Journal of Information Systems and Informatics
Vol. 5, No. 1, March 2023 e-ISSN: 2656-4882 p-ISSN: 2656-5935
DOI: 10.51519/journalisi.v5i1.420 Published By DRPM-UBD

Risk Management Based IT Analysis Using ISO 31000 (Case Study: PT Bawen Mediatama)

Evinia[1], Melkior N.N Sitokdana[2]

[1]Information System Department, Satya Wacana Christian University, Salatiga, Indonesia
Email: [1]682019059@student.uksw.edu, [2]melkior.sitokdana@uksw.edu

Abstract

This study examines the risks of implementing information technology (IT) at PT Bawen Mediatama, a company that has experienced damage to financial institution files due to their IT use. The study uses the ISO 31000 framework to analyze the risks faced by PT Bawen Mediatama, with a focus on identifying the risks and providing recommendations for appropriate risk treatment. The research method is qualitative, and the results indicate that PT Bawen Mediatama faces 20 possible risks, including limited, severe, very severe, and catastrophic level risks. Although the company has implemented risk management, the study concludes that it is not optimal.

Keywords: Risk, ISO 31000, IT Risk Management, Company, Business Process.

1. INTRODUCTION

In today's world of rapid development, information technology is advancing at an exponential rate, and all aspects of life are following suit [1]. Many industries, including the printing sector company PT Bawen Mediatama, have embraced technological advancements to enhance their business processes. For instance, PT Bawen Mediatama has implemented a comprehensive information system, Kompas Gramedia intranet, to record and report financial transactions. Hardware is also used to support the business systems and processes. However, every technology carries inherent risks, including hardware damage, malware, and other IT crimes that can lead to data loss or errors, and hardware damage. Therefore, a risk management analysis is necessary at PT Bawen Mediatama to identify all the existing risks in the organization and provide recommendations for appropriate risk treatment to mitigate the potential negative impact.

Risk management presents a strategic challenge for companies as they face numerous threats. To address this challenge, this study employs the ISO 31000 approach, which is a structured guideline published by the International Organization for Standardization (ISO) on 13 November 2009 [2]. The ISO 31000 approach assists in solving problems related to various contexts/scopes of risk

management [3]. It is widely applicable to different fields, functions, projects, and activities, making it a versatile and effective tool for companies to adopt. The ISO 31000 approach was used in this study's process, while the Failure Mode and Effects Analysis (FMEA) approach was employed for risk analysis. The FMEA approach is widely used for risk analysis due to its ease of operation and its ability to identify potential failures and their impacts [4-5].

Several studies have utilized the International Organization for Standardization (ISO) 31000 research framework for risk analysis, which serves as an international standard for risk management guidelines [6]. One such study conducted by Miftakhatun, analyzed the Ecofo website to determine the possibility of risk emergence and how to minimize future risks. The study employed the ISO 31000 approach, consisting of five stages, and identified a total of 24 possible risks, including three Very Severe, ten Severe, and eleven Limited level risks [7]. In another study by Aprilia Rahmawati and Agustinus Fritz Wijaya, the ITOP application was analyzed for potential risks using the ISO 31000 framework in 2019. The study identified 21 possible risks that could potentially affect the iTop application, including eight severe risks such as network disconnection, poor network quality, human error, and server failures. Additionally, the study identified 17 Limited level risks [8]. In a recent study, Muhammad Ilham Fachrezi focused on the identification, analysis, and management of risks related to information technology asset security. The study used the Failure Mode and Effects Analysis approach and found two low-level risks, eleven intermediate-level risks, and four high-level risks [9]. The unique approach employed in this study is worth noting, distinguishing it from prior research. The primary goal of this study is to examine Risk Management based on IT Analysis using ISO 31000 and to conduct a case study on PT Bawen Mediatama.

2. METHOD

In the information technology risk analysis that uses the Risk Management base at PT Bawen Mediatama, it has research stages that can be seen in Figure 1. The detail of each stage as follow.

2.1 Data Collection Method

This study employed a qualitative method with data collection techniques involving observation and interviews. Qualitative research methods focus on the quality, value, or meaning of existing facts [10]. The IT department was observed and IT heads, supervisors, and managers were interviewed to identify risks. The information provided by these sources was considered valid data as it corresponded to actual conditions and issues [11]. The results obtained from this qualitative approach were used to conduct an analysis to address the problems and issues at PT Bawen Mediatama. The data collected through observation and

interviews were supplemented by risk management analysis techniques based on the ISO 31000 standard.

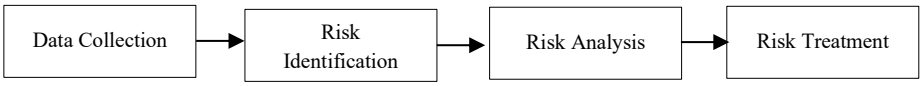

Figure 1. Stages of Research

2.2 Risk Identification

This stage involves the identification of possible risks and the identification of the company's information technology assets to facilitate the process. Risk identification is a structured process of finding and analyzing the risks that exist within a business process and assets, including those resulting from human factors, the systems used by the company, and infrastructure factors such as hardware [11]. Therefore, risk identification at PT Bawen Mediatama aims to identify all possible risks that exist within the company's information technology assets. This process is crucial for the organization to manage and mitigate risks effectively.

2.3 Risk Analysis

The process of risk analysis involves analyzing possible risks using data obtained from the risk identification process to determine the level of risk [12]. The obtained data is then analyzed using a risk management method that follows the ISO 31000 framework as a comprehensive guideline. Possible risks are assessed based on the frequency of likelihood and impact events [13]. Table 1 provides a detailed explanation of risk calculation related to likelihood.

Table 1. Likelihood

Frequency	Category	Information
1	Minor	Chances of happening are small/never happen > 5 Year
2	Limited	Risks may occur within 3-5 years
3	Severe	Risks sometimes occur in the range of 2-4 years
4	Very Severe	Risks often occur in the range of once every 1-2 years
5	Catastrophic	The risk is definitely in the range of < 1 year

Moreover, Table 2 provides an impact assessment for each identified risk. Impact refers to the consequence that would occur if the risk were to materialize at PT Bawen Mediatama. The table consists of 5 possible impact values, with each value

indicating the degree to which the risk could affect the company's business processes. The values range from no impact on the company's activities to severe disruption of the company's operations.

Table 2. Impact Assessment

Information	Value
Risks do not have the possibility to interfere with the course of business processes	1
Has possible risks that tend to interfere slightly with business processes	2
Risks have the potential to interfere with business processes that run	3
Risks have the potential to impede certain parts of the business process	4
Risks have the potential to interfere with the overall activities of the company	5

Based on the values presented in Table 1 and Table 2, the next step is to determine the level of each identified risk. The level of risk is determined by taking into account the frequency of occurrence and the impact of the risk. This is calculated using a formula that considers the impact and frequency values as discussed earlier.

Formula for Calculating Risk Status = Frequency x Impact

The application of the formula mentioned above resulted in the calculation outcomes presented in Table 3.

Table 3. Risk Calculation Matrix

Impact / *Likelihood*	1	2	3	4	5
1	Limited 1	Limited 2	Limited 3	Severe 4	Severe 5
2	Limited 2	Severe 4	Severe 6	Very Severe 8	Very Severe 10
3	Limited 3	Severe 6	Very Severe 9	Very Severe 12	Catastrophic 15
4	Severe 4	Very Severe 8	Very Severe 12	Catastrophic 16	Catastrophic 20
5	Severe 5	Very Severe 10	Catastrophic 15	Catastrophic 20	Catastrophic 25

2.4 Risk Treatment

Risk treatment involves making appropriate decisions based on the level of risk priority, using the results of the previously prepared risk analysis [14]. Its goal is to determine risk management by providing recommendations on control functions that can be implemented to mitigate the identified risks [15] at PT Bawen Mediatama.

3. RESULTS AND DISCUSSION

3.1 Risk Identification

At this stage, two (2) identifications will be conducted, namely identification of information technology assets and identification of risks based on data collected through interviews and direct observation at PT Bawen Mediatama. The first identification is aimed at identifying information technology assets, which can be seen in Table 4.

Table 4. IT Asset Identification of PT Bawen Mediatama

Information Technology Components	Information Technology Assets
Data	User Data, Website Data, Transaction Data, financial data, Employee Data
Hardware	Server Database, Personal Computer
Software	Gramedia Compass Intranet

After identifying the information technology assets, the next step is to identify possible risks based on previous issues. The researchers have classified the possible risks into three factors. Risks can arise from the company's assets, which can be seen in Table 5.

Table 5. Identify Possible Risks

Factor	Risk ID	Risk
Nature and Milieu	R01	> Earthquakes
	R02	> Flood
	R03	> Fire
	R04	> Dust and Dirt
	R05	> Power Outages
Human	R06	> Human Error
	R07	> Misuse of Access Rights
	R08	> Device Theft

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

Factor	Risk ID	Risk
	R09	> Cybercrime
	R10	> Data and Information Incompatibility
	R11	> Employees do not follow the SOP
	R12	> Technical Errors
System and Infrastructure	R13	> Disk Error
	R14	> Logical Attacks Like hacking and malware
	R15	> Overload Database
	R16	> Overheating on Computer Devices
	R17	> Data Corrupt
	R18	> System failure due to network disconnection
	R19	> Software Failure/Damage
	R20	> Web Service Shuts Down Suddenly

Based on the results of risk identification, a total of 20 possible risks have been identified. These risks can be classified into three categories: natural and environmental factors (5 risks), human factors (7 risks), and systems and infrastructure (8 risks). These risks have the potential to affect PT Bawen Mediatama's ability to carry out its business processes and hinder the achievement of its goals.

3.2 Risk Analysis

In this stage, the possible risks identified in the previous stage, namely the risk identification stage, are analyzed. Risk analysis involves determining the value of each possible risk based on the likelihood and impact of events, resulting in a risk score and level for each possible risk. The details of the risk score and level for each possible risk can be seen in Table 6.

Table 6. Risk Analysis

Risk	Likelihood	Impact	Risk Score	Risk Level
> Earthquakes	1	5	5	Severe
> Flood	1	5	5	Severe
> Fire	1	5	5	Severe
> Dust and Dirt	2	2	4	Severe
> Power Outages	1	2	2	Limited
> Human Error	2	2	4	Severe
> Misuse of Access Rights	2	2	4	Severe

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

Risk	Likelihood	Impact	Risk Score	Risk Level
> Device Theft	1	3	3	Limited
> Cybercrime	2	4	8	Very Severe
> Data and Information Incompatibility	2	2	4	Severe
> Employees do not follow the SOP	2	2	4	Severe
> Technical Errors	2	4	8	Very Severe
> Disk Error	2	3	6	Severe
> Logical Attacks Like hacking and malware	3	5	15	Catastrophic
> Overload Database	4	4	16	Catastrophic
> Overheating on Computer Devices	4	3	12	Very Severe
> Data Corrupt	3	4	12	Very Severe
> System failure due to network disconnection	2	3	6	Severe
> Software Failure/Damage	2	3	6	Severe
> Web Service Shuts Down Suddenly	3	4	12	Very Severe

Critical; Must be dealt with quickly
Important; Must be dealt with immediately so as not to level up
Acceptable; Must be handled appropriately and watched out for so as not to cause more harm
Noteworthy

Based on the results of the risk analysis carried out, likelihood was obtained with a score of 1 totaling 6, a score of 2 with a total of 10, a score of 3 with a total of 3, a score of 4 with a total of 2. Then impact with score 2 totaling 6, score 3 with 5, score 4 with 5, and score 5 with 4.

3.3 Risk Treatment

In this final stage, proposals will be made on what control functions can be implemented to manage the identified risks. The proposed control functions or risk treatment measures for each risk can be found in Table 7.

Table 7. Risk Treatment

ID	Risk	Risk Level	Response
R01	Earthquake	Severe	To reduce the possibility of data loss, it is better to keep data instead of just stored in one place.

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

ID	Risk	Risk Level	Response
R02	Flood	Severe	Placing company hardware or infrastructure in a place that does not have the potential to be affected by flooding
R03	Fire	Severe	The need for the provision of a complete fire extinguisher
R04	Dust and Dirt	Severe	The need to carry out regular cleaning in the area of hardware or technology used to minimize the risk of damage.
R05	Power Outages	Limited	The need for regular checks on the generator so that when the generator is needed it can be directly used for electricity diversion.
R06	Human Error	Severe	The need to conduct training to human resources based on predetermined standards Conduct regular checks on the performance of employees who often make mistakes
R07	Misuse of Access Rights	Severe	Providing CCTV in all rooms at once there must be main control and leaders must be diligent in checking employee activity history from checking the system to CCTV
R08	Device theft	Limited	It is necessary to carry out strict guarding of companies such as the procurement of trained security, especially at night.
R09	Cybercrime	Very Severe	The need to protect company data and ensure data confidentiality by using anti-virus software as well as using website security features such as SSL / HTTP services.
R10	Data and Information Incompatibility	Severe	It is necessary to review data and information regularly and systematically so that there are no discrepancies in data or information
R11	Employees do not follow SOPs	Severe	Provide clear and appropriate directions and consequences regarding SOP policies

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

ID	Risk	Risk Level	Response
R12	Technical Errors	Very Severe	Giving warnings such as verbal to written reprimands.
R13	Disk Error	Severe	The need to provide a backup hard drive with a capacity that suits the needs of the company
R14	Logical Attacks Like hacking and malware	Catastrophic	The need to do the server password regularly
R15	Overload Database	Catastrophic	The need to monitor the server and expand the bandwidth capacity of the system.
R16	Overheating on Computer Devices	Very Severe	Place the hardware according to the recommended temperature and perform maintenance on a scheduled basis.
R17	Data Corrupt	Very Severe	Perform periodic data backups
R18	System failure due to network disconnection	Severe	Perform network maintenance at the company periodically to reduce the possibility of system failure due to network disconnection
R19	Software failure/damage	Severe	Perform gradual maintenance on the software to avoid damage
R20	Web Service Shuts Down Suddenly	Very Severe	The need to do regular website maintenance and backup website data

Out of the 20 possible risks that were identified and analyzed, there were 2 risks classified as having a Limited level of risk: power outages and device theft. 11 risks were classified as having a Severe level of risk, including Earthquakes, Floods, Fires, Dust and Dirt, Human Error, Misuse of Access Rights, Data and Information Discrepancies, Employees not following SOPs, Disk Errors, System failures due to network disconnections, and Software Failures/damage. 5 risks were classified as having a Very Severe level of risk, including Cybercrime, Technical Errors, Overheating on Computer Devices, Data Corrupt and Web Services Shut Down Suddenly. Lastly, there were 2 risks classified as having a Catastrophic level of risk: Logical Attacks Such as hacking and malware, and Database Overload. To mitigate these risks, the researcher has provided suggestions for risk treatment that can be applied to prevent possible risks from occurring or interfering with the organization's goals. It is crucial for the organization to take action in anticipation of these risks so that they can be prevented from causing harm or disruption to the organization's operations.

The risks identified were classified into three factors: natural and environmental factors, human factors, and system and infrastructure factors. The risks were then analyzed based on the likelihood and impact, resulting in a risk score and level for each possible risk. The results showed that there were 20 possible risks, with two being limited level risks, 11 being severe level risks, five being very severe level risks, and two being catastrophic level risks. To address the risks, proposed control functions or risk treatments were provided, which aimed to anticipate and mitigate the risks to prevent them from interfering with the company's goals. The risk treatment stage is crucial because it allows the organization to take appropriate action based on the level of risk priority. Overall, this risk management process serves as a comprehensive approach to identify, analyze, and treat potential risks that could impact the organization's operations. By conducting a risk management process, the organization can proactively address potential risks and minimize their impact on the business.

4. CONCLUSION

Based on the analysis of risks faced by PT Bawen Mediatama, it can be concluded that there are 20 possible risks, classified into different risk levels. The Severe level risks, totaling 11, pose a significant threat to the organization's business processes and achievement of its goals. The Very Severe level risks and Catastrophic level risks also need to be addressed by the company. To address these risks, the researcher has provided proposals for risk treatment measures that can be applied by PT Bawen Mediatama. These measures should serve as guidelines for minimizing the impact of risks on the company's operations. It is important to note that PT Bawen Mediatama has made efforts to address the risks identified, but there is still room for improvement in handling these risks. A review of all problems faced by the company is necessary to ensure that its business objectives are achieved. Future research should focus on risk management from the smallest scope to obtain more effective and comprehensive results. In addition, attention to detail regarding the use of risk management guidelines, such as the ISO 31000 framework, is crucial for the perfection of research.

REFERENCE

[1] M. Iso, F. G. Punusingon, M. N. N. Sitokdana, and J. O. Notohamidjojo, 2022, "Analisis Manajemen Risiko Aplikasi SIMFONI Pada Dinas PPA Di Kab. Minahasa Tenggara," vol. 4, no. 2, pp. 25–36.

[2] G. W. Lantang, A. D. Cahyono, and N. Ngalumsine, 2019, "Analisis Risiko Teknologi Informasi pada Aplikasi SAP di PT Serasi Autoraya Menggunakan ISO 31000", Sebatik 2621-069X, Vol. 23 No. 1, pp. 36–43.

[3] U. R. de Oliveira, F. A. S. Marins, H. M. Rocha, and V. A. P. Salomon, 2017, "The ISO 31000 standard in supply chain risk management," J. Clean. Prod., vol. 151, pp. 616–633.

[4] B. Purwanggono and A. Margarette, 2019, "Risk assessment of underpass infrastructure project based on IS0 31000 and ISO 21500 using fishbone diagram and RFMEA (project risk failure mode and effects analysis) method," IOP Conf. Ser. Mater. Sci. Eng., vol. 277, no. 1, p. 012039.

[5] F. Shirvani, W. Scott, G. A. L. Kennedy, and A. P. Campbell, 2019, "Enhancement of FMEA risk assessment with SysML," Aust. J. Multi-Disciplinary Eng., vol. 15, no. 1, pp. 52–61.

[6] T. Ramdhany and R. A. Krisdiawan. 2018, "Analisis Risiko Sistem Informasi Penjualan Berbasis Iso 31000 - Risk Management di PT. Remaja Rosdakarya", Teknol. dan Manaj. Inform., Vol. 3, No. 1, pp. 1–7,

[7] M. Miftakhatun., 2020, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000", *Journal of Computer Science and Engineering (JCSE)*, *1*(2), 128–146. https://doi.org/10.36596/jcse.v1i2.76.

[8] A. Rahmawati, & Wijaya, A. F., 2019, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi ITOP", *Jurnal SITECH : Sistem Informasi Dan Teknologi*, *2*(1), 13–20. https://doi.org/10.24176/sitech.v2i1.3122.

[9] M. I. Fachrezi, A. D. Cahyono, and P. F. Tanaem, 2021, "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000 : 2018 Diskominfo Kota Salatiga," vol. 8, no. 2, pp. 764–773.

[10] S. D. Fitri, D. L. Setyowati, and K. Duma. 2019, "Implementasi Manajemen Risiko Berdasarkan ISO 31000: 2009 pada Program Perawatan Mesin di Area Workshop PT . X", Vol. 6, No. 1, pp. 16–24.

[11] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, "Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ," JURIKOM (Jurnal Ris. Komputer), vol. 7, no. 1, p. 91, 2020, doi: 10.30865/jurikom.v7i1.1791.

[12] Muryanti and K. D. Hartomo, 2021, "Analisis Risiko Teknologi Informasi Aplikasi CATTER PDAM Kota Salatiga Menggunakan ISO 31000," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 8, no. 3, pp. 1265–1277, doi: 10.35957/jatisi.v8i3.948.

[13] S. Rass, S. König, and S. Schauer, 2017, "Defending against advanced persistent threats using game-theory," *PLoS One*, vol. 12, no. 1, pp. 1–45, doi: 10.1371/journal.pone.0168675.

[14] P. S. Ilham Rinaldi, Syarifa Hanoum, 2021, "Identifikasi Tingkat Kematangan Risiko," vol. 10, no. 1.

[15] I. P. A. E. Pratama and M. T. S. Pratika, 2020, "Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018," *J. Telemat.*, vol. 15, no. 2, pp. 63–70.