ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 13 (2023) No. 1, pp. 322-343
DOI:10.33168/JSMS.2023.0118

Business Continuity Management Framework In Electronic System Provider (ESP) Startup Company

Robertus Andi , Ditdit Nugeraha Utama

Computer Science Department, BINUS Graduate Program - Master of Computer Science, Bina Nusantara University, Jakarta 11480, Indonesia
robertus.andi@binus.ac.id; ditdit.utama@binus.edu

Abstract. COVID-19 pandemic forces startup companies in Indonesia to change their work system from working in the office to work from home system, caused instability in various aspects, including the process of economic. To ensure the continuity of a company's business, business continuity management is an important requirement to be owned by a medium-sized company and above. To overcome this problem, a proper business continuity management framework need to be designed and applied in a startup in Indonesia. This study uses several references from researchers who discuss in detailed manner related to business continuity management, while also refer to several international standards such as ISO 27001 annex 17 which related to business continuity, ISO 27005 which related to risk assessment, and ISO 22301 which related to the business continuity process. Plan do check action (PDCA) approach is used in this research to wrap the process. The results of this study are quite in line with expectations with the application of the newly designed business continuity management (BCM) framework in a startup company in Indonesia, which reduce about 42% of the risk level from before. Moreover, during the drill test, adoption of BCM framework shows successful result with 1 hour 27 minutes, significantly below defined maximum tolerable period of disruption (MTPD) and recovery time objective (RTO). In addition, qualitatively the company has a guarantee of business continuity and good governance in order to maintain the reputation and improve the quality of the startup company.

Keywords: Business Continuity; Business Models; Resilience; Value Creation

1. Introduction

The impact of the COVID-19 pandemic changed several business schemes around the world, ranging from business lines, education and even retail began to change activity strategies to maintain the stability and sustainability of their businesses (Liguori, 2020). One of the things that have been quite significant in changing strategies is that offline business schemes have begun to be abandoned and switched to online business. According to (Liguori, 2020), it is undeniable that online business is very dependent on the development of information technology so that business can run well.

Due to the shifting process to online business, companies also need to comply with local regulations. In Indonesia, Bank Indonesia and the Ministry of Communication and Information become the regulator of online businesses, including electronic money provider businesses. One of the regulations is, PP No. 71 of 2019, where every electronic service provider (ESP) requires to register its service (Kominfo, 2020). During the registration process, an ISO 27001 certification is one of the requirements, where business continuity management is a critical item in annex 17.7.1 of the certification (isms.online, 2020). The reliability of business continuity management can be tested through disaster recovery planning to simulate the potential risks, where it form of simulation that resembles the condition of a disaster that occurs in a company historically and or predicts disasters that will occur in the company based on business impact analysis activities, with the aim of obtaining learning related to how to recover if the disaster occurs (Kadam, 20211).

One Indonesian startup company which engaged in transportation and electronic money providers also felt these changes in technological development, thus comply with regulatory compliance is a must, including having a business continuity management. To overcome the problems, we set objectives in this research: (i) design an appropriate business continuity management framework for the electronic service provider company, (ii) simulate a disaster recovery plan to test the reliability of business continuity plan by obtaining asset recovery process time below the determined MTPD and RTO for the electronic service provider company, (iii) decrease the percentage of high and medium risks assets during a risk assessment process.

The rest of the paper is organized as follows. In section 1 we present introduction, followed by literature review in section 2. After that, there will be research methodology in section 3. The next section is results and discussion of the research. The conclusion is presented in section 5.

2. Literature Review

The objective of the research (Bajgoric, 2014) is to establish a comprehensive framework for the application of firm continuity management business. The framework is based on the assertion that BCM should be implemented through a systemic implementation of the "always on" corporate information system. The method used is a system approach to design a systemic framework for the implementation of sustainable computing technology in the context of a "always on" corporate information system. The researcher concluded that the majority of the literature on the implementation of BCM discusses the perspectives and or implications of one or two aspects of BCM, such as organizational strategy, organizational management, planning, risk management, disaster management, and IT, but not as a whole. Consequently, a comprehensive and holistic approach will be effective for identifying the primary BCM implementation frameworks. Based on the concept of the Churchman system, an attempt was made to present such a systemic model in this investigation (1968). It has been demonstrated that in the modern e-business environment, IT platforms running business-critical applications are a crucial component of BC, taking the shape of a "always-on" corporate information system.

(Kadam, 2011) proposes study on how catastrophe recovery plans might operate well inside a certain organization. This study's primary objective is to determine whether or not particular financial cooperatives have an effective disaster management system by referencing disaster avoidance, disaster recovery plan (DRP), and business continuity plan (BCP) in accordance with reserve Bank of India (RBI) guidelines and other international standards. This was accomplished through a planned interview with the Pune branch manager of The Vishweshwar Sahakari Bank Ltd. The researcher performed study utilizing a questionnaire provided by the branch manager of TheVisheshwar Sahakari Bank Ltd., Pune, and compared the results using the gap analysis worksheet.

The purpose of the study was to determine if the selected Bank of India has an effective disaster management system with respect to disaster avoidance, DRP, and BCP in accordance with RBI guidelines, as well as to prove the hypothesis that the selected bank unit did not implement the disaster management system in accordance with RBI guidelines and other international standards. Then, researchers conducted well-scheduled face-to-face structured interviews in response to questions. Researchers also record direct observations or observations by visiting bank branches and utilizing their diverse goods and services, including automatic teller machine (ATM), tele-banking, short messages service (SMS) banking, net banking, mobile applications, point of sales (POS) terminals, and credit and debit cards. The conclusion of the study is that the selected Bank of India has a BCP/DRP plan on their software, but they do not implement the disaster management sysytem in accordance with the RBI's "information security guidelines, electronic banking,

technology risk management, and cyber fraud" and other international standards. The necessity of a solid BCP cannot be overstated. When implementing BCP, there are seven steps to consider, including the ones below, such as the first one: BCP is not a project but a process: BCP is not limited to insurance or plan documentation. Successful BCP aspects include a predetermined renewal and business continuity team, then the holistic approach: BCP should now encompass people, processes, and infrastructure in addition to information technology. The focus of the plan should be on the important business operations and their interdependence. Then, BCP governance, which includes various elements such as management's commitment, control, and direction, clearly written roles and duties, and formal governance processes, ensures that the BCP is continuously updated. The subsequent stages are resistance, which is related to the recovery operation and should not undermine the control environment at the recovery site, is not acceptable. Then, the business partner engagement that focuses on all of the significant business partners should be considered during plan creation and testing. Then, media management is necessary to maintain the company's image throughout a calamity. Media management solutions allow for proactive/systematic responses to media coverage.

According to research (Niemimaa, 2019), the risk assessment performed on medium- to low-end organizations or companies is thoroughly discussed. This research was done because researchers observed that many enterprises and small organizations lack the expertise of information technology and human resources necessary to manage this, particularly in terms of risk management and cyber security. The goal of this article is to report on the findings of a field study comprising over 370 interviews with small business owners regarding their approach to risk management, including cyber crime security threats. Similarly, academics perform in-depth research on the risk assessment procedure (O'Har, 2017). This research was conducted because researchers perceived corporate risk management to be a growing area of interest for the United States Department of Transportation, and a risk list spreadsheet tool was developed to assist users in identifying event risks, determining risk categories, and assessing the likelihood (probability) and consequences (effects) of an event occurring. In connection with the use of risk list tools to assist enterprise and program level risk management in U.S. state transportation departments, foreign transportation agencies, and nontransportation organizations, state of the practice surveys are done.

Other than that from the explanation above regarding several expertise related to BCM ecosystem, Table 1 summarize the rest of journal that referenced on this paper.

Table 1: Literature review summary

No	Author	Method
1	(Bajgoric., 2014)	In this research, the author use system approach to design a systemic framework for sustainable technology implementation, with a concept where company's information system is "always on".
2	(Kadam, 2011)	Conduct research by sending questionnaire to branch manager of The Vishweshwar Sahakari Bank Ltd, Pune and comparing the questionnaire to gap worksheet analysis.
3	(Han, 2012)	Explains the disaster recovery plan as a chain of processes and procedures to recover business processes and assets during incidents or disruptions.
4	(Rongrong, 2019)	Propose a framework to evaluate network security situations from three dimensions: threat, vulnerability, and stability.
5	(Radeschütz, 2015)	Use a framework which has possibility to improve business process by considering a solid view from data process and data operational aspects.
6	(Gibb, 2006)	Use business continuity management framework by considering the best practice and experiences from expertise, while still considering fundamental principles from scientific literatures.
7	(Nurcahyo, 2018)	Define characteristics, phases, and clusters of a startup company scheme.
8	(Wong, 2010)	In this research, three main concepts are used as research methodology: integration, coordination, and preservation.
9	(Niemimaa, 2019)	Methodology of this research is by evaluating the resilience of the business model to contingencies, which is the main area of business continuity.
10	(O'Har, 2017)	Use a methodology which is divided into 4 main areas: risk register survey, analyze survey results, develop risk register tools, prepare final spreadsheet-based risk register tool and user guidance.
11	(Berry, 2018)	Research methodology of this research is by conducting random surveys and interviews with multiple correspondents.

In this research, we also review ISO 27001, ISO 27005, and ISO 22301 frameworks as a reference, as these frameworks are also the fundamental frameworks being used by previously mentioned literatures. After conducting literature review process, we compile a summary of important processes related to

business continuity management.

2.1. Business Continuity Management (BCM)

According to (Bajgoric, 2018; Joachim 2022; Hadjinicolaou et al., 2022), BCM is an innovative business model that enables technological developments to provide significant opportunities for companies that have innovation but are capable of posing significant threats to established companies and their business models. This business model focuses on the sustainability of resources implemented in the current type of business model and the business model itself is not considered despite its strategic threats. Evaluating the resilience of a company's business model to business model disruption can improve a company's business continuity and help build firm business continuity among a company's strategic imperatives. According to (isms.online, 2020) BCM framework is a sequence of processes that aims to ensure continuous business continuity when an incident occurs, so that it does not impact the business directly or indirectly based on ISO 27001: 2013 annex 17 which discusses information security aspects of business continuity management.

2.2. Disaster Recovery Plan (DRP)

According to (Kadam, 2011) DRP is a very complex and intensive process, therefore it requires transfer of technical and information processing resources to minimize the impact of efforts on resource scarcity, project development and implementation of disaster recovery. In addition, plans to restart a business should be part of the normal planning activities of an organization. According to (Han, 2012) DRP is also a series of processes and procedures in activities to restore a business process or an asset, which is carried out when an incident or disruption occurs in a process so that it can affect the work function of the process.

2.3. Business Continuity Plan (BCP)

BCP is the process by which financial institutions ensure the maintenance or restoration of operations, including services to customers when faced with side effects such as natural disasters, technological failures, human errors, or terrorism (Kadam, 2011).

2.4. Risk Assessment

Risk assessment is a process to calculate risk in an entity or a corporation (Rongrong, 2019). In the risk assessment process, multiple components are required including asset, risk level of likelihood, and level of impact.

During risk assessment process, cybersecurity aspect is also considered by calculating confidentiality, integrity, and availability (CIA) value. According to (Alrawashdeh, 2022), cybersecurity has become one of the main dangers of organization’s execuity.

2.5. Business Impact Analysis (BIA)

According to (Radeschütz, 2015) a business analysis approach can be carried out with the process of collecting execution data, operational data related to employee data involved in the business implementation process such as work experience, training, and demographics. Business impact analysis (BIA) can provide a contribution that is able to ensure that the data needed is relevant to be taken into account.

This is also reinforced by (Torabi, 2014), BIA is an important element in the preparation of BCM as a process to be able to analyze the processes and assets contained within a company/organization and what effects arise from the unavailability of these processes and assets. The main objective of the BIA process is to gather and analyze the information needed to codify reports to top managers to prepare a BCP.

3. Research Methodology

The writing process will combine existing processes with scientific papers and business continuity management-related journals, then the process outlined in a new business continuity management framework that can be relied upon, in terms of scalability and performance. During the research, we use PDCA approach based on scientific literature according to (Heng, 2015).

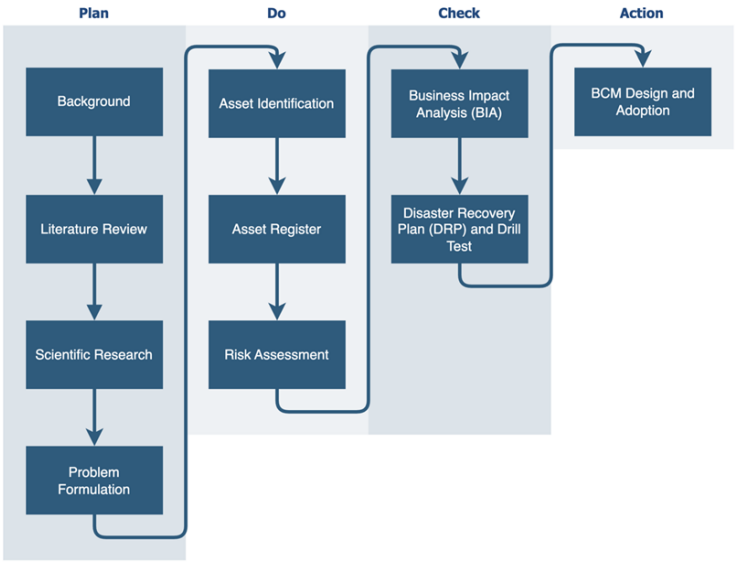

Fig. 1: Research Methodology Process

Figure 2 is a high-level illustration of the BCM process that wants to be applied to ESP startup companies, where this BCM process is an evaluation of the pre-existing BCM process that uses the basis of ISO27001: 2013 information security

management system (ISMS) annex A.17 information security aspect of business continuity management which is considered less comprehensive in covering the BCM process as a whole, scientific literature/literature is related to the BCM process and its related processes and adapts also from the ISO 22301 business sontinuity management system.

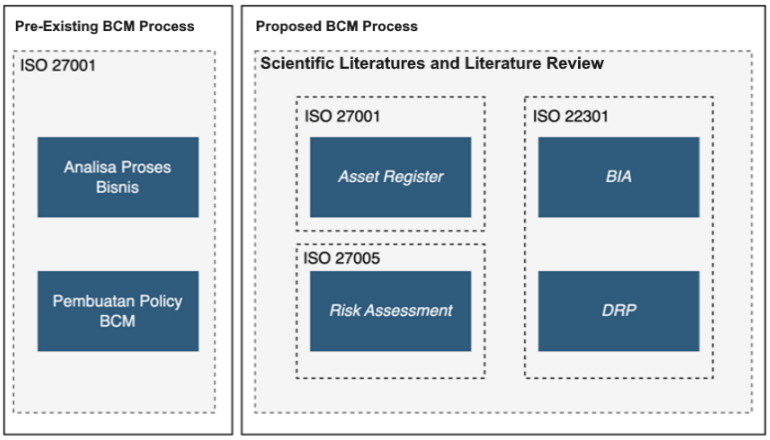

Fig.2: Comparison of BCM process proposal

3.1. Plan

During the planning phase, we review multiple literatures that are related to business continuity management to be used as a reference for the research. During this phase, scientific research is also conducted to form research problems.

3.2. Business Continuity Management

The first action item in the do phase is asset identification, where we conduct classification of category and subcategory of assets to have a clear mapping of company assets. The output of asset identification process is to gather asset value. In the research, we use risk assessment to calculate the asset value. Figure 3 explain how the flow of BCM process and ecosystem.

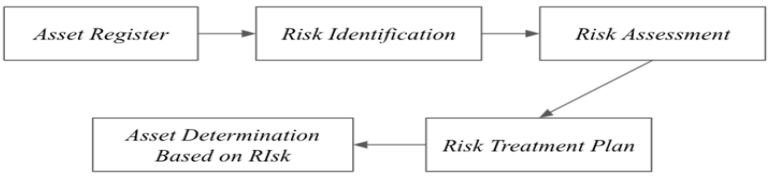

Fig. 3: Risk Assessment Overview Process

During risk assessment process, asset register is conducted to gather visibility-related categorization and risk level of the asset. Table 2 shows asset register form along with fundamentals parameters required. Risk identification was a process to identify and describe IT and information security risk, risk assessment was a

process of analysing the nature and impact of risk as well as determination of risk level, asset determination based on risk was a process in which the analyzed risk against the established risk criteria to determine whether the risk is acceptable, and the risk treatment plan was an activity to modify the risk. The primary objective of the modification is to lower the risk level to an acceptable level. In general, there are four options of risk treatment utilized by: mitigate/reduce the likelihood and/or impact of the risk, avoid the risk, transfer the risk; or accept the risk.

Table 2: Asset register form

No	Asset Name	Sub-Classification	Owner	Confidentiality	Integrity	Availability	Value	Asset Status
1	Asset 1							
2	Asset 2							

Value of the asset register is based on one of information security pillars regarding to CIA. Confidentiality is roughly equivalent to privacy. Confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. It is common for data to be categorized according to the amount and type of damage that could be done if it fell into the wrong hands. More or less stringent measures can then be implemented according to those categories. Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people (for example, in a breach of confidentiality). Availability means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information. Table 3 explain how matrix of CIA being mapped.

Table 3: Matrix of CIA

Maturity of Rating		Description
Confidentiality	1	Asset can be accessed generally.
	2	Specific asset that can only be accessed only by several units in an entity. Information on this asset cannot be published to public.
	3	Confidential asset, which if accessed by public can affect business process of an entity.
Integrity	1	The integrity of an asset does not affect business

		process of an entity.
	2	The integrity of an asset affects business process of an entity.
	3	Seriously affect business process if the integrity of an asset is abused.
	1	Availability of asset does not affect business process.
Availability	2	Availability of asset affects business process.
	3	Business process is affected severely if an asset is not available.

Once confidentiality, integrity, and availability of asset are defined, asset value can be calculated using equations (1). Asset status was defined based on asset value, hence Table 4 explain the categorization of asset status.

$$Asset\ Value = \frac{C\ x\ I\ x\ A}{3} \quad (1)$$

Table 4: Asset status categorization

Asset Value	Asset Status
>2.5	High
1.5-2.5	Medium
<1.5	Low

After asset register is formed, the next step in do phase is risk identification and risk assessment, which the process is dependent to each other, by compiling a risk assessment form as shown in Table 5.

Table 5: Risk assessment form

RISK IDENTIFICATION				RISK ASSESSMENT			
Asset Name	Asset Value	Threat	Vulnerability	Vulnerability Value	Likelihood Value	Risk Level	Risk Category
Asset 001	3	Threat 1	Vuln 1	2	3	18	Low
Asset 002	3	Threat 2	Vuln 2	3	4	36	Medium

In risk assessment form, vulnerability and likelihood value is required. The value range of this parameter is score 1 - 5. For vulnerability, score 1 means the impact of this vulnerability is very low, while for score 5 the impact is very high. Where for likelihood, score 1 means the risk possibility is very unlikely and score 5 is almost always. Once vulnerability and likelihood value is gained, risk level can be calculated, and the risk category of asset can be set based on table 6.

Table 6: Risk category matrix

	Risk Score	Risk Category
Risk Category Matrix	1-6	Low
	7-14	Medium
	15-16	High
	>16	Very High

Based on the asset risk category, another process called risk treatment plan and asset determination plan is conducted. Risk treatment plan is a process to lower the risk while asset determination plan is to select which assets to be focused in business continuity management.

3.3. Check

BIA is conducted during check phase to analyse the impact of disaster, disruption, or any event that affects business process directly. The component of business impact analysis is impact metrics and business continuity concept. During business impact analysis process, we defined MTPD, RTO and RPO values during incident or disaster which refers to the company policy. MTPD is the maximum tolerable time for an incident or disaster to happen for a business. RTO value is also set in the process, this is the time required for recovering asset after incident. The last value, RPO, is the number of data which is lost during the incident.

Parallelly, without waiting for the business impact analysis to be done, the disaster recovery planning can be done with the objective of this process as mitigation and preparation. By conducting disaster recovery planning, during incidents or disruptions an entity should not require a lot of time to recover this business.

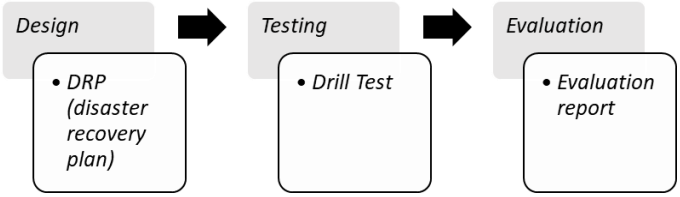

Fig. 4: Business Continuity Management Evaluation Flow

DRP is one component in business continuity management framework which

gives a clear picture of what activities to be done during an incident. During the DRP forming, there is a set of questions to be asked to relevant stakeholders. Once the questionnaire is collected, DRP compilation can be done based on business requirements. The output of DRP process is a runbook which contains a list of activities to be done during testing phase.

Table 7: Guideline question for DRP

No	Guideline	Remark (Yes/No)
1.	Structured risk assessment based on comprehensive Business Impact Analysis (BIA)	Yes/no
2.	Formulating Recovery time objectives (RTO) based on Business Impact Analysis	Yes/no
3.	Clearly documented and tested processes for shifting to secondary/backup systems and sites	Yes/no
4.	Documentation of Action plans, practical manuals and testing procedures.	Yes/no

After DRP is planned, a drill test is conducted to evaluate disaster recovery planning. After that, business continuity management design process can be started. In the drill test, a list of activities from runbook is conducted to simulate the previously formed DRP as well as to calculate whether the defined MTPR and RTO values are already matched the actual business process. Table 8 shows the drill test report form as the output of drill test process.

Table 8: Drill test report form

No	Activity	PIC	Downtime (Yes/No)	Date	Start (Time)	End (Time)	Result
1	Activity 1						
2	Activity 2						

Once drill test activity is finished, an evaluation report is compiled to see whether a drill test is successful or not. A list of components is required in evaluation report, which can be seen in Table 9 below. Evaluation report has to be approved by management of an entity, such as head of information security and head of engineering.

Table 9: Drill test report form

Component	Description
Scope	Explain the scope of DRP and drill test activity
Scenario	Describe the summary of scenario conducted during drill test activity
Activity Details	Elaborate the detail of each activity from drill test, which refers to the previously created runbook
Area for Improvement	Explain which areas need to be improved as the results of the test
Lesson Learned	Elaborate items learned during the testing process that will be useful for business process in the future

3.4. Action

In the action phase, business continuity management framework is designed by considering results of previously conducted activities during plan-do-check phases. Once the BCM is designed, then it is adopted in the organization.

4. Results and Discussion

Establishing the necessary executive management structure to support the BCM planning process is the first step in implementing the BCM framework in ESP startup company. Here, we confirm the inclusion of business units and functions inside the project's scope, as well as the roles and duties of each project participant. This addition is intended to facilitate the efficient execution of work assignments and time targets, which must be determined at a later project stage. During risk mapping process we use ISO 27005 as the best practice.

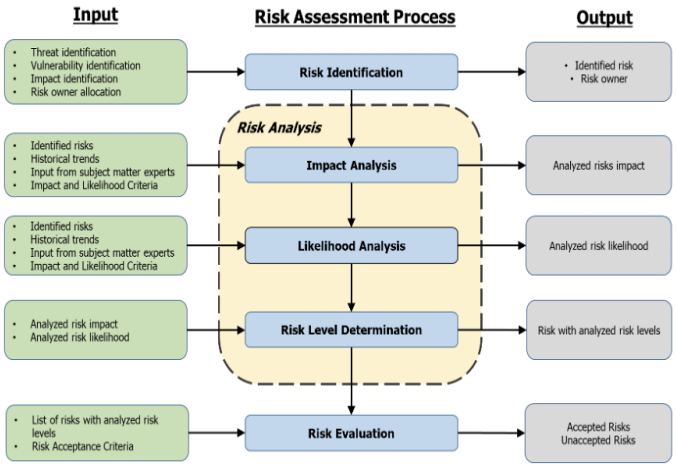

Fig. 5: Risk Assessment Process, adaptation of ISO 27005

During the risk identification, risk likelihood criteria is formed as shown in Table 10 based on number of times the risk happens.

Table 10: Risk likelihood criteria

Category	Criteria
1 - Very Rare	Happened once in three month's time, or Very unlikely to happen (less than 5% volume)
2 - Rare	Happened 2-3 times in three months, or Unlikely to happen (around 5-10% volume)
3 - Seldom	Happened 4-6 times in three months, or Unlikely to recurring (around 10-20% volume)
4 - Often	Happened 6-9 times in three months, or Oftenly happened (20-50% volume)
5 - Almost Always	Happened more than 9 times in three months, or Almost always recurring (more than 50% volume)

Risk impact criteria category is also formed in this process of research, which the level of risk impact defined based on business impact and CIA triad of information security.

Table 11: Risk impact criteria

Level of Impact	Criteria			
	Business Impact (Financial, Reputational, Legal & Compliance, Service Continuity)	Information Confidentiality	Information Integrity	Information Availability
1 - Negligible	This vulnerability is a weakness that causes a negligible asset exposure factor, and the impact of the threat is insignificant	Unauthorized disclosure of internal information	Permanent damage or corruption of public information	Total loss without means of recovery of public Information
2 - Minor	These vulnerabilities are weaknesses that cause minimal or low exposure factors to assets, and Impact threats are minor consequences, damage and/or loss	Disclosure of unlawfully restricted information	Permanent damage or corruption of internal information	Total loss without any means of recovery for internal information
3 - Moderate	This vulnerability is a weakness that causes	Unauthorized disclosure of	Irreversible damage or	Total loss without any

Level of Impact	Criteria			
	Business Impact (Financial, Reputational, Legal & Compliance, Service Continuity)	Information Confidentiality	Information Integrity	Information Availability
	moderate exposure for the asset. This will primarily include vulnerabilities that do not have a severe effect on the process, and impact of the threat is a significant consequence, damage and/or loss	confidential information to limited parties	corruption of restricted information	means of recovery for restricted information
4 - Significant	This vulnerability is a weakness caused by procedural, customer or business reasons, and the impact of the threat is serious consequences, damage and/or loss	Unauthorized public disclosure of confidential information	Permanent damage or corruption of confidential information	Total loss without any means of recovery for confidential information
5 - Highly significant	This vulnerability is an inherent weakness in an asset that causes the highest exposure factor for that asset and, the impact of the threat is worst case, severe and lasting, damage and/or loss.	Unauthorized public disclosure of confidential information and sensitive personal information	Irrecoverable damage or corruption of confidential and sensitive personal information	Total loss without any means of recovery for confidential and sensitive personal information

After risk likelihood and risk impact criterias are formed, matrix of risk level criteria can be formed. The correlation of likelihood level and impact level mapped into 25 probabilities of risk level criteria, each probability determined in each cell of Table 12. With that being said, the risk level criteria probabilities help to determine the risk criteria matrix on the Table 13.

Table 12: Risk level criteria matrix

Level of Impact	Level of Likelihood				
	1 – Very rare	2 – Rare	3 – Seldom	4 – Often	5 – Almost always
1 – Negligible	1 - Negligible, Very Rare	2 - Negligible, Rare	3 - Negligible, Seldom	4 - Negligible, Often	5 - Negligible, Almost Always
2 – Minor	2 - Minor, Very Rare	4 - Minor, Rare	6 - Minor, Seldom	8 - Minor, Often	10 - Minor, Almost Always
3 – Moderate	3 - Moderate,	6 -	9 -	12 -	15 - Moderate,

	Very Rare	Moderate, Rare	Moderate, Seldom	Moderate, Often	Almost Always
4 – Significant	4 - Significant, Very Rare	8 - Significant, Rare	12 - Significant, Seldom	16 - Significant, Often	20 - Significant, Almost Always
5 – Highly significant	5 - Highly Significant, Very Rare	10 - Highly Significant - Rare	15 - Highly Significant, Seldom	20 - Highly Significant, Often	25 - Highly Significant, Almost Always

Table 13: Risk criteria matrix

Acceptance	Risk Level	Description
Not Acceptable	Very High	Requires ongoing executive level oversight. The level of risk ensures that all possible countermeasures are analysed and where possible implemented, to result in a reduction in the level of risk.
	High	An action plan and resources for treatment are required. The level of risk is likely to compromise abilities and should be reduced through treatment strategies if possible.
	Medium	This level of risk should not be automatically accepted but a cost-benefit analysis is needed to determine if treatment is necessary.
Acceptable	Low	The risks are generally acceptable using existing controls and normal operating procedures.

Figure 6 explained the total risk result majority in low area which total 88 total risks with 71.5% based on total population, apart from that the high and medium in total below 30% which is quite good for this organization. After the risk criteria matrix is obtained, risk assessment results can be determined accordingly based on it.

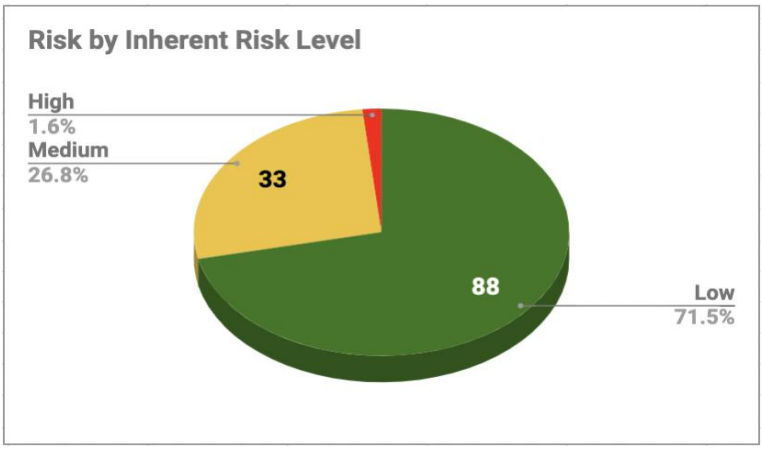

Fig 6: Result of Risk Assessment

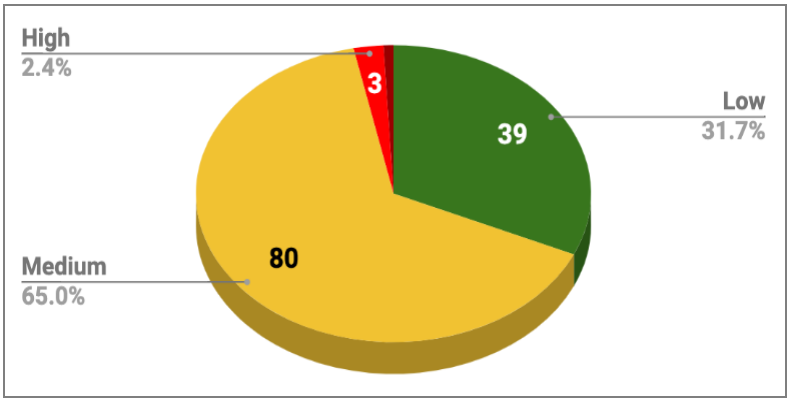

Fig. 7: Result of previous Risk Assessment

Result of risk assessment process in this research is significantly better compared to the previous risk assessment by 39.2%, where there are only 39 assets or 31.7% of the asset population that is in low area on the previous risk assessment. Overall, result of risk assessment conducted in this research has decreased the risk by 42%.

Figure 8 shows in detail how each asset is already registered and mapped into business impact analysis. The impact matrix is defined by management decisions by considering the appetite and vision of the organization.

S/N	Function / Process /Asset	IMPACT OVER TIME ANALYSIS								MTPD *) Maximum Tolerable Period of Disruption	RTO *) Recovery Time Objective
		Impact Area and Level *) see impact metric by hovering on the criteria (notes)	If team and its function / process / activity is disrupted or unavailable for:								
	Source of data		2 Hours	4 Hours	8 Hours	1 Day	7 Days	14 Days	≥ 30 Days	First time where impact = Red (4 – Major or 5 – Catastrophic) Auto filled based on impact over time analysis	RTO must be less or equal than MTPD to provide buffer
...	...	...	...	...	...	...	...	...	...	...	...
2	Physical	Financial	1 – Insignificant	1 – Insignificant	5 – Catastrophic	5 – Catastrophic	5 – Catastrophic	5 – Catastrophic	5 – Catastrophic	4 Hours	2 Hours
		Trust and Reputation	1 – Insignificant	1 – Insignificant	1 – Insignificant	2 – Minor	3 – Moderate	4 – Major	5 – Catastrophic		
		Regulatory & Legal	1 – Insignificant	1 – Insignificant	1 – Insignificant	2 – Minor	3 – Moderate	4 – Major	5 – Catastrophic		
		People	1 – Insignificant	1 – Insignificant	1 – Insignificant	2 – Minor	3 – Moderate	3 – Moderate	3 – Moderate		
		Cyber & Technology Disruption	1 – Insignificant	5 – Catastrophic	5 – Catastrophic	5 – Catastrophic	5 – Catastrophic	5 – Catastrophic	5 – Catastrophic		
...	...	...	...	...	...	...	...	...	...	...	...

Fig 8: Result of business impact analysis

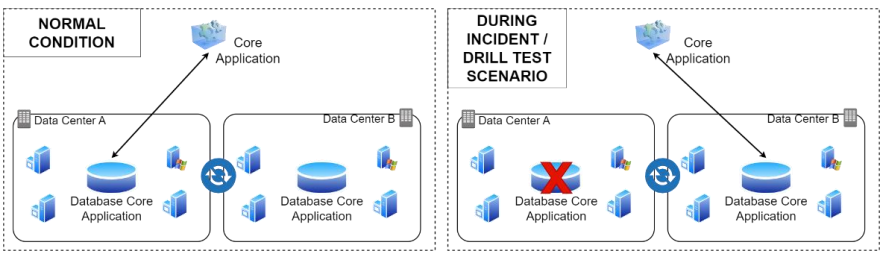

Fig 9: Drill Test Simulation Schema

Drill test was conducted to evaluate the BCM and DRP. In this research, drill test for physical asset - virtual server with unavailable data/information unavailability is conducted. The organization has 2 data centers, data center A as the primary data center and data center B as the disaster recovery data center. During the test, there is one database server that is unavailable from data center A. Thus, DRP process should be executed as soon as possible below the 4 hours MTPD and 2 hours RTO based on the risk impact analysis. During the drill test, the process is considered successful because the recovery time is only 1 hour and 27 minutes, below RTO and significantly below MTPD value.

Table 14: Drill Test Result

Parameter	Defined Value	Test Result	Status
MTPD	4 hours	1 hour 27 minutes	Comply
RTO	2 hours		Comply

After all plan-do-check processes are conducted, business continuity management framework now can be compiled. The BCM framework is compiled as shown in Figure 10.

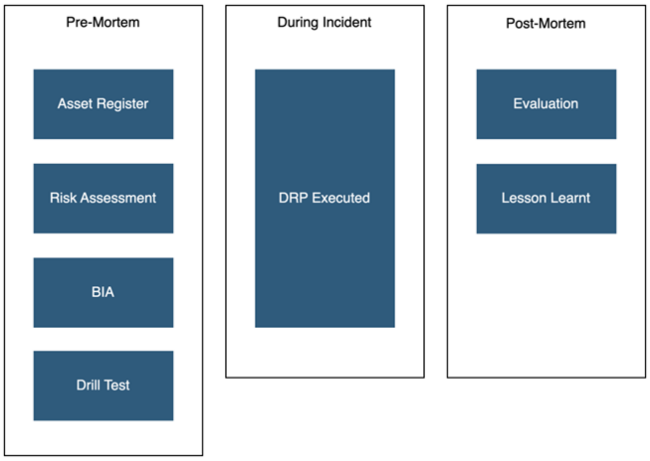

Fig. 10: New BCM Framework

In the new BCM framework, processes are separated into three main phases as shown in Figure 10. On the pre-mortem phase In this phase, asset register, risk assessment, and BIA are conducted with the output of DRP. The plan is simulated on drill test to get the result. Other than that, output of this phase is to detailedly map organization's assets by categorizing them into levels of criticality, and defining the treatment of each asset risk, with that being said, in this phase the entity can figure earlier regarding the exisisting risk and the potential risk that could

happen in the future, and this phase was a fundamental of the BCM process. On the during incident phase, DRP should be run smoothly, to prevent any impact to the business diretly and indirectly, notes on this phase, this phase was the activity needs to be conducted during the disruption/incident is executing the previously defined DRP. The last phase is post-mortem, in this phase the BCM framework need to be evaluated and get insights regarding the previously happened incident as a preventive, correction, and corrective to prevent similar events happened in the organization.

5. Conclusions

This BCM Framework covers the PDCA components of the plan-do-check-act as mandated by any typical ISO management system and divided into 2 schemes which include normal condition and disaster condition based on any dynamic environment issue such as pandemic COVID-19 and any force majeure in the future. On the other hand, the main objective of the new BCM framework include is to increase organizational resilience through business continuity program governance implementation; criticality assessment of functions within organization and its business impact analysis; and exercise and simulations for the selected critical business functions. In addition, it increases employees' vigilance and competency to work around business disruptions until business as usual (BAU) is restored or a new mode of operation is implemented and decreased the significant risk by inherent risk by a total of 42% from the previous role in regards on BCM Implementation which effect on several high and medium severity.

Moreover, this research achieved its pre-defined objectives which design an appropriate BCM framework and simulated the DRP process with MTPD and RTO below the defined values during test result, which is 1 hour 27 minutes, below RTO (2 hours) and significantly below MTPD (4 hours).

References

Alesi, P. (2008). Building enterprise-wide resilience by integrating business continuity capability into day-to-day business culture and technology

Amit, R. &. (n.d.). Value creation in e-business. Strategic Management Journa. Journal of Business Continuity & Emergency Planning, 493-520

Alwarawashdesh, B. &. (2022). A Review on the Challenges and Connections between Cybersecurity and Accounting in Saudi Arabia. Journal of System and Management Sciences, 12(5), 282-296

Baden-Fuller, C. &. (2013). Business models and technological innovation in Long Range Planning. 419-426

Bajgoric, N. (2010). Server operating environment for business continuance. International Journal of Business Continuity and Risk Management, 317-338

Bajgoric. (2014). Information technology, Information systems, Systemic approach, Business continuity. Business continuity management: a systemic framework for implementation, 1-22

Bajgoric. (2018). Reengineering business information systems to support business continuity. Business Continuity and Risk Management, 11-35

Benyoucef, M., & Forzley, S. (2007). Business continuity planning and supply chain management. Supply Chain Forum an International Journal, 14-22

Berry, C. T. (2018). An initial assessment of small business risk management approaches for cyber security threats. Business Continuity and Risk Management, 1-10

Botha, J., & von Solms, R. . (2004). A cyclic approach to business continuity planning. Information Management & Computer Security, 328-337

Bouwman, H., Faber, E., Haaker, T., Kijl, B., & Reuver, M. D. (2008). Conceptualizing the STOF model. Mobile service innovation and business models, 31-70

Bouwman, H., Heikkilä, J., Heikkilä, M., Leopold, C., & Haaker, T. (n.d.). Achieving agility using business model stress testing. Electronic markets, 1-14

Bucherer, E., Eisert, U., & Gassmann, O. (2012). Toward systematic business model innovation: Lessons from product innovation management. Creativity and Innovation Management, 183-198

Ebersberger, B. K. (2021). Hop to it! The impact of organization type on innovation response time to the COVID-19 crisis. Journal of Business Research, 126-135

Gibb, F. B. (2006). A framework for business continuity management. International Journal of Information Management, 128-141

Hadjinicolaou, N., Yannakou, K., & Kader, M. (2022). Using Strategic Foresight to Improve Future Readiness of Project Management. International Journal of Smart Business and Technology, 10(2), 1-12, doi:10.21742/IJSBT.2022.10.2.01

Heng, G. M. (2015). Business Continuity Management Planning Methodology. International Journal of Disaster Recovery and Business Continuity, 9-16

Institute, B. S. (2006). Business Continuity Management Systems

Isms.online. (2020, 9 18). isms.online. Retrieved from isms.online: https://www.isms.online/iso-27001/annex-a-17-information-security-aspects-of-business-continuity-management/

Joachim, J. J. (2022). Embedding Large-Scale Information Technology into the Organization's Work Systems. International Journal of Smart Business and Technology, 10(1), 41-62. DOI:10.21742/IJSBT.2022.10.1.04

Kadam, D. M. (2011). Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) for financial cooperatives in new market economy. Disaster Recovery Plan (DRP) and Business Continuity Plan (BCP) for financial cooperatives in new market economy, 4-13

Kominfo. (2020, 07 1). kominfo.go.id. Retrieved from kominfo: https://aptika.kominfo.go.id/2020/07/pse-wajib-lakukan-pendaftaran-hingga-oktober-2020/

Kramer, A. K. (2020). The potential impact of the Covid-19 pandemic on occupational status, work from home, and occupational mobility. Journal of Vocational Behavior, 4-6

Liguori, E. W. (2020). From Offline to Online: Challenges and Opportunities for Entrepreneurship Education Following the COVID-19 Pandemic. Entrepreneurship Education and Pedagogy, 2-6

Niemimaa, M. J. (2019). Business continuity of business models: Evaluating the resilience of business models for contingencies. International Journal of Information Management, 208-216

O'Har, J. P. (2017). Development of a Risk Register Spreadsheet Tool for Enterpriseand Program-Level Risk Management. Transportation research record, 19-27

Radeschütz, (2015). Business impact analysis—a framework for a comprehensive analysis and optimization of business processes. Computer Science-Research and Development, 69-86

Rongrong, (2019). A Framework for Risk Assessment in Cyber Situational Awareness. IET Information Security, 149-156

Wong, W. N. (2010). The role of business continuity management in organisational long range planning. International Journal of Business Continuity and Risk, 247-258