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

Amrina Friska Apriliana[1], Riyanarto Sarno[2], Yutika Amelia Effendi[3]
[1]Department 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 human-related 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_j), where, i = 1,2, m ... and j = 1,2, ... n.

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

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

$$r_{ij} = \begin{cases} \dfrac{x_{ij}}{Max_i \ (X_{ij})} & if\ j\ is\ benefit\ criteria \\ \dfrac{Min_i \ (X_{ij})}{X_{ij}} & if\ j\ is\ cost\ criteria \end{cases} \quad (2)$$

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

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

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).

$$V_i = \sum_j^n = 1\, W_j r_{ij} \quad (4)$$

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.

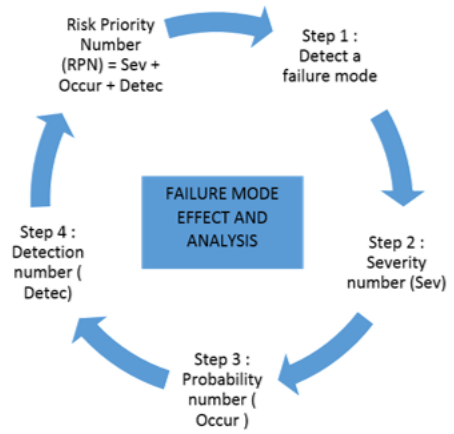

Fig.1. FMEA cycle

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

EDM01 Ensure Governance Framework Setting and Maintenance	EDM02 Ensure Benefits Delivery	EDM03 Ensure Risk Optimisation	EDM04 Ensure Resource Optimisation	EDM05 Ensure Stakeholder Transparency
Align, Plan and Organise				Monitor, Evaluate and Assess
APO01 Manage the IT Management Framework	APO02 Manage Strategy	APO03 Manage Enterprise Architecture	APO04 Manage Innovation	MEA01 Monitor, Evaluate and Assess Performance and Conformance
APO05 Manage Portfolio	APO06 Manage Budget and Costs	APO07 Manage Human Resources	APO08 Manage Relationships	
APO09 Manage Service Agreements	APO10 Manage Suppliers	APO11 Manage Quality	APO12 Manage Risk	
APO13 Manage Security				
Build, Acquire and Implement				Monitor, Evaluate and Assess
BAI01 Manage Programmes and Projects	BAI02 Manage Requirements Definition	BAI03 Manage Solutions Identification and Build	BAI04 Manage Availability and Capacity	MEA02 Monitor, Evaluate and Assess the System of Internal Control
BAI05 Manage Organisational Change Enablement	BAI06 Manage Changes	BAI07 Manage Change Acceptance and Transitioning	BAI08 Manage Knowledge	
BAI09 Manage Assets		BAI010 Manage Configuration		
Deliver, Service and Support				Monitor, Evaluate and Assess
DSS01 Manage Operations	DSS02 Manage Service Requests and Incidents	DSS03 Manage Problems	DSS04 Manage Continuity	MEA03 Monitor, Evaluate and Assess Compliance With External Requirements
DSS05 Manage Security Services		DSS06 Manage Business Process Controls		

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 RISKS

No.	Risk Identification	Frequency of Events	Causes of Risk	Risk Impact
1	Damage to network device hardware	Low Probability	Hardware exposed to liquid attacks, natural disasters, and fires	Network hardware components cannot operate in generating network services for everyday business processes
			The hardware setup is not 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 instantaneously and instantly power outages in a rapidly repeatable time
			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
			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 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 unable to manage the employee's job requirements for Network Access
			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.)
			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 become temporarily paralyzed
			The temperature in the server room cannot balance the heat of the server	The server room temperature increases and makes the hot temperature propagate to the physical

No.	Risk Identification	Frequency of Events	Causes of Risk	Risk Impact
				server
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	Can not send / receive data and information from server / user	Certain Probability	The server is being interrupted	Internal applications and internal websites are inaccessible
			The server is being interrupted	Failure of internet access and data transmission
9	Software system exposed to virus attacks	Failure is almost inevitable	Out of dated antivirus	Software systems are vulnerable to incoming viruses
			Act of human error	Business 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
			Out of dated software	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
13	The corporate network is attacked by hackers	Remote Probability	Security system for network access is not good	Attack of bandwidth theft by Unauthorized User Privilege
			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 process of data access process	Very High Probability	The system applied for data access is interrupted	Data cannot be accessed when needed
16	Miscommunication between employees in the IT department	Moderately 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

PEOPLE		
A1	540	The occurrence of human error in office employees for the use of ICT equipment
NETWORK		
A3 & A5	60	There was a fatal damage to the network architecture (A3) & Network firms attacked by hackers (A5)
SOFTWARE		
A7	480	Software system exposed to virus attacks
HARDWARE		
A14	150	Connector cable on the network is not connected (broken)
DATA		
A28	100	Data theft and data 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

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

[1] 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.