International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Risk Management & Mitigation Plan for Data Center Environment

Jarot S. Suroso, Alkaton Sutikno, Friska Giovanny Br. Ginting, Natasha Angelica

Abstract*: To ensure company stability in running a business, the management team of the company must be aware of risks that could arise under various condition. These risks should be identified and mitigated as early as possible, before its effect the company. No matter what resource its affected, either core or support resource risks must be mitigated to avoid loss and damage to the company. Data Centre is one of the core resources of a company; it keeps the company information and used daily in the company. If by any causes, the data center could not be accessed or function; normally, it would cause a great loss to the company. This paper discussed the used of Facilitated Risk Analysis and Assessment Process *(FRAAP) technique to list and mitigate risk to the company data center. There are four steps of FRAAP technique used in this paper:* creating *risk description list, creating a risk sensitivity profile, creating risk exposure rating, and creating mitigating control list. The used of FRAAP technique, resulted in identification of two type of risk which are confidentiality and availability. The mitigation plan in this paper, cover the steps planned to mitigated risk resulted from information leak (Confidentiality); ex. hacking, virus, Etc. and natural disaster (Availability); ex. Flood, earthquake, fire, Etc. These planned mitigation steps are divided into three lists, which are: Risks response, Emergency Response Steps, Recovery steps, and restoration steps of the company data center.

Keywords: Risk Assessment, Risk Mitigation, Data Center, FRAAP, Company Risk

I. INTRODUCTION

In the evolving services provided in this era, the requirement from both business and customer has created new demands. The demands are to make information available at all times or at least accessible. This demand for information availability will be a mandatory element in the organization no matter what obstacles are there.

The information must be available either during regular business operation and when some problem occurred. The problems itself may strike the organization in the form of a hacker, human error, technical problem or even natural disasters. No matter what the problem the organization encountered, information must be accessible at all time. This affect expectation for Data Centers to function normally to support the organization business.

The data centre was developed related to data security as one of the assets of the organization in addressing data management for operational purposes as secondary storage media and data distribution. Safety management is part of the framework of the data centre that should be assessed by the manager to determine whether compliance with the standards so as to minimize the likelihood of the risk of adverse effects on the organization.

This paper discussed the risk assessment and risk mitigation plan to ensure that the data centre will function normally in any condition possible so that the organization business could run without any problem. This plan ensures that the IT of the data centre is resilient against threats. It led to the expanded field of Business Continuity Management which designed to provide telecommunication, people, and services to include in all critical area of the Data Center.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
Jarot S. Suroso*, Information Systems Management Department, BINUS Graduate Program – Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia. Email: jsembodo@binus.edu
Alkaton Sutikno, Information System Management Department, BINUS Graduate Program - Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia 11480. Email: alkaton.sutikno@binus.ac.id
Friska Giovanny Br. Ginting, Information System Management Department, BINUS Graduate Program - Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia 11480. Email: friskaginting16@binus.ac.id
Natasha Angelica, Information System Management Department, BINUS Graduate Program - Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia 11480. Email: natasha.angelica@binus.ac.id

II. LITERATURE REVIEW

A. Risk and Risk Management

Risk is a term used to described uncertain events which might affect the objective of a project either negatively or positively [1]. The definition of the term which itself may vary, it depends on the perspective of each individual [2]. In information technology, the risk is identified by potential number for every module. Risks should be identified in advance since risk could result in a possibility of loss [3].

Risk	Definitions
Pure risk	A risk which has chance of loss or no loss. *Example*. A building may get affected by fire or not. These are best covered by insurance
Speculative risk	Involves chance of gain/loss. *Example*. A builder may take a risk by promoting a new venture depending upon the prevailing conditions in the vicinity of proposed project, but it may bring him gain/loss.
Fundamental risk	These are external to a project and which, if they materialise, would be on a large scale and cannot be prevented. These risks are associated with major natural, economic, political or social changes and generate large scale losses. Examples are: Floods, earthquakes, fluctuation of exchange rates, etc. This risk may or may not be insurable.
Particular risk	These are project specific risks and are identified within the parameters of a project and can be controlled during the implementation of a project, e.g. quality risks, safety risks, legal risks, etc.

Source: Project Risk Management, D Van Well-Stam et al., Kogan Page Publications, 2003.

Fig. 1 .Risks Classification [1].

In order to identify risks in advance, risk management is done by the related parties (IT, Manager, Expert, staff/ users, etc.). If done effectively, risk management protects the organization assets, reduce loss, and manage cost-effectively based on the mission or objective of the organization [4]. Risk management is a process done continuously; however, to get the best results, it should be implemented at the earliest stage possible in any project [1]. Remember that the points of risk management have to be aligned with the organization goals and strategy [5].

B. Risk Mitigation

Risk mitigation is one of the most important activities that need to be done in Information Technology [6]. A risk mitigation propose is to eliminate, reduce and manage risks to acceptable levels [7]. Decision taken in risk mitigation involves recognizing, generating alternative solutions, choosing among the solutions, and implementing them [8]. To get the most of it and effectively done, a risk mitigation process must be done continuously (Monitoring, assessing, and adjusting) based on the existing risks profile [9].

Remember that mitigating risk does not mean that the risks are entirely gone, but it does reduce the probability of the risks happening. The biggest challenge in processing with risks mitigation is to identify the root cause. Risks mitigation for every risk that might happen and the response planned must be recorded in the risk register. These mitigation plans could change or develop some options in the process [10]. There are five risk mitigation handling options [7]:

1. Assume/Accept
2. Avoid
3. Control
4. Transfer
5. Watch/Monitor

C. Information System Security

Information system security is an essential point in organizations these days. Any risks that associated or impacting the information systems of an organization could result in dire consequences for an organization [11]. IS Security does not focus solely on the technical aspects as a computer or technology is operated by humans [12].

Information Security does not mean that your organization information is private. Having good security is what give your organization information privacy [2]. The objective of IS Security could not be met just by technical and procedural protection. In order to achieve the IS Security objective, it is important to educate every person in the organization about defending the organization against IS Security attack [11]. It is essential to keep working on the organization security, as there is a need for the organization to overcome the future challenge in IT and Security.

D. Business Continuity Management

Business Continuity Management (BCM), refers to the ability and capability of the organization managements to identify any threats to the organization. Other than identifying, providing effective response to safeguard the organization interest, brand and value are included in BCM [13]. At first, BCM was started with Disaster Recovery Planning (DRP). Along the years, it develops into Business Continuity Planning (BCP) which cover the whole organization [14].

The objective of BCM is to allow a business to process normally and managed under adverse condition according to the risk management considerations and crisis management plans [15]. There are three core elements of BCM [16]:

1. Crisis management and communications
2. Business resumption planning
3. IT disaster recovery addresses

In BCM planning, there are seven planning phases in which one of them is concerning risks analysis. In this phase, risks, vulnerabilities, and probabilities are analyzed in detail. This phase is one of the key elements of an organization BCM [17].

E. Data Center

A data center is known as the server farm or the computer room, the data center is where the majority of servers and storage of an enterprise located, operated and managed. A Data Centre has four primary components [18]:

1. White space: Usable raised floor environment or in the case for a data center that does not use a raised floor in its environment, white space shows a usable environment in the data center. White space is usually measured in square feet units.
2. Support infrastructure: support infrastructure is any additional space and any equipment needed in order to support the data center operations. This support infrastructure might include power transformers, uninterruptible power source (UPS), computer room air conditioners (CRACs), remote transmission units (RTUs), etc. In some data center with a specific condition, support infrastructure could require and use space that is 4 or 6 time more than white space.
3. IT Equipment: for Datacenter, it means any equipment needed in order to manage the data center. Some of the equipment are rack, storage, servers, cabling, etc.
4. Operations: in this case, operations mean the operations staff who responsibility is to ensure that the systems are maintained, operated, upgraded and repaired properly and when necessary. In most Companies, the operations staff responsible for the support system and technical operation staff are different and split into different divisions.

III. RESULT AND DISCUSSION

In this paper, the technique used for analyzing and assessing risks regarding the data center is done using FRAAP. Facilitated Risk Analysis and Assessment Process (FRAAP) is a structured risk assessment process which approach is used to manage a risks project in a short timeframe [19]. The organization internal experts do the FRAAP technique. It takes advantage in the sense that no one knows your systems, application, or business better than the people who develop and manage them[20].

The FRAAP technique is implemented for assessing the risks and how to mitigate them in order to ensure that the data center to function normally in any condition. The FRAAP process has four steps [19] :

1. Creating Risk Description List
Describing the risks and resource according to the C-I-A-A risk type (confidentiality, integrity, availability, and Accountability).

Table 1. Risk Description List

#	Risk Type	Risk Description List	Resource
1	Confidentiality	The information regarding company datacenter access got leaked	Employee
2	Availability	Data Centre unable to be accessed due to electrical failure or a natural disaster (Flood, Earthquake, etc.)	Datacenter Computer, Server, UPS, and other IT Equipment

2. Creating a Risk Sensitivity Profile
Describing the severity of the impacted resources and deciding each C-I-A-A sensitivity level for each resource.

Table 2. Risk Sensitivity Profile

#	Resource Impacted	Sensitivity Desc	Confid	Intg	Avail	Acct	Overall
1	Employee	The leak of data center information access to any unauthorized personnel could cause various threat to happen	High	High	High	High	High
2	Datacenter Computer, Server, UPS, and other IT Equipment	A sudden electrical failure or occurrence of natural disaster could result in loss of information that might have a significant impact on the company business	Low	Moderate	High	High	High

3. Creating Risk Exposure Rating
Breaking each risk previously listed into vulnerability, threat and threat category of each resource vulnerability. The threat category used is Natural disaster, Infrastructure failures, Internal abuse, Accidents, External targeted attacks and External mass attacks.

Table 3. Risk Exposure Rating

#	Risk Vuln. Desc	Threat Category	Threat Activity	Like	Sev	Sens	Overall
1	Electrical Failure	External Mass Attack	Failure to power up any important equipment of the data center cause organization business to stop and cause some data loss	Low	High	High	High
2	Earthquake, Flood, Fire, Etc.	Natural Disaster	An occurrence of natural disaster is always unexpected. The effect of a natural disaster could cause physical damage and loss of data	Moderate	High	High	High
3	Unauthorized Access	Internal Abuse	A company internal personnel stole, change, or spread an important/confidential information	Moderate	High	High	High
4	Unauthorized Access	External Targeted Abuse	Virus attack, hacking, or any attempt done by external personnel which target the company data center	Low	High	High	Moderate

4. Creating Mitigating Control List Describe the mitigation control for each risk found and listed. Each control is categorized into one of these types: preventative, detective, or responsive.

Table 4. Mitigating Control List

#	Brief risk desc	Control Type	Control Description
1	Failure to power up datacenter equipment	Preventive	Installing an energy monitor to spot a buildup static electricity
2	Failure to power up datacenter equipment	Responsive	Turning on the electrical generator to supply the needed electrical current to data center equipment in minimum time
3	Earthquake, Flood, Fire, Etc.	Preventive	Installing Temperature control, humidity control and do scheduled back up data to a cloud environment

4	Unauthorized Access	Preventive	Installing an antivirus program, ensuring the operating system is up to date, doing scheduled scanning to detect any issues immediately

The details of risks response, recovery and restoration steps are of the risk's management and risk mitigation regarding data center are as follow:

1. Creating Awareness The first results present from the summary of risk assessment and mitigation plan for PT XYZ data center environment is creating awareness. When exposed to the results, every member of the organization will develop internal awareness at multiple levels of management. This awareness will make the organization management able to allocate the appropriate resources, process, develop and deploy tools in order to manage risk. One example of creating awareness of the risk in the data center environment involved the use of:
   - Emergency Response Steps

Table 5. Emergency Response Step

No	Abnormal Condition	Operational Activity
1	Earthquake >8,5 SR	No response needed
2	Flood	Turn off the power if allowed, no response required
3	Local Fire (Facilities DCO not affected	Turn off the power if allowed, no response required
4	DOC facility is exposed to the impact of fire	Turn off the power if allowed, no response required
5	Computer Virus	Isolation of virus outbreaks
6	Sabotage/piracy	Hacking response

- Recovery Step

Table 6. Recovery Step

No	Abnormal Condition	Impacted Damage	Recovery Step Activities
1	Earthquake >8,5 SR	Anything	Move the operational to Head Quarter
2	Flood	Anything	Move the operational to Head Quarter
3	Local Fire (Facilities DCO not affected	Anything	Resume activity after execution Health & Safety Procedure
4	DCO facility has exposed the impact of fire	Anything	Move the operational to Head Quarter
5	Computer Virus	Small	Personnel standby Re-arrangement
		Big	Move the operational to Head Quarter
6	Sabotage/piracy	Anything	Execution process recovery hacking post

- Restoration step

Table 7. Restoration Step

No	Abnormal Condition	Big Damage	Restoration Step Activities
1	Earthquake >8,5 SR	Anything	Move to facilities DCO, Backup & Restore
2	Flood	Anything	Move to facilities DCO, Backup & Restore
3	Local Fire (Facilities DCO not affected	Anything	N/A
4	DCO facility is exposed to the impact of fire	Anything	Move to facilities DCO, Backup & Restore
5	Computer Virus	Small	N/A
		Big	Move to facilities DCO, Backup & Restore
6	Sabotage/piracy	Anything	N/A

2. Preventing Business Continuity RiskThe second result is preventing business continuity risk. The next important thing in Business Continuity is prevention. The focus is on reducing risk and/or impact of the mitigation plan so the business can run well as usual. Prevent comprises four critical processes:
   - Risk Identification:Enumerating the cause of potential issue related to data centre environment.
   - Risk Assessment:Evaluating the impact of potential disruptions.
   - Risk Treatment:Prioritizing the cause of potential disruptions and developing strategies for reducing and/or mitigating the impact of the business.
   - Risk Monitoring:Monitoring any changes that may occur and cause changes in the risk levels (Increasing or decreasing) daily.
3. Remediating Risk OccurrenceThe third result is remediating risk occurrence. An organization needs a course of action to follow in order to recover from a disruption when it occurs, while the organization takes steps in the prevention stage to reduce its exposure risk cannot be eliminated.
4. Fostering Knowledge Management The fourth is knowledge management. The purpose of knowledge management is to learn from business disruption since they are an indication that the existing plans and contingencies in place may not be adequate. The Business Continuity Plan addresses knowledge management by conducting an annual key performance indicator evaluation for management.

IV. CONCLUSION

No company activities or resource could be wholly protected from any disturbances or damages or risk, especially if the damage is at the center of the company's business, which is known as the data center.

These disturbances or damages or risk could originate either from nature or people, intended or not intended. Risks that arise affect not only a company's technological capabilities but also its business operations. If this is not explicitly handled, it affects not only operational risk but also reputational risk and a reduction in the end-user quota.Effective risk reduction must be supported by the following:

1. Active management supervision;
2. through business impact analysis and risk assessment;
3. Drawing up an appropriate business continuity plan;
4. Testing BCP; and
5. An examination is carried out by the internal auditor.

As described in this document, the results of the risks mitigation plan focused on how to mitigate risk resulted from information leak and natural disaster (flood, earthquake, fire, etc.). This risk mitigation plan is necessary to keep the company's condition stable and to ensure that the company's business work normally without any problem.

REFERENCES

1. K. Srinivas, "Process of Risk Management," in Process of Risk Management, IntechOpen, 2018, pp. 0–16.
2. M. W. Harkins, Managing Risk and Information Security. Apressopen, 2016.
3. B. Anthony and N. C. Pa, "A review on tools of risk mitigation for information technology management," J. Theor. Appl. Inf. Technol., vol. 81, no. 1, pp. 92–101, 2015.
4. S. Al-Dhahri, M. Al-Sarti, and A. Abdul, "Information Security Management System," Int. J. Comput. Appl., vol. 158, no. 7, pp. 29–33, 2017.
5. S. Shokouhyar and F. Panahifar, "An information system risk assessment model : A case study in online banking system An information system risk assessment model : a case study in online banking system Sajjad Shokouhyar *, Farhad Panahifar , Azadeh Karimisefat and Maryam Nezafatbakhsh," no. January, 2018.
6. N. ChePa, B. Anthony Jn, R. Nor Haizan, and M. Azrifah Az, "A Review on Risk Mitigation of IT Governance," Inf. Technol. J., vol. 14, no. 1, pp. 1–9, 2015.
7. N. Katende, "Implementing Risk Mitigation, Monitoring, and Management in IT," Comput. J., no. July 2017, 2017.
8. N. Che Pa, B. Anthony Jnr, Y. Y. Jusoh, R. N. H. Nor, and T. N. Mohd Aris, "A risk mitigation decision framework for information technology organizations," J. Theor. Appl. Inf. Technol., vol. 95, no. 10, pp. 2102–2113, 2017.
9. No Title. .
10. R. Ahmed, "Risk Mitigation Strategies in Innovative Projects," in Key Issues for Management of Innovative Projects Downloaded, no. 2017, 2017, pp. 267–322.
11. Z. Shouran, T. K. Priyambodo, and A. Ashari, "Information system security: Human aspects," Int. J. Sci. Technol. Res., vol. 8, no. 3, pp. 111–115, 2019.
12. O. Safianu, "Information System Security Threats and Vulnerabilities : Evaluating the Human Factor in Data Protection Information System Security Threats and Vulnerabilities : Evaluating the Human Factor in Data Protection," no. September, 2016.
13. E. Krell, Management Accounting Guideline: Business Continuity Management. 2006.
14. L. L. Kim and A. Amran, "Factors Leading to the Adoption of Business Continuity Management (BCM) in Malaysia," Glob. Bus. Manag. Res., vol. 10, no. 1, pp. 179–196, 2018.
15. The GSMA, "Effective Business Continuity Management Guidelines for Mobile Network," ASHA Lead., vol. 22, no. 8, Aug. 2017.
16. K. Penuel, M. Statler, R. Hagen, and P. Mcilwee, "Business Continuity Management," in Encyclopedia of Crisis Management, 2013.
17. G. M. Heng, "Business Continuity Management Planning Methodology," Int. J. Disaster Recover. Bus. Contin., vol. 6, no. November, pp. 9–16, 2015.
18. M. Bullock, "Data Center Definition and Solutions Data Center topics covering definition, objectives, systems and solutions.," 2009. [Online]. Available: https://www.cio.com/article/2425545/data-center-definition-and-solutions.html#what. [Accessed: 03-Feb-2020].
19. E. Wheeler, Security Risk Management Building an Information Security Risk Management Program from the Ground Up. Elsevier Inc., 2011.
20. thomas R. Peltier, Information Security Risk Analysis. Auerbach Publications, 2005.

Information system, competitive intelligence, knowledge management, computer network, e-learning, multimedia and research methodology.

Jarot S. Suroso is an Associate Professor of Magister Management of Information System at Bina Nusantara University Jakarta, Indonesia. His major research interests include management information system, competitive intelligence, knowledge management, computer network, e-learning, multimedia and research methodology.

Alkaton Sutikno Information Majoring student Information Systems Management of Magister Management of Information System at Bina Nusantara University Jakarta, Indonesia.

Friska Giovanny Br. Ginting Majoring student Information Systems Management of Magister Management of Information System at Bina Nusantara University Jakarta, Indonesia.

Natasha Angelica Majoring student Information Systems Management of Magister Management of Information System at Bina Nusantara University Jakarta, Indonesia.