Journal of Information Systems and Informatics
Vol. 4, No. 2, June 2022 e-ISSN: 2656-4882 p-ISSN: 2656-5935
http://journal-isi.org/index.php/isi Published By DRPM-UBD

Information Technology Risk Management on Semarang Regency BPS Application Using ISO31000:2018

Sandra Gita[1], Penidas Fiodinggo Tanaem[2]

[1,2]Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga, Indonesia
Email: [1]682018120@student.uksw.edu, [2]penidas.fiodinggo@uksw.edu

Abstract

BPS Semarang Regency is an agency engaged in calculating census statistics, BPS Semarang Regency has implemented SI / IT to support the performance carried out. BPS Semarang Regency has an application in the form of ICS or better known as the Integrated Collection System, where this application is used in calculating population censuses, economic censuses, and agricultural censuses. However, there is always a risk from the application, one of the risk impacts that has occurred such as human error, the server that suddenly goes down becomes an obstacle for users in running the application. With SI/IT risk management conducted to minimize risk, it will be carried out using the ISO31000:2018 framework. It is hoped that this risk management can be used as a guideline for BPS Semarang Regency in dealing with existing risks. The results of this risk analysis are in the form of proposed recommendations from risk actions on risks based on the impact and frequency of events. That way BPS Semarang Regency can prevent and minimize risks so that the function of the ICS application can run optimally.

Keywords: risk analysis, risk management, ISO31000

1. INTRODUCTION

Information technology in this era is an important opportunity for companies that can be used to develop the company's business and develop business processes in certain agencies, all companies and agencies need information technology in supporting the role of organizational activities. The role of applications as information system media is most widely used in agencies and companies[1]. Therefore, each agency is indirectly competing to improve their SI/IT. However, with the increasing information technology of agencies or companies, there are increased threats of risk opportunities that can occur at any time. No matter how good the information technology used by an agency or company, it must always be followed by risks that will threaten the company's performance, so a risk control is needed by conducting appropriate risk management for a company[2].
Risk management is an appropriate method for an agency to control risks, by conducting risk analysis to evaluating risks. So that the expected results in the form

of recommendations on risk control can be maximized and as expected by the agency[3]. The case study in this study is BPS (Central Statistics Agency) Semarang Regency, the Central Statistics Agency is a Non-Ministerial Government agency that is responsible to the President. BPS has duties such as conducting a Population Census, conducting an Agricultural Census, and conducting an Economic Census, providing quality statistical data, and strengthening the National Statistics System through good guidance and coordination. With so many duties and responsibilities of BPS, the agency has an application that helps in business processes that are carried out instantly, one of the applications used by BPS is the ICS application, namely the Integrated Collection System, this application is used in collecting population census data, and various other censuses, so that the data generated from the application is real and can be accounted for.

The ICS application is extremely helpful in business processes in BPS Semarang Regency, but what needs to be considered is that this application also has many risks and possible risks that can occur at any time that can interfere with the business process of BPS Semarang Regency. As an example that can be clearly seen the existing risks in the form of Human Error, Overheating, and Server Down so that it is very necessary to analyze and evaluate risk management in the ICS application at BPS Semarang Regency by identifying the risks and potential risks that exist and how the impact of possible risks that will occur, so that later it will produce appropriate risk control recommendations and needed by BPS Semarang Regency on the ICS application. From this problem, a risk analysis is needed using the ISO 31000:2018 framework, where ISO31000:2018 has broader standards and reviews and can be applied in various scopes of the institute and is more ideal than other standards[4].

ISO or the National Standards Organization which brings with it the ISO31000: 2018 framework to the public contains risk management standards centered on SI / IT governance or IT Governance [5]. With the publication of the 2018 version which is the latest version of ISO31000, it is expected to replace the standard that is currently widely used differently in various companies as well as those that implement ISO31000[6]. ISO 31000:2018 is a standard tool used as a demand for companies in building and improving foundations and is a suitable framework for use in company conditions that prioritize SI / IT risk management. The framework also spans the rules, objectives, and commitment to developing an SI/IT risk management project[7]. In a framework that also includes planning, capabilities for workers, business processes and business activities used in regulating the management of risks to the business performance of companies and agencies. In risk management using ISO 31000: 2018 proves that the risk value can be set in 3 levels, namely risk with low, medium, and high levels[8].
The purpose of this study is to assist BPS Semarang Regency in improving risk management performance, by minimizing the risks and potential risks contained

in the ICS application and providing appropriate recommendations on the risks that have been identified or risks that can at any time appear and interfere with the performance of the ICS system[9]. Based on previous research on risk management using ISO 31000:2009, it was conducted by Driantami, Suprapto and Perdanakusuma in 2018. The study was conducted with the NIST framework 800-30 case studies conducted in the Sales System of PT Matahaari Department Store Malang Town Aquare Branch. The study found three important points that can be taken such as: (1) In risk management, it is carried out with the ISO 31000 framework, which will be carried out with a more technical framework such as NIST 800-30. (2) In the case of using ISO 31000 it is possible to display the risk value in three levels, namely low, medium, and high. (3) Appropriate research recommendations such as risk control for the risk of human error (error in system operation), to avoid the risk of credential theft rights and reduce the risk of unstable connection risks. [10].

Rilyani, Firdaus and Jatmiko in 2015 conducted information technology risk management research using ISO 31000 conducted at I-Ggracial Telkom University as a case study. In research activities, so many processes are conducted that support risk management activities, to get the following results of risks to the i-Gracias system. That is, the risk has the highest level which is the risk that finds a position rating in probability as well as an impact value that shows in a high level. The i-Gracias system can see that the risk with the highest risk value is the Database Server which is often Down. Given the impact that can cause this risk to occur, not all iGracias services are difficult to operate and need to implement such risk management in a timely and timely manner [11].

In addition, Stefan Agustinus conducted research in 2017 with the title "Information Technology Risk Analysis in the HRMS Program". In this case, the study is conducted on the topic of risk assessment of assets that are around the company. In this study, it was found that 2 risks that may occur have a high level of risk and 18 risks were also found that occupy the medium risk level that allows disruptions to the company's performance / business. With the risk assessment, it is hoped that it can minimize the losses caused by these risks. Risk management focuses on high-risk assets by identifying their causes and then finding the right solution[6].

2. METHODS

The method used in the presentation of risk management research on ICS applications at BPS Semarang Regency is conducted using the case study research method, which is a suitable method for this research because it focuses on a specific ICS application audience. The approach taken in this study is also conducted using quantitative methods, with this approach researchers are directly

involved in the field and assess as well as observe case studies on ICS applications to obtain real data certainty obtained from the object of the case study[12].

2.1. Research Methods

The research method conducted at BPS Semarang Regency on risk management was carried out using the ISO31000: 2018 framework. ISO31000 is a guide for the application of risk through 3 elements, namely principles, frameworks and processes. Where the principle of ISO31000 as the basis of risk management, the framework as a systematic arrangement of risk management, while the process as a risk management activity is interrelated and interrelated with each other. In the 2018 version, ISO31000 simplified the 2009 version. Several things have been changed, including the naming of "Principles and Guidelines" to "Guidelines", a reduction in the number of pages that has shrunk from 24 pages to 16 pages[13]. In addition, the principles of risk management have also changed, from 11 principles in the 2009 version to 1 goal and 8 principles in 2018. The principle regarding "creation and value protection" in 2009, was transformed into a risk management goal. Two principles, namely "the decision-making part" and "explicitly addressing uncertainty", were removed. The other eight principles simplified the statement to (1) integrated, (2) structured and comprehensive, (3) customized, (4) inclusive, (5) dynamic, (6) the best available information, (7) human and cultural factors, and (8) continuous improvement. A more detailed picture in the research method using ISO31000: 2018 in the research on risk management in ICS applications contained in BPS Semarang Regency, can be seen in figure 1[5].

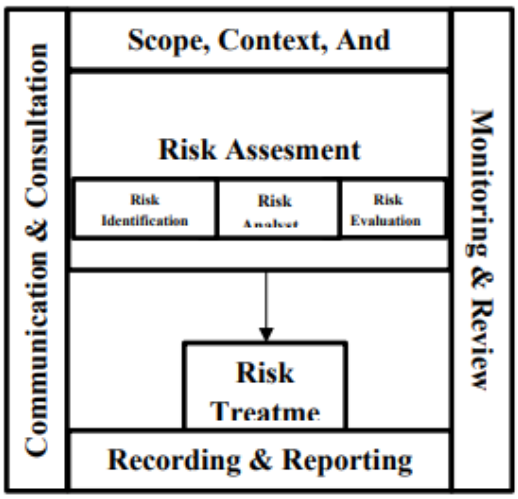

Figure 1. Research Methods

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

The above steps are carried out in research on SI / IT risk management in ICS applications at BPS Semarang Regency, with the above steps, starting from risk assessment to risk treatment. In the risk assessment stage, there are several sub-stages, including.

1. Risk Identification which is a step in how to obtain data and present data on risks that may arise and interfere with business processes in activities carried out regarding the ics application in BPS Semarang Regency[14].
2. Risk Analysis is a risk analysis method that includes risk assessment, risk grouping, to management activities and policies around risk in the ICS application at BPS Semarang Regency[15].
3. Risk Assessment is a process used to compare risks according to risk levels starting with the risk that has the lowest value to the risk that has the highest value that has been found during risk analysis. So that through risk evaluation, it has the aim of helping the risk acceptance process after the results of the risk analysis[16].

The risk treatment stage involves the selection of an appropriate risk recommendation that can be used in controlling risks so that appropriate risk control can be carried out for BPS Semarang Regency.

3. RESULTS AND DISCUSSION

3.1 Risk Assessment

The first step that needs to be done regarding the risk assessment on ICS applications at BPS Semarang Regency. This step goes through several stages such as firstly identifying risks, then analyzing risks, and finally evaluating risks.

3.2 Risk Identification

a. Asset identification

In the first stage, the identification of assets related to the ICS application is carried out, where these assets include data assets, software assets, and hardware assets. Focus On identifying the 3 assets.

Table 1. Asset Identification

INFORMATION SYSTEM COMPONENTS	ASSET
DATA	Population data, regional data, statistical data
SOFTWARE	ICS system
HARDWARE	Smartphone

b. Identify Possible Risks

Next, enter the identification of possible risks, you can classify in 3 appropriate factors, namely natural factors, human factors, and system or infrastructure factors. The results of the identification of possible risks can be seen in table 2.

Table 2. Identify Possible Risks

FACTOR	ID	POSSIBLE RISK
NATURAL	R001	Flood
	R002	Fire
	R003	Earthquake
	R004	Rainstorm
HUMAN	R005	Human Error
	R006	Abuse of access rights
	R007	Data theft and Leaks
	R008	Theft hardware
	R009	Hacking
	R010	User Interface that is difficult to understand
	R011	Damage to facilities
	R012	New employees who are still lay with system
SYSTEM DAN INFRASTRUCTURE	R013	Bad network connection
	R014	Breakdown hardware
	R015	Data server that is often down
	R016	Data loss
	R017	Overheat
	R018	Trouble Backup
	R019	System error
	R020	Powerless

Based on the results of the risk identification, it found 20 possibilities that are possible risks.

c. Identify the Impact of Possible Risks

Next in this step, identification of the risk impact of possible risks contained in the ICS application is carried out. At this stage, an analysis of the possible impacts that can be caused by the possible risks has been identified in table 2. The impact analysis can be seen in table 3.

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

Table 3. Identify the Impact of Possible Risks

FACTOR	ID	POSSIBLE RISK	IMPACT
NATURAL	R001	Flood	Assets that are exposed to air floods can cause damage
	R002	Fire	Can cause damage to buildings and company assets
	R003	Earthquake	Can cause damage to assets
	R004	Rain Storm	Allows for damage
HUMAN	R005	Human Error	There is a miscommunication of data on the system
	R006	Abuse of access rights	Allows other employees to access other users
	R007	Data theft and Leaks	Company data can be leaked
	R008	Theft hardware	Company financial loss
	R009	Hacking	A bugged system can result in leaking company data or damage to software
	R010	User Interface that is difficult to understand	Users are confused about running the system
	R011	Damage to facilities	Cause financial loss and damage to company assets
	R012	New employees who are still lay with system	Delay in syncing company data
SYSTEM DAN INFRASTRUCTURE	R013	Bad network connection	Users have difficulty accessing the system
	R014	Breakdown hardware	Assets will be difficult to use
	R015	Data server that is often down	Difficulty in accessing system data
	R016	Data loss	Lost company data

	R017	Overheat	Hardware temperature increases causing possible damage
	R018	Trouble Backup	Data cannot be backed up
	R019	System error	User cannot access the system
	R020	Powerless	The system cannot be accessed online

3.3 Risk Analysis

Risk analysis can be used as an assessment of any potential that is possible to be categorized as a risk that exists at the stage of identifying potentials that allow as risks to be carried out using a table of likelihood criteria or the frequency of events of possible risks occurring.

Table 4. Likelihood Criteria Table

LIKELIHOOD		**DESCRIPTION**	**EVENT**
SCORE	Criteria		**FREQUENCY**
1	Rare	The risk never happened	>2 Year
2	Unlikely	Risk is rare	1 – 2 Year
3	Possible	Risk of occurrence but not often	7 – 12 Year
4	Likely	Frequent risk	4 – 6 Month
5	Certain	The risk is certain	1 – 3 Month

Next, the value of each risk impact that occurs is determined, this can be seen from the impact table which consists of possible risks, in the impact evaluation table combined into 5 criteria and the impact is assessed based on no effect to a very influential impact.

Table 5. Impact Criteria

IMPACT		**DESCRIPTION**
SCORE	Criteria	
1	Insignificant	The risk is not so disturbing activities
2	Minor	The risk of making activities a little hampered
3	Moderate	The risk of hampering business activities

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

4	Major	The risk is very disturbing the company's business activities
5	Catasirophic	The company's activities are very disrupted

Next, after obtaining the criteria from the frequency of events in table 4 and the impact criteria in table 5, an assessment of the possible risks to the frequency of events and the criteria for the impact that will occur is then carried out.

Table 6. Likelihood and Impact Assessment

FACTOR	ID	POSSIBLE RISK	LIKELIHOOD	IMPACT
NATURAL	R001	Flood	1	4
	R002	Fire	2	2
	R003	Earthquake	1	5
	R004	Rainstorm	2	3
HUMAN	R005	Human Error	4	3
	R006	Abuse of access rights	2	2
	R007	Data theft and Leaks	1	2
	R008	Theft hardware	1	3
	R009	Hacking	1	3
	R010	User Interface that is difficult to understand	2	1
	R011	Damage to facilities	1	3
	R012	New employees who are still lay with system	4	2
SYSTEM DAN INFRASTRUCTURE	R013	Bad network connection	4	4
	R014	Breakdown hardware	2	4
	R015	Data server that is often down	4	4
	R016	Data loss	1	4
	R017	Overheat	4	1

	R018	Trouble Backup	1	2
	R019	System error	3	4
	R020	Powerless	3	3

In table 6, the value of each possible risk has been determined in the event frequency table and impact criteria table.

3.4 Risk Evaluation

In this step, risk evaluation is carried out, namely evaluating by assessing all possible risks that will be identified previously. So that through this analysis, the results will be grouped into a risk evaluation matrix according to 3 levels, namely low level, medium level, and high level.

Table 7. Matrix Risk Evaluation

Likelihood	Certain	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Possible	3	Low	Medium	Medium	Medium	High
	Unlikely	2	Low	Low	Medium	Medium	Medium
	rare	1	Low	Low	Low	Medium	Medium
	Impact		1	2	3	4	5
			Insignificant	Minor	Moderate	Major	Catastrophic

Furthermore, each identity of possible risks is entered into the risk assessment matrix according to the criteria for the frequency of events with the criteria for impact that have been previously identified.

Table 8. Risk Evaluation Matrix Based on Likelihood and Impact

Likelihood	Certain	5					
	Likely	4	R017	R012	R005	R013 R015	
	Possible	3			R020	R019	
	Unlikely	2	R010	R002 R006	R004	R014	

	rare	1		R007 R018	R008 R009 R011	R001 R016	R003
	Impact		1	2	3	4	5
			Insignificant	Minor	Moderate	Major	Catastrophic

In the next stage, the risk matrix is described into a table form that has been sorted according to the High, Medium, and Low-level levels.

Table 9. Grouping Risks by Tiers

ID	POSSIBLE RISK	Likelihood	Impact	Risk Level
R013	Bad network connection	4	4	High
R015	Data server that is often down	4	4	High
R001	Flood	1	4	Medium
R003	Earthquake	1	5	Medium
R004	Rain storm	2	3	Medium
R005	Human Error	4	3	Medium
R012	New employees who are still lay with system	4	2	Medium
R014	Breakdown hardware	2	4	Medium
R016	Data loss	1	4	Medium
R017	Overhead	4	1	Medium
R019	System error	3	4	Medium
R020	Powerless	3	3	Medium
R002	Fire	2	2	Low
R006	Abuse of access rights	2	2	Low
R007	Data theft and Leaks	1	2	Low
R008	Theft hardware	1	3	Low
R009	Hacking	1	3	Low
R010	User Interface that is difficult to understand	2	1	Low
R011	Damage to facilities	1	3	Low
R018	Touble Backup	1	2	Low

After analysis, 20 possible risks are generated and grouped according to the risk level. found several possible risks to be classified into risk levels that have a high

level, namely 2 potential risks, namely: R013 and R015. In addition, several risks are also classified into risk level levels that have a medium level of 10, namely: R001, R003, R004, R005, R012, R014, R016, R017, R020 and R019. Up to the potential risks that are classified at the level of risk levels with a low category there are 8, namely: R002, R006, R007, R008, R009, R010, R011, and R018.

3.5 Risk Treatment

Risk assessment is carried out, then the risk treatment stage is carried out. Where the purpose of this study will produce recommendations for risk actions that have been described in the table of proposed risk treatment in accordance with the level of risk.

Table 10. Proposed Risk Treatment

ID	POSSIBLE RISK	Risk Level	Risk Action
R013	Bad network connection	High	Changing the internet component with the new ISP (Internet Service Provider)
R015	Data server that is often down	High	Checking the database occasionally
R001	Flood	Medium	Placing non-waterproof infrastructure tools in a safe place
R003	Earthquake	Medium	Providing quality fire extinguishers
R004	Rainstorm	Medium	Reinforce walls and provide lightning rods
R005	Human Error	Medium	Conduct training and share knowledge with new users
R012	New employees who are still lay with system	Medium	Making appropriate SOP and conducting training and sharing knowledge to new employees
R014	Breakdown hardware	Medium	Setting up asset insurance for hardware
R016	Data loss	Medium	Do checking database and backup regularly
R017	Overhead	Medium	Provide air conditioning in the room
R019	System error	Medium	Perform system updates, antivirus, and perform system updates

R020	Powerless	Medium	Providing generators for companies
R002	Fire	Low	Provide a safe place for assets
R006	Abuse of access rights	Low	Provides access restrictions for each user and enforces a running time login system
R007	Data theft and Leaks	Low	Installing CCTV, and also installing several sensors in every corner of the room
R008	Theft hardware	Low	Installing CCTV, and also installing several sensors in every corner of the room
R009	Hacking	Low	Improve system security
R010	User Interface that is difficult to understand	Low	Changing the system display becomes simpler
R011	Damage to facilities	Low	Provide rules not to commit vandalism
R018	Touble Backup	Low	Perform periodic system backups

Table 10 produces risk treatment recommendations that can be applied to minimize the possibility of risk in ICS applications in BPS Semarang Regency.

4. CONCLUSION

The results of the SI / IT risk management research using ISO31000: 2018 on ICS applications in BPS Semarang Regency which were passed with risk assessment stages to the risk treatment stage which resulted in various recommendations for possible risks. By using ISO31000:2018, risk management in ICS applications at BPS Semarang Regency becomes structured, because with the principles contained in ISO31000: 2018, researchers can carry out risk analysis with stages that are in accordance with ISO guidelines. Based on the stages that have been carried out, 20 possible risks were obtained that could interfere with the performance of the ICS application and business processes in BPS Semarang Regency. In this case, 2 potential risks were obtained that have a high level which in the results have been stated that the network connection is poor, and the server down has a high level. In addition, in the second class, 10 potential risks were obtained that have a rare medium level which in the results have been mentioned, namely flooding, fire, lightning, human error, and several other potential risks that are available in the table. And, at the rare low level has 8 possible risks with which include earthquakes, abuse of access rights, data theft, hardware theft, hacking, elusive user

interfaces, vandalism, and trouble backups. It is hoped that the research can be used as a guideline for BPS Semarang Regency to minimize possible risks that can interfere with the performance of ICS applications and business processes contained in BPS Semarang Regency.

REFERENCES

[1] C. Fiarni, A. S. Harjanto, and Z. W. Muller, "Pengukuran Kinerja Proses Pengembangan Software Berbasis Kerangka Kerja Scrum Dengan Acuan Model CMMI-DEV 1.3," *Semin. Nas. Apl. Teknol. Inf.*, vol. 1, no. 1, pp. 26–32, 2014.

[2] Angraini and I. D. Pertiwi, "Analisa Pengelolaan Risiko Penerapan Teknologi Informasi Menggunakan ISO 31000," *J. Ilm. Rekayasa dan Manaj. Sist. Inf.*, vol. 3, no. 2, pp. 70–76, 2017, [Online]. Available: http://ejournal.uin-suska.ac.id/index.php/RMSI/article/view/4317.

[3] A. Menggunakan and F. Cobit, "TEKNOLOGI INFORMASI TERHADAP STRATEGI BISNIS (Studi Kasus PT . BRI , Tbk) Adityawarman Universitas Diponegoro ABSTRACT Strategic alignment between Information Technology (IT) and business has become CIOs and CEOs primary concern nowadays . This shows ," vol. 1, pp. 166–177.

[4] G. W. Lantang, A. D. Cahyono, and N. Ngalumsine, "Analisis Risiko Teknologi Informasi Pada Aplikasi Sap Di Pt Serasi Autoraya Menggunakan Iso 31000," *Sebatik 2621-069X*, vol. 23 No. 1, pp. 36–43, 2019, doi: 1410-3737.

[5] I. Lanin, "Standar Baru Manajemen Risiko ISO 31000:2018," *IBFG Institute*, 2018. https://ibfgi.com/risk-management-31000/ (accessed Apr. 12, 2018).

[6] S. Agustinus, A. Nugroho, and A. D. Cahyono, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 pada Program HRMS," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 1, no. 3, pp. 250–258, 2017, doi: 10.29207/resti.v1i3.94.

[7] F. L. Nice and R. V. Imbar, "Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000," *J. Inform. dan Sist. Inf.*, vol. 2, no. 2, pp. 1–11, 2017.

[8] M. Monica, didik Kurniawan, and R. Prabowo, "Analisis Manajemen Risiko Sistem Informasi Pengelolaaan Data English Proficiency Test (EPT) dan Portal Informasi di UPT Bahasa Universitas Lampung Menggunakan Metode ISO 31000," *J. Komputasi*, vol. 8, no. 1, pp. 83–90,

2020, doi: 10.23960/komputasi.v8i1.2351.

[9] F. M. Hutabarat and A. D. Manuputty, "Analisis Resiko Teknologi Informasi Aplikasi VCare PT Visionet Data Internasional Menggunakan ISO 31000," *J. Bina Komput.*, vol. 2, no. 1, pp. 52–65, 2020, doi: 10.33557/binakomputer.v2i1.792.

[10] C. A. Suprapto and S. Assegaff, "Analisis Dan Perancangan Knowledge Management System Pada Sma Negeri 6 Kota Jambi," *J. Manaj. Sist. Inf.*, vol. 3, no. 3, pp. 973–988, 2018.

[11] A. Novia Rilyani, Y. A. Firdaus W ST, and D. S. Dwi Jatmiko, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus : i-Gracias Telkom University) Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study : i-Gracias Telkom University)," *e-Proceeding Eng.*, vol. 2, no. 2, pp. 6201–6208, 2015.

[12] D. E. Adi and N. Susanto, "Analisis Manajemen Risiko Aktivitas Pengadaan pada Percetakan Surat Kabar," *J. Metris*, vol. 18, pp. 113–118, 2017.

[13] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," *J. Comput. Sci. Eng.*, vol. 1, no. 2, pp. 128–146, 2020, doi: 10.36596/jcse.v1i2.76.

[14] P. P. Thenu, A. F. Wijaya, and C. Rudianto, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan Cobit 5 (Studi Kasus: Pt Global Infotech)," *J. Bina Komput.*, vol. 2, no. 1, pp. 1–13, 2020, doi: 10.33557/binakomputer.v2i1.799.

[15] A. R. Tampubolon and Suhardi, "Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000 : 2009 Studi Kasus : Pembobolan ATM BCA Tahun 2010," *J. Telemat.*, vol. 7, no. 2, pp. 1–10, 2011.

[16] 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.

[17] N. M. Sirait and A. Susanty, "Analisis Risiko Operasional Berdasarkan Pendekatan Enterprise Risk Management (Erm) Pada Perusahaan," *Ind. Eng. Online J.*, vol. 5, no. 2012, p. 4, 2016.