ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 112

International Conference on Business, Economic, Social Science, and Humanities – Economics, Business and Management Track (ICOBEST-EBM 2019)

Design Business Continuity Plan of Data Center Using ISO 22301:2012

Rahadian Arief
Departemen Magister Sistem Informasi
Universitas Komputer Indonesia
Bandung, Indonesia
arief_fijcell@yahoo.co.id

Yeffry Handoko Putra
Departemen Magister Sistem Informasi
Universitas Komputer Indonesia
Bandung, Indonesia
tugasmsi.yeffry@gmail.com

***Abstract*—The purpose of this study is to design a BCP framework that adapts to the needs of the company. Research design using qualitative method. Data collection in this research using observations, interviews, and questionnaires. Stages in evaluating are planning research, determining the scope of the evaluation, data collection and processing, evaluation reports, and evaluation analysis. This design used ISO 23301 guidelines. From the results of research using the BCP framework shows that the Disaster Recovery Plan has not been formed as part of BCP. In this study, to evaluate Risk Assessment, Business Impact Analysis, and Recovery Strategy. The final results of the Risk Assessment explain the occupying business processes rank and influence the final results of the main Risk Assessment at ERP application and mailing system.**

Keywords—Disaster, Recovery, Risk Assessment, Business Impact Analysis, Datacenter

I. Introduction

PT XYZ is a BUMN company producing vaccines and antisera, currently developing into a Life Science. In helping the activities of them the role of information technology is very important, so it can facilitate activities, especially production, distribution, finance, mailing, customer relation, and etc. To know the governance impact from disaster, it is necessary to evaluate the management of information technology that runs through the evaluation of information technology in main data center which has been done by the assessment to evaluate the information technology related to impact information system.

Many studies have reported how to evaluation of information system as shown by Caesar Fajriansah [9], Humdiana [10], Andrea Giacchero [11], Francesco Giordano [11], Massimiliano M Schiraldi [11], Meshal Alabdulwahab [12], and Davor Filipović [13], Mate Krišto [13], Najla Podrug [13]. From the results of several studies above, that the assessment of IT governance is small, which becomes the differentiator of this research is done in Data Center, so it can be the related method in conducting the assessment of system implementation.

The purpose of this study is to measure the ability of PT XYZ to deal with disasters, especially in the Data Center section and evaluate the impact that will occur.

II. Research Method

This research used a qualitative method. The research begins by collecting the initial data needed, the data is obtained from internal company documents such as company policy, organizational structure, SOP, IT infrastructure, and existing disaster documentation. The company's internal data then used as input material in determining the scope of the BCP design that will be carried out. Then after the scope of the research is determined, data is collected on the possibility of threats and opportunities for potential disasters, both from internal sources and from external sources of the company, then the data is used as input in the process of identifying the possibility and potential threats to the company.

Furthermore, in the Risk Assessment analysis process that will produce a Risk Analysis using OCTAVE and to then be collected data to be processed in the Business Impact Assessment through interviews, or discussions with IT Managers. Based on the results of the Risk Assessment and Business Impact Analysis, the BCP strategy plan is selected to be the main reference in preparing BCP documents.

III. Results and Discussion

Based on the study of documents and results interviews obtained data about business processes, IS / IT conditions and risk analysis at PT.XYZ, then immediately formed Risk Assessment, Business Impact Assessment, and Strategy Plan.

A. *Risk Assessment*

Risk analysis using OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) can help in identifying the possible risks and threats that can occur from IT assets owned. The stages in the OCTAVE method are identifying critical assets, identifying security needs of critical assets, identifying threats, identifying security practices that have been carried out by the organization, identifying key components of IT and identifying technological vulnerabilities. Following are the outputs generated from each OCTAVE phase.

TABLE I. Table Risk Assessment

Risk ID	Risk	SEV	Cause of interference	OCC	RPN
R1	Server not running	8	Earthquake	2	160
			Flood	2	160
			Fire	2	160
			Damage of the building	2	160

Risk ID	Risk	SEV	Cause of interference	OCC	RPN
			Human Error	3	96
		7	Power Down	5	175
		7	Generator and UPS not working	5	175
R2	Server Performance Down	5	Processor *overload*	4	60
R2	Server Performance Down	5	RAM *overload*	4	80
R2	Server Performance Down	5	Storage overload	4	40
R3	Data damage on the server	7	DDOS attack to Server	3	84
R3	Data damage on the server	7	Negligence of Database Administrator	4	112
R4	Lost Data	7	Virus attack	2	42
R4	Lost Data	7	Negligence of Database Administrator	3	84
R5	Didn't have spare Datacenter	7	Didn't have spare Datacenter	10	700
R6	The Application get crash	8	Server Down	5	280
R6	The Application get crash	8	The power shutdown	5	360
R6	The Application get crash	8	Hacker attack	3	168
R6	The Application get crash	8	Viruses attack	3	168
R7	The Email server get crash	8	Server Down	5	280
R7	The Email server get crash	8	The power shutdown	5	360
R7	The Email server get crash	8	Hacker attack	3	168
R7	The Email server get crash	8	Viruses attack	3	168
R8	The data cannot be accessed	7	The power shutdown	5	70
R8	The data cannot be accessed	7	Server Down	4	84
R9	The data manipulated	9	The hacker manipulated the data	2	144
R9	The data manipulated	9	Username is used by others	2	144
R10	Data was stolen	9	The hacker steal the data	2	144
R11	Data was lost	8	Negligence of human	3	216
R11	Data was lost	7	Server crash	3	189

B. Bussiness Impact Analysis

At this stage the business impact analysis is by identifying Information System or Information Technology services with prioritizing the critical level of each service. The following is a prioritization of critical levels for each IT service owned by the organization.

TABLE II. BUSSINESS IMPACT ANALYSIS

Business Functional	Business Process Related Systems	Critical level	Description
ERP Service	ERP Application	High	This service supports business activities of the company which are related to Financial Accounting Dept., Accounting Management Dept., HRD and Supply Chain Dept.
CRM Service	CRM Application	High	This service supports the business activities of the company that are related to the Customer Relationship Management Dept.
Email Service	Mail server	High	The Email Server service is used to share information that is used by all employees of PT XYZ. Besides that, it is also used to exchange information with clients or people outside of PT XYZ.
Internet Service	Internet Service Provider	High	This service ensures internet availability by all employees.

C. Recovery Strategy

By looking at the risk assessment table, we can see that fires and natural disasters will result in lost power, that's a very high threat and must be anticipated immediately by build a Disaster Recovery Center in a safe place and far away from natural disasters.

TABLE III. TABLE RECOVERY STRATEGY

Incident	Impact	Improvement
Power Supply Failed	Server, ERP Application, Email Service, and Storage not running	Repair building power installation. Using power generator. Using UPS.
Fire	Shutdown power on Data Center Room	Call firefighters. Extinguishing the fire. Activated Data Center on Disaster Recovery Center.
Flood, Earthquake	Shutdown power on Data Center Room	Activated Data Center on Disaster Recovery Center.
Don't have Disaster Recovery Center	Data Center will not be active immediately.	Must build Disaster Recovery Center.

IV. CONCLUSION

From the analysis based on various obtained data, the analysis of the impact of disruption/disaster on the company is made based on the level of impact to and the likelihood. The final results of the Risk Assessment explain the occupying business processes rank and influence the final results of the main Risk Assessment at ERP application and mailing system. The highest rating is in fires, the backup of data center didn't have Earthquakes, Power Outages, and Human Errors, and the lowest level is in virus attacks, server hangs and full storage media.

REFERENCES

[1] ISACA, "Business Continuity Management Audit/Assurance Program," 2011.

[2] ISO 22301, "Societal security — Business continuity management systems — Requirements," 2012.

[3] ISO 31000:2009, "Risk Management - Princples and Guidelines," 2009.

[4] C. a. D. Alberts, "OCTAVE Method Implementation Guide V2.0, Pittsburgh, PA: Software Engineering Institute, Carnegie," 2005.

[5] B. Supradono, "Manajemen Resiko Keamanan Informasi Dengan Menggunakan Metode OCTAVE (Operationally Critical Threat, Asset, And Vulnerability Evaluation)," Media Elektrika, 2009, Vol 2, No 1, pp. 4-8,

[6] D. Stamatis, "Failure Mode and Effect Analysis (FMEA): From Theory to Execution, Milwaukee," 2003.

[7] ISO 22317:2015, "Societal Security, Business Continuity Management Systems - Business Impact Analysis," 2015.

[8] www.reliasoft.com, "Examining Risk Priority Numbers in FMEA," visited on 30/12/2017

[9] Fajriansah, Perancangan Business Continuity Plan Berbasis Risiko Pada Sub Direktorat Pengembangan Sistem Informasi, Direktorat Pengembangan Teknologi Dan Sistem Informasi, 2017.

[10] Humdiana, Perancangan Business Continuity Plan: Studi Kasus Pada PT.PAM, 2016.

[11] Andrea Giacchero, Francesco Giordano, Massimiliano M. Schiraldi, From Business Continuity to Design of Critical Infrastructures: Ensuring the Proper Resilience Level to Datacentres, 2013.

[12] Meshal Alabdulwahab, Disaster Recovery and Business Continuity From a Natural or Man-Made Disasters, 2016.

[13] Davor Filipović, Mate Krišto, Najla Podrug, Impact of Crisis Situations on Development of Business Continuity Management in Croatia, 2018.