Risk Analysis on the development of a Business Continuity Plan

Alexander Setiawan
Informatics Engineering
Faculty of Industrial Technology
Petra Christian University
Surabaya, Indonesia
alexander@petra.ac.id

Adi Wibowo
Informatics Engineering
Faculty of Industrial Technology
Petra Christian University
Surabaya, Indonesia
adiw@petra.ac.id

Andrew Hartanto Susilo
Informatics Engineering
Faculty of Industrial Technology
Petra Christian University
Surabaya, Indonesia
m26410008@john.petra.ac.id

Abstract—**In the era of globalization increasingly advanced enterprise engaged in the sale of concrete iron will execute business processes by using software, hardware, networking, and others. Judging from the condition and the current reality of this company did not rule out the occurrence of the risk due to the problems in terms of data security, data integrity, hard disk damage, IT business continuity process.**

In this research conducted a risk analysis of the entire area of IT and business processes within the company. As for the area to be analyzed by means of analyzing the business continuity that is based on the Standard ISO 27002: 2005 chapter 14, and analyze IT Domain and perform risk assessment and risk mitigation.

The risks are found is their dependence on outsourced programmers who acts as a consultant, so rarely do risk assessment in IT companies, the unavailability of a Disaster Recovery Plan and IT Security Plan, an evaluation of the permissions are less common, and no one specifically designated for IT management, lack of training or, and the absence of a standard or framework. The results of this risk analysis can help companies recognize and avoid the risks of what might happen and can avoid the danger of business continuity, so that the company can take action to prevent or deal with the risks that would happen.

Keywords—Business Continutity Plan; Disaster Recovery Plan; IT Domain; Risk Assessment; Risk Mitigation.

I. INTRODUCTION

Disaster is a natural occurrence, human deeds, or a combination of the two that occur suddenly. The result in a tremendous negative impact for continuity life. In the event of a disaster, the element is directly related to or affected must respond by taking effective remedial action Adjusted as well as restore the condition as before or become is a good [1].

Disaster in relation to disaster recovery plan is anything that disrupts the running of business processes than hampering a company in carrying out its function. Disaster generally deemed crippling if the disaster nullifies one or more of the following resources: human resources, facilities, communications, power, and access to information. In this case the business planning method continuity plan is very appropriate applied [2].

The Business Continuity Plan was created to prevent disturbance against normal business activity. Business Continuity Plan is designed to protect critical business processes from Failure / natural or man-made disaster and consequently the loss of capital. In relation to unavailability for normal business processes. Business Continuity Plan is a strategy to minimize the effects of interference and to enable business processes to continue take place.

Disruptive events are all forms of good security breaches that are Intentional or not that causes the business can not operate normally. Aim Business Continuity Plan is to minimize the effects of such disturbing events on the company. Aim the main Business Continuity Plan is to reduce the risk of financial loss and increase the company's ability in the recovery process as soon as possible of an event that disturb. Business Continuity Plan also helps minimize the costs associated with that event interfere with it and reduce the risks associated with it.

II. THEORETICAL BASIS

A. *Business Continuity Plan (BCP)*

Business Continuity Plan is a methodology which is used to create and approve a plan for defending the continuity of business operations before, during or after a disaster disturb [3].

Business continuity planning is made to prevent delays in normal business activity. Business Continuity Plan is designed to protect vital business processes from damage or natural or man-made disasters, and losses arising from the unavailability of normal business processes (routine, as usual). Business continuity plan is a strategy used to minimize the effects of disruptions and strives to re-run a business process company [3].

The purpose of BCP is to minimize the effect of the event or disaster in a company. The main benefits of business The continuity plan is to reduce the risk of financial and financial liabilities improve the company's ability to recover from

disaster or interruption as soon as possible. Business continuity planning should also can help minimize costs and reduce risk with respect to the event of the disaster [3].

BCP can be part of the company's learning efforts help reduce operational risk, related to management control weak information. This process can be integrated with improving information security and risk management practices.

Revealed that Business Continuity Plan (BCP) and Disaster recovery Plan (DRP) are helpful companies prepare for disaster recovery activities. But before the plan is made, it is very important that the risks and potential impacts can be well studied, this is the foundation of BCP and DRP [4].

B. Proce Business Continuity Plan (BCP) Process

According to Federal Financial Institutions Examination Council, there are 4 important processes in the business continuity plan, including [5]:

- Business Impact Analysis
- Risk Assessment
- Risk Management
- Risk Monitoring and Testing

The above four processes represent a continuous cycle that is need to be upgraded from time to time based on changes from potential threats, business operations, audit recommendations, and test results. In addition to this process should cover every critical business and technology function support it. Such as policies, standardization, and integrated processes into the overall process of business continuity plan [5]. Here are 9 steps to promote the Business Continuity Plan (BCP) : [7] :

- Visualize business functions top down
- Create items of tasks that are executed on a bottom-up basis.
- Prioritize work only on the main functions
- Create categories and organize problems into manageable parts
- Minimize risk, this is the main objective of the business continuity plan
- Organize staff to react during disasters
- Practice disaster event (simulation), so staff familiar with procedure response
- Sponsor / Champion, participation to demonstrate and communicate the importance of recovery plan
- Monitor supply chain and partner plan

C. ISO 27002 : 2005

The ISO 27002: 2005 in chapter 14 it discusses the relationship between IT disaster recovery planning, business continuity management and contingency planning, from analysis and documentation through plan testing. In ISO 27002: 2005 chapter 14 there are 5 points [6]:

- Including information security in the business continuity management process
- Business continuity and risk assessment
- Developing and implementing continuity plans including information security
- Business continuity planning framework
- Testing, maintaining and re-assessing business continuity plans

III. MODEL AND BUSINESS STRATEGY

Business continuity policy is an early stage of BCP in order to recognize business processes. This policy should be proactive and include preventive, detective and corrective controls. BCP itself is the most critical corrective control. The next step recognizes business processes through risk assessment to identify: The risks faced by each business unit, key business processes that must be re-operated quickly in the event of disruptions, cost-effective measures that can be proposed in order to address risks, assessments must be conducted by an independent party External or internal company whose job is to conduct assessment or audit) formally using a certain methodology. The steps taken for making the step BCP can be seen in Fig 1.

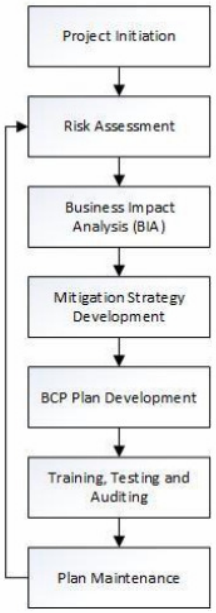

Fig. 1. The Step Business Continuity Plan (BCP)

Risk that threaten business continuity organizations can be reduced by applying Risk mitigation strategies. There are 4 (four) strategies that can be selected and implemented within the organization, such as:

1. Risk Acceptance. This strategy is not really part of the mitigation strategy because it accepts no risk will reduce the effects of those risks. But risk acceptance is part of risk

management. This strategy is a low cost management strategy, but it will cost money Recovery is high after the risk occurs.

2. Risk Avoidance. This strategy is the opposite of risk acceptance strategy, where this strategy can reduce risk to the lowest point with very high management costs, but the cost of recovery is low. The strategy is to turn off the system that has a high critical value. Can also move the system to a place away from the risk.

3. Risk Limitation. This strategy is the most common strategy used by business people strategies undertaken among them by doing how many actions to limit the occurrence of a risk. For example by doing daily backups of data businesses that have a high critical value.

4. Risk Transference. This strategy is done by transferring the risk to the other party and it is clear the transfer this risk is related to cost expenditure. One common example is insurance.

IV. EVALUATION OF IT ON RISK DOMAIN

Based on the interview data and sampling from the company side, then here are some risk factors faced by the company can be seen in Table 1.

TABLE 1. STANDARD RISK DOMAIN

Standard ISO 27002 : 2005	Risk Domain
Chapter 14.1.1 Including Information Security in the business continuity management process	• Existing IT only meet the needs only, there is no special budget for it. If the deficiency or any new damage will add new items. • Without the software, the work will be slower and the number of jobs that can be completed less because it has to do the recording manually. With the software it is easier to integrate related data and speed up workmanship.
Chapter 14.1.2 Business continuity and risk assessment	• IT strategy is owned because the business model of the company is not too demanding the formation of a specific IT strategy • There is but do not know when it depends on the board of directors. While this IT support has been able to meet the needs of the company • The programmer that is used now is outsourced programmer, the company does not have IT staff who act as programmer. If an outsider is requested as a programmer may be harmful to the company as it may cause data leakage.
14.1.3 Developing and Implementing continuity Plans including information security	• There isn't framework is used to underlie corporate IT • To restore a downed server usually takes 2-3 days. To recover damaged data takes about 2 days. • There is never any testing or precautionary measure because it focuses more on problem solving
Chapter 14.1.4 Business Continuity Planning Framework	• The framework is indispensable for the company and can be harmful if there is no framework
Chapter 14.1.5 Testing, maintaining and re-assessing business continuity plan	• Software developed due to changes or problems, but not developed according to the changing times • There are restrictions on permissions and backups, but no coding protection • Software development is only limited to maintenance if there is error in the software, because companies prefer to make new software more perfect than developing the shortcomings of old software

Risk assessment is obtained from the multiplication of likelihood value and impact value. To obtain the likelihood value and the impact value of each risk, several criteria are needed to assess the scale. Factors that can influence the occurrence of a risk (likelihood) are threat / threat factor and vulnerability factor. The criteria used to assess likelihood is the likelihood of the extent to which this potential vulnerability may cause or develop a threat. Can be rated as high or medium or low. Likelihood definition describes three assessments can be seen in Table 2.

TABLE 2. LIKELIHOOD DEFINITION

Level	Result
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised

Based on Table 2 of Likelihood Definition, an assessment can be made, as shown below:

- High: 8-10 (possibly a vulnerability can be a threat, very high and its control is still not effective)
- Medium: 5-7 (the possibility of a vulnerability can be a threat, not high and not low or can be said to be common and its control can still block vulnerabilities into threats)
- Low: 1-4 (possibly a vulnerability can be a threat, very small and its control can prevent or hinder it properly)

In addition to the likelihood assessment of how vulnerable a risk factor becomes a threat, it is also worth considering how often a vulnerability occurs and can pose a threat. The assessment can be seen in Table 3. Risk Probability of Occurrence

TABLE 3. RISK PROBABILITY OF OCCURRENCE

Probability range	Natural Language Expression	Probablity Value used for calculation	Numeric Score
90%-100%	It often happens	95%	5
68%-89%	Maybe it will happen	78,5%	4
51%-67%	May occur about half of the time	59%	3
21%-50%	Not how often happens	35,5%	2
1%-20%	Never happen	10,5%	1

The result of likelihood aspect assessment for all risks based on observation and confirmation result by company side can be seen in Table 4.

TABLE 4. EVALUATION OF RISK

ID	Risk Factor	Likelihood	Impact Probability	Result	Level Risk
1.	Data backup only physically and on site only, and never checked the results of backup or refresh data, so the IT system is not safe	7	4.75	33.25	High
2.	There has never been Risk Assessment in the IT field so it is not so understand the risk of IT well. The maintenance process is only done when the problem occurs (handling is not prevention).	9	3.45	31.05	High
3.	Staff controlling IT is an outsource programmer who acts as an IT consultant.	8	3.25	26.00	Medium
4.	There is no written agreement between the company and the employee who has stopped related to information security and company data.	7	3.08	21.56	Medium
5.	No training or security zones related to security and incidents within the company.	7	2.65	18.55	Medium
6.	No special person is assigned to manage IT, just an IT staff just so that the dependence on the staff. IT staff is also only role in doing maintenance and give suggestions about the existing IT conditions.	6	2.53	15.18	Medium
7.	There is no evaluation process from existing IT systems	5	2.48	12.40	Low

V. CONCLUSIONS AND SUGGESTIONS

The conclusion of this research is the company in achieving its business objectives using IT as a supporter of business processes in the company and running well because there is no IT incident that directly threaten the business process of the company. In addition, risk critical such as physical data back up, staff who control IT is an outsider company and never done risk assessment if handled will improve the business continuity of the company.

As for some things that can be used as suggestions in the next development process is to continue the process of risk analysis to the audit process to assess the performance and condition of IT in the company.

REFERENCES

[1] Priambodo, S. Arie. Panduan praktis menghadapai bencana. Yogyakarta: Kanisius, 2009.

[2] Bernes, C. James. A Guide to Business Continuity Planning. John Willey & Sons, LTD. 2001.

[3] Snedaker, Susan. Business Continuity and Disaster Recovery Planning for IT Professionals, Syngress Publishing. 2007.

[4] Blokdijk, Gerard., ITIL IT Service Management-100 Most Asked Questions on IT Service Management and ITIL Foundation Certification, Training and Exams. Quensland: Emereo Publishing. 2008.

[5] FFIEC Press Release. The *Federal Financial Institutions Examination Council* (*FFIEC*). *https://www.ffiec.gov/press_2015.htm.* 2015.

[6] http://www.iso27001security.com/html/27002.html

[7] Jerry N. Luftman, "Managing the Information Technology Resource Resources", International Edition, First Edition, Pearson Education Inc., 2004.