W_1, W_2, W_3, ..., W_j]$
- 5. Create a conformity assessment table for each alternative on each criterion.
- 6. Create a decision matrix (X). Decision matrix (X) is formed from a table of conformity assessment of each alternative on each criteria. We determine the value (X) of each alternative (A_i) on each criterion (C_i), where, i = 1,2, m ... and j = 1,2, ... n.

$$X = \begin{bmatrix} X_{11} & X_{12} & \cdots & X_{1j} \\ \vdots & & & \vdots \\ X_{i1} & X_{i2} & \cdots & X_{ij} \end{bmatrix}$$
(1)

 Normalize the matrix to make decisions by calculating the value of the alternative A_i performance rating (rij) on criterion C_j.

$$\eta_{ij} = \begin{cases} \frac{x_{ij}}{\max_i \quad (x_{ij})} & \text{if } j \text{ is benefit criteria} \\ \frac{\min_i \quad (x_{ij})}{x_{ij}} & \text{if } j \text{ is cost criteria} \end{cases}$$
(2)

8. The result of the rank of the normalized performance performance (r_{ii}) forms the normalization matrix (R).

$$R = \begin{bmatrix} r_{11}r_{12} & \cdots & r_{1j} \\ \vdots & & \vdots \\ r_{i1}r_{i2} & \cdots & r_{ij} \end{bmatrix}$$
(3)

9. The final preference value (V_i) is derived from the sum of the matrix of line line normalization (R) weighing the preference (W) of the matrix of the corresponding element column (W).

$$V_i = \sum_{i=1}^{n} W_i r_{ii} \tag{4}$$

3. FMEA (Failure Mode Effect Analysis)

A formal analysis method for systematic failure identification technique and related risk (effect) estimates is the definition of FMEA (Failure Mode Effect Analysis). FMEA was developed in 1950 by engineers in order to solve the problems which might happen from the destruction of the military system. The FMEA method is also a method used in the study of system reliability as a first step. This method involves many components, assemblies, and subsystems that identify failure, cause and effect. A particular FMEA worksheet will record every component, assembly and failure effect that arises. In additional, FMEA is also defined as a collection of systematic activities aimed at:

- a. To know and evaluate the potential failure of the product or process as well as the impact of the failure
- b. To identify actions that may reduce the likelihood of failure occurring
- c. To document the entire process

Primary focus of FMEA is on analyzing products, both at the system and sub-systems level to gain an understanding of the quality issues arising from the design and functionality of the product. FMEA is conducted to investigate the manufacturing and assembly procedures to identify, and analyze potential failures that arise due to incorrect process design [8].

Fig.1 shows the FMEA cycle. When performing the design and process stages of FMEA, the components analyzed need to be identified first. Then, the type of failure (failure modes) should be determined and recorded. Once these types of failures are known, the consequences of component failure through certain modes of failure should be investigated and recorded. Based on this assessment, component scenarios failing through failure mode will be given probability of occurrence (O), score for consequence severity (S), and score to detect failure during design process (D). Values for O, S and D typically range from 1 to 10 called the Risk Priority Number (RPN) and the assessment is usually given by the engineer subjectively but represents the reality. The entire Risk Priority Number (RPN) is calculated by multiplying O, S and D, and will then be used as a metric to calculate the importance of component failure.



Fig.1. FMEA cycle

Risk analysis outcomes require defects and reasons to improve suggestions and actions, provide reasonable advice, and assess whether corrected actions reduce risks in the range acceptable to RPNs and severity ratings. According to score criteria are given defects and causes S, O, D, calculate the RPN value, and match the RPN value and severity to determine if defects and reasons are within acceptable range, and whether improvements and recommendations are required [9].

4. COBIT 5

COBIT 5 discusses governance and management in using information technology to fit the company's goals. As a standard that integrates a number of standards and frameworks including ISO, TOGAF, PRINCE2 / PMBOOK, CMMI and ITIL, COBIT 5 has five principles to consider in implementing IT Governance.

This framework is based on the experience of more than 15 years of many companies and IT communities in the areas of risk, security, insurance, and business. The COBIT Framework is also adopted by an organization to ensure it is efficient operations, lower costs, and improve control of IT infrastructure.

The existence of COBIT 5 is intended to assist stakeholders in determining what they need, what value-added is expected from information and technology with IT control, to realize benefits, IT risk management, run business processes based on procedures [10].

The COBIT reference model process divides IT governance and management processes into two main areas of activity governance and management. Of the two areas, each has a domain process [11]:

- Governance: has one domain EDM that contains five governance processes.
- Management: has four domains similar to the areas of responsibility of PBRM including APO, DSS, BAI, and MEA.

The process is one of seven enabler categories for corporate governance and IT governance that define the process as a set of practices that are influenced by policies and procedures that take input from a number of sources (including others processes) in the company, manipulating inputs and generating outputs (e.g. products, services).

TABLE I. PROCESS REFERENCE MODEL

	THEEL I. I	COCLOD ICLI LI	LITEL MODE	L
EDM01	EDM02	EDM03	EDM04	EDM05
Ensure	Ensure	Ensure	Ensure	Ensure
Governance	Benefits	Risk	Resource	Stakeholder
Framework	Delivery	Optimisation	Optimisation	Transparency
Setting	5	1	1	1 5
and				
Maintenance				
	Alian Plan	and Organise		Monitor
	Aligh, I lan	and Organise		Evaluate
				and Assess
A DO01	40002	40002	A DO04	MEA01
Managa	AFO02 Managa	Ar 003	Ar004	Manitan
the IT	Strategy	Entermise	Immersion	Evaluate and
Mana and	Strategy	Ambitactume	mnovation	
From avvoria		Architecture		Assess
Framework	10000	10005	12000	Performance
APO05	APO06	APO07	APO08	Conformance
Manage	Manage	Manage	Manage	Conformatice
Portfolio	Budget and	Human	Relationships	
	Costs	Resources		
APO09	APO10	APO11	APO12	
Manage	Manage	Manage	Manage	
Service	Suppliers	Quality	Risk	
Agreements				
	APO13	Manage		
	Sec	urity		
	Build, Acquire	and Implement		Monitor,
				Evaluate
				and Assess
BAI01	BAI02	BAI03	BAI04	MEA02
Manage	Manage	Manage	Manage	Monitor,
Programmes	Requirement	Solutions	Availability	Evaluate and
and	s	Identification	and Capacity	Assess
Projects	Definition	and Build	1 2	the System of
BAI05	BAI06	BAI07	BAI08	Internal
Manage	Manage	Manage	Manage	Control
Organisation	Changes	Change	Knowledge	
al	changes	Acceptance	This mouge	
Change		and		
Enablement		Transitioning		
BAI09	Manage	BAI010	Manage	
D/ 110 / 1	vete	Config	uration	
ASS	Doliner Com	as and Summart	aration	Moniton
	Deliver, Servi	ce and Support		Monitor,
				Evaluate
DCC01				and Assess
D5501	DSS02	DSS03	DSS04	MEA03
Manage	DSS02 Manage	DSS03 Manage	DSS04 Manage	MEA03 Monitor,
Manage Operations	DSS02 Manage Service	DSS03 Manage Problems	DSS04 Manage Continuity	MEA03 Monitor, Evaluate and
Manage Operations	DSS02 Manage Service Requests	DSS03 Manage Problems	DSS04 Manage Continuity	MEA03 Monitor, Evaluate and Assess
Manage Operations	DSS02 Manage Service Requests and	DSS03 Manage Problems	DSS04 Manage Continuity	MEA03 Monitor, Evaluate and Assess Compliance
Manage Operations	DSS02 Manage Service Requests and Incidents	DSS03 Manage Problems	DSS04 Manage Continuity	MEA03 Monitor, Evaluate and Assess Compliance With
DSS01 Manage Operations	DSS02 Manage Service Requests and Incidents Manage	DSS03 Manage Problems DSS06	DSS04 Manage Continuity Manage	MEA03 Monitor, Evaluate and Assess Compliance With External
DSS01 Manage Operations DSS05	DSS02 Manage Service Requests and Incidents Manage urity	DSS03 Manage Problems DSS06 J Busi	DSS04 Manage Continuity Manage ness	MEA03 Monitor, Evaluate and Assess Compliance With External Requirements

Table I explains the domains which contain in COBIT 5 and consist of 5 domain processes, such as: Align, Plan and Organize (APO); Build, Acknowledge and Apply (BAI); Provide, service and support (DSS); Monitor, Evaluate and Asses (MEA) and Evaluate, Direct and Monitor (EDM). Each domain is divided into 37 processes. This domain process will be evaluated based on stakeholder needs according to problem identification.

III. METHODOLOGY

The first step in this methodology is identifying risks. To identify the risk is by using the reference contained in COBIT 5, in this study the domains used are DS01, DS02, DS05 and BAI03.

The second step is to calculate the weight using FMEA method. In determining the weight on FMEA each risk is categorized according to the IT component then assigned a value of 1-10 for each Severity, Occurance, and Detection. Once completed calculated will get the highest risk results.

The third step is calculating the weight by using AHP method to determine the criteria. Weight calculation results from AHP will be used in determining the risk management ratings implemented in PT. PLN Persero - East Java Distribution by using SAW method. Risk management in this research is miscommunication among employees in IT department, fatal damage to network architecture, unable to send/receive data and information from server/user, connector cable on unrelated network, and data theft and data modification by irresponsible parties.

IV. RESULT AND ANALYSIS

In this section, before identifying risks, there are some problem statements that include the beginning of the risk. Based on the information we get, at the completion stage, there is data at risk at this point in one particular center, that is, the hardware component of the network on the server.

The information we get related to IT objectives, IT components, IT controls, and data transmission disruption. Data collection techniques we use are interviews and direct observation with technicians IT Department office, PT. PLN Persero - East Java Distribution. The problem here is related to information technology risk in the IT Department as an IT-based enterprise service provider that will be grouped based on information system components i.e. procedures, hardware, software, data, and people. So based on the identification of potential risks, they will be managed in accordance with the process of IT Risk Management.

Furthermore, based on the identification of potential risks to the IT network, then analyzed the cause and effect of these risks. The analytical process is supported by sources of data collection through interviews and direct object observations accompanied by the IT Helpdesk team.

So the following analysis as shown in Table II is the identification of the causes and the impact of risk on the implementation of IT networks by PT. PLN Persero - East Java Distribution which is accompanied by potential frequency occurrence for some risks that have been happened before.

TABLE II. RESULTS OF IDENTIFYING CAUSES AND IMPACTS OF

No	Risk	Frequency	Causes of	Risk
	Identification	of Events	Risk	Impact
1	Damage to network device hardware	Low Probability	Hardware exposed to liquid attacks, natural disasters, and	Network hardware components cannot operate in generating network
			liles	everyday

. Identification of Events Risk Impact business processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes processes process processes processes procespress processes	No	Risk	Frequency	Causes of	Risk
2 Damage to UPS Server Low Probability UPS is exactly standard Network management hardware can be physically disabled and disabled 2 Damage to UPS Server Low Probability UPS is exposed to liquid attacks, natural disasters, and fires UPS is unable to activate instantaneousl y and instantly power outages in a rapidly repeatable time 3 Theft of hardware Remote Probability The condition of the main power supply (electricity) is unstable UPS is unable to activate instantaneousl y and instantly power outages in a rapidly repeatable time 3 Theft of hardware Remote Probability The physicall security of the network hardware out of date when not good Loss of network hardware out of date when network increasing 4 Server performance is unstable and starts to decline Moderate Probability Server hardware out of date when network increasing Loss of network hardware assets and can sect and can shorten the server is less ischedule 5 Server maifunction Moderate Probability Server memory asset and can shorten the server is easily damaget bio erapuicrements for Network hardware out of server performance life 6 The server is easily damaget heat Internet systems and networks been used 6 The server is easily damaget heat Internet systems and networks become temporarity performance 6 The server is eserver The server room cancet heat Internet systems and networks become temporarity propresenture propaget to temporatu	•	Identification	of Events	Risk	Impact
2 Damage to UPS Server Low Probability UPS is exposed to iquid attacks, natural disasters, and fires UPS is upply upply (electricity) is unstable UPS is upply upply (electricity) is unstable 3 Theft of hardware Remote Probability The condition of the main power supply (electricity) is unstable UPS is upply upply (electricity) is unstable 3 Theft of hardware Remote Probability The physicall security of the network manager is not a payly repeatable time Loss of network manager is not supply (electricity) is unstable 4 Server performance is unstable and starts to decline Remote Probability Server nom manager is not good Loss of network manager is not supply (electricity) is unstable 5 Server memory malfunction Moderate Probability Server nom manager is not good The server is unable to network manager is not good 5 Server memory malfunction Moderate Probability Server memory requirements for Network tarific is increasing Reduce server operating performance is schedule 6 The server is overheated Low Probability The server is less schedule Reduce server operating performance iffe 6 The server is overheated Low Probability The server in the server in the server in the server performance is schedule Internet systems and network become temporating performance increases and network become temporating					processes
2 Damage to UPS Server Low Probability UPS is exposed to liquid attacks, natural disasters, and fires UPS is unstable usastable usastable usastable UPS is unstable usastable usastable usastable UPS is unstable usastable usastable usastable UPS is unstable usastable usastable usastable usastable usastable UPS is unstable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable usastable userver usastable usastable usastable usast					Network
2 Damage to UPS Server Low Probability UPS is exposed to liquid attacks, natural disasters, and fires UPS is us mable to activate 2 Damage to UPS Server Low Probability The condition of the main power supply (electricity) is unstable UPS is unable to activate 3 Theft of hardware Remote Probability The condition of the main power supply (electricity) is unstable UPS is unable to activate 3 Theft of hardware Remote Probability The physically security of the network hardware out of date when manager is not good Loss of network traffic is increasing 4 Server performance is starts to decline Moderate Probability The physically security of the network hardware out of date when manager is not good The server is unable to manage the employee's job requirements for Network Access 5 Server malfunction Moderate Probability Server memory capacity has been used of server is easily damaged and can short the server is easily damaged an tetworks b				The hardware	management
2 Damage to UPS Server Low Probability UPS is exposed to liquid attacks, natural disasters, and fires UPS is usable UPS is usable 2 Damage to UPS Server Low Probability UPS is exposed to liquid attacks, natural disasters, and fires UPS is usable 3 Theft of hardware Low Probability The condition of the main power supply (electricity) is unstable UPS is unable to activate instantaneousl y and instantly power outages in a rapidly repeatable time 3 Theft of hardware Remote Probability The physical security of the network manager is not good US so of network manager is not good 4 Server performance is starts to decline Moderate Probability Server memory capacity has scheduled The server is unable to manage the employce's job requirements scheduled 5 Server memory malfunction Moderate Probability Server memory capacity has been used nore than 70% The server is easily damaged and can shorten the scrver is erver is less scheduled 6 The server is overheated Low Probability The server memory maintenance scheduled Reduce server operating performance 6 The server is overheated Low Probability The server memory maintenance scheduled Network the server performance 6 The server is overheated Low Probability The server memory maintenance schedule Reduce server operating promance 6 <				setup is not	hardware can
2 Damage to UPS Server Low Probability UPS is exposed to liquid attacks, natural disabled UPS is ustable instantaneousl y and instantly power outages in a rapidly repeatable time 3 Theft of hardware Low Probability The condition of the main power supply (electricity) is unstable UPS is unable to activate 3 Theft of hardware Remote Probability The physical security of the room is unstable UPS is unable to activate 4 Server hardware Remote Probability The physical security of the room is unstable Lows of network hardware out of date when network hardware out of date when network Loss of network hardware out of date when network hardware out of date when network hard.cccss scheduled The server is casily damaged and can shorten the server is less scheduled 5 Server memory malfunction Server memory maintenance schedule Reduce server operating performance (log respond, han, etc.) 6 The server is overheated Internet systems and networks heat Internet systems and networks heat 6 The se				exactly	be physically
2 Damage to UPS Server Low Probability UPS is exposed to liquid attacks, natural disasters, and fires UPS is unable to activate instantaneously and instantly power outages in a rapidly repeatable time 2 Damage to UPS Server Low Probability The condition of the main power supply (electricity) is unstable UPS is unable to activate instantaneously and instantly power outages in a rapidly repeatable time 3 Theft of hardware Remote Probability The physical security of the network hardware out of date when not good Loss of network network hardware out of date when network traffic is increasing Loss of network network hardware out of date when network traffic is increasing The server is unable to mage the employee's job requirements for Network Access 4 Server performance is unstable and starts to decline Moderate Probability Server memory malfunction The server is easily damaged and can short the server is less scheduled The server is easily damaged and can short the server is ess scheduled 5 Server memory malfunction Moderate Probability Server memory easily damaged and can scheduled Reduce server operating performance (log respond, hang, etc.) 6 The server is overheated Low Probability The server memory malfunction Internet schedule 6 The server is overheated Low Probability The server memory malfunction Internet schedule 6 The server is overheated Internet schedule Intern				standard	disabled and
2 Damage to UPS Server Low Probability UPS is exposed to liquid attacks, natural disasters, and fires to activate instantaneousl y and instantly power outages in a rapidly repeatable time UPS is unable to activate instantaneousl y and instantly power outages in a rapidly repeatable time UPS is unable to activate instantaneousl y and instantly power outages in a rapidly repeatable time UPS is unable to activate instantaneousl y and instantly power outages in a rapidly repeatable time UPS overheat or overcool which can cause dew (liquid) 3 Theft of hardware Remote Probability The physical security of the network manager is inort good Loss of network manager is inort good 4 Server performance is unstable and starts to decline Moderate Probability Server hardware assets and can be misused 5 Server memory malfunction Moderate Probability Server hardware asset server is increasing The server is easily damaged (long respont, hand, been used 6 The server is overheated Server memory malfunction Reduce server memory malfunction Server hardware asset and can shorten the server is less scheduled Reduce server operformance life 6 The server is overheated Low probability The server memory malfunction Used memory servers are not effective for memory maintenance schedule Used memory servers are not effective for memory malfunction 6 The server is overheated Low probability The server memory maintenance schedule Internet systems and networks heat					UPS is unable
2 Damage to UPS Server Low Probability Low Probability The condition of the main power supply (electricity) is unstable instantaneousl y and instantly power outages in a rapidly repeatable time UPS is unable to activate instantaneousl y and instantly power outages in a rapidly repeatable time UPS overheat 3 Theft of hardware Remote Probability The physical security of the network hardware out of date when network increasing Loss of network instantaneousl y and instantly power outages in a rapidly repeatable time 3 Theft of hardware Remote Probability The physical security of the network increasing Loss of network increasing 4 Server performance is starts to decline Moderate Probability Server network increasing The server is unable to manage the employee's job requirements for Network increasing 5 Server memory malfunction Moderate Probability Server memory capacity has been used more than 70% The server is usable to manage the enployee's job requirements for Network Access 6 The server is overheated Low Probability Server memory capacity has been used more than 70% Reduce server operating performance of server gets excessive heat Internet systems and networks become temporarily paralyzed 6 The server is owerheated Low Probability The server server performance of server memory maintenance schedule Internet systems and networks become temporarily paralyzed				UPS 1s	to activate
2 Damage to UPS Server Low Probability Low Probability The condition of the main power supply (electricity) is unstable y and instantly power outages in a rapidly repeatable time 3 Theft of hardware Remote Probability The physical security of the network hardware UPS overheat or overcool 3 Theft of hardware Remote Probability The physical security of the network hardware Loss of network manager is not good 4 Server performance is unstable and starts to decline Moderate Probability Server hardware out of date when network taffic is increasing The server is easily damaged and can shorten the server is less scheduled The server is easily damaged and can shorten the server is less scheduled 5 Server memory malfunction Moderate Probability Server memory capacity has been used requirements for Network Reduce server operating erver server performance life 6 The server is overheated Server memory malfunction Server memory maintenance scheduled Reduce server operating server 6 The server is overheated Low probability The server memory maintenance schedule Used memory data storage 6 The server is overheated Low probability The server memory maintenance schedule Internet systems and networks become temporarity paralyzed 6 The server is overheated The server room temporating performance schedule Internet systems an				exposed to	instantaneousl
2 Damage to UPS Server Low Probability isasters, and fires power outages in a rapidly repeatable time UPS is unable to activate instantaneousl y and instantly power outages in a rapidly repeatable time UPS is unable to activate instantaneousl y and instantly power outages in a rapidly repeatable time UPS overheatt or overcool which can cause dew (liquid) 3 Theft of hardware Remote Probability The physical security of the network manager is not good Loss of network manager hardware 4 Server performance is unstable and starts to decline Moderate Probability Server hardware out of date when network traffic is increasing The server is unable to manage the employee's job requirements for Network traffic is increasing The server is easily damaged and can shorten the server is less schedule 5 Server memory malfunction Moderate Probability Server memory capacity has been used more than 70% The server is easily damaged and can shorten the server is easily damaged and can shorten the server performance life 6 The server is overheated Low Probability The absence of server memory maintenance schedule Used memory servers are not effective for data storage secount temporative increases and makes the hot temporative propagate to promaget to propaget to				natural	y and instantly
2 Damage to UPS Server Low Probability fires in a rapidly repeatable time UPS is unable to activate instantaneously y and instantly power outpaces in a rapidly repeatable time UPS overheat or overcool which can cause dew unstable 3 Theft of hardware Remote Probability The physical security of the network hardware USS overheat or overcool which can cause dew unstable 4 Server performance is unstable and starts to decline Moderate Probability Server hardware out of date when network traffic is increasing The server is unable to manager is not good 5 Server memory malfunction Moderate Probability Server hardware network The server is easily damaged and can server is less scheduled The server is easily damaged and can server is less scheduled 6 The server is overheated Low probability Server memory maintenance of server memory maintenance Reduce server operformance ife 6 The server is overheated Low probability The server memory maintenance of server memory maintenance schedule Used memory servers are not effective for data storage 6 The server is overheated Low probability The server memory maintenance schedule Internet systems and makes the hot temperature increases and makes the hot temperature increases and makes the hot				disasters, and	power outages
2 Damage to UPS Server Low Probability Low Probability The condition of the main power supply (electricity) is unstable UPS is unable to activate instantaneously y and instantly power outages in a rapidly power outages in a rapidly in a rapidly power outages in a rapidly in a rapidly in a rapidly power outages in a rapidly in a				fires	in a rapidly
2 Damage to UPS Server Low Probability The condition of the main power supply (electricity) is unstable to activate instantaneously yower outages in a rapidly repeatable time or overcool which can cause dew (liquid) 3 Theft of hardware Remote Probability The physical security of the network hardware UPS overheat or overcool which can cause dew (liquid) 3 Theft of hardware Remote Probability The physical security of the network manager is not good Loss of network manager hardware assets and can be misused 4 Server performance is unstable and starts to decline Moderate Probability Server hardware out of date when network traffic is increasing The server is easily damage the employee's job requirements for Network 5 Server memory malfunction Moderate Probability Server memory capacity has been used more than 70% The server is easily damaged more than 70% 6 The server is overheated Low Probability The server memory maintenance scheduled Reduce server operating performance life 6 The server is overheated Low Probability The server memory capacity has been used more than 70% Network hag, etc.) 6 The server is overheated Low Probability The server memory capacity has been used more than 70% Internet systems and networks become temporatily paralyzed		D			UPS is unable
Server performance is unstable and starts to declineLow Probabilityof the main power supply (electricity) is unstableinstantaneously y and instantly inside the or overcool which can ecause dew (liquid)3Theft of hardwareRemote ProbabilityThe physical security of the network ardware out of date when not goodLows of network manager is not goodLoss of network manager is not good4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when network traffic is increasingThe server is unable to manage the employee's job requirements for Network access5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%The server is easily damaged and can server is easily damaged instantaneous server is easily damaged and can server is easily damaged in the server is easily damaged in the server in the server in the server room cannot balance the he	2	Damage to UPS	Low	The condition	to activate
4Server performance is unstableRemote robabilityServer manager is not goodServer network hardwareNoderate ProbabilityServer manager is increasingUsed memory requirements for Network hardware4Server performance is unstable and starts to declineModerate ProbabilityServer manager is not goodThe server is easily damaged increasingThe server is easily damaged and can server is less scheduledThe server is easily damaged increasing5Server memory malfunctionModerate ProbabilityServer manager is not goodThe server is easily damaged and can server is less scheduledThe server is easily damaged and can server is less server performance in increasingThe server is easily damaged and can server is less server performance if the server is casily damaged and can server is less server performance life5Server memory malfunctionModerate ProbabilityServer memory capacity has performance of server memory maintenance scheduleNoderate server is casily damaged and can server is casily damaged in etwork hang, etc.)6The server is overheatedServer memory maintenance scheduleNoderate server in the server in the		Server	Probability	of the main	instantaneousl
3Theft of hardwareRemote ProbabilityCelectricity is unstablepower outages in a rapidly repeatable time3Theft of hardwareRemote ProbabilityThe physical security of the network hardwareLoss of network manager is not good3Theft of hardwareRemote ProbabilityThe physical security of the network hardware or om manager is not goodLoss of network matware4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when network traffic is increasingThe server is unable to manage the employee's job requirements for Network traffic is increasingThe server is easity damaged and can server is less scheduled5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance life6The server is overheatedLow ProbabilityServer capacity has been used more than 70%Used memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverInternet systems and networks become temporative increases and makes the hot temperature progagate to the			Tiobuonity	power supply	y and instantly
3Theft of hardwareRemote ProbabilityTemperature and humidity inside the room is unstableUPS overheat or overcool which can cause dew (liquid)3Theft of hardwareRemote ProbabilityThe physical security of the network manager is not goodLoss of network masets and can be misuade4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when networkThe server is unable to manager is not goodThe server is unable to manager the employee's job requirements for Network5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%The server is easily damaged and can shorten the server is leasily damaged increasing6The server is overheatedLow ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance life6The server is overheatedLow ProbabilityThe server memory maintenance scheduleUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server memory maintenance scheduleInternet systems and networks become temporarily paralyzed6The server is overheatedLow ProbabilityThe server memory maintenance scheduleInternet systems and networks become temporarily paralyzed				(electricity) is	power outages
3 Theft of hardware Remote Probability Temperature and humidity inside the room is unstable UPS overheat or overcool which can cause dew (liquid) 3 Theft of hardware Remote Probability The physical security of the network hardware room manager is not good Loss of network manager is not good 4 Server performance is unstable unstable and starts to decline Moderate Probability Server hardware or increasing The server is unable to of ate when network traffic is increasing The server is easily damaged and can shorten the server performance life 5 Server memory malfunction Moderate Probability Server memory capacity has been used more than 70% Reduce server operating performance life 6 The server is overheated Low Probability Server memory capacity has been used more than 70% Used memory servers are not effective for data storage 6 The server is overheated Low Probability The server memory maintenance schedule Used memory servers are not effective for data storage 6 The server is overheated Low Probability The server memory maintenance schedule The server room cannot balance the heat of the server The server room temperature propagate to server				unsidule	repeatable time
3Theft of hardwareRemote Probabilityand humidity inside the room is unstableor overcool which can cause dew (liquid)3Theft of hardwareRemote ProbabilityThe physical security of the network hardware room manager is not goodLoss of network manager assets and can be misused4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when network traffic is increasingThe server is easily damaged and can shorten the scheduled5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70% Reduce server of server of server maintenance scheduledThe absence of server of server systems and network hang, etc.)6The server is overheatedLow ProbabilityThe server memory capacity has been used memory capacity has been used memory maintenance scheduleUsed memory servers are not effective for dat a storage6The server is overheatedLow ProbabilityThe server room capacity has been used memory maintenance scheduleInternet systems and networks become temporarily paralyzed6The server is overheatedLow probabilityThe server room cannot balance the heat of the serverInternet systems and networks become temporarily paralyzed				Temperature	UPS overheat
3Theft of hardwareRemote Probabilityinside the room is unstable security of the network hardware inot goodWhich can cause dew (liquid)3Theft of hardwareRemote ProbabilityThe physical security of the network hardware inot goodLoss of network manager is not good4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when network traffic is increasingThe server is unable to manage the employee's job requirements for Network traffic is increasingThe server is unable to manage the employee's job requirements for Network traffic is increasingThe server is unable to manage the employee's job requirements for Network and can server is less scheduled5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance (log respond, hang, etc.)6The server is overheatedLow ProbabilityThe server server servers are not memory maintenance scheduleUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server memory maintenance scheduleInternet systems and networks heat6The server is overheatedLow probabilityThe server room cannot balance the heat of the serverInternet systems and networks heat				and humidity	or overcool
3Theft of hardwareRemote Probabilityroom is unstable unstable security of the network hardware room manager is not goodLoss of network manager assets and can be misused4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when network traffic is increasingThe server is unable to manage the employee's job requirements for Network traffic is increasingThe server is unable to manage the employee's job requirements for Network traffic is increasingThe server is unable to manage the employee's job requirements for Network traffic is increasingThe server is easily damaged and can shorten the server memory capacity has been used more than 70%5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance (long respond, hang, etc.)6The server is overheatedLow ProbabilityThe server memory capacity has been used more than 70%Used memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverInternet systems and makes the hot temperature increases and makes the hot temperature propagate to the				inside the	which can
3Theft of hardwareRemote ProbabilityThe physical security of the network hardware room manager is not goodLoss of network manager is not good4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when network traffic is increasingThe server is unable to manage the employee's job requirements for Network traffic is increasingThe server is unable to manage the employee's job requirements for Network traffic is increasingThe server is easily damaged and can shorten the server performance easily damaged and can shorten the server is less scheduled5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance life6The server is overheatedLow ProbabilityThe server memory capacity has been used more than 70%Used memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverInternet systems and networks become temporature increases and makes the hot temperature propagate to the heat of the server				room is	cause dew
3Theft of hardwareRemote ProbabilityInterpretation security of the network hardwareLoss of network manager is not good4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when network traffic is increasingThe server is unable to manage the employee's job requirements for Network Access5Server memory malfunctionModerate ProbabilityServer hardware out of date when network traffic is increasingThe server is easily damaged and can shorten the server performance life5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance (log respond, hang, etc.)6The server is overheatedLow ProbabilityThe server regets excessive heatUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverInternet systems and network server from the server room cannot balance the heat of the server				The physical	(iiquid)
3Theft of hardwareRemote Probabilitynetwork hardware room manager is not goodnetwork manager is not good4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when network traffic is increasingThe server is unable to manage the employee's job requirements for Network Access5Server memory malfunctionModerate ProbabilityMaintenance server is less scheduledThe server is easily damaged and can shorten the server performance life5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance (log respond, hang, etc.)6The server is overheatedLow ProbabilityThe server regets excessive heatUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverInternet systems and network heat of the server				security of the	Loss of
3Interfor hardwareRethou Probabilityhardware room manager is not goodInterfor manager is not good4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when network traffic is increasingThe server is unable to manage the employee's job requirements for Network Access5Server memory malfunctionModerate ProbabilityServer memory maintenance server is less scheduledThe server is easily damaged and can shorten the server performance life5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance life6The server is overheatedLow ProbabilityThe server regets excessive heatUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverInternet server room cannot balance the heat of the serverThe server room cannot balance the heat of the server		Theft of	Remote	network	manager
4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when network traffic is increasingThe server is unable to manage the employee's job requirements for Network Access4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when network traffic is increasingThe server is easily damaged and can server is less scheduled5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance (log respond, hang, etc.)6The server is overheatedLow ProbabilityThe server gets excessive heatUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverInternet systems and networks become temporature increases and mankes the hot temperature propagate to	3	hardware	Probability	hardware	hardware
4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when network traffic is increasingThe server is unable to manage the employee's job requirements for Network Access5Server memory malfunctionModerate ProbabilityMaintenance server is less scheduledThe server is easily damaged and can shorten the server performance life5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance life6The server is overheatedServer ProbabilityReduce server operating performance life6The server is overheatedLow ProbabilityThe server gets excessive heatUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverInternet systems and networks become temperature in the server room cannot balance the heat of the serverThe server room temperature increases and makes the hot temperature propagate to			5	room	assets and can
4 Server performance is unstable and starts to decline Moderate Probability Server hardware out of date when network traffic is increasing The server is unable to manage the employee's job requirements is increasing 5 Server memory malfunction Moderate Probability Maintenance server is less scheduled The server is easily damaged and can shorten the server performance life 5 Server memory malfunction Moderate Probability Server memory capacity has been used more than 70% Reduce server operformance (long respond, hang, etc.) 6 The server is overheated Low Probability The server rest effective for data storage 6 The server is overheated Low Probability The server room cannot balance the heat of the server room temperature in the server room temperature propagate to temperature propagate to temperature propagate to temperature				not good	be misused
4Server performance is unstable and starts to declineModerate ProbabilityServer hardware out of date when network traffic is increasingunable to manage the employee's job requirements for Network Access5Server memory malfunctionModerate ProbabilityMaintenance server is less scheduledThe server is easily damaged and can server performance life5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance (long respond, hang, etc.)6The server is overheatedLow ProbabilityThe server gets excessive heatUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverInternet systems and networks become temporarily paralyzed				Some	The server is
4Server performance is unstable and starts to declineModerate ProbabilityIndividue out of date when network traffic is increasingmanage the employee's job requirements for Network Access5Server malfunctionModerate ProbabilityMaintenance server is less scheduledThe server is easily damaged and can shorten the server performance life5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance life6The server is overheatedLow ProbabilityThe absence of server memory maintenance scheduleUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverInternet systems and networks become temporarily paralyzed				Server	unable to
4Server performance is unstable and starts to declineModerate Probabilitynetwork traffic is increasingemployee's job requirements for Network Access5Server malfunctionModerate ProbabilityMaintenance server is less scheduledThe server gerformance life5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance (long respond, hang, etc.)6The server is overheatedLow ProbabilityThe server memory maintenance scheduleUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server memory maintenance scheduleUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverThe server room cannot temperature in the server room cannot balance the heat of the serverInternet room temperature propagate to temperature				of date when	manage the
4Server performance is unstable and starts to declineModerate Probabilitytraffic is increasingrequirements for Network Access4mastable and starts to declineModerate ProbabilityMaintenance server is less scheduledThe server is easily damaged and can shorten the server performance life5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance (long respond, hang, etc.)6The server is overheatedLow ProbabilityThe server gets excessive heatUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server room cannot balance the heatInternet systems and networks become temperature in the server room cannot balance the heat of the serverThe server room cannot balance the heat of the server				network	employee's job
4 performance is unstable and starts to decline Moderate Probability increasing Access Access 5 Server memory malfunction Moderate Probability Maintenance server is less scheduled The server is easily damaged and can shorten the server performance life 5 Server memory malfunction Moderate Probability Server memory capacity has been used more than 70% Reduce server operating performance (long respond, hang, etc.) 6 The server is overheated Low Probability The absence of server memory maintenance schedule Used memory servers are not effective for data storage 6 The server is overheated Low Probability The server room cannot balance the heat of the server Internet systems and networks become temporarily paralyzed		Server		traffic is	for Network
Instable and starts to declineProbabilityThe server is easily damaged and can shorten the server performance life5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance (long respond, hang, etc.)6The server is overheatedLow ProbabilityThe server gets excessive heatUsed memory server memory maintenance schedule6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverInternet systems and networks become temporarily paralyzed	4	performance is	Moderate	increasing	Access
5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance (long respond, hang, etc.)6The server is overheatedLow ProbabilityThe server gets excessive heatUsed memory server memory maintenance scheduleUsed memory server memory memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server gets excessive heatInternet systems and networks become temporarily paralyzed		starts to decline	Probability		The server is
6The server is overheatedLow ProbabilityMaintenance server is less scheduledand can shorten the server performance life6The server is overheatedModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance (long respond, hang, etc.)6The server is overheatedLow ProbabilityThe absence of server memory maintenance scheduleUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverInternet systems and networks become temperature in the server room cannot balance the heat of the server		starts to deenne			easily damaged
6 The server is overheated Low Probability Server memory capacity has been used more than 70% Reduce server operformance life 6 The server is overheated Noderate Probability Server memory capacity has been used more than 70% Reduce server operformance (long respond, hang, etc.) 6 The server is overheated The absence of server memory maintenance schedule Used memory servers are not effective for data storage 6 The server is overheated Low Probability The server reserver in the server room cannot balance the heat of the server Internet systems and networks become temporarily paralyzed				Maintenance	and can
6 The server is overheated Low The server is overheated Low The server is overheated Internet server room cannot balance the server room cannot balance the server room cannot balance the basen to temperature probability The server room cannot balance the basen to temperature propagate to room cannot balance the basen to temperature propagate to room cannot balance the basen to temperature propagate to room cannot balance the basen to temperature propagate to room cannot balance the basen to temperature propagate to room cannot balance the basen to temperature propagate to room cannot balance the basen to temperature propagate to room cannot balance the basen to temperature propagate to room cannot balance the basen temperature propagate to room cannot balance the propagate to room cannot propagate to prop				scheduled	server
5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance (long respond, hang, etc.)6The server is overheatedImage: Comparison operation					performance
5Server memory malfunctionModerate ProbabilityServer memory capacity has been used more than 70%Reduce server operating performance (long respond, hang, etc.)6The server is overheatedImage: Server memory maintenance scheduleUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server gets excessive heatInternet systems and networks become temporarily paralyzed6The server is overheatedLow ProbabilityThe server room cannot balance the heat of the serverInternet systems and networks become temporarily paralyzed				-	life
5 Server memory malfunction Moderate Probability memory capacity has been used more than 70% operating performance (long respond, hang, etc.) 6 The server is overheated The absence of server memory maintenance schedule Used memory effective for data storage 6 The server is overheated Low Probability The server gets excessive heat Internet systems and networks 6 The server is overheated Low Probability The temperature in the server room cannot balance the heat of the server The server room gagate to other				Server	Reduce server
5 Derivation Probability requertines been used more than 70% performance (long respond, hang, etc.) 6 The server is overheated The absence of server memory maintenance schedule Used memory servers are not effective for data storage 6 The server is overheated Low Probability The server gets excessive heat Internet systems and networks 6 The server is overheated Low Probability The temperature in the server room cannot balance the heat of the server The server room cannot		Server memory	Moderate	capacity bas	operating
6 The server is overheated Low Probability The server is temperature in the server room cannot balance the server room cannot balance the beat of the server room cannot balance the probability Internet server room cannot balance the probability room cannot balance the probab	5	malfunction	Probability	been used	performance
6 The server is overheated Low Probability The server room cannot balance the server room cannot balance the server room cannot balance the heat of the server room cannot balance the server ro			5	more than	(long respond,
6The server is overheatedLow ProbabilityThe server of server memory maintenance scheduleUsed memory servers are not effective for data storage6The server is overheatedLow ProbabilityThe server gets excessive heatInternet systems and networks become temperature in the server room cannot balance the heat of the server				70%	nang, etc.)
6 The server is overheated Low Probability The server is temperature in the server room cannot balance the heat of the server The server is overheated <td></td> <td></td> <td></td> <td>The absence</td> <td>Used memory</td>				The absence	Used memory
6 The server is overheated Low Probability The server is temperature in the server room cannot balance the heat of the server The server is overheated The server is temperature in the server room cannot balance the heat of the server The server is overheated The server is temperature in the server room cannot balance the heat of the server The server is temperature in the server is the hot temperature in the server is the s				of server memory	servers are not
6 The server is overheated Low Probability The server is temperature in the server room cannot balance the heat of the server The server is overheated The server is temperature in the server room cannot balance the heat of the server The server is overheated The server is temperature in the server room cannot balance the heat of the server The server is temperature in the server is the server is temperature in the server is the server i				maintenance	effective for
6 The server is overheated Low Probability The server is the server in the server room cannot balance the heat of the server Internet systems and networks become temporarily paralyzed 6 The server is overheated Low Probability The server room cannot balance the heat of the server				schedule	data storage
6 The server is overheated Low Probability The server gets excessive heat systems and networks become temporarily paralyzed 6 The server is overheated Low Probability The server room cannot balance the heat of the server metworks become temporarily paralyzed					Internet
6 The server is overheated Low Probability gets excessive heat networks become temporarily paralyzed 6 The server is overheated Low Probability The temperature in the server room cannot balance the heat of the server metworks become temporarily paralyzed				The server	systems and
6 The server is overheated Low Probability The temperature in the server room cannot balance the heat temporarily paralyzed The server room temperature increases and makes the hot temporarily paralyzed temporarily temperature in creases and makes the hot temperature propagate to temperature				gets excessive	networks
6 The server is overheated Low Probability The temperature in the server room cannot balance the heat of the server				heat	temnorarily
6 overheated Low overheated Probability Low heat of the server transmission of the balance the beat of the server transmission of the temperature in the server transmission of the balance the temperature propagate to the temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature t		The			paralyzed
Probability Probability temperature in the server room cannot balance the heat of the server temperature in the server room cannot server temperature in the server room cannot temperature in the server room cannot temperature in the server temperature in the server temperature in the server room cannot temperature in the server temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature temperature	6	I he server is	Low	The	The server
in the server room cannot balance the heat of the server		overneated	Probability	temperature	room
room cannot balance the heat of the server				in the server	temperature
balance the temperature heat of the propagate to				room cannot	makes the hot
heat of the propagate to server				balance the	temperature
server				heat of the	propagate to
the physical				server	the physical

No	Risk	Frequency	Causes of	Risk
•	Identification	of Events	Risk	Impact
7	Connector cable on the network is not connected (broken)	Moderate Probability	Improper cable structuring and act of human error	Temporary internet access and data transmission failure
8 8 8 8 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Can not send / receive data and information from server / user	Certain Probability	The server is being interrupted	Internal applications and internal websites are inaccessible Failure of
			being interrupted	internet access and data transmission
9	Software system exposed to virus attacks	Failure is almost	Out of dated antivirus	Software systems are vulnerable to incoming viruses Business
		mevitable	Act of human error	process activity is inhibited
10	Damage to software on PC employees and PC for network operations	Very High Probability	Error in installation or configuration of software (act of human error)	Software has interruption
			software	system crashes
11	Remote Desktop Attacks on the element of deliberate negativity on PC employees	Low Probability	Security for User Account authentication is not good	There is a modification of data and company information on the software system on the PC
12	There was a fatal damage to the network architecture	Remote Probability	Error in installation or configuration of network infrastructure (act of human error)	Network failure in operation for data transmission
			Hacker attacks	Modification of deliberate elements on the network architecture
	The corporate		Security system for network access is not good	Attack of bandwidth theft by Unauthorized User Privilege
13 network attacked b hackers	network is attacked by hackers	Remote Probability	There is a vulnerability to access to the network by unknown users	The occurrence of information modification and information theft outside the supervision of the network manager
14	Data theft and data modification by irresponsible parties	Remote Probability	Security system and firewall for data access less powerful	Company data is duplicated and can be misused
15	Failure in	Very High	The system	Data cannot be

No	Risk Identification	Frequency of Events	Causes of Risk	Risk Impact
	process of data access process	Probability	applied for data access is interrupted	accessed when needed
16	Miscommunicati on between employees in the IT department	Moderatel y High Probability	SOP of organizational responsibility and risk management SOP is not available	Failure in the work process for IT Service management
17	The occurrence of human error in office employees for the use of ICT equipment	Failure is almost inevitable	SOPs for governance of ICT devices are not available	Employee activity is hampered and inefficient due to small problems of using ICT devices

The next step is to calculate the risks using FMEA method. From the calculation using FMEA method, we will obtain the following results as explained in Table III. We categorize the results into people, network, software, hardware, and data.

TABLE III. RESULTS OF FMEA METHOD			
	PEOP	LE	
		The occurrence of human	
A1	540	error in office employees for	
		the use of ICT equipment	
	NETW	ORK	
		There was a fatal damage to	
13 & 15	60	the network architecture (A3)	
AJ & AJ	00	& Network firms attacked by	
		hackers (A5)	
SOFTWARE			
۸7	480	Software system exposed to	
A/		virus attacks	
HARDWARE			
		Connector cable on the	
A14	150	network is not connected	
		(broken)	
DATA			
		Data theft and data	
A28	100	modification by irresponsible	
		parties	

Based on Table III, it clearly shows the highest risk results from the calculation using FMEA method. There are 6 risks that affect the running of business processes. Next, we need to know that the risks outcome by using AHP SAW method. So, we combine 2 methods, AHP and SAW to identify the risks in order to get the maximum results.

TABLE IV.	RESULTS OF	AHP SAW	METHOD

IIIDEE	TIBLE IT REDUETD OF THE SITE METHOD			
PEOPLE				
A2	0,833083	Miscommunication between employees in the IT department		
NETWORK				
A6	0,933354	There was a fatal damage to the network architecture		
SOFTWARE				
A8	0,933354	Cannot send / receive data and information from server / user		

HARDWARE				
A14 0,958346		Connector cable on the network is not connected (broken)		
DATA				
A28	0,871209	Data theft and data modification by irresponsible parties		

From Table IV, we get the information that the results of AHP SAW has highest risk for each category. It has 5 risks at all. From the results calculated by using FMEA and AHP SAW methods, there are 2 risks which are the same, namely the category of hardware and data.

V. CONCLUSION

This research proposes collaboration of several theories to support the risk management process using COBIT 5 as the basis for identification and mapping of risk probabilities. In addition, FMEA or Failure Mode and Effect Analysis and AHP SAW are used to manage Risk Assessment to rank risk priorities. Thus, from the results of our research analysis is from the weighted risk potential calculation by FMEA and AHP SAW method, 9 priority risk with the highest potential RPN (Risk Priority Number) and weight value is very important.

ACKNOWLEDGMENT

Authors give a deep thank to Department of Information Technology Management and Department of Informatics, Institut Teknologi Sepuluh Nopember for supporting this research.

REFERENCES

 R. Sarno and Y. A. Effendi, "Hierarchy Process Mining from Multi-Source Logs," Telecommunication, Computing, Electronics and Control (TELKOMNIKA), Vol.15, No.4, 2017

DOI: http://dx.doi.org/10.12928/telkomnika.v15i4.6326

- [2] Y. A. Effendi and R. Sarno, "Non-Linear Optimization of Critical Path Method," International Conference on Science and Information Technology (ICSITech), pp.90-96, 2017. DOI: 10.1109/ICSITech.2017.8257091
- [3] K. D. Febriyanti, R. Sarno, and Y. A. Effendi, "Fraud Detection on Event Log Using Fuzzy Association Rule Learning," International Conference On Information & Communication Technology And System (ICTS), pp.149-154, 2017. DOI: 10.1109/ICTS.2017.8265661
- [4] Y. A. Effendi and R. Sarno, "Discovering process model from event logs by considering overlapping rules," 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), pp. 1-6, 2017. DOI: 10.1109/EECSI.2017.8239193
- [5] Y. A. Effendi and R. Sarno, "Discovering optimized process model using rule discovery hybrid particle swarm optimization," 3rd International Conference on Science in Information Technology (ICSITech), pp. 97-103, 2017. DOI: 10.1109/ICSITech.2017.8257092
- [6] S. J. Seyedmohammadi, "Application of SAW, TOPSIS and fuzzy TOPSIS models in cultivation priority," 2017.
- [7] R. E. Setyani, "Flood-prone Areas Mapping at Semarang City By Using Simple," in CITIES 2015 International Conference, Intelligent Planning Towards Smart Cities, Surabaya, 2015.
- [8] J. S. Rahul Renu, "A Knowledge Based FMEA to Support Identification and Management of," in 6th CIRP Conference on Assembly Technologies and Systems (CATS), 2016.
- [9] D. Y. Sun, "Research on the Defects and Improvement of Internal," in International Conference on Service System and Service Management (ICSSSM), China, 2017.

- [10] S. E. R. Fitroh, "Determining Evaluated Domain Process through," in 5th International Conference on Cyber and IT Service Management (CITSM), Denpasar, 2017.
- [11] ISACA, Cobit 5 Enabling Processes, USA: ISACA, 2012.