ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 13 (2023) No. 2, pp. 409-427
DOI:10.33168/JSMS.2023.0228

Evaluation of the Implementation of Business Continuity Management Using COBIT 2019 Framework in Public Sector

Yohanes Beato Dionisius, Ditdit Nugeraha Utama

Computer Science Department, Binus Graduate Program – Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia, 11480
yohanes.dionisius@binus.ac.id, ditdit.utama@binus.ac.id

Abstract. The research is based on the global struggle with the COVID-19 pandemic, where countries are facing challenges in managing the flow of essential goods, including medical devices, medicines, and consumer goods. In this regard, the Indonesian National Single Window System (SINSW) can play a critical role in managing the import and export of goods required to combat the pandemic. The experience of the pandemic has emphasized the need for SINSW to enhance its capacity to meet demands in normal and emergency situations. Therefore, Lembaga National Single Window (LNSW), a unit of the Ministry of Finance, needs to develop and evaluate its business continuity governance to meet domestic needs and business requirements. To measure the level of business continuity management capability, this study utilizes the COBIT 2019 framework, specifically the DSS (Deliver, Service, Support) 04 domain. The research aims to address the problem of measuring the level of business continuity management capability and providing recommendations for improving LNSW's business continuity governance. Based on the assessment, the DSS04 - Managed Continuity process capability value owned by LNSW has only partially achieved level 1 process capability, and further activities and work products are required to fulfill the next level of achievement. The study is expected to contribute to LNSW by providing a mapping of the maturity level of business continuity management and recommendations for improvement based on the evaluation results. By enhancing the level of business continuity management capability, it is anticipated that the quality of public services will improve. Moreover, the author's work paper, which utilizes the COBIT 2019 framework to assess the level of capability, can be utilized by LNSW as a self-assessment tool for regularly evaluating business continuity management and as a reference for future researchers in this field.

Keywords: Business continuity management; business impact analysis; cobit 2019; public sector.

1. Introduction

The Indonesian government has demonstrated its commitment to enhancing public services in export, import, and logistics through the establishment of the Lembaga National Single Window (LNSW) via the Presidential Regulation No. 44 of 2018 that concerns the Indonesia National Single Window (INSW). This initiative aims to offer transparent, consistent, efficient, and simplified public services that comply with national and international standards. The LNSW is underpinned by dependable information and communication technology, as well as a service-oriented and control-balanced approach. The availability of a Service Level Agreement that is customized to the requirements of all stakeholders is also part of this effort to improve the quality of public services.

The national export, import, and logistics services are constantly being improved, and in early 2020, the System of Indonesian National Single Window (SINSW) was put to the test during the pandemic. Countries worldwide are grappling with the COVID-19 pandemic, including the challenge of managing the flow of essential goods like medical equipment, medicine, and consumer goods. SINSW played a crucial role in handling the pandemic by establishing and implementing export and import services for emergency goods, such as the Emergency Response Permit application. In response to the pandemic experience, SINSW must enhance its capacity to ensure readiness in responding to demands in both normal and emergency situations. The pandemic has been a significant wake-up call for Indonesia and other countries to improve their services.

The question of how to develop a tool to evaluate the maturity level of Business Continuity Management (BCM) using the capability model method as a self-assessment tool for LNSW is a major concern. The author chose to use COBIT 2019 because it provides a range of management and governance processes. Unlike COBIT 4.1, COBIT 2019's focus is on information technology governance, and it includes a domain that emphasizes business continuity governance processes, which is the DSS04 domain (Deliver, Service, Support). The reason for selecting the DSS04 domain is that it aims to continue critical business operations and maintain information availability at an acceptable level during a significant disruption.

Furthermore, we offer a case study analysis in the public sector, specifically on LNSW, which is a unit under the Ministry of Finance of the Republic of Indonesia that manages INSW and implements SINSW to electronically handle various types of documents related to export, import, and national logistics. These documents include customs documents, quarantine documents, licensing documents, port/airports documents, and others. LNSW has been continuously leveraging IT/IS to support its business processes, which aligns with the aspects of IT governance as stipulated by current government regulations.

2. Theoretical View

2.1. Definition of Business Continuity Management

The implementation of BCM can prevent severe consequences caused by business disruptions. BCM is a comprehensive management process that involves identifying potential threats to an organization and assessing their impacts on business operations. It also provides a framework for building business resilience by enabling effective responses to safeguard the interests of key stakeholders, reputation, image, and ability to produce services or products, as defined by the International Organization for Standardization (2006). Meanwhile, Kliem (2015) described business continuity (BC) as a discipline that involves developing, implementing, and maintaining strategies and procedures to ensure the continuity or recovery of essential business processes. Business preparedness, which is a subset of BC, helps an organization to sustain and serve consumers by continuing or recovering services or products before, during, and after an event.

To handle and recover from disturbances or disasters, organizations need to choose the most efficient and effective methods. However, there will always be a trade-off between the cost of prevention or recovery and the time required for the organization to recover, as illustrated in Fig. 1. This trade-off must be considered carefully. Several frameworks are available to guide the implementation of BCM, including COBIT 2019 (DSS04-Manage process Continuity), ISO 22301:2012 Business Continuity

Management System, BS 25999, NFPA 1600 Standard on Disaster / Emergency Management and Business Continuity Programs, and NIST Special Publication 800-34 Contingency Planning Guide for Information Technology Systems.

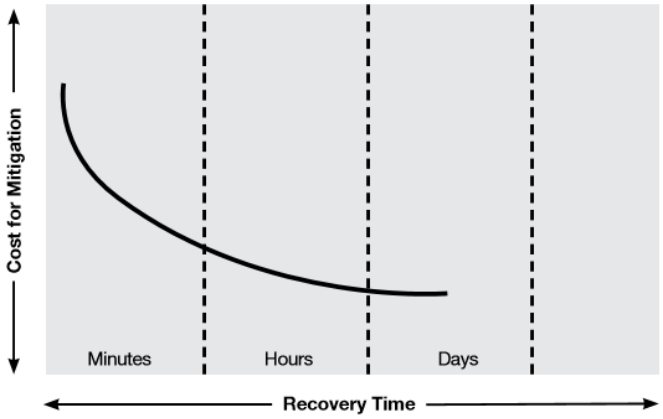

Fig. 1: Trade-Off between Cost and Disaster Recovery Time

2.2. Cycles / Main Activities of Business Continuity Management

While there may be some variations between frameworks, the overall BCM process can typically be divided into six main activity steps, as illustrated in Fig. 2. The first step is risk assessment, which involves evaluating risks associated with activities, processes, and systems within the BCM cycle. This includes identifying risks, analyzing their likelihood and impact, and evaluating their overall level of risk. The results of the risk assessment activities are then used to develop control measures aimed at mitigating identified risks.

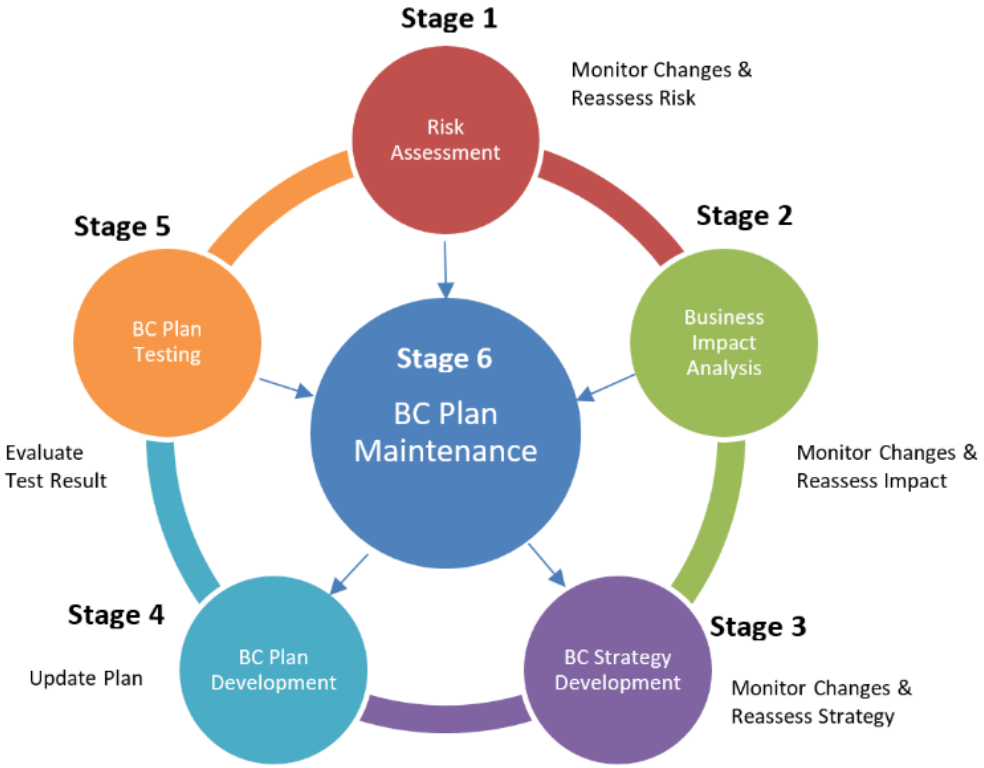

Fig. 2: Cycles / Main Activities of Business Continuity Management

In this stage, the focus is on evaluating potential threats to business continuity and identifying the risks that could impact the organization, taking into account their probability of occurrence and potential

impact. The main goal of this step is to manage risks by implementing one or more risk control options, such as accepting the risk, avoiding it, mitigating it, or transferring it.

The next step in the BCM process is the Business Impact Analysis (BIA). During this stage, critical information is gathered such as the key areas that affect the organization's objectives and the processes within them, the potential financial and operational impact on the organization, and the necessary requirements to restore critical business processes in case of disruptions.

The third stage of BCM is Business Continuity Strategy Development, which aims to formulate a strategy that fulfills the recovery requirements identified in the BIA stage. This strategy comprises a selection of activities or recovery steps that can be implemented as alternative resources in case critical resources are unavailable. Typically, the recovery requirements can be categorized into four areas: work area, IT systems and infrastructure, manufacturing/production/service areas, and crucial data and records. The business continuity strategy development framework involves four phases, namely, recovery requirement identification (Phase A), recovery option identification (Phase B), availability time assessment (Phase C), and funding capability assessment (Phase D).

The fourth stage involves the development of the Business Continuity Plan (BCP). The BCP is composed of procedures and guidelines that can be employed by an organization to reduce the impact of a disaster on its operations. By establishing procedures and guidelines at the outset, critical decisions can be avoided during a crisis. The acceptability of the business continuity plan is determined by two criteria. The first criterion is that the plan must be comprehensive, encompassing all critical processes, and taking into account all phases of recovery, including initial response and notification, problem assessment and escalation, disaster declaration, plan implementation logistics, recovery and resumption, and normalization. The second criterion is feasibility, which means the plan is current, adaptable, and not challenging to implement within the available budget, team, resources, and facilities.

Stage 5 of the BCM process is BCP Testing. The main aim of this stage is to confirm that the strategies, assumptions, activities, procedures, and guidelines outlined in the BCP are effective against potential disruptions and to identify any weaknesses in the plan. Stage 6 is BCP Maintenance, which is equally important despite having a tested and proven BCP. The ever-changing environment and conditions of the organization necessitate making appropriate adjustments to ensure that the BCP still meets the comprehensive and suitable criteria. The goal of this stage is to keep the BCP current, complete, accurate, and ready to implement. The maintenance process can be divided into four phases, beginning with change management and ending with auditing the BCP.

2.3. COBIT 219

COBIT is a framework that assists enterprises, such as companies, organizations, or governments, in managing and utilizing their IT assets or resources to achieve their goals. The use of IT is essential for today's companies as technology and information processing are critical to achieving their objectives. The scope of enterprise IT is not limited to the IT department of an organization.

The COBIT 2019 framework distinguishes between governance and management and clarifies the differences between them. Governance and management have distinct activities, require different organizational structures, and are oriented towards different goals. According to ISACA (2019), governance ensures that stakeholder needs, circumstances, and options are evaluated to establish balanced, agreed-upon enterprise objectives. It also ensures that direction is established through prioritization and decision-making, and that performance and compliance are monitored in relation to the established direction and objectives. The board of directors, headed by the chairperson, is typically responsible for overseeing corporate governance. In larger, more complex enterprises, certain governance duties may be delegated to specific organizational structures at the appropriate level. Management, on the other hand, designs, builds, operates, and oversees activities in accordance with the governance body's established guidelines to accomplish corporate goals.

COBIT 2019 introduces several changes compared to previous versions, according to ISACA (2019). First, the new version emphasizes flexibility and openness. COBIT now uses design factors to

allow for customization that aligns with the user's specific context. Additionally, COBIT's open architecture permits the addition or modification of emphasis areas within the core model. Second, COBIT aims to stay current and applicable by promoting the use of various sources, including the latest IT standards and compliance regulations. Third, COBIT can be both prescriptive and descriptive, and the conceptual model provides a recipe-like approach to creating a customized IT governance system. Finally, COBIT 2019 incorporates the COBIT performance management paradigm and introduces the concepts of maturity and capability to improve compatibility with CMMI.

The development of COBIT 5 and other frameworks served as a foundation for COBIT 2019, which is applicable to several standards and frameworks within the IT governance field. COBIT's established status as the overarching framework for IT governance is supported by its conformance with related standards. Future versions of COBIT will allow users to submit ideas for content upgrades, which will be regulated contributions deployed on an ongoing basis. COBIT's architecture is designed to keep pace with advancements in science and evolution.

ISACA (2019) states that the COBIT framework divides its governance and management goals into five domains. These domains are named using verbs that describe the main goal and the specific area of activity found within each domain. The Evaluate, Direct, and Monitor (EDM) domain groups the governance goals. Within this domain, the governing body evaluates strategic possibilities, directs senior management on selected options, and monitors strategy implementation. On the other hand, management goals are grouped in four domains. The first of these is Align, Plan, and Organize (APO), which covers the entire process of IT planning, execution, and maintenance. The second is Build, Acquire, and Implement (BAI), which focuses on defining, acquiring, and implementing IT solutions and integrating them into business processes. The third domain is Deliver, Service, and Support (DSS), which deals with the operational delivery and support of IT services, including security. Lastly, the Monitor, Evaluate, and Assess (MEA) domain is responsible for monitoring IT performance and ensuring compliance with internal and external requirements.

Every company must establish, adapt, and maintain a governance system that consists of various components to meet governance and management objectives. These components include processes, organizational structure, policies and procedures, information, culture and behavior, skills and competencies, and services, infrastructure, and applications.

According to (ISACA, 2019), a process is a collection of practices and actions designed to achieve a specific purpose and produce outputs that contribute to overall IT-related goals. The organizational structure is where most decisions are made within a company. Principles, policies, and frameworks integrate desired behavior into practical rules for daily business operations. The information generated and used by the company is widely disseminated throughout the organization, and COBIT emphasizes the importance of this information for effective corporate governance systems. The culture, ethics, and behavior of individuals and organizations are often underestimated in terms of their impact on the success of governance and management activities. People, skills, and competencies are necessary for sound decision-making, implementation of remedial actions, and successful completion of all activities. Services, infrastructure, and applications refer to the technology and infrastructure that support the governance system for enterprise IT processing.

3. Related Works

(Yanthestya & Gondodiyoto, 2013) employed various research methods. Firstly, they conducted a literature review to establish a framework or theoretical foundation to support the evaluation of research projects. Secondly, they conducted field research to gather factual data from the current system, which served as empirical data. Thirdly, they conducted a comparative analysis with ISO 22301, whereby the empirical data obtained from the field research was compared with the ISO 22301 standardization. The goal was to identify and evaluate any weaknesses or shortcomings when compared to the reference framework or theoretical basis obtained through the literature review. Lastly, the authors provided

recommendations for correcting any existing weaknesses or deficiencies so that they align with the reference framework or theoretical basis obtained through the literature review.

In their study, (Iqbal et al., 2016) utilized COBIT 5, an IT Governance framework, as a reference when evaluating BCP. The decision to use COBIT 5 was based on a comparative analysis of multiple IT Governance Frameworks, in which COBIT was deemed the most effective based on various parameters. The researchers chose to use an IT Governance framework because of the advantages it offers in terms of providing guidance for conducting evaluations. Primary data was collected through questionnaires and interviews in nine different areas of employment at DSSDI UGM, supplemented by secondary sources such as literature reviews and examinations of IT service delivery documentation. The analysis showed that the process capability level of COBIT 5, which served as a benchmark for assessing BCP at DSSDI, was consistently at capability level 1. Based on the findings, it can be concluded that DSSDI has implemented information technology governance in the area of BCP, but there is room for improvement in managing the output of BCP and implementing it more regularly in the future.

After reviewing the existing literature, the authors identified a gap in the research. In the previous study, the authors used the ISO 22301 framework, while the current study utilized the COBIT 2019 framework due to its comprehensive nature that clearly delineates responsibilities between governance and management. The second study used the COBIT 5 framework with 18 process domains and all corresponding management practices, which, in the authors' opinion, did not have a focused scope on BCM. In contrast, the current research only focused on one process domain and examined each work product and management practice within that domain.

4. Research Methodology

This study examines the implementation of business continuity management within the information systems of LNSW. By utilizing the Capability Model from the COBIT 2019 framework, the study identifies which aspects of IT activities are effective and which require improvement to achieve the organization's goals aligned with its vision and mission. The study collected primary data directly from respondents and informants from the organization, including the organization's vision and mission, IT resources (including applications, information, infrastructure, and involved employees), IT processes, and IT benefits for the organization. Secondary data, which included information on the LNSW's general conditions, policies related to business continuity management and IT services, IT strategic plans, and information and communication network infrastructure data, was obtained from sources such as journals, books, and other available print or online resources. The specified framework is illustrated in Fig. 3. for further clarification.

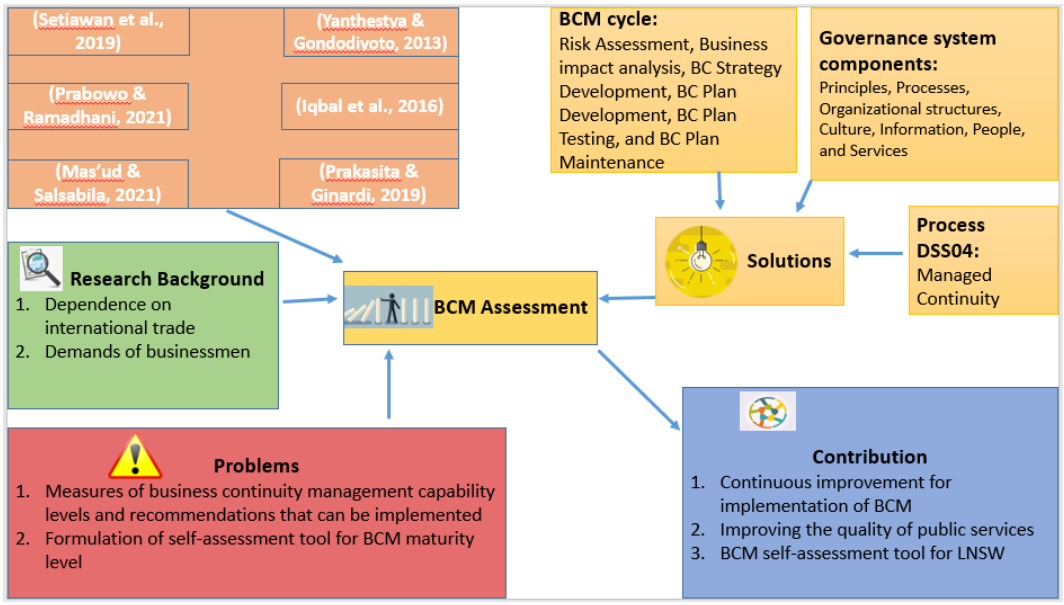

Fig. 3: Research Mindset

Figure 3 illustrates the research mindset, which is based on a fundamental approach that begins with the identification of two critical elements: the problem statement and the benefits of addressing the problem. The focus of this study is on updating the BCM process based on two fundamental factors, which are highlighted in the framework. The problem statement identifies two critical issues: the measurement of the maturity level of BCM and the recommendations that can be implemented in LNSW. Additionally, the authors developed a self-assessment tool, based on the COBIT 2019 framework, to evaluate BCM regularly.

The primary goal of this research is to aid LNSW in enhancing its business continuity management capability by implementing the recommended suggestions. This is expected to improve the quality of public services offered by the organization. Furthermore, the self-assessment working paper formulated by the authors based on the COBIT 2019 framework is envisioned to serve as a monitoring and evaluation tool for LNSW to conduct regular BCM assessments and as a point of reference for future researchers investigating this area of study.

The process of evaluating the capability of a BCM process involves a series of steps that are carried out sequentially for each process. The first step involves determining whether the process being assessed has achieved capability level 1, with indicators that are specific and unique for each process. The assessment is focused on the attainment of the outcome of the process attributes (PA) capability level 1. The second step is to determine if the selected process has achieved capability levels 2 to 5, with assessment criteria that are general and applicable to all processes but differ for each level of capability. The third step involves documenting and summarizing the capability levels for all the assessed processes. Finally, areas for improvement for the assessed process are identified and presented to management for the purpose of process improvement.

To evaluate the process capability level, it is necessary to conduct an assessment of process attributes (PA). The outcome of the PA assessment for each level is categorized into four different categories. Table 1 contains the rating scale for the IT governance process attributes, which explains each category in detail.

Table 1: IT Governance Process Attribute Rating Scale

Category	Description	Achievement
N: *Not achieved*	There is little to no evidence that the attributes of the process being evaluated have been achieved.	0 up to 15%

Category	Description	Achievement
P: *Partially achieved*	There is some evidence of the strategy and some evidence that the evaluated process attributes were achieved. Achievement of some attributes may involve some unpredictability.	> 15 up to 50%
L: *Largely achieved*	There is evidence of a methodical approach and significant accomplishment of the process attributes that were evaluated. Some of the shortcomings associated with this attribute might be present in the evaluation process.	> 50% up to 85%
F: *Fully achieved*	There is evidence that the examined process attributes were fully achieved, together with a thorough and systematic approach. Regarding the qualities found in the evaluated procedure, there are no notable flaws.	> 85% up to 100%

The capability level of an organization can be determined if the attributes at that level meet either "fully achieved (F)" or "largely achieved (L)" category, and the attribute values for all levels below meet the "fully achieved (F)" category. The standard process attribute rating scale is mentioned in Table 2, which demonstrates the application of the scale. Each process capability level, except for level 0, has a set of attributes. Level 1 (Performed process) has only one attribute, namely PA1.1 Process performance, which measures the extent to which process objectives are achieved. Level 2 (Managed process) has two attributes, namely PA 2.1 Performance management, which measures the extent to which process implementation is managed, and PA2.2 Work product management, which measures the extent to which the work products produced by the process are managed appropriately. Level 3 (Established process) has two attributes, namely PA3.1 Process definition, which measures the extent to which standard processes are maintained to support process execution, and PA3.2 Process deployment, which measures the extent to which standard processes are implemented effectively as processes to achieve outcomes. Level 4 (Predictable process) has two attributes, namely PA4.1 Process measurement, which measures the extent to which the measurement results are used to ensure that the implementation of the process can support the achievement of process objectives in order to achieve organizational goals, and PA4.2 Process control, which measures the extent to which processes are managed quantitatively to produce a process that is stable, capable, and predictable within defined limits. Level 5 (Optimizing process) has two attributes, namely PA5.1 Process innovation, which measures the extent to which changes to the process are identified from an analysis of the (general) causes of variation and from an investigation of the innovation approach in process implementation, and PA5.2 Process optimization, which measures the extent to which changes to the definition, management, and implementation of processes have an effective impact on achieving process improvement objectives.

Table 2: Process Attribute Rating Scale Standard

Process Attributes	Level 1 Performed	Level 2 Managed	Level 3 Established	Level 4 Predictable	Level 5 Optimising
PA 5.2 – *Process Optimisation* PA 5.1 – *Process Innovation*					**L/F**
PA 4.2 – *Process Control* PA 4.1 – *Process Measurement*				**L/F**	**F**
PA 3.2 – *Process Deployment*			**L/F**	**F**	**F**

Process Attributes	Level 1 Performed	Level 2 Managed	Level 3 Established	Level 4 Predictable	Level 5 Optimising
PA 3.1 – *Process Definition*					
PA 2.2 – *Work Product Management* PA 2.1 – *Performance Management*		**L/F**	**F**	**F**	**F**
PA 1.1 – *Process performance*	**L/F**	**F**	**F**	**F**	**F**

It has been reported that COBIT 2019 provides a framework for process capability based on CMMI (ISACA, 2019). Each process for governance and management objectives can operate at one of five capability levels, ranging from 0 to 5. The capability level of a process indicates how well it is applied and functioning. COBIT's core model assigns capability levels to all process activities, allowing for a clear definition of the processes and activities required to reach different capability levels. Table 3 outlines the definition of IT governance process capability levels. This study used several techniques to collect data and evaluate the implementation of BCM, including document analysis, distributing questionnaires to responsible officials/employees, and conducting field observations to ensure the appropriateness of BCM process activities with existing documentation.

Table 3: Definition of IT Governance Process Capability Level

CAPABILITY LEVELS	DEFINITION
Level 0 (*Incomplete Process*)	The process is not implemented or fails to achieve the stated goals. At this level, evidence to suggest the achievement of systematic process objectives is incomplete or non-existent.
Level 1 (*Performed Process*)	The implemented process has achieved the goals set for the process.
Level 2 (*Managed Process*)	Processes that have been implemented at the performed process level are now executed with proper management (planned, monitored, and adjusted) and outputs have been defined, controlled, and properly maintained.
Level 3 (*Established Process*)	Processes that have been implemented at the managed process level are now implemented using processes that are able to achieve the expected outcomes.
Level 4 (*Predictable Process*)	Processes that have been implemented at the level of established processes, now operate within defined limits to achieve process outcomes.
Level 5 (*Optimising Process*)	Processes that have been implemented at the predictable process level are now continuously improved to meet current and future business objectives.

5. Result and Discussion

The Single Window system in Indonesia was developed as a result of the agreement made by the Leaders of ASEAN member countries, referred to as the Bali Concord II, in 2003. Subsequently, the ASEAN economic ministers signed an agreement in Kuala Lumpur in 2005, to establish and implement the ASEAN Single Window (ASW). The National Single Window system in Indonesia, which is responsible for the development and implementation of the Single Window system, is operated through the INSW Portal. Presidential Regulation Number 76 of 2014 established the Pengelola Portal Indonesia National Single Window (PP INSW) to manage the INSW Portal, under the authority of the Minister of Finance. In 2018, through Presidential Regulation Number 44 of 2018 concerning the Indonesia National Single

Window, the name PP INSW was changed to LNSW and was given the responsibility of managing INSW and administering the INSW system. LNSW has new functions, which include formulating and implementing guidelines for INSW management and SINSW implementation, providing facilities for submission, inclusion, and elimination of post-border trade regulations at SINSW, carrying out communication, coordination, and cooperation in the field of National Single Window system in national and international forums, and conducting harmonization and synchronization of business processes between ministries/agencies in the context of implementing INSW.

In accordance with the Minister of Finance Regulation Number 78/PMK.01/2022 on the Organization and Work Procedures of LNSW, LNSW is a subordinate unit that reports to the Minister of Finance. LNSW's main responsibility is to manage and administer the INSW system, which handles electronic customs documents, quarantine documents, licensing documents, port/airport documents, and other documents related to exports, imports, and national logistics documents. LNSW's organizational structure comprises the Secretariat, the Directorate of Business Process Efficiency, the Directorate of Information Technology, and the Directorate of Service, Data, and Partnership Management.

The primary responsibility for implementing IT governance in LNSW rests with the LNSW IT Steering Committee and the LNSW Chief Information Officer (CIO). These two entities were established as representatives of the LNSW leadership for managing IT-related aspects. The LNSW IT work unit, specifically the Information Technology Directorate, coordinates the technical implementation of IT governance. This involves the Directorate of Business Process Efficiency, the Directorate of Service, Data, and Partnership Management, and the Secretariat, who manage specific processes as part of LNSW's IT governance. The membership of the LNSW KPTIK, as determined by the Regulation of the LNSW Head Number 8/LNSW/2020, comprises five LNSW officials, including the Head of LNSW as Director, the Director of Information Technology as Chairman, the Secretary as Member, the Director of Business Process Efficiency as Member, and the Director of Service, Data, and Partnership Management as Member.

According to Minister of Finance Regulation Number 122/KM.1/SJ.2/2019, the analysis of job descriptions within LNSW indicates that the BCM management process is implemented across every unit in the organization. The LNSW Secretariat is responsible for conducting organizational risk management and each unit possesses a risk management charter. The Performance Planning and Management Subdivision is responsible for identifying, assessing, mitigating, and periodically evaluating organizational risks. The Directorate of Business Process Efficiency prepares business impact analysis which is updated regularly in a discussion forum attended by business process owners and IT units. The Information Technology Directorate is responsible for preparing policies related to the management of IT service continuity and regularly conducting IT service continuity plan testing activities such as application drills. This directorate also prepares and updates disaster recovery plans and compiles IT risks. The Governance and IT Program Management Section prepares policies and disaster recovery plans, the ICT Operations Section conducts testing, and the Information Security and ICT Infrastructure Management Section prepares IT risks. The Directorate of Service, Data, and Partnership Management is responsible for managing the IT service catalog, which is regularly compiled and updated by the Service Quality Assurance Section. Furthermore, this directorate coordinates with other ministries/agencies in the event of a disruption to the LNSW system.

Management objective DSS04 is comprised of eight management practices that include defining the business continuity policy, objectives, and scope; maintaining a continuity strategy; developing and implementing a business continuity response; exercising, testing, and reviewing the BCP; reviewing, maintaining, and improving the continuity plan; conducting continuity plan training; managing backup arrangements; and conducting post-resumption reviews. Additionally, there are eighteen work products associated with this process. A literature review shows that eight of the work products have a weight of 2, while the remaining ten have a weight of 1. The weight of each work product is valued at 1. The assessment of the organization's capability level is conducted through document analysis and observation.

If the organization has a management practice and work product, it is marked as "Y" (Yes) and assigned a value according to its weight. On the other hand, if the organization does not have a management practice or work product, it is marked as "N" (No) and given a value of 0. Table 4 provides a detailed assessment of each work product.

Table 4: Work Product DSS04

Work Product	Weight	(Y/N)	Value
Policy and objectives for business continuity	2	Y	2
Disruptive incident scenarios	2	Y	2
Assessments of current continuity capabilities and gaps	2	Y	2
Business impact analyses	1	Y	1
Continuity requirements	1	Y	1
Approved strategic options	1	Y	1
Incident response actions and communications	2	N	0
Business continuity plan	2	N	0
Test objectives	2	N	0
Test exercises	2	N	0
Test results and recommendations	2	N	0
Results of review of plans	1	N	0
Recommended changes to plans	1	N	0
Training requirements	1	N	0
Monitoring results of skills and competencies	1	N	0
Test results of backup data	1	Y	1
Post-resumption review report	1	N	0
Approved changes to the plans	1	N	0

The first management practice is to define the business continuity policy, objectives and scope. It has 4 activities and each activity has a weight of 2. Based on document analysis and observation, this DSS04-BP1 management practice gets a score of 8 from all activities. The details of this DSS04-BP1 are described in Table 5.

Table 5: Management practice DSS04-BP1

Activities	Weight	(Y/N)	Value
1. Identify internal and outsourced business process and services activities that are critical to the enterprise operations or necessary to meet legal and/or contractual obligations.	2	Y	2
2. Identify key stakeholders and roles and responsibilities for defining and agreeing on continuity policy and scope.	2	Y	2
3. Define and document the agreed-on minimum policy objectives and scope for business continuity and embed the need for continuity planning in the enterprise culture.	2	Y	2
4. Identify essential supporting business processes and related IT services.	2	Y	2

The second management practice is maintaining a continuity strategy. It has 8 activities and each activity has a weight of 1. Based on document analysis and observation, this management practice with code DSS04-BP2 gets an 8 score from all activities. The details of this DSS04-BP2 are described in Table 6.

Table 6: Management practice DSS04-BP2

Activities	Weight	(Y/N)	Value
1. Identify potential scenarios likely to give rise to events that could cause significant disruptive incidents.	1	Y	1
2. Conduct a business impact analysis to evaluate the impact over time of a disruption to critical business functions and the effect that a disruption wouldhave on them.	1	Y	1
3. Establish the minimum time required to recover a business process and supporting IT based on an acceptable length of business interruption and maximum tolerable outage.	1	Y	1
4. Assess the likelihood that threats that could cause loss of business contiunuity and identify measures that will reduce the likelihood and impact through improved prevention and increased resilience.	1	Y	1
5. Analyse continuity requirements to identify the possible strategic business and technical options	1	Y	1
6. Determine the conditions and owner of key decisions that will cause the continuity plans to be invoked.	1	Y	1
7. Identify resource requirements and costs for each strategic technical option and make strategic recommendations.	1	Y	1
8. Obtain executive business approval for selected strategic options.	1	Y	1

The third management practice is to develop and implement a business continuity response. It has 8 activities and each activity has a weight of 1. Based on document analysis and observation, this management practice with code DSS04-BP3 gets a score of 6 from all activities. The details of this DSS04-BP3 are described in Table 7.

Table 7: Management practice DSS04-BP3

Activities	Weight	(Y/N)	Value
1. Define the incident response actions and communications to be taken in the event of disruption. Define related roles and responsibilities, including accountability for policy and implementation.	1	Y	1
2. Develop and maintain operational BCPs containing the procedures to be followed to enable continued operation of critical business processes and/or temporary processing arrangements, including links to plans of outsourced service providers.	1	Y	1
3. Ensure that key suppliers and outsource partners have effective continuity plans in place. Obtain audited evidence as required.	1	Y	1
4. Define the conditions and recovery procedures that would enable resumption of business processing, including updating and reconciliation of information databases to preserve information integrity.	1	Y	1
5. Define and document the resources required to support the continuity and recovery procedures, considering people, facilities and IT infrastructure.	1	Y	1

6. Define and document the information backup requirements required to support the plans, including plans and paper documents as well as data files, and consider the need for security and off-site storage.	1	Y	1
7. Determine required skills for individuals involved in executing the plan and procedures.	1	Y	1
8. Distribute the plans and supporting documentation securely to appropriately authorised interested parties and make sure they are accessible under all disaster scenarios.	1	Y	1

The fourth management practice is exercise, test and review the BCP. It has 6 activities and each activity has a weight of 2. Based on document analysis and observation, this management practice with code DSS04-BP4 gets a score of 0 for all activities. The details of this DSS04-BP4 are described in Table 8.

Table 8: Management practice DSS04-BP4

Activities	Weight	(Y/N)	Value
1. Define objectives for exercising and testing the business, technical, logistical, administrative, procedural and operational systems of the plan to verify completeness of the BCP in meeting business risk.	1	Y	1
2. Define and agree on with stakeholders exercises that are realistic, validate continuity procedures, and include roles and responsibilities and data retention arrangements that cause minimum disruption to business processes.	1	Y	1
3. Assign roles and responsibilities for performing continuity plan exercises and tests.	1	Y	1
4. Schedule exercises and test activities as defined in the continuity plan.	1	Y	1
5. Conduct a post-exercise debriefing and analysis to consider the achievement.	1	Y	1
6. Develop recommendations for improving the current continuity plan based on the results of the review.	1	Y	1

The fifth management practice is to review, maintain and improve the continuity plan. It has 4 activities and each activity has a weight of 1. Based on document analysis and observation, this management practice with code DSS04-BP5 gets a score of 1 from all activities. The details of this DSS04-BP5 are described in Table 9.

Table 9: Management practice DSS04-BP5

Activities	Weight	(Y/N)	Value
1. Review the continuity plan and capability on a regular basis against any assumptions made and current business operational and strategic objectives.	1	N	0
2. Consider whether a revised business impact assessment may be required, depending on the nature of the change.	1	Y	1
3. Recommend and communicate changes in policy, plans, procedures, infrastructure, and roles and responsibilities for management approval and processing via the change management process.	1	N	0

4. Review the continuity plan on a regular basis to consider the impact of new or major changes to: enterprise organisation, business processes, outsourcing arrangements, technologies, infrastructure, operating systems and application systems.	1	N	0

The sixth management practice is conduct continuity plan training. It has 3 activities and each activity has a weight of 1. Based on document analysis and observation, this management practice with code DSS04-BP6 gets a score of 0 for all activities. The details of this DSS04-BP6 are described in Table 10.

Table 10: Management practice DSS04-BP6

Activities	Weight	(Y/N)	Value
1. Define and maintain training requirements and plans for those performing continuity planning, impact assessments, risk assessments, media communication and incident response. Ensure that the training plans consider frequency of training and training delivery mechanisms.	1	N	0
2. Develop competencies based on practical training including participation in exercises and tests.	1	N	0
3. Monitor skills and competencies based on the exercise and test results.	1	N	0

The seventh management practice is managing backup arrangements. It has 5 activities and each activity has a weight of 1. Based on document analysis and observation, this management practice with code DSS04-BP7 gets a score of 4 from all activities. The details of this DSS04-BP7 are described in Table 11.

Table 11: Management practice DSS04-BP7

Activities	Weight	(Y/N)	Value
1. Back up systems, applications, data and documentation according to a defined schedule, considering: • Frequency (monthly, weekly, daily, etc.) • Mode of backup (e.g., disk mirroring for real-time backups vs. DVD-ROM for long-term retention) • Type of backup (e.g., full vs. incremental) • Type of media • Automated online backups • Data types (e.g., voice, optical) • Creation of logs • Critical end-user computing data (e.g., spreadsheets) • Physical and logical location of data sources • Security and access rights • Encryption	1	Y	1
2. Ensure that systems, applications, data and documentation maintained or processed by third parties are adequately backed up or otherwise secured. Consider requiring return of backups from third parties. Consider escrow or deposit arrangements.	1	Y	1
3. Define requirements for on-site and off-site storage of backup data that meet the business requirements. Consider the accessibility required to back up data.	1	Y	1
4. Roll out BCP awareness and training.	1	N	0

5. Periodically test and refresh archived and backup data.	1	Y	1

The eighth management practice is conducting post-resumption review. It has 4 activities and each activity has a weight of 1. Based on document analysis and observation, this management practice with code DSS04-BP8 gets a score of 0 for all activities. The details of this DSS04-BP8 are described in Table 12.

Table 12: Management practice DSS04-BP8

Activities	Weight	(Y/N)	Value
1. Assess adherence to the documented BCP	1	N	0
2. Determine the effectiveness of the plan, continuity capabilities, roles and responsibilities, skills and competencies, resilience to the incident, technical infrastructure, and organisational structures and relationships.	1	N	0
3. Identify weaknesses or omissions in the plan and capabilities and make recommendations for improvement.	1	N	0
4. Obtain management approval for any changes to the plan and apply via the enterprise change control process.	1	N	0

The working papers showed that the level 1 capability assessment resulted in 50% falling under the partially achieved category. This percentage is calculated by dividing the total value of work products and management practices by the total weight of work products and management practices. Since the rating scale does not reach the fully achieved level at level 1, the assessment cannot proceed to level 2.

The conditions and areas for improvement to enhance the DSS04 process capability are outlined as follows. The evaluation results indicate that LNSW's capability level for the DSS04 - Manage Continuity process has only partially achieved level 1 of process capability (partially achieved performed process), and there are still some activities and work products that need to be completed to meet the level 1 achievement. LNSW has implemented governance and control activities by establishing policies, objectives, and scope of service/business process continuity, and maintaining a service/business process continuity strategy. However, there are some weaknesses in the base practice of the DSS04 – Manage Continuity process that can be improved. These include the lack of a service/business process continuity plan (BCP) that includes organizational disaster scenarios beyond IT disaster scenarios, and the absence of a review of the BCP's effectiveness based on actual disaster events and required improvement efforts.

The assessment results reveal that LNSW's process capability in DSS04 - Manage Continuity has only partially achieved the level 1 process capability target, with a score of 50%. There are still several activities and work products that must be completed to meet level 1 requirements. LNSW has established governance and control measures, including policies, objectives, and service/business process continuity scope, and maintains a service/business process continuity strategy. However, there are several shortcomings in the base practices of the DSS04 - Manage Continuity process that need improvement, such as the absence of a BCP containing organizational disaster scenarios, which are not limited to IT disaster scenarios and its implementation, and there has been no review of the BCP's effectiveness based on actual disaster events and the necessary remedial measures for the BCP.

Based on the survey conducted among employees responsible for risk management, strategic planning, and IT management at LNSW, the findings indicate that all respondents, or 100%, considered BCM to be an important aspect for the organization. Meanwhile, 42% of respondents highlighted the need for BCM to be urgently implemented, while the remaining 58% suggested that BCM should be given priority. However, only a small percentage of employees possess a sufficient understanding of BCM. The results also revealed several factors that may have contributed to this lack of understanding, including BCM-related competencies being limited to certain individuals or units, infrequent or

nonexistent BCM training, irregular dissemination of BCM-related information, and the absence or limited scope of policies pertaining to BCM beyond IT-related matters.

The following are potential improvements that LNSW could implement to enhance their business continuity management capabilities according to their objectives, strategies, risks, and available resources. To meet level 1 capability targets, LNSW could focus on creating a service/business process continuity plan (BCP) that covers organizational disaster scenarios, rather than just ICT disaster scenarios, and ensure its implementation. Additionally, they could review the effectiveness of the BCP in light of actual disaster events and implement corrective measures as needed. To achieve level 2 capability targets, LNSW could implement provisions or guidelines for versioning documents to facilitate document tracking. They could also determine necessary hard competencies to identify training needs, apply the risk-control matrix in process management, develop and implement a communication plan that specifies responsibilities, target audience, content, timing, and approach, and establish a quality plan with quality criteria for work product content and structure.

6. Conclusions

After collecting data and assessing the level of business continuity management capability, it was found that LNSW's business continuity management is generally at level 1 (partially achieved performed process). The goal of the management objective is to maintain acceptable business operations in case of significant disruptions, which has been achieved to some extent through risk assessment, business impact analysis, preparation of a Disaster Recovery Plan (DRP), and DRP testing. However, the activities carried out only cover the IT aspect and do not fully cover all main cycles/activities of BCM.

Since LNSW is a large-scale organization with critical business processes in the state finance field, it needs to ensure resilience in terms of business continuity. Therefore, LNSW should strive to achieve its business continuity management objectives, which include quickly adapting, continuing business operations, and maintaining resource and information availability at an acceptable level when significant disruptions occur, such as threats, opportunities, or demands.

The integrated application of the BCM framework in LNSW needs to be seen as a priority, considering the critical role of LNSW and the existence of disaster risks that can disrupt business processes. In addition, the implementation of BCM needs to be an integral part of the routine activities of LNSW, not just as a temporary project.

The analysis and discussion's findings allow for the conclusion that there are four things that need to be prioritized for the development of the early stages of BCM implementation in the LNSW environment, namely determination of policies governing the implementation of BCM in LNSW; and increasing awareness and competence of LNSW officials/employees related to BCM; determination of a clear and applicable strategy and BCP; procurement of facilities/infrastructure and equipment ready for use in a disaster situation.

The BCM maturity level assessment tool using the COBIT 2019 framework has been developed by the author to assess the level of capability obtained for each attribute of a process which is stated at five levels, starting from level 0 to level 5 and this tool can be used as a tool self-assessment for LNW as a tool to evaluate BCM periodically. Indicators for level 1 capabilities are specific and different for each process. The assessment is carried out on the outcome of the process attributes (PA) of level 1 capability. The assessment criteria for capability level 2 to level 5 are generic/common for all processes, but are different for each level of capability. PA assessment is needed to be able to assess the level of capability of a process. The results of the assessment of the fulfillment of process attributes at each level are classified into four categories.

As for suggestions that can be submitted to get better results in further research, namely the next level of capability assessment can be carried out using other process areas related to BCM for more comprehensive research; and BCM assessments can use governance system components which are carried out by first identifying the assessment criteria for each component with a rating scale.

Acknowledgment

We would like to thank Direktorat Teknologi Informasi LNSW and Bina Nusantara University, especially for Binus Graduate Program, Master of Computer Science, for the opportunity for us to conduct the research.

References

Aleksandrova, S., Aleksandrov, M., & Vasiliev, V. (2018). Business Continuity Management System. *Proceedings of the 2018 International Conference "'Quality Management, Transport and Information Security, Information Technologies'", IT and QM and IS 2018*. https://doi.org/10.1109/ITMQIS.2018.8525111

Alhazmi, O., & Malaiya, Y. (2013). Evaluating disaster recovery plans using the cloud. *Proceedings - Annual Reliability and Maintainability Symposium*. https://doi.org/10.1109/RAMS.2013.6517700

Alhazmi, O., & Malaiya, Y. (2012). Assessing disaster recovery alternatives: On-site, colocation or cloud. *Proceedings - 23rd IEEE International Symposium on Software Reliability Engineering Workshops, ISSREW 2012*. https://doi.org/10.1109/ISSREW.2012.20

APEC. (2014). How to promote Business Continuity Planning to mitigate the impact of disasters A guide for government officials. *APEC's Emergency Preparedness Working Group*, 32. http://publications.apec.org/file-download.php?filename=BCP-file - FINAL FOR PRINTING NOV 2014.pdf&id=1588

Asnar, Y., & Giorgini, P. (2008). Analyzing business continuity through a multi-layers model. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5240 LNCS*. https://doi.org/10.1007/978-3-540-85758-7_17

Bakar, Z., Yaacob, N., & Udin, Z. (2015). The effect of business continuity management factors on organizational performance: A conceptual framework. *International Journal of Economics and Financial Issues*, 5, 128–134.

Bimantoro, A., & Jayadi, R. (2022). IT Governance Measurement using COBIT 5 for Evaluating IT Project Management Aspect: Case Study of Insurance Company. *Journal of System and Management Sciences*, 12(6), 315–333. https://doi.org/10.33168/JSMS.2022.0620

Boehmer, W. (2009). Survivability and business continuity management system according to BS 25999. *Proceedings - 2009 3rd International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2009*. https://doi.org/10.1109/SECURWARE.2009.29

Boehmer, W., Brandt, C., & Groote, J. (2009). Evaluation of a business continuity plan using process algebra and modal logic. *TIC-STH'09: 2009 IEEE Toronto International Conference - Science and Technology for Humanity*. https://doi.org/10.1109/TIC-STH.2009.5444515

Cerullo, V., & Cerullo, M. (2004). Business continuity planning: A comprehensive approach. *Information Systems Management*, 21(3). https://doi.org/10.1201/1078/44432.21.3.20040601/82480.11

Curtis, P. (2006). Maintaining Mission Critical Systems in a 24/7 Environment. In *Maintaining Mission Critical Systems in a 24/7 Environment*. https://doi.org/10.1002/0470089040

Doughty, K. (2000). Business continuity planning: Protecting your organization's life. In *Business Continuity Planning: Protecting Your Organizations Life*. https://doi.org/10.1201/1079/43277.29.6.20011201/31749.4

Faertes, D. (2015). Reliability of supply chains and business continuity management. *Procedia Computer Science*, 55. https://doi.org/10.1016/j.procs.2015.07.130

International Labour Organization. (2011). Multi-hazard Business Continuity Management Guide for small and medium enterprises. In *ILO Programme on Crisis Response and Reconstruction*.

International Monetary Fund. (2011). Operational Risk Management and Business Continuity Planning for Modern State Treasuries. *Technical Notes and Manuals*, 2011(05). https://doi.org/10.5089/9781475504705.005

International Organization for Standardization. (2006). ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements. *Wired Mag*, 14(6).

Iqbal, Widyawan, & Mustika. (2016). Evaluasi Business Continuity Plan Menggunakan COBIT 5 (Studi Kasus: DSSDI Universitas Gadjah Mada). *Http://Etd.Repository.Ugm.Ac.Id/Home/Detail_pencarian/106191*.

ISACA. (2019). COBIT 2019 Framework Introduction and Methodology. In *www.icasa.org/COBITuse*.

ISO. (2012). ISO22301 Societal security — Business continuity management systems - Requirements. In *Societal Security – Business Continuity Management Systems – Requirements*.

Kato, M., & Charoenrat, T. (2018). Business continuity management of small and medium sized enterprises: Evidence from Thailand. *International Journal of Disaster Risk Reduction*, 27, 577–587. https://doi.org/10.1016/J.IJDRR.2017.10.002

Kliem, R. (2015). Business continuity planning: A project management approach. In *Business Continuity Planning: A Project Management Approach*. https://doi.org/10.1201/b18989

Lavigne, F., De Coster, B., Juvin, N., Flohic, F., Gaillard, J. C., Texier, P., Morin, J., & Sartohadi, J. (2008). People's behaviour in the face of volcanic hazards: Perspectives from Javanese communities, Indonesia. *Journal of Volcanology and Geothermal Research*, 172(3–4), 273–287. https://doi.org/10.1016/J.JVOLGEORES.2007.12.013

Legowo, N., & Juhartoyo, Y. (2022). Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001. *Journal of System and Management Sciences*, 12(3), 181–199. https://doi.org/10.33168/JSMS.2022.0310

Lindström, J., Samuelsson, S., & Hägerfors, A. (2010). Business continuity planning methodology. *Disaster Prevention and Management: An International Journal*, 19(2), 243–255. https://doi.org/10.1108/09653561011038039

Loomba, A., & Mavroleon, J. (2013). Antidote for Panic: Managing Business Continuity Projects Effectively. *PMI® Global Congress 2013—North America, New Orleans, LA, October*.

Mas'ud, I., & Salsabila, R. (2021). PERANCANGAN BUSINESS CONTINUITY PLAN PADA PT. XYZ. *Jurnal Sistem Informasi Dan Sains Teknologi*, 3(1). https://doi.org/10.31326/sistek.v3i1.803

Păunescu, C. (2017). How prepared are small and medium sized companies for business continuity management? *Quality - Access to Success*, 18(161).

Păunescu, C., & Argatu, R. (2020). Critical functions in ensuring effective business continuity management. Evidence from romanian companies. *Journal of Business Economics and Management*, 21(2). https://doi.org/10.3846/jbem.2020.12205

Păunescu, C., Popescu, M., & Blid, L. (2018). Business impact analysis for business continuity: Evidence from Romanian enterprises on critical functions. *Management and Marketing*, 13(3). https://doi.org/10.2478/MMCKS-2018-0021

Perdikaris, J. (2014). Physical Security and Environmental Protection. In *Physical Security and Environmental Protection*. https://doi.org/10.1201/b16861

Prabowo, W., & Ramadhani, R. (2021). Perancangan Contingency Planning Disaster Recovery Unit Teknologi Informasi Menggunakan Nist Sp800-34. *Techno.COM*, 20(1).

Pradana, E., & Kusuma, R. (2019). Sistem Evaluasi Kesiapan Internal Audit Penerapan Business Continuity Management. *JAS-PT (Journal Analisis Sistem Pendidikan Tinggi Indonesia)*, 3(2). https://doi.org/10.36339/jaspt.v3i2.418

Prakasita, E., & Ginardi, H. (2019). Tinjauan Kesiapan Terhadap Implementasi Business Continuity Management Systems (BCMS) Berbasis ISO 22301 dan ISO 27001 (Studi Kasus: PT. JPK). *Informatika Mulawarman : Journal Ilmiah Ilmu Komputer*, 13(2). https://doi.org/10.30872/jim.v13i2.902

Rittinghouse, J., & Ransome, J. (2006). Business Continuity and Disaster Recovery for InfoSec Managers. In *Business Continuity and Disaster Recovery for InfoSec Managers*. https://doi.org/10.1016/B978-1-55558-339-2.X5000-1

RSM Indonesia. (2017). Managing Business Continuity. *The Jakarta Post*. https://www.rsm.global/indonesia/en/insights/articles/managing-business-continuity

Sahebjamnia, N., Torabi, S., & Mansouri, S. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*, 242(1). https://doi.org/10.1016/j.ejor.2014.09.055

Setiawan, I., Waluyo, R., & Pambudi, W. (2019). Perancangan Business Continuity Plan dan Disaster Recovery Plan Teknologi dan Sistem Informasi Menggunakan ISO 22301. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, 3(2). https://doi.org/10.29207/resti.v3i2.911

Storkey, I. (2011). *Operational Risk Management and Business Continuity Planning for Modern State Treasuries*. International Monetary Fund. https://books.google.co.id/books?id=uFQZEAAAQBAJ

Suguna, S., & Suhasini, A. (2015). Overview of data backup and disaster recovery in cloud. *2014 International Conference on Information Communication and Embedded Systems, ICICES 2014*. https://doi.org/10.1109/ICICES.2014.7033804

Torabi, A., Giahi, R., & Sahebjamnia, N. (2016). An enhanced risk assessment framework for business continuity management systems. *Safety Science*, 89. https://doi.org/10.1016/j.ssci.2016.06.015

Tucker, E. (2015). Business Continuity from Preparedness to Recovery: A Standards-Based Approach. In *Business Continuity from Preparedness to Recovery: A Standards-Based Approach*. https://doi.org/10.1016/C2012-0-06413-7

United Nations. (2018). Gearing E-Government to Support Transformation towards Sustainable and Resilient Societies. In *United Nations e-Government Survey 2018*.

Wheatman, V. (2001). *Aftermath: Disaster Recovery*. https://www.gartner.com/en/documents/341017

Yanthestya, L., & Gondodiyoto, S. (2013). Evaluasi Business Continuity Plan dan Disaster Recovery Plan dengan Menggunakan Standarisasi ISO 22301 pada PT Sigma Cipta Caraka. *Http://Library.Binus.Ac.Id/Collections/Ethesis_detail.Aspx?Ethesisid=TSA-2014-0030*.

Zsidisin, G., Melnyk, S., & Ragatz, G. (2005). An institutional theory perspective of business continuity planning for purchasing and supply management. *International Journal of Production Research*, 43(16). https://doi.org/10.1080/00207540500095613