JURNAL INFORMATIKA
Vol. 12, No 1, January 2018, pp. 17-23
ISSN: 1978-0524

A basic element of it business continuity plan: systematic review

Yusrida Muflihah [1,*], Apol Pribadi Subriadi

Magister Sistem Informasi, Institut Teknologi Sepuluh Nopember
Jalan Raya ITS, Sukolilo, Surabaya, 60111
*[1] yusridamuflihah@gmail.com**
** corresponding author*

ABSTRACT

Implementation of IT in the enterprise raises the possibility of various risks arising from threats and disturbances. Companies need to have business continuity planning (BCP), so that the company's business processes can be sustain in normal or critical situations. BCP is a methodology used to create and validate plan to sustain business operations continuously before, during, and after disasters or disturbing events. BCP is an important part of Business Continuity Management (BCM) and is a step that can be taken to reduce the negative impact of business interruptions caused by internal and external. The current condition of the Business Continuity Plan is the lack of understanding of the key elements of the business continuity plan design that leads companies to realize what business continuity plan are or do not know what is needed to make BCP and BCP owned by the company still lack in completeness of the business continuity strategy. Based on the present condition, this research aims to explore the elements of BCP based on business continuity standard that is COBIT 5 Domain: Manage Continuity, ISO 22301: 2012 Business Continuity Management System, ITIL IT Service Continuity Management and related business continuity plan research. The results of the research are BCP has 8 main elements, determining the need of business continuity management, business continuity review, risk analysis, business impact analysis, business continuity strategy, disaster recovery plan, employee training, BCP testing, where the eight elements can be categorized into two are managerial and technical.

Keywords:
Business continuity plan
Cobit 5 domain
ISO 22301:2012
ITIL IT service
Continuity management

I. Introduction

In improving business continuity, the company has several strategies that support the company's goals, one of which is the utilization of information technology (IT). Currently, IT has been applied to small-to-medium business with a laptop or desktop, up to large companies with the existence of information systems and servers. When a company starts to implement IT, then at that time a company will have various risks arising from threats and disturbances. Potential causes of business interruption in the company not only caused by external such as natural disasters, but internal including human error, utility disturbance and threat of harm from outside. To ensure that business process can survive in normal or critical situations and have resilience to possible risks, an organization needs to have a business continuity plan or so-called Business Continuity Plan (BCP).

The Business Continuity Plan (BCP) is a methodology used to create and validate plans to maintain continuous business operations before, during, and after disasters or disturbing events. Research conducted by [1], emphasizes that BCP is an important part of Business Continuity Management (BCM) and is a step that can be taken to reduce the negative impact of business interruptions caused by internal and external. Cummings, Haag & McCubbrey's 2005 study of companies with large-scale data loss without BCP found the following data: 43% of these firms never reopened, 51% of the companies closed within 2 years and only 6% of those companies can survive for long periods of time.

Regardless of the importance of the Business Continuity Plan, the current condition shows that there is still limited understanding of the Business Continuity Plan. The survey by Ernst & Yong Global Information Security on the business plan of all firms in the world shows that 53% of companies have BCP, but the BCP owned by the company is still lacking in the completeness of the business continuity strategy, as there is no consideration of the analysis business impact, priority of

DOI: 10.26555/jifo.v12i1.a8370
W : http://journal.uad.ac.id/index.php/JIFO
E : jifo@uad.ac.id

critical business processes along with IT and BCP testing [2]. A survey conducted by the Calgary Emergency Management Agency on 300 local businesses showed that 69% conveyed the reason the company did not have a BCP due to not being aware of what business continuity plan are or not knowing what it would take to make BCP [3].

The purpose of this research is to know the main elements of the Business Continuity Plan, so the company can know the need in developing a business continuity plan. In achieving that goal, the stages are looking for journals discussing the elements of BCP, reviewing journals, review of business continuity related standards i.e. ISO 22301: 2012, COBIT 5 Domain: Manage Continuity and ITIL IT Service Continuity Management, after which to identify elements based on the results of previous research review and standard.

II. Literature

A. Business Continuity Plan

Business Continuity is an activity undertaken by the organization to ensure that critical business functions will be available to customers, suppliers, and other entities that have access to those functions [4]. Business Continuity Management requires a plan to cover things about business continuity, this plan is called Business Continuity Plan or BCP. Business Continuity Planning (BCP) is a process of identifying and protecting the critical business processes and resources that needed to keep the business process to remain at an acceptable level, protecting all the resources and preparing procedures to ensure the survival of an organization at a time when business exposed to threat (Hiles, 2007). Meanwhile, according to ISO 22301: 2012, business continuity plan (BCP) is defined as the document contains a procedure that aims to guide the company to respond, recover, resume, restore the company's business processes to a level that has been defined earlier after an interruption (Technical Committee ISO/TC 223, 2012). Business Continuity Plan is the process of identifying critical business functions, prioritizing resources to support functions, and developing strategies to sustain operations prior to business interruption or crisis events (Federal Office for Information Security, 2013). BCP is an ongoing process of identifying disaster and vulnerability of the organization, the likelihood of occurrence of a disaster, the potential consequences for the objectives and success of the strategy, the effectiveness of applicable controls and strategies to improve performance and efficiency [5]. Another definition of the Business Continuity Plan (BCP) under the SANS Institute is an activity necessary to keep an organization sustain during periods of displacement or disruption to normal operating processes [6].

B. ISO 22301:2012 Business ContinuityManagement System

ISO 22301: 2012 is an output of the International Organization for Standardization (ISO) that focuses on business continuity management system (BCMS). ISO 22301: 2012 is the development of British Standard BS 259999-2: 2007. This standard is enabled to keep the business from potential interference that can occur. ISO 22301: 2012 specifies the need to plan, build, implement, operate, monitor, review, maintain and continually improve a documented management system to protect, reduce the likelihood of occurring, preparing, responding and recovering from disruptions (Technical Committee ISO/TC 223, 2012). According to [7]. ISO 22301: 2012 has benefits, including: (1) identifying and managing current and future threats for business, (2) using proactive approaches to minimize the impact of incidents; (3) managing critical functions before and during times of crisis, (4) minimize downtime during incidents and increase recovery time. ISO 22301: 2012 applies the "Plan-Do-Check-Act" (PDCA) cycle model to perform phases in the BCMS framework. This is done to maintain consistency of standards with other system management standards such as ISO 9001 quality management systems, ISO 14001 environmental management systems, ISO / IEC 27001 information security management systems.

C. Cobit 5 Domain: Manage Continuity

COBIT is a collection of best practices for IT governance that can assist auditors, management, and users in bridging the gap between business risk, the need for control and other technical issues. There are two areas in COBIT 5, which are governance and management. Both areas consist of 5 domains and 37 processes. COBIT 5 is based on 5 key principles for IT governance and organizational management. These five principles enable organizations to establish effective governance and

management, capable of optimizing the investment and use of IT. COBIT 5 has 5 main domains: Evaluate, Direct and Monitor (EDM), Align, Plan and Organize (APO), Build, Acquire and Implement (BAI), Deliver, Service and Support (DSS) and Monitor, Evaluate and Assess (MEA). Domains Deliver, Service and Support (DSS) focus on delivering IT, process and system support that enables effective and efficient IT implementation. In addition, DSS domains focus on improving IT services to customers. One of the processes in the DSS which aims to continue critical business activities and maintain the availability of information in accordance with the standards of the organization or company is DSS04. DSS04 contains guidance in ensuring that IT services in the organization are always available. DSS04 has eight key management practices [8].

III. Method

The following sections describe the steps undertaken in this study so that the research can be completed systematically, purposefully and clearly. The work flow of this research, as follows:

- Looking for a journal on the elements of the Business Continuity Plan Journal searches are conducted on various sources. Keywords used to obtain the appropriate journal are business continuity plan, business continuity plan element, business continuity plan component, business continuity plan methodology.
- Selecting a journal Journals generated from the search stage are then selected as appropriate. In choosing a journal, do a review of the business continuity plan element. The content of the selected journal is required to have a criterion that is to discuss the elements or components of the business continuity plan.
- Reviewing selected journals Journals that have been found and selected then done reviews so that the list of business continuity plan elements. Journal conducted a review of 6 journals.
- Conduct a review of the standard on business continuity There are three standards with business continuity, namely ISO 22301: 2012, COBIT 5 Domain: Manage Continuity and ITIL IT Service Continuity Management. The third standard is a review to find out what is discussed in the standard related to the business continuity plan.
- Identify the elements of the Business Continuity Plan The next step is to analyze the results of the previous review and standard, so that will be known elements of the Business Continuity Plan

IV. Results and Discussion

In this study, the determination of elements of the Business Continuity Plan is conducted by conducting literature studies on research that discusses elements of BCP and based on the standard of business continuity such as ISO 22301: 2012 Business Continuity Management and COBIT 5 Domain: Manage Continuity. Meanwhile, ITIL: IT Service Continuity Management is not a reference in the determination of BCP elements, with the reasons ITIL IT Service Continuity Management focuses more on the risks faced by IT services, disaster measures and how to restore IT services, the focus of the Disaster Recovery Plan (DRP). Table 1 will summarize the elements of the Business Continuity Plan based on previous research and standardized on business continuity.

Table 1. Summarize Element BCP

Reference	Statement	Element
Elements of BCP based on Previous Research		
(Virginia Cerullo, [9])	Business continuity planning process, should discuss three interrelated goals, are: identification of the main risks of business interruption, develop a plan to prevent or mitigate the impact of identified risks, and provide employee training and test plans to ensure their effectiveness	Business Impact Analysis Disaster Recovery Plan Employee Training
(Dey, [10]	There are three components of the business continuity planning, are: perform risk analysis and its impact on business, identify priorities, classify critical areas or business functions along with assets and determine the maximum duration of tolerance for interruptions, and incident handling and recovery of damage or loss and restore operations to its original state.	Business Impact Analysis Risk Analysis Disaster Recovery Plan
(S.A. Torabi, [11])	Business impact analysis is used to develop an appropriate business continuity plan	Business Impact Analysis
(S. Ali Torabi, [12])	Risk assessment is used to develop appropriate BCPs to address identified risks	Risk Analysis
(Goldberg, [13])	The first step in implementing business continuity planning is business impact analysis. Business impact analysis becomes an integral and sustainable center in the business continuity planning process. BIA is basically an inventory and ranking by the importance of all business process utilities.	Business Impact Analysis
(Jacques Botha, [14])	DRP is an active component of BCP.	Disaster Recovery Plan
Elements of BCP based on Standard		
ISO 22301:2012 Business Continuity Management (Technical Committee ISO/TC 223, [14])	From the standard comparisons, it was concluded that ISO 22301: 2012 describes the principles of the business continuity management process delivered through the Plan-Do-Check-Act (PDCA) cycle. The principles of business continuity are: 1. In managing business continuity, an organization needs to define the need to build a business continuity management system, the specific needs of the upper management roles in BCMS including the definition of communication 2. A determination of how to account for what happened (resources), as well as develop procedures used to manage the damage or disturbance that occurs in the organization 3. There is a determination of business sustainability strategy 4. The existence of determining the risks and their impact on the business. 5. Measuring the performance of business continuity management, the conformity of existing BCMS with international standards and management expectations, further identifying and acting against BCMS incompatibility.	Determination of business continuity management needs Disaster Recovery Plan Business continuity strategy Risk analysis Business impact analysis Business continuity review
COBIT 5: Manage Continuity (ISACA, [12])	Based on standard comparisons, it is concluded that COBIT 5: DSS04 Manage Continuity describes the role of the Business Continuity Plan that can be used to manage the continuity and elements of the business continuity plan. Elements of the business continuity plan according to COBIT 5: DSS04 Manage Continuity: 1. Information on the intrusion and critical activities of the company. 2. Testing the business continuity plan and enabling innovative solutions during the execution of the plan and assisting in the verification of plans that have been made. 3. Management review to ensure sustainability and effectiveness and adjustment of plans adjusted to the control so that the sustainability plan can be updated and in line with business needs. 4. Training for third parties both internal and external parts and defining the roles of the parties' responsibilities in the event of disruption. 5. Maintain the availability of critical business information and data backup management.	Risk Analysis Business Impact Analysis BCP Testing Disaster Recovery Plan Business Continuity Review Employee Training

Based on Table 1, there are some elements of the Business Continuity Plan: risk analysis, business impact analysis, business continuity review, business continuity management requirements, disaster recovery plans, employee training and BCP testing. Of the eight elements, can be categorized into two elements:

- Managerial elements consist of determining the needs of business continuity management, business continuity review, risk analysis, business impact analysis
- Technical elements consist of disaster recovery plans, employee training and BCP testing. The division of elements into two categories assumes derived from the definition or explanation of the focus of each element that the managerial element is an element in the process of business continuity requiring participation from management due to a process that requires discussion, policy, and understanding of the company's business processes. Technical elements are the elements that lead to operational and technical actions to safeguard business continuity before, during and after disruption / disaster. Table 2 shows a grouping based on research results.

Table 2. Grouping Element Based on Research Result

	Virginia	**Dey**	**S.A. Torabi**	**Goldenberg**	**Jacques Botha**	**ISO 22301:2012**	**COBIT 5: Domain Manage Continuity**
Managerial	√	√	√	√	-	√	√
Technical	√	√	-	-	√	√	√

The grouping done in Table 2 technical categories. Here is a diagram that will clarify the mapping of each element based on the reference that has been obtained (Figure 1).

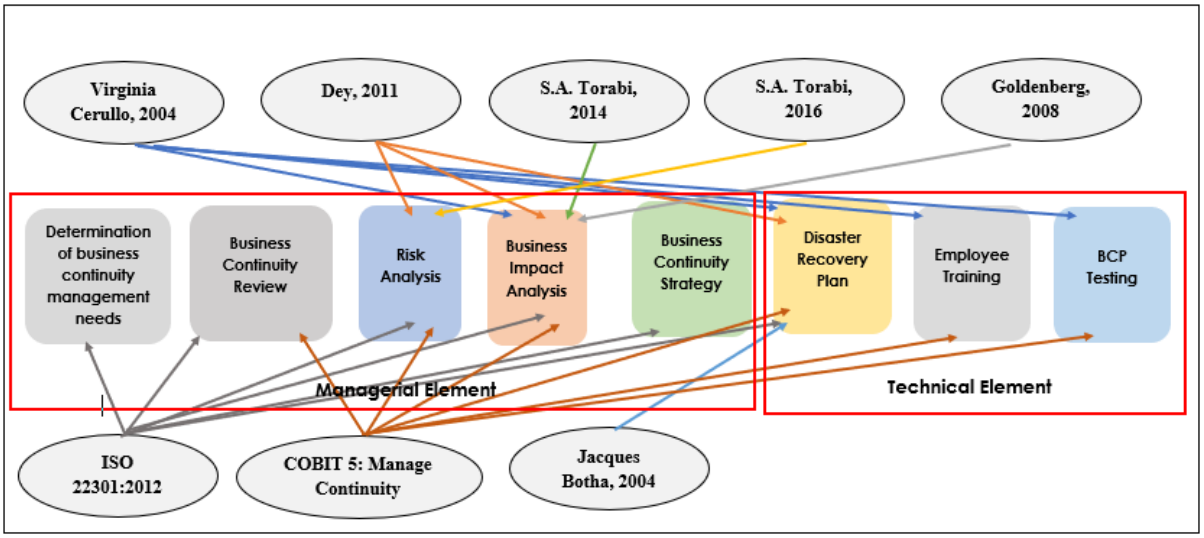

Fig. 1. *Mapping Element and Reference*

Based on Figure 1, it can be seen that there are different elements of the research results and standard. For example: in ISO 22301: 2012 does not include elements of employee training and testing of BCP, while COBIT 5 DSS04: Manage Continuity include these elements, in other side ISO 22301: 2012 includes determining the need for business sustainability management, but COBIT 5 DSS04: Manage Continuity is not available the element. Here is an explanation of each of the BCP elements:

Table 3. Explanation of each Element

Elements	Short Description	References
Determination of business continuity management needs	Detailing initial needs on the scope of management related to objectives, scope, management roles, resources, and communication.	(Technical Committee ISO/TC 223, 2012)
Business Continuity Review	A review of business continuity viewed from the capabilities and effectiveness of business continuity defined in the business continuity plan and provides feedback from the business continuity discrepancy used to improve and improve business continuity performance.	(ISACA, 2012) (Technical Committee ISO/TC 223, 2012)
Risk Analysis	Identifying possible risks, risk assessments and impacts of risk.	(S. Ali Torabi, 2016) (Dey, 2011)
Business Impact Analysis	Identification and prioritization of business functions along with assets, determination of the duration of interference tolerance, and the identification of the impact of interference.	(Dey, 2011) (Goldberg, 2008) (Virginia Cerullo, 2004) (Technical Committee ISO/TC 223, 2012)
Business Continuity Strategy	Determination of liability for the disruptive effects that interfere with the business process and the development of procedures for the management of damage or disruption	(Technical Committee ISO/TC 223, 2012)
Disaster Recovery Plan	Handling of incidents, procedures during interruption and details of the parties concerned, recovery of interference.	(Dey, 2011) (Virginia Cerullo, 2004)
Employee Training	Training process that includes the delivery mechanism of the training, the implementation of training consisting of exercises and examinations, and monitoring of competencies based on the results of exercises and examinations.	(ISACA, 2012)
BCP Testing	Making the flow of testing, testing and improvement based on test results performed.	(Virginia Cerullo, 2004)

V. Conclusion

Based on the research that has been done, it can be concluded that Business Continuity Plan has eight elements are determining the need of business continuity management, business continuity review, risk analysis, business impact analysis, business continuity strategy, disaster recovery plan, employee training, BCP testing. Of the eight elements can be categorized into two categories are technical elements and managerial elements. The managerial element is an element that in the process of business continuity management participation is required due to a process that requires discussion, policy, and understanding of the company's business processes, this category consists of elements determining the needs of business continuity management, business continuity review, risk analysis, and business impact analysis. Technical elements, meanwhile, are the elements that lead to operational and technical action towards maintaining business continuity before, during and after disruption / disaster, this category consists of elements of business continuity strategy, disaster recovery plan, employee training and BCP testing.

References

[1] Ali Asgary, A. S. (2011). Modelling the Adaptation of Business Continuity Planning by Businesses Using Neural Network. Intelligent System in Accpunting, Finance and Management, 89-104.

[2] Calgary Emergency Management Agency. (2015, October 19). Calgary Chamber. Retrieved from Survey Findings: Business Continuity Planning Still Low in Calgary's Business Community: https://www.calgarychamber.com/insight/blog/survey-findings-business-continuity-planning-still-low-calgarys-business-community

[3] Dey, M. (2011). Business Continuity Planning (BCP) Methodology-Essential For Every Business. IEEE GCC Conference and Exhibition (pp. 19-22). Dubai: IEEE.

[4] Ernst & Young LLP. (2002). Global Information Security Survey. Federal Office for Information Security. (2013). Business Continuity Management for SMEs using the Cloud. Bonn: Federal Office for Information Security (BSI).

[5] Goldberg, E. M. (2008). Sustainable Utility Business Continuity Planning: A Primer, An Overview and A Proven Culture-Based. The Electricity Journal, 67-74.

[6] Griffith University. (2013). Business Continuity Management Framework. Queensland: Griffith University.

[7] Hiles, A. (2007). The Definitive Handbook of Business Continuity Management Second Edition. West Sussex: John Wiley & Sons Ltd.

[8] ISACA. (2012). COBIT 5 Enabling Processes. Rolling Meadows: ISACA.

[9] Jacques Botha, R. V. (2004). A Cyclic Approach to Business Continuity Planning. Information Management and Computer Security, 328-337.

[10] K. Venclova, H. U. (2013). Advantages and Disadvantages of Business Continuity Management. International Jpurnal of Social, Behavioral, Educational, Economic, Business and Industrial Enginee, 895-899.

[11] Rupal Choundhary, D. (. (2016). Business Continuity Planning: A Study of Framework, Stadards and Guidelines for Banks IT Services. International Journal of Emerging Research in Management & Technology, 33-40.

[12] S. Ali Torabi, R. G. (2016). An Enhanced Risk Assessment Framework for Business Continuity Management Systems. Safety Science, 201-218.

[13] S.A. Torabi, H. R. (2014). A New Framework for Business Impact Analysis in Business Continuity Management (with a case study). Safety Science, 309-323.

[14] SANS Institute. (2002). Introduction to Business Continuity Planning. Retrieved from SANS: https://www.sans.org/reading-room/whitepapers/recovery/introduction-business-continuity-planning-559

[15] Technical Committee ISO/TC 223. (2012). ISO 22301 Societal Security-Business Continuity Management Systems-Requirement. Switzerland: ISO.

[16] Virginia Cerullo, M. J. (2004). Business Continuity Planning: A Comprehensive Approach. Information Systems Management, 70-78.