E-ISSN: 2963-4946
Vol. 1 No. 12 September 2023

Asian Journal of
Social and Humanities
https://ajosh.org/

Performance Evaluation of Business Continuity Plan in Dealing with Threats and Risks in Cilegon Companies Use ISO 22301:2019 & NIST Sp 800-30 R1 Frameworks Case Study: PT. X

Hendaryatna[1], Gerry Firmansyah[2], Budi Tjahyono[3], Agung Mulyo Widodo[4]
[1,2,3,4] Universitas Esa Unggul, Indonesia
Email: h3nd4ry@gmail.com, gerry@esaunggul.ac.id, budi.tjahjono@esaunggul.ac.id, agung.mulyo@esaunggul.ac.id

* Correspondence: gerry@esaunggul.ac.id

KEYWORDS

Electronic Based Government System, Business Continuity Plan, Business Continuity Management System, Risk Analysis, Framework, Best Practice ISO, NIST

ABSTRACT

This research was conducted at PT.X which is located in Cilegon, Merak-Banten. Seeing the geographical location of PT.X which is in a disaster-prone area, the company must ensure an effective business continuity process. In accordance with government regulations on Electronic-Based Government Systems (SPBE) related to corporate and government business activities, companies must be able to ensure business continuity in every condition that poses a threat and risk, but with no specific obligation that is the basis for the company's business continuity if it does not have a Business Continuity Plan (BCP) process, it will get a sanction. The purpose of this research is to evaluate the existing BCP process at PT X Cilegon and provide recommendations for a standardized BCP framework in the company to ensure business continuity as the company's Business Continuity Management System (BCMS) to avoid all threats and risks. BCP has standards regulated in ISO 22301: 2019 as its framework, and in BCP there is a risk analysis process and this research will be carried out using the NIST SP 800-30 Revision 1 method as its best practice. The evaluation results show that the previous BCP process at PT X Cilegon was not in accordance with the standards and the risk analysis carried out was still based on the ISO that the company had implemented but not ISO 31000 which is the risk management standard, so this study provides recommendations for a BCP framework that is in accordance with the standards and risk analysis with risk analysis methods that produce risk priorities.

Introduction

In principle, every company should have what is called a Business Continuity Planning (BCP) in their company. Business continuity planning is a process that companies undertake to create a prevention and recovery system from potential threats such as natural disasters or cyberattacks. It is designed to protect personnel and assets and ensure that they can function quickly in the event of a disaster. There is no obligation not to have a BCP in principle - but it is recommended as explained in the decision, its purpose is to provide guidance for companies in preparing BCPs to protect business continuity from the impact of disasters or pandemics and to prevent the spread of viruses and cyberattacks within the company. BCP should help the company; however, companies that do not create their own BCP do not face any sanctions (Association, 2019).

Cilegon City is one of the municipalities in Banten Province established and enacted by Law No. 15 of 1999 dated April 27, 1999, along with Depok as Regional Level II Municipalities (Muflihah & Subriadi, 2018). Cilegon City consists of 8 districts and 43 sub-districts, with a population estimated at 404,426 in 2017, and a land area of 175.50 km² with a density of 2,304 people/km² according to data from the Ministry of Home Affairs of the Republic of Indonesia (Permendagri) Number 72 of 2019 concerning Amendments to the Minister of Home Affairs Regulation Number 137 of 2017 concerning Administrative Region Codes and Data. In its development, Cilegon City has shown rapid progress in various fields, including physical, social, and economic development. This progress is inseparable from the city's structure as the gateway between the islands of Java and Sumatra, supported by numerous large industries such as steel and chemical industries, which are rapidly advancing companies in Indonesia and have a significant impact on trade and services, including the continuously growing population. Along the coastline, especially in the coastal areas of Cilegon, almost all are covered and controlled by these large industries. Due to the presence of numerous large industries, Cilegon City is known as an industrial city. Geographically, some of these companies can be directly observed via Google Maps.

Based on information from the Meteorology, Climatology, and Geophysics Agency (BMKG) as reported by CNN Indonesia, Cilegon City has the potential for a major earthquake accompanied by a tsunami. Data indicates that the Sunda Strait tsunami on December 22, 2018, came suddenly without any prior warning from any party, claiming more than 430 lives and causing infrastructure damage in the coastal areas from Pandeglang to Cilegon (Solihuddin et al., 2020). Considering the geographical position and assumptions about the impact of natural disasters, Cilegon City has a high potential for natural threats (Haryadi et al., 2019).

Even though there is no obligation to have a BCP, companies and governments must take preventive actions as referred to in the above government regulations. Particularly, companies and governments that provide services to consumers and the public are at risk of operational disruption in their internal information systems, which can result in financial losses due to economic activity disruption and loss of public trust. As one of the essential aspects of maintaining the sustainability of both large and small industrial and governmental activities in Cilegon City, and given the potential for tsunamis, earthquakes, as mentioned above, it also includes the potential threat of human-based IT security breaches and cyberattacks (Amirullah & Subriadi, 2019).

Based on the information provided, the author is interested in conducting research on the readiness of BCP in chemical companies in the Cilegon region. However, due to the sensitivity of the data, the author will only conduct a case study in one of the companies in Cilegon, referred to as PT.X. The goal is to determine if the company's business activities are prepared in the event of unexpected incidents, especially potential tsunamis as mentioned above, and to conduct a more in-depth analysis of this potential.

In a previous study titled 'Evaluation of the Business Continuity Planning Framework at PT. Lotte Chemichal Titan Nusantara' by Mochammad Ikmal Amirullah and Apol Pribadi Subriadi (2019), it was mentioned that the BCP framework by Yusrida could become a standard for business continuity planning in a company because it details the BCP process (Russo et al., 2023). However, this framework does not conduct a detailed risk and threat analysis, so companies implementing this framework may not address risks according to their priority.

Research in this study will be conducted qualitatively in the evaluation using ISO 22301 and threat and risk analysis using NIST SP 800-30 Revision 1. Therefore, this topic will be useful as a reference and will assist in improving the quality of business continuity systems for companies and all stakeholders, including students.

Based on the Cilegon Risk Index from the IRBI, it may be moderate, but the potential for a tsunami, as indicated by BMKG, still exists, and it can be concluded that a tsunami can occur at any time. Based on PPRI No. 71 of 2019, Article 20, paragraph 1, and Presidential Regulation 95 of 2018 concerning Electronic-Based Government Systems (SPBE), Article 40, paragraph (1) relates to the continuity of business activities for companies and governments. There is no specific obligation that would serve as the basis for companies to receive sanctions if they do not have BCP, so some companies may not have a BCP. The research problem to be discussed in this study is the evaluation of BCP using the ISO 22301:2019 framework with a threat and risk analysis method using NIST 800-30 R1.

The purpose of this research is to provide recommendations regarding the framework for business continuity planning (BCP) that suits the needs of the company (Pertiwi & Apol Pribadi, 2016). To achieve this, several objectives will be met, including: a) Identifying threats and risks according to NIST SP 800-30 R1. b) Identifying factors that play a role in the creation of the BCP framework with ISO 22301:2019. c) Formulating the BCP framework.

BCP (*Business Continuity Plan*)

According to Hiles, BCP is the process of identifying and protecting critical business processes and the resources necessary to keep business processes at acceptable levels, protecting all resources and setting up procedures to ensure the survival of the organization at a time when the business is exposed to threats (Aristoteles et al., 2020; Choi et al., 2021). Meanwhile, according to ISO 22301:2012, BCP is defined as a document containing procedures that aim to guide companies in responding, restoring, continuing, restoring the company's business processes to a predetermined level after a disruption (Budiyanto et al., 2019; Pramudya & Fajar, 2019). According to the ISO/TC Technical Committee 223 years, 2012 BCP is the process of identifying critical business functions, prioritizing resources to support functions, and developing strategies to maintain operations before business interruptions or crisis events (Margherita & Heikkilä, 2021). And according to the Federal Office for Information Security 2013, BCP is an ongoing process for identifying organizational disasters and vulnerabilities, the likelihood of disaster occurrence, potential consequences for strategy goals and success, the effectiveness of applicable controls and strategies to improve performance and efficiency (Pambudi & Ramli, 2023). So BCP deals with identifying, obtaining, developing, documenting and testing resources and procedures so that an organization's critical business processes can be maintained during any disaster or incident (Russo & Reis, 2020).

ISO (International Standard organization)

ISO 22301:2019 is an output from the International Standard Organization (ISO) that focuses on business continuity management systems or Business Continuity Management System (BCMS). This standard is used to develop business continuity according to the magnitude and type of impact that may or may not be accepted by the organization after a disruption.

A BCMS emphasizes the importance of (Standardization, 2019):

- Understand organizational needs and the need to define business continuity policies and objectives
- Operate and maintain response processes, capabilities, and structures to ensure the organization will be safe from disruptions.
- Monitor and review the performance and effectiveness of the BCMS
- Continuous improvement based on qualitative and quantitative measures.

According to Stelios and Georgios, adding that BCM is essential to ensure business continuity and reduce the operational, legal, financial, and other consequences arising from a disaster. And according to Jack, states that an updated and detailed plan, prepared to manage disruption, is essential to mitigate the risks and their effects and costs. Jack comments that organizations that prepare plans and related managerial activities have a higher probability of survival.

NIST SP 800-30 R1

The objective of risk assessment from NIST SP 800-30 R1 is to inform decision-makers and support risk response by identifying (Al Fikri et al., 2019; Astri et al., 2023; Eryawana et al., n.d.):

i. Relevant threats to the organization or threats directed through the organization to others;
ii. Vulnerabilities, both internal and external, to the organization;
iii. Impacts (i.e., hazards) on the organization that may occur considering the potential threats exploiting vulnerabilities; and
iv. The likelihood of loss.
v. The outcome is the determination of risk (usually a function of hazard level and likelihood of occurrence).

Risk assessment can be conducted at three levels in the risk management hierarchy as shown in Figure 65, namely (Afiansyah et al., 2023):

Tier 1 (organizational level),
Tier 2 (mission/business process level),
Tier 3 (information system level).

In Tier 1 and 2, organizations use risk assessment to evaluate, for example, systemic information security risks related to organizational governance and management activities, mission/business processes, enterprise architecture, or information security program funding. In Tier 3, organizations use risk assessment to more effectively support the implementation of the Risk Management Framework (i.e., security categorization; security control selection, implementation, and assessment; common control authorizations; and security control monitoring) (Kuntari et al., 2018).

There are three main processes in NIST SP 800-30 R1: risk assessment, risk mitigation, and risk evaluation. In the risk assessment process, there are nine steps involved, namely system characteristics, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendations, and result documentation (Ulfa & Immawan, 2021).

Research Methods

In this study the methodology used was qualitative through literature studies, interviews and questionnaires. Literature studies are conducted using sources from the internet, journals, reference books on BCP and BCM. The purpose of the literature study is to find out how to analyze BCP threat and risk evaluation materials. The survey for data collection is carried out by looking directly at PT. X Cilegon and other supporting documents (Putra & Soewito, 2023). Interviews were conducted to obtain the right information from trusted sources to support data collection. The questionnaire is carried out by providing a set of questions or questions asked to respondents to answer.

The research was conducted using case studies at PT. X Cilegon and the research will be conducted in April and May 2023. The framework used in this study refers to ISO 22301 to evaluate the results of ongoing system analysis and NIST-800-30-R1 to evaluate threats and risks (Russo & Reis, 2021).

The stages of research used in this writing are carried out by identifying problems through literature studies, observations, interviews and questionnaires as a collection of information and data for analysis. Literature studies are carried out to compare, find and see the best practice will be used to analyze the running system, analyze and expand the existing system and provide recommendations on the results of the analysis that has been carried out.

Results and Discussions

1. BCP Analysis at PT X Cilegon

The ongoing system analysis in this study includes the process flow and procedure of BCP (*Business Continuity Plan) at PT.* X. Based on the process, the results of data collection provide an overview of the BCP process flow at PT. X Cilegon can be seen in the following x figure:

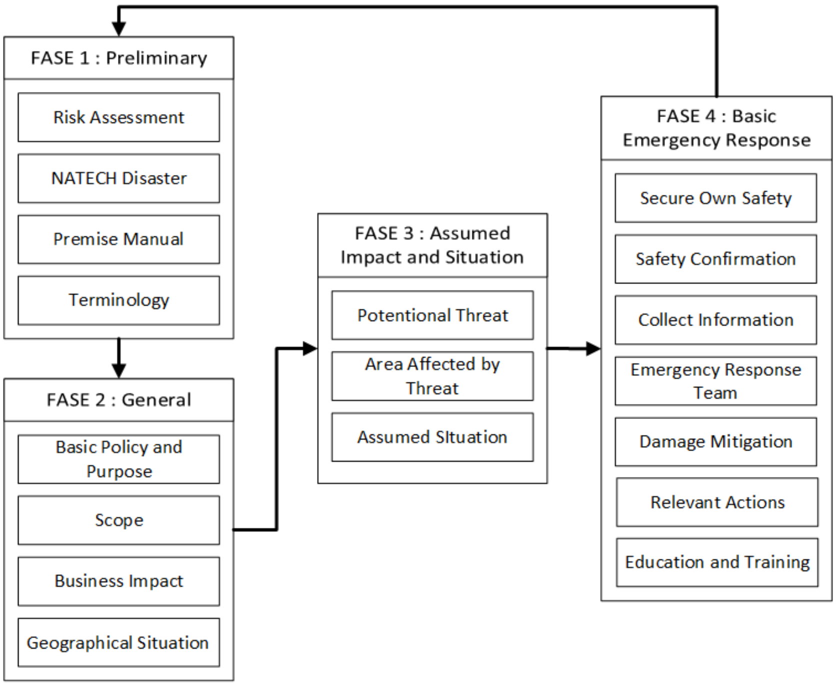

Figure 2 - BCP Process Flow PT. X Cilegon

Based on the existing BCP process flow, the company implements the flow which is a formulation of the existing BCP procedure and is taken based on the ISO that has been implemented by the company and the existing *Responsible Care*. Based on the results of the study, ISO 22301 became the *Best Practice* in determining BCP in the company. Business *continuity plan* design at PT. X Cilegon is as follows:

1. Clause 4 (Organizational Context), focuses on the process of identifying assets and threats to PT. X Cilegon where the process of identifying assets owned and threats that may occur is used to support the risk management process.
2. Clause 5 (Leadership), focuses on the design of the business continuity plan and the *design of the duties and responsibilities of the management as a whole and each part of the organizational structure in order to create a business* continuity plan commitment.
3. Clause 6 (Planning), focuses on guiding procedures for overall business continuity and designing strategic objectives according to company needs.
4. Kalusal 7 (Support), focuses on the process of designing an effective *business continuity plan* management and depends on the ability of human resources in the company and is able to assign each task to a competent person in charge as well as conduct appropriate training and improve support services.

2. Threat and Risk Analysis and Evaluation

Analysis and evaluation of threats and risks from this study was conducted based on best practice using the NIST 800-30-R1 method. At this stage an assessment of the identified risks and evaluations have been carried out for each risk scenario.

2.1 Risk Identification

In this phase, the process of discovering, recognizing, or describing risk attributes will be carried out, and risk identification is done through the following steps:

1. Asset Identification

This process is based on the analysis of factors considered for all assets in the company. Each asset is given a score for each critical factor and assigned a weight for each criterion. The weighting values are determined by the risk owner and risk personnel within the organization. To calculate the weighted factor analysis, each asset is given a score for critical factors and assigned a weight for each criterion. The weighted factor analysis criteria consist of:

- Criterion 1 (impact on revenue - 30%)
- Criterion 2 (impact on profitability - 40%)
- Criterion 3 (impact on public image - 30%)

To assess critical factors, scores range from 0.1 to 1.0, and criteria are given weights from 1 to 100, each weighted to indicate the importance of the criteria set for the organization. The range of values obtained is based on NIST SP 800-30 Revision.

2. Threat Identification

The identification of threats begins with identifying existing threat sources, and in this process, threat sources are categorized into four categories: Adversarial, Accidental, Structural, and Environmental. In this research, the identified threat sources are as follows, as shown in table 1.

Table 1 - List of Threat Sources PT. X

Code	Threat Source Type	Description	Characteristics
SA1	ADVERSARIAL - Individuals - Outsider - Insider - Trusted Insiders - Privileges Insiders - Group - Adhoc - Established - Organization - Competitor - Supplier - Mitra - Customers - Nation country	Individuals, groups, organizations or countries seeking to exploit an organization's dependence on cyber resources (i.e. information in electronic form, information and communication technology, and the communication and information capabilities provided by these technology companies).	Capability, Intent, Targeting
SA2	ACCIDENTAL - Users - User/Administrator Special User	Wrong actions done by individuals in carrying out their daily responsibilities.	effect range

Code	Threat Source Type	Description	Characteristics
SA3	STRUCTURAL - Information Technology (IT) Equipment - Storage - Processing - Communication - Appearance - Sensor - Controller - Environmental Control - Temperature / Humidity Control - Power supply - Software - Operating system - Network - General Purpose Application - Mission Specific Applications	Failure of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances that exceed expected operating parameters.	effect range
SA4	ENVIRONMENTAL - Natural disasters or man-made disasters - Fire - Flood / Tsunami - Hurricane / Tornado - Storm - Earthquake - Bombing - Overrun - Unusual Natural Events (eg sunspots) - Infrastructure Failure/Outage - Telecommunications - Electrical power	Natural disasters and failures of critical infrastructure on which the organization relies, but which are outside of the organization's control. Note: Natural and man-made disasters can also be characterized in terms of severity and/or duration. However, because the threat source and threat event are strongly identified, severity and duration may be included in the threat event description (for example, a Category 5 hurricane causes extensive damage to a facility housing mission critical systems, rendering the system inoperable for three weeks).	effect range

The next process is to identify each threat that allows a threat event to occur based on all existing threat sources and obtain the following threat events in table 14.

Table 14 - Threat events at PT. X

Code	Threat Events	Description
PA1	Perform perimeter network reconnaissance/scan.	Adversaries use commercial or free software to scan organizational boundaries to gain a better understanding of information technology infrastructure and increase the ability to launch successful attacks.
PA2	Gather information by using open sources to find organizational information.	Adversaries mine publicly accessible information to gather information about an organization's information systems, business processes, users or personnel, or external relations which can then be used by adversaries to support attacks.
PA4	Conduct reconnaissance and surveillance of targeted organizations.	Adversaries use various means (e.g. scanning, physical observation) from time to time to inspect and assess organizations and ascertain points of vulnerability.
	Performs internal reconnaissance directed by malware.	Adversaries use malware installed within an organization's perimeter to identify opportunity targets. Because scanning, checking, or surveillance does not cross the line, it is not detected by externally deployed intrusion detection systems.
PA3	Making phishing attacks.	Adversaries impersonate communications from legitimate/trustworthy sources to obtain sensitive information such as usernames, passwords or SSNs. Common attacks occur via e-mail, instant messaging, or similar means; usually redirects users to websites that appear to be legitimate, but actually steal information entered.
PA4	Create and operate fake cover organizations to inject malicious components into the supply chain.	Adversaries create fake front organizations by presenting legitimate suppliers in critical life cycle paths who then inject corrupted/malicious information system components into the organization's supply chain.
PA5	Sending known malware to an organization's internal information systems (for example, viruses via email).	Adversaries use common delivery mechanisms (e.g. email) to install/inject known malware into an organization's information system.
PA6	Introducing counterfeit or tampered hardware into the supply chain.	Adversaries intercept hardware from legitimate suppliers. The adversary modifies the hardware or replaces it with damaged or modified hardware.
PA7	Incorporate critical components that have been tampered with into organizational systems.	The adversary replaced, through the supply chain, tampered with insiders, or some combination thereof, critical information system components with modified or tampered components.
PA8	Install a general purpose sniffer on an information system or network controlled by the organization.	Adversaries install surveillance software into an organization's information systems or internal networks.

Code	Threat Events	Description
PA9	Exploiting known vulnerabilities in mobile systems (e.g., laptops, PDAs, smartphones).	Adversaries take advantage of the fact that transportable information systems are outside the organization's physical protection and corporate firewall logical protection, and compromise systems based on known vulnerabilities to gather information from those systems.
	Compromising information systems or devices used externally and reintroducing them into the company.	Adversaries install malware on information systems or devices while they are outside the organization with the aim of infecting the organization when reconnected.
PA10	Compromising the design, production and/or distribution of information system components (including hardware, software and firmware).	Adversary compromised the design, production, and/or distribution of critical information system components to certain suppliers.

Next, for the subsequent process, identify all threats that affect information security aspects such as confidentiality (initial as 'C'), integrity (initial as 'I'), and availability (initial as 'A'). This identification process is based on the following questions:

- What are the threats to assets that you know of or suspect?
- What is the most dangerous threat to the organization?
- Which threats would be the most expensive to recover from if an attack occurs?
- Which threats require the largest expenditures to prevent them?

3. Identification of Existing

Controls In this process, security controls that have been implemented by the company to protect organizational assets from threats are identified. Through the observation method, 15 security controls for assets were identified. Table 2 shows the list of existing controls.

.

Table 2- List of Security Controls

Code	Current Security Controls
KK1	Maintenance for periodic prediction and prevention
KK2	Control and review of automatic update systems
KK3	Confidential data control
KK4	Access control restrictions
KK5	Use of strong passwords with best practice recommendations
KK6	Periodically review access rights
KK7	Requires changing passwords periodically
KK8	Use of least privilege
KK9	Failure log access control
KK10	Periodic maintenance of physical assets (tools/machinery/HR).
KK11	Periodic system/person/equipment/machine monitoring
KK12	Regular and ongoing training

Code	Current Security Controls
KK13	The existence of a sustainable and binding contract basis
KK14	There are safety standards after installation
KK15	Regular testing/testing of systems/procedures/work instructions

4. Vulnerabilities Identification

Vulnerability identification means the extent to which the company has implemented controls to protect assets from threats. Vulnerabilities that don't have a corresponding threat may not require implementing controls, but still need to be identified and monitored. However, ineffective implementation of controls or controls that do not work properly can be vulnerabilities. In obtaining vulnerability results, we used reference vulnerability sources from OWASP's top ten [49]. Table 3 shows a list of vulnerabilities.

Table 3 - List of Vulnerabilities

Cod e	vulnerability
K1	Implementation of ineffective information security policies
K2	Late in replacing obsolete tools/machines
K3	Documents and files are not encrypted
K4	Vulnerable and end of support components (expired/aging)
K5	Insecure design system
K6	Cryptographic failure
K7	Failure results in data/system backup
K8	Tool/machine/system malfunction
K9	There are no spare parts/persons
K10	Software configuration error
K11	Improper installation of tools/machines
K12	Lack of job/information security training
K13	Lack of testing/testing of tools/machines/systems
K14	There is a software bug
K15	Incorrect device installation
K16	User limitations
K17	Lack of employee awareness causes work errors/unintentional deletion of system/data files/operates tools/machines incorrectly
K18	The security system update did not go well
K19	Inadequate security
K20	Low awareness of the importance of work safety and security

2.2 Risk Analysis

The risk analysis process is the activity of mapping assets, asset values, threats, security controls, vulnerabilities, and impacts on aspects of the CIA. Risk analysis is intended to obtain the results of the impact assessment and identify possible information security risks.

In this study, the risk analysis calculation uses a formula to find semi-quatitative values as follows:

$$\boxed{Risk = \frac{(\,a * b\,)*(\,y\% * z\,)}{In}}$$

$$\boxed{w = Number\ of\ Threats * Max.\ Risk\ Scale}$$

Information:

a: Value Likelihood (likelihood)
b: Threat Probability
y: Asset weight value
z: Assess the possible loss
w: Divisor Value

The results of this risk analysis calculation can then be used as a basis for determining existing risk levels to be used as risk priority recommendations based on the risk scale.

2.3 Risk Evaluation

Risk evaluation in this discussion aims to compare the results of risk analysis with risk criteria and then determine whether the risk rankings are acceptable or tolerable. The stages of risk evaluation include prioritizing risks based on their magnitude, following these criteria [20]:

- The highest-risk level receives the highest priority.
- If there are multiple risks with the same risk magnitude, the priority is determined based on the order of impact areas, from the highest to the lowest, according to the extent of their losses.
- If there are still multiple risks with the same magnitude and impact area, then the priority is determined based on the order of the highest to lowest risk categories according to the loss frequency.
- If there are still multiple risks with the same magnitude, loss value, and loss frequency, then the risk priority is determined based on the risk owner's consideration.

Risk determination is the initial step before prioritizing risks. The risk prioritization matrix is classified based on the NIST 800-30-R1 method and represents the matrix of the relationship between assets and threats. Figure 3 illustrates the risk prioritization matrix.

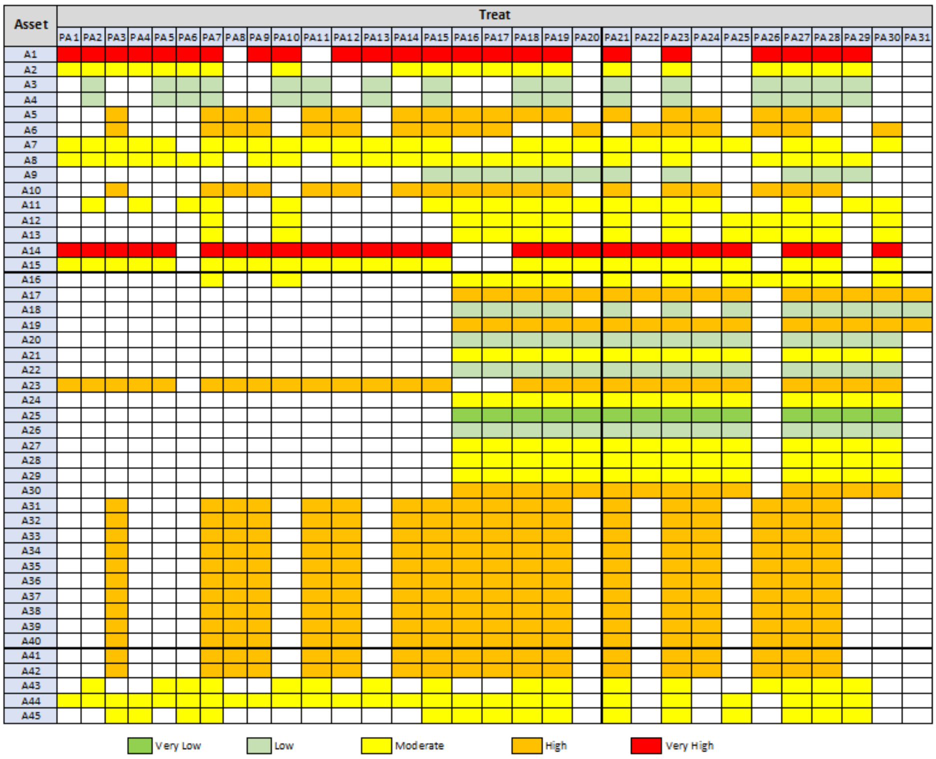

Figure 3 - Risk Priority Matrix

From the matrix above, risk priority can be determined based on the level of risk represented in the color above, so that it gets:

- 2 Assets with a very high risk priority.
- 19 Assets with high risk priority.
- 16 Assets with medium risk priority.
- 7 Assets with low risk priority.
- 1Assets with very low risk priority.

3. Recommendations and Results

The results of this study show that the BCP process at PT. X Cilegon has not implemented the BCP process standard with the ISO 22301:2019 framework. And based on the results of observations with data collection using questionnaires, it is known that the BCP process carried out by PT. X Cilegon is not yet comprehensive due to the absence of a patented BCP procedure because the process is still not up to standard. So that this research produces recommendations for the BCP process framework in accordance with ISO 22301: 2019 standards and carries out risk management using the NIST SP 800-30 Revision 1 method as best practice (Damalia et al., 2021). Figure 4 shows the recommendations for a standard-compliant BCP framework.

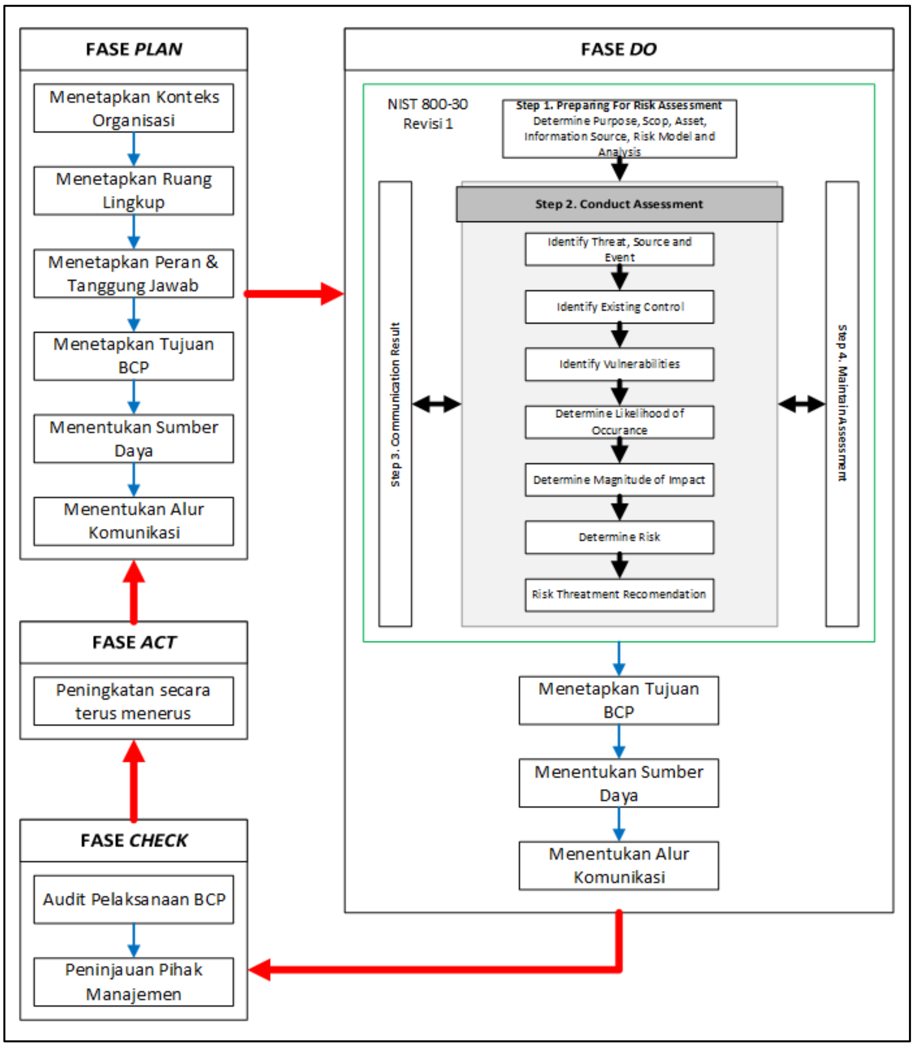
FASE PLAN
Menetapkan Konteks Organisasi
Menetapkan Ruang Lingkup
Menetapkan Peran & Tanggung Jawab
Menetapkan Tujuan BCP
Menentukan Sumber Daya
Menentukan Alur Komunikasi
FASE DO
NIST 800-30 Revisi 1
Step 1. Preparing For Risk Assessment Determine Purpose, Scop, Asset, Information Source, Risk Model and Analysis
Step 2. Conduct Assessment
Identify Threat, Source and Event
Identify Existing Control
Identify Vulnerabilities
Determine Likelihood of Occurance
Determine Magnitude of Impact
Determine Risk
Risk Threatment Recomendation
Step 3. Communication Result
Step 4. Maintain Assessment
Menetapkan Tujuan BCP
Menentukan Sumber Daya
Menentukan Alur Komunikasi
FASE ACT
Peningkatan secara terus menerus
FASE CHECK
Audit Pelaksanaan BCP
Peninjauan Pihak Manajemen

Figure 4 - Recommended BCP Framework

Conclusion

Based on the observations made in the company, the identified problem is that PT. X Cilegon is located in a geographically vulnerable area to disasters, which could potentially impact the company's business continuity. Therefore, in the government regulations regarding Electronic-Based Government Systems (SPBE), business continuity and governance are mentioned. However, there is no official regulation that mandates the implementation of a business continuity plan (BCP).

In this context, some companies have initiated the implementation of BCP, but many of them do not align with existing standards. In a previous study that evaluated the BCP framework by implementing Yusrida's BCP, no risk analysis was conducted, which could result in prioritized recommendations for risks and threats based on the company's specific conditions. This situation is similar to PT. X Cilegon, which has already implemented BCP and developed its process based on their self-made policies and existing standards.

The importance of BCP for a company has become a necessity. This research evaluates the BCP implemented by PT. X, following ISO 22301:2019 standards and incorporating risk analysis using the NIST SP 800-30 Revision 1 method.

The evaluation results indicate that the BCP implemented by PT. X is not yet effective because the process is not comprehensive. This research provides recommendations for a BCP framework that aligns with ISO 22301:2019 standards, supported by the risk analysis method of NIST SP 800-30 Revision 1. The risk analysis conducted provides recommendations for prioritizing risks based on the likelihood of threats and risks, as well as the sources of threats that may arise within the company based on its assets. This enables the company to implement an effective BCP process.

References

Afiansyah, H. G., Sunaringtyas, S. U., & Amiruddin, A. (2023). Perancangan Rencana Pemulihan Bencana Menggunakan NIST SP 800-34 Rev 1, NIST SP 800-53 Rev 5 dan SNI 8799 (Studi Kasus: Unit TI XYZ). *Jurnal Teknologi Informasi Dan Ilmu Komputer, 10*(2), 329–338.

Al Fikri, M., Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency. *Procedia Computer Science, 161*, 1206–1215.

Amirullah, M. I., & Subriadi, A. P. (2019). Evaluasi Kerangka Kerja Perencanaan Keberlangsungan Bisnis pada PT. Lotte Chemical Titan Nusantara. *SISFO VOL 8 NO 2*, *2*.

Aristoteles, A., Febrianto, I., Andrian, R., & Indrianti, I. (2020). IDENTIFIKASI RISIKO SISTEM INFORMASI BP-REMUN UNIVERSITAS LAMPUNG MENGGUNAKAN METODE NIST SP 800-30. *Jurnal Pepadun, 1*(1), 100–108.

Association, N. F. P. (2019). *NFPA 1600, Standard on continuity, emergency, and crisis management*. Quincy, MA: NFPA.

Astri, R. A., Jazman, M., & Saputra, E. (2023). Cybersecurity Supply Chain Risk Management Using NIST SP 800-161r1. *KLIK: Kajian Ilmiah Informatika Dan Komputer*, *3*(6), 595–601.

Budiyanto, E. H., Gurning, R. O. S., Pitana, T., & Sebayang, I. Z. (2019). *Risk Assessment Based on Business Continuity Management in PT. X on Harbour Tug Shipping Companies*. EasyChair.

Choi, J., Cheung, C., & Lee, D. (2021). Comparative Study of Administrative Business Continuity Plan (BCP) for DISASTER Management of Metropolitan Areas in Korea and Japan. *International Journal of Human & Disaster*, *6*(2), 59–68.

Damalia, R., Ambarwati, A., & Setiawan, E. (2021). Analisis Manajemen Risiko It Sistem Administrasi Bisnis Retail Menggunakan Metode NIST SP 800-30 Revisi 1. *INTECOMS: Journal of Information Technology and Computer Science, 4*(2), 271–281.

Eryawana, I. G. N. M. P., Sasmitaa, G. M. A., & Cahyawan, A. A. K. T. A. (n.d.). *NIST SP 800-30*.

Haryadi, E., Abdussomad, A., & Robi, R. (2019). Implementasi Sistem Backup Data Perusahaan Sebagai Bagian dari Disaster Recovery Plan. *Sainstech: Jurnal Penelitian Dan Pengkajian Sains Dan Teknologi*, *29*(2).

Kuntari, N. L., Chrisnanto, Y. H., & Hadiana, A. I. (2018). Manajemen Risiko Sistem Informasi di Universitas Jenderal Achmad Yani Menggunakan Metoda OCTAVE Allegro. *Seminar Nasional Teknologi Informasi*, *1*, 551–559.

Margherita, A., & Heikkilä, M. (2021). Business continuity in the COVID-19 emergency: A framework of actions undertaken by world-leading companies. *Business Horizons*, *64*(5), 683–695.

Muflihah, Y., & Subriadi, A. P. (2018). A basic element of it business continuity plan: systematic review. *Jurnal Informatika Ahmad Dahlan*, *12*(1), 17–23.

Pambudi, R. D., & Ramli, K. (2023). INFORMATION SECURITY RISK MANAGEMENT DESIGN OF SUPERVISION MANAGEMENT INFORMATION SYSTEM AT XYZ MINISTRY USING NIST SP 800-30. *Jurnal Teknik Informatika (Jutif)*, *4*(3), 591–599.

Pertiwi, G. P., & Apol Pribadi, S. (2016). *KERANGKA KERJA BUSINESS CONTINUITY PLAN (BCP) UNTUK TEKNOLOGI INFORMASI PERUSAHAAN Studi Kasus: PDAM KOTA SURABAYA*.

Pramudya, G. W., & Fajar, A. N. (2019). Business Continuity Plan using ISO 22301: 2012 in IT solution company (pt. ABC). *Int. J. Mech. Eng. Technol*, *10*(2), 865–872.

Putra, A. P., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005: 2018 and NIST SP 800-30 for Insurance Sector. *International Journal of Advanced Computer Science and Applications*, *14*(4).

Russo, N., & Reis, L. (2020). Updated analysis of business continuity issues underlying the certification of invoicing software, considering a pandemic scenario. *Advances in Science, Technology and Engineering Systems Journal*, *5*(6), 845–852.

Russo, N., & Reis, L. (2021). Methodological approach to systematization of Business Continuity in organizations. In *Handbook of Research on Multidisciplinary Approaches to Entrepreneurship, Innovation, and ICTs* (pp. 200–223). IGI Global.

Russo, N., Reis, L., Silveira, C., & Mamede, H. S. (2023). Towards a Comprehensive Framework for the Multidisciplinary Evaluation of Organizational Maturity on Business Continuity Program Management: A Systematic Literature Review. *Information Security Journal: A Global Perspective*, 1–19.

Solihuddin, T., Salim, H. L., Husrin, S., Daulat, A., & Purbani, D. (2020). Sunda Strait Tsunami Impact In Banten Province And Its Mitigation Measures. *Jurnal Segara*, *16*(1), 15–28.

Standardization, I. O. for. (2019). *Security and Resilience: Business Continuity Management Systems-Requirements*. International Organization for Standardization.

Ulfa, A. A., & Immawan, T. (2021). Analisis Manajemen Risiko Dengan Penerapan ISO 31000 Pada Proses Machining (Studi Kasus: Perusahaan AB). *Integrasi: Jurnal Ilmiah Teknik Industri*, *6*(2), 42–52.