Journal of Information Systems and Informatics
Vol. 6, No. 4, December 2024 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v6i4.955 Published By DRPM-UBD

Risk Analysis of Business Continuity Plan in Light Steel Company Using ISO 31000 Framework

Johanes Fernandes Andry[1], Kevin Christianto[2], Yunianto Purnomo[3], Francka Sakti Lee[4], Bernadus Gunawan Sudarsono[5]

[1,2,3,4]Information System Department, Bunda Mulia University, Jakarta, Indonesia
[5]Information System Department, Bung Karno University, Jakarta, Indonesia
Email: [1]jandry@bundamulia.ac.id, [2]kevin.hikoza@gmail.com, [3]ypurnomo@bundamulia.ac.id, [4]flee@bundamulia.ac.id, [5]gunawanbernandus@ubk.ac.id

Abstract

Light Steel Company is an industry engaged in manufacturing, has adopted technology and has a data center. The purpose of this study is to provide a guide and strategy for preventing risks and actions to minimize and overcome risks that can be used and implemented, so that the company's business processes can continue to run sustainably. This study uses Business Continuity Plan (BCP) using ISO 31000. Data collection is used by an interviewing employee who works at this organization. The analysis shows there are 15 possible risks that will hinder the operation of Light Steel companies based on the risk level high, medium, and low categories. High risk level is 26.7%, there are 4 possible risks, namely R05 (Loss of spare parts), R06 (Unscheduled maintenance and care for trucks and equipment spare parts), R10 (Server down) and R012 (Network connection problems). Medium risk level is 26.7%, there are 4 possible risks, namely R02 (flood), R07 (Cybercrime), R08 (Hacking), and R011 (Sudden power outage). Finally for low risk level is 46.6%, there are 7 possible risks, namely R01 (Earthquake), R03 (Dust), R04 (Fire), R09 (Abuse of access rights), R13 (Overheat), R14 (Data Corrupt), and R15 (Virus Attack, Malware).

Keywords: Risk Management, BCP, ISO 31000, Company

1. INTRODUCTION

Currently, the flow of information technology knows no boundaries of space and time. Information technology is increasingly used and makes people feel that technology is one of the most important needs [1]. Information technology is used to support core business activities and support business activities within related companies or organizations [2]. The majority of companies or organizations cannot carry out their business activities without implementing Information Technology (IT). The success of IT implementation in an organization requires protection against various threats and disruptions in order to prevent IT risks that can harm the performance and business operations of the

organization [3]. Risks can occur due to natural, human, technological factors [4]. These risks can appear suddenly and have the potential to cause damage to an organization, so immediate attention is needed to risk mitigation [5]. In order to ensure business continuity in such critical or risky conditions, it is important for organizations to have a BCP [6]. BCP is a method that designs and validates plans to maintain the continuity of business functions not only focused on before, during, but also after a disaster [7].

BCP acts as a proactive discipline that includes identifying vulnerabilities and risks and planning to mitigate, accept or if business disruption occurs [8]. The implementation of BCP is very important, considering that's a complete set of procedures used to maintain the resilience of an organization in the face of disasters, disruptions, or unexpected changes [9]. The main purpose of BCP is to ensure that activities, including customer service, can continue even in situations of problems or disruptions [10]. Light steel company is an industry engaged in manufacturing. This company has adopted technology and has a data center and has its own server. Currently, Light Steel companies are growing rapidly, playing a crucial role in the country's economy, and are subject to various risks [11]. Some risks include natural disasters such as volcanic eruptions, landslides, tsunamis, etc. In addition, there are also risks caused by humans such as sabotage, fires, cybercrime, power outages, and IT system failures. Head office in Central Jakarta, which is an urban area that rarely experiences natural disasters such as volcanic landslides, landslides, tsunamis, etc. Some disasters still have the potential to occur such as earthquakes, fires, sabotage, cybercrime, power outages, etc.

Companies need to maintain business continuity during a disaster, minimize confusion during a disaster, reduce data loss, accelerate recovery, and maintain the company's image [12]. In order to minimize the magnitude of the risk that can occur due to disasters or incidents, it is necessary to take action to minimize risks by using a business continuity plan so that the company can continue even when a threat occurs [13]. Therefore, it is necessary to design a business continuity plan for companies using the ISO 3100 method. This method is a generally recognized standard in risk management (RM) that provides a comprehensive framework for identifying, analyzing, evaluating, monitoring, and communicating risks [14]. ISO 31000 provides guidelines for the framework, basis and process in risk management. ISO is used as a risk management architecture and ensures the realization of risk management in the organization [15]. ISO 31000 risk management assessment, companies can minimize the possibility of risks that can damage the company's value and see opportunities in achieving organizational goals [16]. This design aims to help Light Steel companies by providing a guide and strategy for preventing risks and actions to

minimize and overcome risks that can be used and implemented by company's business processes can continue to run sustainably.

2. METHODS

Research Stages are the stages of the process flow applied in conducting research that will be described as follows.

1) Problem Identification, this stage is carried out to detect the problems that the research wants to address. The problem to be raised is the mitigation of possible risks that will occur using the ISO Framework in Companies.
2) Data Collection, this stage is carried out through observation, interviews with one employee who works at an organization and literature studies.
3) Making BCP with the ISO 31000 method, this standard provides general guidance on how to identify, assess, control and monitor risks in an organization [17]. ISO 31000 analysis there are 5 stages, can be seen in Figure 1. Risk Management Process from ISO 31000 as follow.
   a) Consultation, objective: engage stakeholders and facilitate information sharing,
   b) Establishing the Context, objective: define the external and internal environment in which the organization operates.

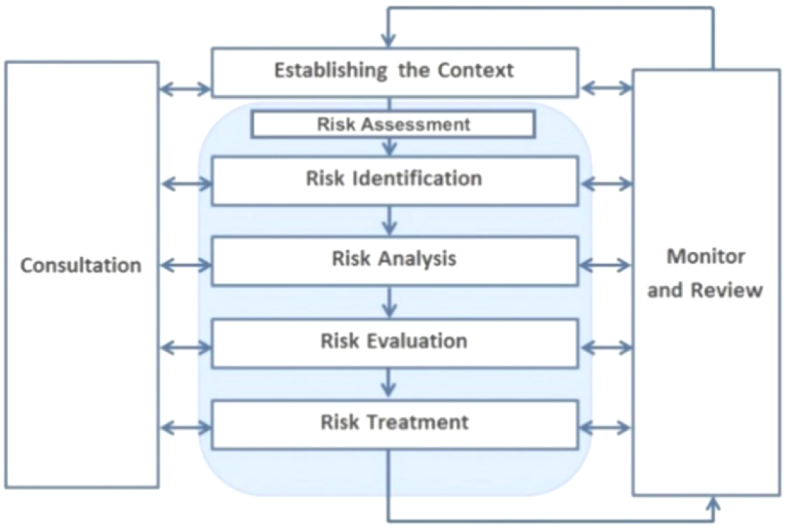

Figure 1. Risk Management Process from ISO 31000 [20]

   c) Risk Assessment, this stage involves systematically identifying, analyzing, and evaluating risks. It consists of three sub-steps, including are 1) Risk Identification: discovering potential risks that could impact objectives, 2) Risk Analysis: understand the nature of the risks and

estimate their likelihood and impact. 3) Risk Evaluation: determine the significance of identified risks and prioritize them for treatment, and 4) Risk Treatment: develop and implement actions to manage risks.

d) Monitoring and Review, objective: Continuously assess the effectiveness of the risk management process and adapt to changes [18]. By implementing ISO 31000, organizations can improve their ability to face emerging challenges and opportunities, while minimizing the negative impacts that can be caused by existing risks [19].

4) Conclusions and Results, this stage will produce a BCP draft that is given to the company which can be used as a guide for the company in taking actions to mitigate and overcome risks.

3. RESULTS AND DISCUSSION

3.1 Consultation

This first stage discusses risk management based on ISO 31000 through observation and interviews with one employee working at this organization. The focus of this interview is to discuss the permits required in the context of risk management, with the aim of obtaining evidence to support the process. The communication and consultation process are identified as the first stage in risk management, where stakeholders exchange information and opinions regarding risks and how to manage them. In decision making, it is important to identify and consider the communication and consultation process carried out by stakeholders. During the implementation of risk management, it is important for the communication and consultation process to continue, involving both internal and external parties as stakeholders. It's been involved in a two-way communication and consultation process with various parties. This includes collaboration with external parties such as vendors, investors, other companies, and the government, as well as internal interaction with employees in sub-fields. The company involves internal and external stakeholders through holding regular meetings and conferences. Discusses and communications about various problems faced. One aspect of the problems discussed includes risks related to natural/environmental factors, humans, and hardware and systems.

3.2 Establishing the context

This second stage discusses establishing the external and internal context.

3.2.1. Establishing the External context

The external context for companies refers to the external context in which the organization seeks to achieve its stated goals. External parties are as follow.

1) Vendors: important for companies in terms of providing solutions and assistance related to the procurement of products needed to support the smooth running of business processes. Companies need to work with vendors to meet the product needs that are essential for their operations.
2) Investors: Light Steel companies collaborate with investors in the context of equipment sales as an effort to obtain investment funds, both in the short and long term. This collaboration is intended to increase the company's profits.
3) Companies and governments: Light Steel companies collaborate to manage and meet their needs through equipment sales, with the aim of obtaining mutual benefits.

3.2.2. Establishing the Internal context

The internal context for Light Steel companies refers to the internal context in which the organization seeks to achieve its stated goals. Internal parties, namely:

1) Vision and Mission: as previously described, this is known as one of the largest and most complete distributors of equipment spare parts in Indonesia.
2) Organizational structure: provides a detailed description of the roles and authorities in the company.
3) Employees/HR: very crucial in a company, therefore, the company is committed to carrying out the recruitment and training process properly.

3.3 Risk Assessment

This third stage discusses the identification of assets related to data, software, and hardware including Sales Data, Shipping Tracking Data, Laptop, Printer, Server, Wi-Fi, Internet and Mobile Phone.

3.3.1 Risk Identification

This stage discusses identifying risks after identifying assets against data, software and hardware. Based on the results of interviews and data collection from several documents, the company needs to identify risks from all factors such as nature/environment, humans, and hardware and this system has the potential to affect the continuity of the company's business operations. The process of identifying risks is adjusted to the location of the company located in Central Jakarta, considering the characteristics of the business processes and services prepared by the company. After the risks are identified, the next process is to determine the level of likelihood of occurrence and the extent of the impact that may arise if these risks occur. The next step is to determine the risk response or procedures that need to be taken by the company in mitigating these risks. A

company, from previous research, there are 15 possible risks [20] that may occur and are classified into 3 types, and these risks are categorized in the code "R". These 15 possible risks can threaten the continuity of the Company and the personnel in it. Having a mature selection and mitigation policy is very important for any company, including a light steel company to be able to minimize the risks that occur and downtime and continue the business operational process optimally after a disaster. In order to be able to describe the above, the formation of a BCP design is necessary in taking action to minimize risks so that the company can continue even when threats occur, as shown in Table 1 Risk List.

Table 1. Risk List

	Risk	**Description**
Nature/Environment	Earthquake (R01), L=1, I=2	Damage to spare part equipment in the warehouse and laptop hardware and disrupted company activities
	Flood (R02), L=3, I=3	Company activities are disrupted
	Dust (R03), L=2, I=2	Damage to spare part equipment and hardware easily overheats, slows down hardware performance, and hampers company activities
	Fire (R04), L=1, I=1	Damage to spare part equipment and hardware stops company activities
Human	Loss of spare parts (R05), L=5, I=5	Hinders recording spare part availability and customer dissatisfaction and material losses
	Unscheduled maintenance and care for spare parts (R06), L=5, I=5	Damage to trucks and spare parts, hampering spare part sales and delivery
	Cybercrime (R07), L=4, I=1	Company data leaks
	Hacking (R08), L=4, I=1	Wiretapping and system disruptions occur
	Abuse of access rights (R09), L=2, I=1	User personal data can be tapped or misused
Hardware* dan *System	Server down (R10), L=4, I=4	Unable to access the Eglobe application and hampers company activities
	Sudden power outage (R11), L= 3, I=3	Difficulty in accessing the Eglobe application and disrupting company activities
	Network connection loss (R12), L=4, I=4	Difficulty in accessing the Eglobe application which causes customer dissatisfaction and a bad reputation
	Overheat (R13), L=2, I=2	Laptop hardware is disrupted and hampers sales activities
	Data Corruption (R14),	Data is damaged, data loss and disrupted

	Risk	Description
Nature/Environment	Earthquake (R01), L=1, I=2	Damage to spare part equipment in the warehouse and laptop hardware and disrupted company activities
	Flood (R02), L=3, I=3	Company activities are disrupted
	Dust (R03), L=2, I=2	Damage to spare part equipment and hardware easily overheats, slows down hardware performance, and hampers company activities
	Fire (R04), L=1, I=1	Damage to spare part equipment and hardware stops company activities
	L=2, I=1	company activities
	Virus, Malware attacks (R15), L=3, I=1	Data loss and disrupted company activities, data corrupt

3.3.2. Risk Analysis

After mapping the risks and impacts, the next stage is to analyze the risks. In this stage, an assessment of the risks will be carried out with reference to the likelihood criteria, namely the magnitude of the frequency or how often the risk occurs and the impact criteria, namely the magnitude of the effect or how big the impact of the risk is displayed in Table 2 Likelihood and Impact.

3.3.3. Risk Evaluation

After identifying the risks and all their impacts, the final stage of the Risk Assessment is the Risk Evaluation, which is entered into the matrix, namely high in red, medium in yellow and low in green. The process of evaluating the risk will use the Risk Evaluation Matrix, namely a combination of Likelihood (L) and Impact (I) indicators as a reference. After identified risk possibilities into the risk evaluation matrix according to Likelihood and Impact, the next stage is to group the 15 risk possibilities into high for red, medium for yellow and low levels for green. From this risk evaluation process, 15 possible risks were identified that had been analyzed and grouped according to their risk levels. Of these, there are 4 risks that are classified as high risk, namely R05, R06, R10, and R12. A total of 4 risks are included in the medium risk level, involving R02, R07, R08, and R11. In addition, there are 7 risks that are included in the low risk level, involving R01, R03, R04, R09, R13, and R15, can be seen in Table 3 Matrix Risk Evaluation Base on Likelihood and Impact.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 2. Likelihood and Impact.

Likelihood		Frequency per Year / month	Description
Rating	**Criteria**		
01	Rare	> 2 years	The risk that occurs does not hinder the operation of the agency and the operation of the application.
02	Unlikely	1 - 2 years	The risk that occurs slightly hinders the operation of the application. However, the central activities of the agency are not disrupted
03	Possible	7 - 12 moths	The risk that occurs results in disruption to the running of some agency activities and the operation of the application.
04	Likely	4 - 6 moths	The risk that occurs holds back almost all agency activities and the operation of the application.
05	Almost Certain	1 - 3 moths	The risk that occurs stops the agency's activity in operating the application due to total disruption.

This fourth stage discusses handling after completing the risk identification process related to assets in a company. The next stage involves the risk treatment process, where specific actions are taken against possible risks that have been grouped according to their risk levels. Details of the proposed risk treatment are R01for provide or prepare a backup server. R02 for place vital equipment in a location that is safe from potential flooding, and companies need to prepare a backup infrastructure provision plan including hardware and network devices. R03 to conduct routine checks on room cleanliness and hardware to minimize the risk of damage. R04 for move the backup server to a different location, companies must design a backup infrastructure plan including hardware and network devices, provide a light fire extinguisher in the agency building to prevent fires. R05 for providing inventory. R06 for schedule maintenance when the application is not busy, and the truck is not being used. R07 for protecting data requires data privacy measures with security software that is always updated, implement security features on the website, such as SSL/HTTPs services, and replace pirated software with licensed ones. R08 for routinely changing account passwords periodically increases system security. R09 for implementing a policy of limiting one user to one device. R10 for performing routine data backups on the agency's main database every day, reduce server load to prevent server downtime. R11 to provide UPS or generators as needed. R12 for the need for bandwidth management. R13 to provide a room with air conditioning and add a cooling system to all hardware. R14 for using original applications and routinely back up data after the input process. R15 to provide antivirus and perform updates.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Table 3. Matrix Risk Evaluation Base on Likelihood and Impact

Almost Certain	05					R05 R06
Likely	04	R07 R08			R10 R12	
Possible	03	R15		R02 R11		
Unlikely	02	R09 R14	R03 R13			
Rare	01	R04	R01			
Impact		**01**	**02**	**03**	**04**	**05**
		Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**

3.4 Monitoring and Review

This fifth stage discusses monitoring and review, the results obtained are in the form of responses and suggestions that can be built by parties who are directly involved in managing data, software and hardware. Light steel companies manage and monitor the implementation of risk management. The entire process of activities is involved by related parties, including the management of companies, employees, and all other parties both internal and external to the company. In implementing this process, companies involve regular meetings and conferences as a means to communicate and prepare reports related to IT implementation, including risks that may hinder the company's business processes. In these regular meetings and conferences, strategies for handling and preventing risks that occur are also discussed, with the aim of mitigating risks in the future.

4. CONCLUSION

ISO 31000 to provide a guide and strategy for preventing risks and actions to minimize and overcome risks both before, during, but also after a disaster that can be used and implemented by the company's business processes can continue to run sustainably, and have gone through all stages, starting from the first stage of communication and consultation, the second stage of establishing the context, there are 2 contexts, namely external and internal, the third stage of risk assessment, there are three processes, namely: risk identification, risk analysis and risk evaluation, the fourth stage of risk treatment and finally monitoring and review. From these stages, there are 15 possible risks that will disrupt the performance of industry based on the risk level categories high, medium, and low. For high risk level there are 4 possible risks, namely R05 (Loss of light steel spare parts), R06 (Unscheduled maintenance and care for trucks and spare parts), R10 (Server down) and R012 (Network connection problems). Next for medium risk level there are 4 possible risks, namely R02 (flood), R07 (Cybercrime), R08 (Hacking), and R011 (Sudden power outage). Finally for low risk level there are 7

possible risks, namely R01 (Earthquake), R03 (Dust), R04 (Fire), R09 (Abuse of access rights), R13 (Overheat), R14 (Data Corrupt), and R15 (Virus Attack, Malware). These possible risks occur due to natural/environmental factors, humans, hardware and systems which if not fixed will create problems for companies. Thus, it is hoped that this research can be used by organizations in regulations to mitigate possible risks that may occur and disrupt light steel companies.

REFERENCES

[1] Y. Gao and D. Xu, "Exploration of Dance Teaching Mode Based on the Information Technology Era," *Front. Art Res.*, vol. 3, no. 3, pp. 32–35, 2021, doi: 10.25236/far.2021.030307.

[2] M. El Khatib, "BIM As a Tool To Optimize And Manage Project Risk Management," *Int. J. Mech. Eng.*, vol. 7, no. 1, pp. 6307–6323, 2022.

[3] J. J. Kassema, "Information Technology (IT) Contingency Plan as part of the Business Continuity Plan: Case of IT Services Delivery Industry," *SSRN Electron. J.*, 2019, doi: 10.2139/ssrn.3496143.

[4] S. Fani and A. Subiadi, "Trend of Business Continuity Plan: A Systematic Literature Review," *ICBLP*, no. 2019, 2020, doi: 10.4108/eai.13-2-2019.2286164.

[5] J. A. R. C. Jayalath and S. C. Premaratne, "Analysis of Key Digital Technology Infrastructure and Cyber Security Consideration Factors for Fintech Companies," *Int. J. Res. Publ.*, vol. 84, no. 1, pp. 128. – 135, 2021, doi: 10.47119/ijrp100841920212246.

[6] S. V. Fani and A. P. Subriadi, "Business Continuity pPan: Examining of Multi-Usable Framework," *Procedia Comput. Sci.*, vol. 161, pp. 275–282, 2019, doi: 10.1016/j.procs.2019.11.124.

[7] I. Mas'ud and R. Salsabila, "Perancangan Business Continuity Plan Pada PT. XYZ," *J. Sist. Inf. dan Sains Teknol.*, vol. 3, no. 1, pp. 1–14, 2021, doi: 10.31326/sistek.v3i1.803.

[8] M. R. Purnama, M. B. Adityawan, K. S. Pribadi, M. Farid, Widyaningtias, and A. A. Kuntoro, "Tsunami Risk Assessment in Business Continuity Planning for Palu Special Economic Zone," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 1065, no. 1, 2022, doi: 10.1088/1755-1315/1065/1/012053.

[9] I. Setiawan, R. Waluyo, and W. A. Pambudi, "Perancangan Business Continuity Plan dan Disaster Recovery Plan Teknologi dan Sistem Informasi Menggunakan ISO 22301," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 3, no. 2, pp. 148–155, 2019, doi: 10.29207/resti.v3i2.911.

[10] B. Prieto, "Enterprise Risk Management in the Engineering and Construction," *PM World J.*, vol. XI, no. V, pp. 2330–4480, 2022.

[11] E. C. Ali and N. C. Ali, "Business Continuity Plan of the Micro and Small Enterprises in Cotabato City during the COVID-19 Pandemic and Its Effect to Business Performance," *Eur. J. Bus. Manag. Res.*, vol. 8, no. 3, pp. 124–127, 2023, doi: 10.24018/ejbmr.2023.8.3.1916.

[12] A. Berrichi and Z. Azarkan, "Business Continuity Plan facing COVID-19 : From necessity to Alterities Business Continuity Plan facing COVID-19 :," *HAL oepn Sci.*, vol. 2, no. 4, pp. 597–617, 2021, doi: 10.5281/zenodo.5149419.

[13] F. T. Kurniati and R. R. Huizen, "Sosialisasi Strategi Business Continuity Plan Memasuki Era Baru (New Normal)," *War. LPM*, vol. 24, no. 4, pp. 788–798, 2021.

[14] T. F. Rahardian and A. F. Wijaya, "Risk Analysis of Web-Based Information Systems on CV Mega Komputama Uses ISO 31000," *J. Inf. Syst. Informatics*, vol. 4, no. 2, p. 442, 2022.

[15] E. Evinia and M. N. N. Sitokdana, "Risk Management Based IT Analysis Using ISO 31000 (Case Study: PT Bawen Mediatama)," *J. Inf. Syst. Informatics*, vol. 5, no. 1, pp. 380–390, 2023, doi: 10.51519/journalisi.v5i1.420.

[16] F. A. Alijoyo, "The use ISO 31000:2018 in Indonesian Fintech Lending Companies: What Can We Learn?," *J. Bus. Manag. Stud.*, vol. 4, no. 1, pp. 16–22, 2022, doi: 10.32996/jbms.2022.4.1.3.

[17] J. F. Andry, N. Karepowan, and H. Tannady, "Disaster Recovery Planning for It/Is of Hospitality Industry Using Nist Sp 800-34 Rev.1 Method," *J. Theor. Appl. Inf. Technol.*, vol. 102, no. 8, pp. 3562–3569, 2024.

[18] D. Y. Bernanda, Y. Charolina, O. Azhari, C. Pangrestu, and J. F. Andry, "Identification of Potential and Planning for Disaster Recovery Using the Iso/Iec 24762 Standard At Xyz University," *J. Teknoinfo*, vol. 17, no. 1, p. 140, 2023, doi: 10.33365/jti.v17i1.2295.

[19] J. F. Andry, H. Tannady, G. D. Rembulan, Gerry, and Honni, "Disaster Recovery Design at Higher Education Institutional Using ISO 27021 Method.pdf," *Soc. Sci. J.*, vol. 12, no. 5, pp. 1211–1217, 2022.

[20] J. F. Andry, L. Liliana, H. Tannady, and A. S. Arief, "Data Centre Risk Analysis Using ISO 31000:2009 Framework," *J. Phys. Conf. Ser.*, vol. 2394, no. 1, 2022, doi: 10.1088/1742-6596/2394/1/012032.