JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Implementation of ISO 3100 for Network Hardware Resource Allocation At PT. Angkasa Pura Balikpapan (Case Study: Sultan Aji Mahmud Sepinggan Airport)

[1]Arthareza Raja Prihatama, [2]Indha Suci Ramadani,[3]Joy Nashar Utama Jaya
[1]arthareza_raja.18@stmik-borneo.ac.id, [2]Indha_suci.18@stmik-borneo.ac.id,[3]joy.nashar@stmik-borneo
STMIK Borneo Internasional
Sistem Informasi, Balikpapan,Indonesia

Abstract : *PT.Angkasa Pura or more known as Angkasa Pura Airports is a state firm is a pioneer in Indonesia as a airport that opens commercialy since 1962. since then the firm has been growing so fast to have a branch in almost every major city in Indonesia, particularly in Balikpapan named Sultan Aji Muhammad Sepinggan International Airport, with an infrastructure that is huge and wide it also needs network infrastructure structured and efficient in everyday operational event. Every hardware that belongs in office or inside the airport itself must be working normally each day, no exception wheter it is for private or public must working normally each day. That is why, The role of IT RISK MANGEMENT is very important to taking care IT related problems in PT.Angkasa Pura. the purpose of this journal is to looking for an application regarding Angkasa Pura system information, on how to anticipate IT Risk. the presence of IT Risk Management on a company, especially PT.Angkasa Pura will surely helps to taking choices made that wiloccur,while occur and after occuring event. This journal will be presentating imagery about resource allocation for hardware that connected to the Network using ISO 31000 Framework. Framework ISO 31000 is to be used in this journal for guidelines for implementing risk management choices and supporting the standart to achieve the goal and taking care of Risk Management in a Company*

Keywords : Information, ITInfrastructure, Network, Risk Management.

I. INTRODUCTION

A. BACKGROUND

The rapid development of Information Technology (IT) helps humans to be faster and more efficient with all the problems that arise every day, Indonesia itself is no exception with the impact of the wave from the following technological developments. Where the field of Information Technology is widely used to organize and process resource data quickly and safely with the aim of minimizing existing threats of damage.

Nor does the Implementation of Information Technology also target companies such as PT. Angkasa Pura II in Balikpapan with Sultan Aji Mahmud Sepinggan Airport in general as follows:

1. Create a stable and secure network
2. Protecting private and public networks
3. Maintain and maintain existing hardware at the airport and office
4. Create a new network for new sections in company-owned areas if needed
5. Allocate new hardware resources to replace new ones

The use of information technology in a The company is very important, especially at PT. Angkasa pura. This is to support business processes and improvement of the technology service system used in the company. Use of technology effective and efficient information will help work becomes faster and easier for worked on. But behind the desired job in order to maintain the quality of service, always available impact on the risks of using IT. IT risks can arise from the planning process implementation and evaluation of IT in every process business (Pratama, 2019). Risk can happen only, because the risk can not be known when happens and is uncertain. Therefore, risk management must be carried out well. Risk management can help to minimize, prevent, and deal with problems that emerging.

B. Problem Formulation

Based on the background that has been described, the formulation of the problem is as follows:

1. What is the probability of damage to hardware or network assets at PT. Angkasa Pura?
2. How to analyze the possible risk of damage to hardware and network assets at PT. Angkasa Pura?
3. How is the framework applied to the company PT.Angka Pura based on the ISO 3100 framework?
4. What are the results of the risk evaluation at the PT.Angkasa Pura company?

C. Purpose

The purpose of making this journal is to produce a risk management implementation document on the allocation of network hardware resources using the ISO 31000 framework design.

II. Literature Review

Network resources or network resources are hardware (hardware) that will be connected to the network system. Hardware on the computer includes memory, hard disk, printer and so on. Usually, in a company, of course, computer tools are used together or commonly referred to as resource sharing. Sharing resources serves to be able to share data or information between computers. The existence of this resource sharing, users can easily share hardware where its use can be more efficient. The use of these resources cannot be separated from the risks to their use.

In general, risk can be interpreted as a possibility that will occur from an event or the impact of that possibility. In information technology itself, risk is the end result of asset value and the vulnerability of a system to threats that arise in the company. All activities or activities both within the organization or company will of course have risks that must be faced because the risks contain uncertainty. Risks can occur due to lack of information about things in the future.

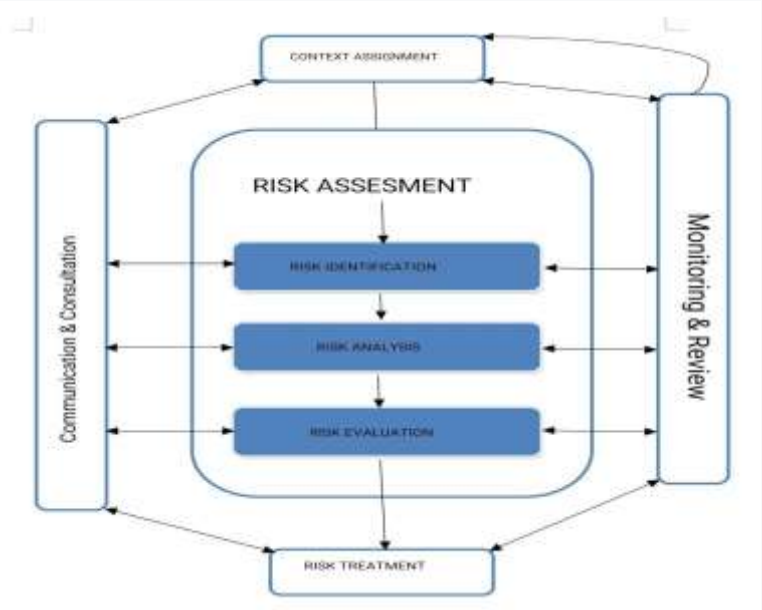
The types of risks can also be distinguished based on the consequences, as follows.

1. Unacceptable Risk, which is a risk that is eliminated or if possible transferred to another party because it is unacceptable.
2. Undesirable Risk, which is a risk that requires handling / risk mitigation to an acceptable level.
3. Acceptable Risk, namely the type of risk that can be accepted because the impact is still within acceptable limits.
4. Negligible Risk, which is a risk whose impact is so small that we can ignore it.

Risk management is a process within the company carried out by company managers to assess and make appropriate decisions on all risks to increase the likelihood of success or avoid or reduce the possibility of failure that will occur in the future. An assessment of this management risk is the identification of vulnerabilities or threats to the information resources that exist in the company in order to avoid or reduce any risks that will occur both from a financial standpoint, the achievement of appropriate business goals, as well as the response that will be taken to the impact of these risks.

Risk management is an iterative process. That is, the corporate environment is an environment that will continue to change which will cause the emergence of new threats or risks. In supervising risk management, companies must maintain a balance of products produced, costs incurred, effectiveness, and the values of data information that must be protected. Companies must make the right decisions based on the possibility of these threats, data and others. A risk management is designed and built within the company not only for risk identification.

However, the risk management system must be able to measure and predict the impact of these risks. The end result is in the hands of the manager whether the risk is still acceptable or not.International standard risk management refers to ISO 31000. This standard describes a risk management implementation framework starting from risk identification, risk analysis and risk evaluation as Figure 1. Figure 1 describes a simplified version of the ISO 31000 risk management process. The key stages in the process are represented as risk assessment and risk management. (Abisay, 2014)



Picture 1.IT Risk Management Process

IT Risk Management Function

Some of the functions of the existence of IT risk management are as follows

1. To provide an understanding of good decision-making, and management so that there is little possibility of risk
2. Save time, cost and effort by using tools for business risk
3. Integrating IT management on business risk into overall risk management
4. Assist the company in understanding what the risks to the company are and the risks and tolerances that are accepted

Benefits of Risk Management for Companies

The existence of risk management in a company can help companies improve their performance and deal with conditions that could be detrimental to the company. Some of the benefits are as follows:

- The failure of the threat can be prevented so that the losses are not too large
- Improve public image, which means it can protect the company from pure risk
- The existence of information provided to the management of the company about changes in products, markets, business environment and others needed in the risk management process
- Can calculate and measure the amount of risk exposure and determine a more precise allocation of sources of funds as well as risk limits

PT. Angkasa Pura, which is an airport company, has certainly applied various resources to information technology as a support for its business processes, where in its use, users must manage their information technology properly in order to prevent or avoid dangerous risks.

III. Discussion

A. ISO 3100 . Framework

The results of the observation process carried out within 2 (two) days at Sultan Aji Muhammad Sepinggan Airport, and even though they think about determining the next best step to reduce the risks that may occur.The ISO 3100 framework explains that leadership and commitment to the SAMS Airport board of directors have responsibility for the management and supervision of all Information Technology assets located in the SAMS Area.

The first, looking at the results of observations on assets and systems as well as IT networks in the airport area and airport offices. And with discussions conducted with one of the airport IT staff, we researchers were able to plan for overcoming risks based on ISO 3100 also stated for the integration of risk management depending on the understanding of the different structures depending on the destination, target and from Sultan Aji Muhammad Sepinggan Airport.

Second, understand and analyze the company and its context regarding the purpose of implementing ISO 31000, which is to provide guidelines on managing risk management in organizations in general, the standards used for all types of risks including business continuity, market, currency, credit, operational and information security risks.

Third, the allocation of IT resources, with many ways that can be done to limit information security risks can be very influential to carry out the next stage in the implementation of ISO 31000, in ISO 31000 the SAMS Airport director must ensure the right resources for the risk management section, so that it can cover not only individuals, skills, experience, competencies, methods and organizational processes. SAMS Airport is also required to consider the ability of its competent staff to handle risks before they occur and the constraints that occur on IT assets in the SAMS Airport Area.

Fourth, improvement and maintenance to adjust conditions to minimize risks that may occur in the system network or hardware assets in the airport area, the director must also supervise all recent changes to assets or network systems at the airport, both positive and negative. The Director must also make improvements, adjustments, adequacy and effectiveness of the ISO 3100 framework so that it runs well and is well integrated. The slightest gap that appears will cause problems both small and big in the future. After the implementation goes well, the improvements made will also contribute significantly to the security side of the network and the growth of the company or airport.

B. Result of risk observation

The results obtained from risk identification were carried out using observations and a little discussion with airport IT staff. With the results issued and classified into 3 risk scopes, namely:

	Risk Identified	**Yes**	**No**
1	User Used Service	31	0
2	Hardware Equipment	19	12
3	Data Corrupt	19	12
4	Discontinued Maintenace	31	0
5	Network Disconnected	31	0
6	Hacking to PC	3	28
7	Virus attack (Soft)	19	12
8	Virus attack (hard)	3	28
	Disaster Risk	**Yes**	**No**
1	Terror or Theft	31	0
2	fire	31	0
3	earthquake	31	0
4	Tsunami	31	0
5	electricity	31	0

6	flood	31	0

Table 1.1 *Distribution of the results of observations and information in Risk Identification*

Data table 1 attaches almost all the risks that have been successfully identified and can be classified into categories that have been matched. With each risk there are some staff opinions that are not affected by the risk. Like point 2 Hardware Equipment, this is because each IT staff has their own duties.

In the case of disaster risks, some of these risks can occur because of the position that is influenced by the landscape where SAMS Airport stands, namely being on the seafront which allows earthquakes, fires can occur instantly. Things like theft have a low probability because the airport security system is high and has security and cctv available 24 hours.

The results of the identification obtained by the researcher understand the risks that occur, the risks that can occur as a result of the interaction between the system used and the user where each party has different interests. Which is the main point where the potential risks and opportunities most often occur.

C. Risk Observation Analysis

The results of the observations that have been made are analyzed with 2 types of values. Namely the probability value (the possibility of this risk occurring) and the effect value (the effect that will be generated on the IT Risk plan). Tables 2.1 and 2.2 show the types of risks that have been identified and classified into the 2 points above.

No	Identified Risk	Probability	Effect
1	User Used Service	3	High
2	Hardware Equipment	2	Medium
3	Data Corrupt	1	Low
4	Discontinued Maintenace	2	Medium
5	Network Disconnected	2	Medium
6	Hacking to PC	2	Medium
7	Virus attack (Soft)	3	High
8	Virus attack (hard)	2	Medium
	Disaster Risk		
1	Terror or Theft	3	High
2	fire	2	Medium
3	earthquake	1	Low
4	Tsunami	1	Low
5	electricity	3	High
6	flood	2	Medium

Table 2.1 *Analysis of Probability Observation Value*

Each kind of risk value that exists in the probability value explains the possibility of this risk to occur if a failure to monitor causes the risk to occur.The existing probability results to control risk have a high threat value so that the improvement and maintenance of the staff must be increased through diligent monitoring and regular maintenance. By going through the procedures that have been set so that the risk can be considered neutral and returns to the Moderate status so that it requires adequate monitoring and maintenance.

No	Identified Risk	Probability	Effect
1	User Used Service	3	High
2	Hardware Equipment	2	medium
3	Data Corrupt	3	High
4	Discontinued Maintenace	3	High
5	Network Disconnected	3	High
6	Hacking to PC	3	High
7	Virus attack (Soft)	3	High
8	Virus attack (hard)	2	medium
	Disaster Risk		
1	Terror or Theft	3	High
2	fire	3	High
3	earthquake	3	High
4	Tsunami	3	High
5	electricity	3	High

6	flood	3	High

Table 2.2 *Analysis of Effect Observation Value*

In table 2.2, the effect that may occur has a level of risk that is still considered reasonable, only with regular maintenance and monitoring actions will allow airport IT resources to function properly and normally. However, with Network Disconnected points which have level 3 (High) periodic repairs must be carried out especially for the existing Public Wifi in the airport building.Negligence of system users that will cause fires, natural risks such as earthquakes, tsunamis and floods are external threats, asset theft is also an external threat that can be prevented with a reliable security system.

D. Evaluation of Risk Results

Evaluation Aims to see the risks that are considered prioritized for prior repairs or more periodic maintenance, risk evaluation can be seen in table 3.1

No	Identified Risk	Skor Nilai	Prioritas
1	User Used Service	6	1
2	Hardware Equipment	4	3
3	Data Corrupt	4	3
4	Discontinued Maintenace	5	2
5	Network Disconnected	5	2
6	Hacking to PC	5	3
7	Virus attack (Soft)	6	1
8	Virus attack (hard)	4	3
	Disaster Risk		
1	Terror or Theft	6	1
2	fire	5	2
3	earthquake	4	3
4	Tsunami	4	4
5	electricity	6	1
6	flood	5	2

Table 3.1 *Risk Evaluation Results*

IV. Conclusion

A. Conclusion

From the results and discussion described above, it can be seen that the risks from information technology threats that come from internal and external parties in the development of a company are one of the references for companies to be better at managing or supervising all threats that are visible or invisible in the company. the company's own assets, especially important assets such as hardware and the company's network system, where one part of the malfunction can cause temporary paralysis of the information system running at SAMS Airport.

SAMS Airport itself is one of the airports under the auspices of PT. Angkasa Pura II (Persero) which is located in the city of Balikpapan. It has a sophisticated and capable information system where out of 8 points the probability of a threat that endangers airport IT only 2 points that reach a high value which is still considered high. good and does not require high-level supervision or maintenance, in terms of work and IT skills, 5 Points that are in the Medium value are a good thing because this requires IT to check and maintain properly sometimes like once a week to conduct a survey where Hardware used at the airport is still considered suitable for use.

B. Suggestion

Risk is something that can never be avoided, especially where there are consequences from these risks, in large companies this is very important to be monitored, where this uncertainty can cause companies to lose profits significantly with things that need to be considered as .

a) The company must monitor and control IT Risk threats as small as possible.
b) Conduct weekly meetings for supervision of company assets including hardware and office system networks
c) Maintaining the factors that support the implementation of ISO 3100 and IT Risk Management by asking for encouragement from the Director of the airport.

REFERENCES

[1]Abisay, George, Terry & Nurhadi, 2014. 'RISK MANAGEMENT AT SOEKARNO HATTA AIRPORT BASED ON ISO 31000', *UMM e-journal*, pages 117-118

[2]Erlika, Yeni, Herdiansyah, Izman, Muhammad, Mirza, Haidar, A 2020,' Analysis of IT Risk Management at Bina Darma University Using ISO31000', *GLOBAL INFORMATICS SCIENTIFIC JOURNAL*, VOL. 11 No. JULY 01 2020, pages 57-60
Network Resource Sharing Administration, viewed May 24, 2021, http://www.sibro21.org/2016/11/administration-berbagi-source-daya.html

[3]Pratama, Ananda, Randito 2019,' IT RISK MANAGEMENT PLAN USING ISO 31000 AT PT ANGKASA PURA 1 SURABAYA', *FACULTY OF TECHNOLOGY AND INFORMATICS, STIKOM SURABAYA INSTITUTE OF BUSINESS AND INFORMATION*, viewed 24 May 2021, http://repository.iddinamika.iddinamika. /id/eprint/3720/1/15410100183-2019-STIKOMSURABAYA.pdf

[4]Cahyono, Dwika, Ariya, W, F, Agustinus, Mahardika, Bima, Krisdana 2019,' RISK MANAGEMENT OF INFORMATION TECHNOLOGY USING ISO 31000 : 2018 (CASE STUDY: CV. XY)', SEBATIK 1410-3737, page 1