Journal of Information Systems and Informatics
Vol. 4, No. 1, March 2022 e-ISSN: **2656-4882** p-ISSN: **2656-5935**
http://journal-isi.org/index.php/isi Published By DRPM-UBD

Information Technology Asset Security Risk Management at the Secretariat of the Salatiga City DPRD Using ISO 31000

Margaretha Ayuningtyas[1], Penidas Fiodinggo Tanaem[2]

[1,2]Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Salatiga, Indonesia
Email: [1]682018112@student.uksw.edu, [2]penidas.fiodinggo@uksw.edu

Abstract

The lack of resources that have an information technology background in handling information technology asset security risks makes it asset management in the Secretariat of the Salatiga City DPRD less optimal. The application of risk management is very necessary, especially in the security of information technology assets in agencies because it can help all existing business process activities in agencies so that they can run well. For this reason, it is necessary to implement information technology asset security risk management using ISO 31000 in these agencies. By implementing the ISO 31000 framework at the Secretariat of the Dprd Kota Salatiga can assist agencies in achieving goals, making decisions, improving performance, and effectively allocating and using resources for risk management. The purpose of this study is to identify, analyze, and handle information technology security risks that exist in the Secretariat of the Salatiga City DPRD. The method used by this research is a qualitative approach, namely case study. The result of this study is that there are 20 possible risks that can interfere with business processes in the Secretariat of the Salatiga City DPRD, including 3 possible high-level risks, 12 possible medium-level risks, and 5 possible low-level risks.

Keywords: IT Asset Security, ISO 31000, Risk Management, Risk Assessment

1. INTRODUCTION

The use of information technology in a government agency is an important thing and cannot be separated from its business processes. However, in the use of information technology will pose risks that can interfere with the course of business processes. Therefore, a careful planning is also needed so that the vision and mission of the agency can be carried out properly and optimally. The security aspect is very important. This is a very important asset that also needs to be maintained and protected properly, so that business processes can run well. Information security must achieve three main objectives, namely aspects of information confidentiality, integrity, and availability of information, and prevent events such as damage, loss, and even personal information from being passed on to irresponsible people. [1].

Risk is the possibility of an event that can cause harm to the company or agency [2]. Risk management is the process of identifying risks, analyzing risks, and evaluating risks. Risk management aims to manage risk and provide recommendations on how to handle risk to achieve optimal results[3]. The risk management process also helps to make better decisions and improve efficiency [4]. With the existence of risk management can minimize the occurrence of risks that can have a big impact on agencies. In a government agency, many important documents must be stored in the system and recover regularly so that they are maintained security and there is no damage or data loss. Therefore, a government agency also needs to create risk management to analyze future possibilities.

The Secretariat of the Regional People's Representative Council (DPRD) of Salatiga City, Central Java Province located on Jalan Letjend Sukowati No. 51 is a regional people's representative institution, which is placed as a component of the local government agency agency responsible for carrying out the functions of carrying out the functions of the DPRD, namely the functions of legislation, budget, and supervision. Based on interviews conducted with the head of the trial, minutes, and publications, Mr. Aris Diyanto, S.H., M.H. showed that the problem of IT implementation at the Secretariat of the Salatiga City DPRD is that some resources do not have an information technology background to cause a lack of understanding in the use of information technology and how to handle in case of incidents of damage to information technology assets in the agency. However, the management of IT infrastructure, the Secretariat of the Salatiga City DPRD has met IT security standards and has a structured policy regarding special treatment in the management of IT assets, but this has not been fully achieved optimally. Information technology assets are an important part of an agency. If IT assets get threats and attacks from inside and outside, it can pose a great risk in the government agency itself and can interfere with ongoing business processes and can even be stopped. Therefore, the importance of risk management in handling, controlling, and protecting IT assets by conducting risk assessments to monitor risks, handle risks, and minimize risks that may occur in the Secretariat of the Salatiga City DPRD in the future.

Based on the description above, the problem studied in this study is how to identify and manage the risks that exist in the Secretariat of the Salatiga City DPRD. To find out the value of risk on information technology assets in the Secretariat of the Dprd of Salatiga City, ISO 31000 is used. By implementing the ISO 31000 framework at the Secretariat of the Dprd Kota Salatiga can assist agencies in achieving goals, making decisions, improving performance, and effectively allocating and using resources for risk management. Iso 31000 risk management standard or guideline consists of three components, namely principles, frameworks, and processes [5]. The principles of risk management are the philosophy of risk management, but the framework is a structured and systematic risk management system and process, and in the process, risk management activities and interconnected sequentially [6]. One of the things that sets ISO 31000 apart from other risk management standards is a broader conceptual perspective than other standards. This is demonstrated by the existence of a risk management framework known as "Plan-Do-Check-Action" which presents the application of quality control principles [7]. The purpose of this study is: (1) identify and manage information technology security risks that exist in the Secretariat of the Salatiga City DPRD, (2) know the level of risk to the security of information technology assets, and (3) mitigate risks that occur in the Secretariat of the Salatiga City DPRD.

In previous research related to the ISO 31000 standard entitled "Information Technology Risk Analysis Using ISO 31000 in the HRMS Program" in 2017. This research involves Risk Assessment for assets around the company, particularly in the HRMS program. In this study there are 2 possible risks that are high risk, 18 possible risks with moderate risk that can hinder the company's performance, and 6 possible risks with low risk [8]. Other research related to ISO 31000 was conducted at the Communication, Informatics, Persandian and Statistics Office (DISKOMINFOPS) indragiri Hilir Regency, Tembalang City, Riau Province. The study used ISO 31000:2018 guidelines in establishing a risk management system for the security of IT assets at the agency. In this study, 45 risks were identified, including 14 low-level risks, 16 moderate risks, and 15 high-risk [9].

Further research on Information Technology Risk Analysis Using ISO 31000 (Case Study: Sales System of PT Matahari Departement Store Malang Town Square Branch). Based on the results of this research analysis, there are appropriate risk management recommendations, namely reducing the risk of human error (error in system operation), avoiding the risk of password authentication, and reducing the risk of unstable connections [7]. In addition to the above research, the research using ISO 31000 is Risk Management Analysis Using ISO 31000 on Smart Canteen SMA XYZ. The results of the study obtained from the risk assessment process using matrix tables resulted in 1 extreme risk, 2 high risk, 4 medium risk, and 5 low risks. This research is expected to reduce the risk that occurs in Smart Canteen SMA XYZ [10]. Referring to previous studies, this study will apply information technology asset security risk management at the Secretariat of the Salatiga City DPRD using the ISO 31000 standard. It is hoped that this research can help the Secretariat of the Salatiga City DPRD in achieving goals, improving risk management, improving performance, and allocating and using resources in handling risks effectively.

2. METHOD

Research conducted at the Secretariat of the Salatiga City DPRD on the risk management of information technology asset security using a qualitative approach, namely case study, which focuses on one research object. The data collection used is primary data by making observations directly to the agency and conducting interviews with employees of the relevant agencies. By conducting observations and interviews, researchers obtain data on existing issues and conduct risk assessments for the security of information technology assets in these agencies. In addition to using primary data, the author in conducting research management using secondary data is by obtaining data indirectly in the form of literature.

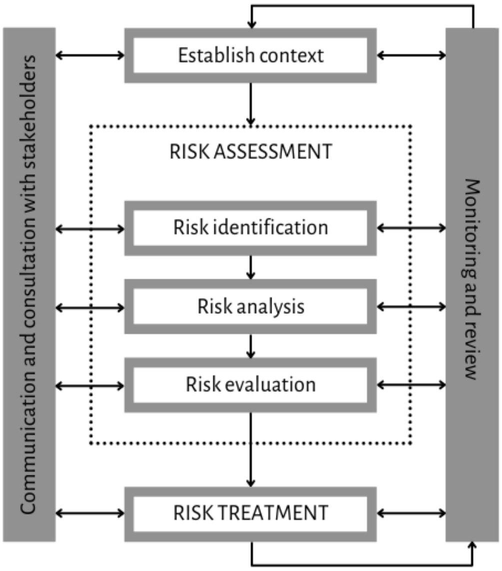

Figure 1. Risk Management Process

In addition to using data collection techniques, another method used is the risk management analysis method that refers to ISO 31000. In figure 1 there are several stages of risk management:

1) Risk Assessment
   Is an assessment of possible risks that can threaten the achievement of the intentions and objectives of the Secretariat of the Salatiga City DPRD. In the risk assessment there are 3 (three) processes including:
   a. Risk Identification
      It is the process of studying, identifying and recording risks. It aims to find out the risks that can affect the purpose of the agency.
   b. Risk Analyst
      It is a process of determining the level of potential that arises and can be prioritized properly later when implementing a risk management plan [11].
   c. Risk Evaluation

Risk evaluation is carried out to compare the results of risk analysis with established risk criteria. The goal is to find out the severity of the risk that must be followed up.

2) Risk Treatment

At this stage the researcher makes recommendations or actions on risks that may occur with the aim to manage the risk or minimize the existing risk [12]. The 4 (four) categories of risk treatment include [13]:

a. Risk Avoidance
Used to avoid conditions that can cause a risk.
b. Risk Reduction
Used to reduce the potential or impact of risk.
c. Risk Acceptance
Acceptable, that is, fully responsible for the risks arising.
d. Risk Sharing
Used to shift risk to other options to reduce the impact of risk.

3) Communication and Consultation with Stakeholders

It is an interactive process in terms of exchanging information and opinions aimed at helping stakeholders understand risks, as a basis for decision-making [14].

4) Monitoring and Review

It aims to ensure that the implementation of risk management runs according to plan and as a basis for making periodic improvements to the risk management process [15].

3. RESULT AND DICUSSION

3.1 Risk Assessment

This stage is a risk assessment stage at the Secretariat of the Salatiga City DPRD. There are 3 (three) stages in the risk assessment process, namely risk identification, risk analysis, and risk evaluation.

1) Risk Identification

In this risk identification stage, it aims to identify possibilities - possible risks that occur in the future obtained through the interview process at the Secretariat of the Salatiga City DPRD. Some possible risks and their impacts can be seen in Table 1 below.

Table 1. Risk Identification

ID	LIKELIHOOD	IMPACT
R001	Data loss	1. Loss of employee data

		2. Loss of annual performance plan data
R002	Kebocoran data	Loss of important agency data
R003	Human Error	Work processes are hampered
R004	Unstable network connection	1. Communication hampered 2. The process of sending and receiving files becomes hampered
R005	Server down	1. Inhibition of ongoing business processes 2. Existing apps are not working properly
R006	Damage to hardware	1. Reduce the number of agency assets 2. Hinder employee performance
R007	Data backup failure	Data loss
R008	Virus attack	Data yang ada menjadi hilang
R009	Unscheduled maintenance	1. The cessation of business processes 2. Delay in sending documents
R010	Abuse of access rights	Agency data leak
R011	Overload	Server performance becomes hampered
R012	Overheat	Running application software becomes slow
R013	Web service dies suddenly	Data loss
R014	Electrical interference	Disrupting the course of business processes
R015	Fire	1. Damage to agency facilities 2. Material loss 3. Inhibiting agency activities
R016	Flood	1. Damage to agency facilities 2. Material loss 3. Inhibiting agency activities
R017	Earthquake	Disrupting the course of business processes
R018	Data corrupt	Program inaccessible
R019	CCTV is not working properly.	Reduced level of security
R020	Generators don't work properly	Inhibiting agency activities

2) Risk Analysis

After identifying the risk, the next stage is risk analysis to conduct an assessment of the identified risks. This risk assessment is obtained from the possibility of risk (likelihood) and the impact of the occurrence of risk (impact) in Table 2 for likelihood value and Table 3 for impact value.

Table 2. Likelihood Value

VALUE	CRITERION	DESCRIPTION	FREQUENCY PER EVENT
1	Rare	Risk almost never occurs	> 5 years
2	Unlikely	Risk is rare	2 - 5 years
3	Possible	Risk sometimes occurs	1 - 2 years
4	Likely	The risk is happening	7 - 12 month
5	Certain	Risks often occur	1 - 6 month

Table 3. Impact Value

NILAI	KRITERIA	DESKRIPSI
1	Insignificant	Risk does not interfere with business processes
2	Minor	Risk slightly disrupting business processes
3	Moderate	Risk of disrupting business processes
4	High	The risk of disrupting business processes that can lead to losses
5	Major	A very fatal risk and interferes with the entire business process

After conducting a risk assessment on the possibility of risk (likelihood) in Table 2 and the impact of risk (impact) in Table 3, then assess the possibilities - possible risks to information technology assets in the Secretariat of the Salatiga City DPRD that have been identified along with likelihood and impact assessments . Assessment of possibilities - possible risks can be seen in Table 4.

Table 4. Risk Analysis

ID	KEMUNGKINAN	LIKELIHOOD	IMPACT
R001	Data loss	3	3
R002	Data leak	2	4
R003	Human error	3	3
R004	Unstable network connection	4	3
R005	Server down	2	4
R006	Damage to hardware	5	2
R007	Data backup failure	3	4
R008	Serangan virus	3	3
R009	Unscheduled maintenance	4	4
R010	Abuse of access rights	2	2
R011	Overload	3	3
R012	Overheat	2	2
R013	Web service dies suddenly	2	2
R014	Electrical interference	3	3
R015	Fire	1	5
R016	Flood	1	4
R017	Earthquake	2	2

R018	Data corrupt	2	3
R019	CCTV is not working properly.	2	1
R020	Generators don't work properly	3	3

After conducting a risk analysis through the likelihood table, it can be concluded that in the rare criteria (almost never occurs) there are 2 possible risks that occur, namely in fires and floods. In the unlikely criteria (rarely) there are 8 possible risks that occur, namely data leakage, server down, misuse of access rights, overheating, web services die suddenly, earthquakes, corrupt data, and CCTV does not work properly. In the criteria possible (sometimes occurs) there are 7 possible risks that occur, namely data loss, human error, data backup failure, virus attacks, overload, electrical disturbances, and generators do not function properly. In the likely criteria (often occurs) there are 2 possible risks that occur, namely unstable network connections, unscheduled maintenance, and flooding. In certain criteria (definitely occur) there is 1 possible risk that occurs, namely damage to hardware.

The results of the risk analysis of the impact table (impact) get the result that the insignificant impact there is 1 possible risk that is, CCTV does not function properly. Minor impacts there are 5 possible risks, namely, damage to hardware, misuse of access rights, overheating, web service dies suddenly, and earthquakes. Moderate impact there are 8 possible risks, namely, data loss, human error, unstable connections, virus attacks, overload, electrical interference, corrupt data, and generators do not work properly. High impact there are 5 possible risks, namely, data leakage, server down, data backup failure, and unscheduled maintenance. Major impacts there are 1 possible risk, namely, fire.

3) Risk Evaluation

After conducting a risk analysis, the next stage is a risk evaluation which is used to see the level of risk or risk impact that occurs from the highest level of risk to the lowest. At this stage of risk evaluation, it will be inserted into the matrix based on the likelihood and impact contained in Table 5.

Tabel 5. Matrix Evaluasi Risiko

LIKELIHO	Certain	5	Moderate	Moderate	High	High	High
	Likely	4	Low	Moderate	High	High	High
	Possible	3	Low	Low	Moderate	High	High
	Unlikely	2	Low	Low	Moderate	Moderate	High
	Rare	1	Low	Low	Low	Moderate	Moderate

O **D**			🟩	🟩	🟩	🟨	🟨
IMPACT			1	2	3	4	5
			Insignificant	Minor	Moderate	High	Major

The Risk Evaluation Matrix is a matrix used in risk assessment to determine the level of risk by considering the possibility or probability of severity of consequences or risk impacts aimed at increasing risk visibility and to assist agencies in the process of taking center. The risk evaluation matrix has 3 parts of which:

1) Low, usually depicted in green indicates that an event does not cause high risk and the risk is negligible.
2) Moderate, usually depicted in yellow indicates that an event requires special attention to reduce its severity.
3) High, usually depicted in red which indicates that an event is dangerous and must be addressed immediately

Table 6. Matrix Risk Evaluation Based on Likelihood and Impact

L I K E L I H O O D	Certain	5	🟨	🟨 R006	🟥	🟥	🟥
	Likely	4	🟩	🟨	🟥 R004	🟥 R009	🟥
	Possible	3	🟩	🟩	🟨 R001 R003 R008 R011 R014 R020	🟥 R007	🟥
	Unlikely	2	🟩 R019	🟩 R010 R012 R013 R017	🟨 R018	🟨 R002 R005	🟥
	Rare	1	🟩	🟩	🟩	🟨 R016	🟨 R015
IMPACT			1	2	3	4	5
			Insignificant	Minor	Moderate	High	Major

In Table 6, mapping the possible risks and impacts of risk in one matrix is by entering the risk ID into the matrix box. The trick is to multiply 2 numbers (1 likelihood number and 1 impact number). The value of each risk can be seen from Table 4. Risk Analysis. After the results are found, then the risk is seen to enter the low, moderate, or high category and it is also seen that the risk of entering into which criteria is appropriate.

Table 7. Risk Grouping by Level

ID	LIKELIHOOD	LIKELIHOOD	IMPACT	LEVEL
R004	Unstable network connection	4	3	High
R007	Data backup failure	3	4	High
R009	Unscheduled maintenance	4	4	High
R001	Data loss	3	3	Moderate
R002	Data leak	2	4	Moderate
R003	Human error	3	3	Moderate
R005	Server down	2	4	Moderate
R006	Damage to hardware	5	2	Moderate
R008	Virus attack	3	3	Moderate
R011	Overload	3	3	Moderate
R014	Electrical interference	3	3	Moderate
R015	Fire	1	5	Moderate
R016	Flood	1	4	Moderate
R018	Data corrupt	2	3	Moderate
R020	Generators don't work properly	3	3	Moderate
R010	Abuse of access rights	2	2	Low
R012	Overheat	2	2	Low
R013	Web service dies suddenly	2	2	Low
R017	Earthquake	2	2	Low
R019	CCTV is not working properly.	2	1	Low

After mapping the possible risks and impacts of risks in the matrix, the next stage is grouping risks based on their level to see the handling of risks that are a priority. In the table of 7 stages of the risk evaluation process above, there are 22 possible risks that have been analyzed and grouped based on the risk level. There are 3 possible risks that are categorized into high-level risk levels, namely R004, R007, and R009. There are 12 possible risks categorized into medium-level risk levels, namely R001, R002, R003, R005, R006, R008, R011, R014, R015, R016, R018, and R020. And there are 5 possible risks that are categorized into low-level risk levels, namely R010, R012, R013, R017, and R019. The higher the likelihood and severity of the risk, the higher the strategy for handling.

3.2 Risk Treatment

After conducting the risk evaluation process, the next stage that will be carried out is the risk treatment stage. In this stage will provide actions in the form of a review of the treatment in dealing with risks that have been grouped based on the level of risk in table 7. In table 8, it is expected to minimize the risks that will occur in the Secretariat of the Salatiga City DPRD.

Table 8. Proposed Risk Treatment

ID	KEMUNGKINAN	LEVEL	TINDAKAN RISIKO	KATEGORI
R004	Unstable network connection	High	1. Notify the operator if there is a network problem so that it can be fixed immediately 2. Replacing a better ISP (Internet Service Provider)	Risk Reduction
R007	Kegagalan backup data	High	1. Perform data backups periodically 2. Always pay attention to storage memory usage	Risk Avoidance
R009	Maintenance tidak terjadwal	High	Arrange maintenance schedules regularly 1. There is a maintenance notice before maintenance is carried out, preferably 60 minutes before maintenance begins	Risk Reduction
R001	Kehilangan data	Moderate	Every important data is given a password Monitoring via CCTV 1. Perform data backups periodically	Risk Avoidance
R002	Kebocoran data	Moderate	Encrypt data	Risk Avoidance
R003	Human error	Moderate	1. Conduct training to human resources regarding the use of technology 2. Divide tasks according to everyone's abilities	Risk Reduction
R005	Server down	Moderate	1. Monitoring data center 2. Perform server maintenance regularly	Risk Reduction
R006	Kerusakan pada hardware	Moderate	Give responsibility to each user to always use hardware in accordance with existing procedures	Risk Acceptance

R008	Serangan virus	Moderate	1. Using antivirus 2. Perform data backups periodically	Risk Sharing
R011	Overload	Moderate	1. Server monitoring 2. Optimizing the database	Risk Reduction
R014	Gangguan listrik	Moderate	Provides an automatic generator set	Risk Sharing
R015	Kebakaran	Moderate	Menyediakan alarm dan alat pemadam pembakaran	Risk Sharing
R016	Banjir	Moderate	1. Putting critical infrastructure and data tools in a flood safe place 2. Periodic checking and cleaning of waterways	Risk Reduction
R018	Data corrupt	Moderate	1. Perform data backups periodically 2. Using antivirus 3. Clean up on the PC periodically to avoid viruses and cause corrupt data	Risk Avoidance
R020	Genset tidak berfungsi dengan baik	Moderate	Perform maintenance regularly	Risk Reduction
R010	Penyalahgunaan hak akses	Low	1. Set access limits for each device 2. Change passwords periodically	Risk Avoidance
R012	Overheat	Low	1. Put hardware as recommended 2. Add fans on each hardware	Risk Reduction
R013	Web service mati tiba - tiba	Low	There is a maintenance notification before maintenance is carried out, preferably 60 minutes before maintenance starts so that the data that is being input is not lost	Risk Reduction
R017	Gempa bumi	Low	Provide a safe enough place to place important devices and data	Risk Sharing

R019	CCTV tidak berfungsi dengan baik	Low	Perform maintenance regularly	Risk Reduction

From the results of risk treatment, there are 5 possible risks that fall into the risk avoidance category, namely R001, R002, R007, R010, and R018. There are 10 possible risks that fall into the risk reduction category, namely R003, R004, R005, R009, R011, R012, R013, R016, R019, and R020. There is one possible risk that falls into the category of risk acceptance, namely R006. There are 4 possible risks that fall into the risk sharing category, namely R008, R014, R015, and R017.

4. CONCLUSSION

Based on research conducted at the Secretariat of the Salatiga City DPRD on information technology asset security risk management using the ISO 31000 standard, it was carried out in several stages, including risk identification, risk analysis, risk evaluation to risk treatment. From these various stages, this risk analysis identified 20 possible risks that could interfere with business processes in the Secretariat of the Salatiga City DPRD. There are 3 possible high-level risks, 12 possible medium-level risks, and 5 possible low-level risks.

Then it can be concluded that the Secretariat of the Salatiga City DPRD must have resources that have an information technology background, especially in handling information technology asset security risks effectively. With this can minimize the possibility of risks that occur in the future, because if there are no resources that understand the handling of the security risks of information technology assets and a system, server, and network experiencing disruptions, then all business processes that are running will become hampered and have a bad impact on the agency. Especially in the possibility of high-level risk (high level) which should be of particular concern in these government agencies. With this research, it is expected that it is expected that it asset management will be more optimal so that it can improve the performance of agencies.

REFERENCES

[1] E. Purwanto, "Keamanan Informasi," www.bpptik.kominfo.go.id, 2014. https://bpptik.kominfo.go.id/2014/03/24/404/keamanan-informasi/.

[2] J. Ecleas, "Analisis Manajemen Risiko Teknologi Informasi Software PEGA Menggunakan ISO 31000," JATISI (Jurnal Tek. Inform. dan Sist. Informasi), vol. 8, no. 1, pp. 209–224, 2021, doi: 10.35957/jatisi.v8i1.601.

[3] R. V. I. Francisca Lady Nice, "Analisis Risiko Teknologi Informasi pada Lembaga Penerbangan dan Antariksa Nasional (LAPAN) pada Website SWIFTS Menggunakan ISO 31000," Juisi, vol. 2, no. 2, pp. 1689–1699, 2016.

[4] G. Mochammad Husein and R. V. Imbar, "Analisis Manajemen Risiko

Teknologi Informasi Penerapan Pada Document Management System di PT. JABAR TELEMATIKA (JATEL)," J. Tek. Inform. dan Sist. Inf., vol. 1, no. 2, pp. 75–87, 2015, doi: 10.28932/jutisi.v1i2.368.

[5] Y. N. Qintharah, "Perancangan Penerapan Manajemen Risiko," JRAK J. Ris. Akunt. dan Komputerisasi Akunt., vol. 10, no. 1, pp. 67–86, 2019, doi: 10.33558/jrak.v10i1.1645.

[6] K. B. Mahardika, A. F. Wijaya, and A. D. Cahyono, "Manajemen Risiko Teknologi Informasi Menggunakan Iso 31000 : 2018 (Studi Kasus: Cv. Xy)," Sebatik, vol. 23, no. 1, pp. 277–284, 2019, doi: 10.46984/sebatik.v23i1.572.

[7] H. T. I. Driantami, Suprapto, and A. R. Perdanakusuma, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)," J. Pengemb. Teknol. Inf. dan Ilmu Komput., vol. 2, no. 11, pp. 4991–4998, 2018.

[8] 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.

[9] R. M. Candra, Y. N. Sari, I. Iskandar, and F. Yanto, "Sistem Manajamen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000 : 2018," J. CoreIT, vol. 5, no. 1, pp. 19–28, 2019.

[10] 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.

[11] B. Wijayantini, "Model Pendekatan Manajemen Risiko," Jeam, vol. XI, no. 2, pp. 57–64, 2012.

[12] R. H. Pangestu, A. D. Cahyono, and P. F. Tanaem, "Analisis Manajemen Resiko Aplikasi SIPP di Pengadilan Negeri Salatiga Kelas 1B Mengunakan ISO 31000," J. Comput. Inf. Syst. Ampera, vol. 2, no. 1, pp. 43–57, 2021, doi: 10.51519/journalcisa.v2i1.59.

[13] L. D. Berliana and A. R. Tanamaah, "Analisis Risiko dengan Metode ISO 31000 pada Disperinnaker Kota Salatiga Bidang Industri," JATISI (Jurnal Tek. Inform. dan Sist. Informasi), vol. 8, no. 3, pp. 1105–1118, 2021, doi: 10.35957/jatisi.v8i3.1037.

[14] L. Mahadewi, "Proses Manajemen Risiko," https://swa.co.id/swa/my-article/proses-manajemen-risiko, 2017. https://swa.co.id/swa/my-article/proses-manajemen-risiko.

[15] Nabilatul Fanny and Anindiya Soviani, "Analisis Manajemen Risiko Di Ruang Filing RSUD dr Soediran Mangun Sumarso Wonogiri Tahun 2020," Infokes J. Ilm. Rekam Medis dan Inform. Kesehat., vol. 10, no. 2, pp. 12–19, 2020, doi: 10.47701/infokes.v10i2.1027.