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

Risk Analysis of Web-Based Information Systems on CV Mega Komputama Uses ISO 31000

Theodorus Fide Rahardian[1], Agustinus Fritz Wijaya [2]

[1,2]Fakultas Teknologi Informasi , Universitas Kristen Satya Wacana, Salatiga, Indonesia
Email: [1]682018165@student.uksw.edu, [2]agustinus.wijaya@uksw.edu

Abstract

CV. Mega Komputama Salatiga is a business engaged in sales that provides a variety of IT products and the CV has implemented the use of SI / IT in supporting business activities carried out. CV. Mega Komputama uses the website "megakomputama.com" to support product sales and marketing, product storefronts and interact with customers. But in the world of management, there must always be possible risks that can occur and can interfere with the business activities of users of the system. Therefore, the risk analysis of the information system includes the source of risk, possible risks, and the impact of risks on the CV website. Mega Komputama is indispensable. This study used the ISO 31000: 2018 framework with the hope of being able to identify and minimize the risks that may occur on the Mega Komputama website.

Keywords: ISO 31000, Risk Analysis, Risk Management

1. INTRODUCTION

In the era of revolution 4.0, the role of technology in human activities today is very large, therefore almost every organization or company pays attention to technological developments, especially information technology. The development of Information Technology (IT) from year to year is growing. Such developments are due to the increasing needs of the organization. Each component in information technology must be able to run well in accordance with their respective duties and functions so that it can help the organization carry out business processes and achieve the organization's vision and mission [1]. Information technology must be managed properly so that company goals can be achieved, and the company's business processes can run without IT problems that interfere with operational processes and even the company's business continuity.

The management of Information Systems or Information Technology in a business unit is indeed very important as well as CV. Mega Komputama Salatiga. CV. Mega Komputama is an official distributor that sells various IT products

such as laptops, cameras, PCs, Tablets, accessories, computers, and other official IT equipment which of course is equipped with an official warranty supported by the relevant vendor's service center. Mega Komputama has paid more attention to the importance of IT / SI as can be seen from the existence of the "megakoputama.com" Website. The website is presented to answer the IT needs of its customers easily, cheaply and under warranty. On the "megakomputama.com" website, there are various features that make it easier for customers to get the items they need such as WhatsApp contacts which are available on the website just by clicking on the Available WhatsApp logo. In addition, on the website there is a product storefront and an online catalog.

Information technology is indeed inseparable from the business processes of a company. However, various threats and risks to the system in carrying out business processes can interfere with and even paralyze the company's system activities so that the system cannot carry out its duties optimally [2]. These risks and threats can be faced by compiling good risk management or management as a consideration for the company to make appropriate decisions. Based on these problems, research is needed to document various kinds of possible risks and priorities for these risks to the company.

One risk that is quite often a concern is SI/IT Security. The security aspect is very important in information systems. This is a very important asset that must be considered and protected properly, to ensure the smooth running of the company's business. Currently, the rapid development of technology and the ease of use of technology will create opportunities for risks to information, which will affect the smooth running of the company's business. If in carrying out its business a Company does not maintain it properly in terms of its security, it will cause various problems that can affect the Company's business processes. On the other hand, the use of information technology can also have a negative impact on the company, this is what is called risk [3]. Risk management is to provide an overview of the risks that can arise from various factors that adversely affect the performance of the organization's information technology to stakeholders so that they can make decisions in anticipation of risks that may occur [1].

The use of information technology if it can be maximized will be a plus for the company, but still the technology applied in the company has its drawbacks. The shortcomings of information technology can pose possible threats and risks, these risks can of course interfere with the company's business. Not only information technology plays an important role in the running of a company but

it is necessary to have competent human resources (HR), the systems and infrastructure in the company must also be adequate [4]. The previous research was information technology risk analysis research using ISO 31000 in the ITOP application by Aprilia Rahmawati in 2019. Risk analysis in the study focuses on the open-source APPLICATION CMDB (Configuration Management Data Base) iTop which functions to connect the operational it processes of PT. ABCD. From the results of the research risk analysis, there are 21 possible risks that have the potential to interfere with the performance of the iTop application. There are 8 possible risks that are included in the medium level of risk and there are 17 possible risks that are included in the low level of risk [5].

The next Related Analysis Research is Information Technology Risk Management on the Ecofo Website Using ISO 31000 by Miftakhatun in 2020. This research uses the ISO 31000 method on the Ecofo website, where the process of implementing risk management is managed and monitored by the business division of KPH Banyumas Timur. The results of this study in the form of risk documentation were found, namely identified 24 possible risks where there are 3 high-level risks, 10 medium-level risks, and 11 low-level risks that can be used as a reference for prevention, handling and maintenance of information technology assets in the future [6]. Information Technology Risk Analysis research using ISO 31000 was also carried out by Augie David Manuputty and Sukma Arta Atmaja in 2020, the case study carried out was the AHO Office Application at PT. Source Alfaria Trijaya, Tbk (SAT). This study aims to determine and identify possible technology risks in AHO Office applications. The results of this study are that of the 19 risks associated with AHO Office application assets, there are 3 risks that have a level of risk with an extreme risk level, there are 7 risks with a moderate risk level, and there are 2 risks with a low risk level. These results are used as a tool for policymakers to develop documentation related to company risk management [4].

Based on these studies, there is a relationship with the research that will be carried out by the author, namely the risk analysis of the information system using ISO 31000 which aims to identify possible risks that arise, the impact of these risks, the level of risk, and risk treatment of possible risks that exist. The update in this study is that from the three previous studies all using the ISO 31000: 2009 Framework while in this study using the ISO 31000: 2018 framework. This research also focuses on medium-sized businesses, namely CVs. while the previous research focused on information technology owned by government agencies and large companies (PT). The research that the author will do is an analysis of information technology risks on a CV. Mega Komputama is

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

expected to be able to produce documentation of possible risks that can arise along with the level of impact of these risks on CV information technology. Mega Komputama and recommendations on risk treatment that can be done to minimize existing risks. With risk management, the risks that arise can be reduced in impact so that they are less detrimental and have a significant effect on the company [7].

2. METHODS

2.1. Research Method

This research is about risk management using the ISO 31000 framework. Framework ISO or International Organization for Standardization (ISO) 31000, is an international standard that applies risk management. The purpose of the ISO framework is to provide world-recognized risk management guidelines and principles[8]. Risk management is the process of identifying, analyzing, and evaluating risks that can help CV. Mega Komputama to manage risks on megakomputama.com websites. Risk is a potential danger that may arise from some application of the process at this time or some event in the future. Risk is the arbiter of uncertainty in a goal [9]. The security risk of information technology (IT) is an error that occurs in a process related to information resulting from several intentional or unintentional events that have a negative impact on the stage of processing information [10]. Usually, this risk will be contrary to the goals of the company or organization. ISO 31000:2018 is one of the guidelines for the application of risk which consists of three elements, namely the principle, framework, and process[11]. In this study, researchers used the Case Study Research method with a qualitative approach. With this method the researcher will be easy to obtain data and analyze the possible risks to the object of case study. The stages in this study will adjust to the stages of risk management in the ISO 31000: 2018 framework. The data used in this study is primary data related to the Mega Komputama website obtained through interviews with internal parties from CV. Mega Komputama.

2.2. Data Collection Method

The data collection method in this study was to use interview techniques with CV internal parties. Mega Komputama to process primary data in the form of all information related to the Mega Komputama website

2.3. Data Analysis Method

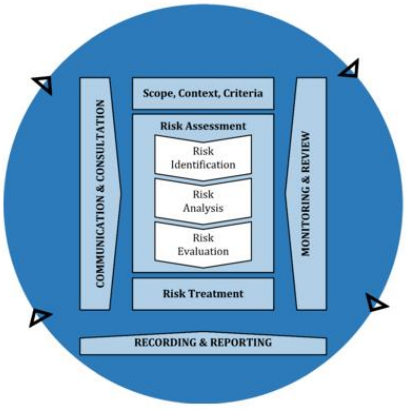

Figure 1. Data Analysis Methods [12]

The analysis method used in this study is in accordance with the stages of the ISO 31000: 2018 framework. The stages are as follows:

1. Communication & Consultation, the purpose of communication and consultation is to assist relevant stakeholders in understanding the risks, the basis for decision-making and the reasons why certain actions are necessary. Communication seeks to increase awareness and understanding of risks, whereas consultation involves obtaining feedback and information to support decision-making.
2. Scope, Context and Criteria, the purpose of setting the scope, context and criteria is to adjust the risk management process, allowing effective risk assessment and proper risk treatment. The scope, context and criteria involve the definition of the scope of the process, and the understanding of the external and internal context.
3. Risk Assessment, this stage aims to find out whether the Mega Komputama website has acceptable risks or not. In this stage, it is divided into several stages:
    a. Risk Identification, the purpose of risk identification is to find, recognize, and describe risks based on the information obtained. Relevant and appropriate information is important in identifying risks [13].
    b. Risk Analyst, the purpose of risk analysis is to understand the nature of the risk and its characteristics including, if appropriate, the level of risk. Risk analysis involves a detailed consideration of uncertainty, sources of risk, consequences, possibilities, events, scenarios, controls, and their effectiveness. An event can have many causes and consequences and can affect many goals [12].

c. Risk Evaluation, the purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of risk analysis with established risk criteria to determine where additional measures are needed [12].
d. Risk Treatment, the purpose of risk treatment is to select and implement options to deal with risks. Risk treatment involves the iterative process of:
   - formulate and select risk handling options.
   - planning and implementing risk treatment.
   - assess the effectiveness of that treatment.
   - decide whether the remaining risks are acceptable; (if unacceptable, take further care) [12].

4. Monitoring and Review, the purpose of monitoring and review is to ensure and improve the quality and effectiveness of process design, implementation, and results. Continuous monitoring and periodic review of the risk management process and its results should be a planned part of the risk management process, with clearly defined responsibilities [12].
5. Recording and Reporting, The risk management process and its results must be documented and reported through appropriate mechanisms [12].

3. RESULT AND DISCUSSION

3.1 Risk Assessment

This stage is the risk assessment stage on the CV Website. Mega Komputama Salatiga. In the risk assessment process of cv website. Mega Komputama consists of 3 stages, namely: Risk identification, risk analysis, and risk evaluation.

3.2 Risk Identification

3.2.1 Asset Identification

The first stage in risk assessment is the identification stage of assets related to the CV Website. Mega Komputama Salatiga, can be in the form of data, hardware, and software. To obtain data on assets related to the CV Website. Mega Komputama through interviews and observations. The process is carried out by means of an interview with cv employees. Mega Comutama part of The Administrator's Website. The following is a breakdown of assets related to the CV Website. Mega Komputama based on the results of interviews with speakers, can be seen in the table below:

Table 1. Asset Identification

Information System Components	Website Mega Komputama Assets
Data	Product Data, Article Data
Software	CMS : OpenCart Web Hosting : Rumahweb
Hardware	Laptop, Database server

From the results of interviews and observations to identify Mega Komputama's assets, three components of the information system were obtained that were used as a reference in risk management analysis. The first is a Data asset that contains product data and article data. The second is that software assets consist of CMS using OpenCart and Web Hosting using Rumahweb. The Opencart application is used to manage content on the website while Rumahweb is used to manage and run servers, secure the website, and ensure that data on the website can be opened through a browser by website visitors. And the third is assets in the form of Hardware, namely laptops and database servers.

3.2.2 Identify Possible Risks

The next step is to identify possible risks that can be a threat to the Mega Komputama Website. Possible risks can be grouped according to 3 factors namely, natural factors, human factors and system and infrastructure factors. What can be seen in the table below:

Table 2. Identify Possible Risks

Factors	ID	Possible Risk
Nature	R1	Earthquake
	R2	Volcano eruption
	R3	Lightning
	R4	Flood
	R5	Fire
Human	R6	Human Error
	R7	Data leak
	R8	Access abuse
	R9	User interface is difficult to understand
	R10	New employees who don't understand the system workflow
	R11	Device or data theft
	R12	Lack of quantity and quality of human resources
Systems and	R13	Server down

Infrastructure	R14	Overheat
	R15	Data corrupt
	R16	Power outage
	R17	Backup failure
	R18	Unstable network connection
	R19	Software error
	R20	Damage hardware

From the risk identification stage, 20 possible risks were found from three factors, namely natural factors, human factors and system and infrastructure factors.

3.2.3 Identify the Impact of Possible Risks

After knowing the identification of possible risks, the risk impact of possible risks is obtained as follows:

Table 3. Identify the Impact of Possible Risks

Factors	ID	Possible Risk	Impact
Nature	R1	Earthquake	Damage the infrastructure and business activities a halt
	R2	Volcano eruption	Damage the infrastructure and business activities a halt
	R3	Lightning	Damage the infrastructure and stalling the business activities
	R4	Flood	Damage the infrastructure and disrupt the business activities
	R5	Fire	Damage the infrastructure and business activities a halt
Human	R6	Human Error	The data entered on the website does not match
	R7	Data leak	Data can be misused by other parties
	R8	Acses abuse	Data can be deleted / changed by other parties
	R9	User interface is difficult to understand	Have the difficulty to operating the website
	R10	New employees who don't understand the system workflow	Difficulty on operating the system

	R11	Device or data theft	Data can be misused, financial loss
	R12	Lack of quantity and quality of human resources	There is no successor who understands the overall workflow of the website
Systems and Infrastructure	R13	Server down	Unable to access database and website
	R14	Overheat	Can damage hardware due to temperature rise
	R15	Data corrupt	User cannot see valid data
	R16	Power outage	The business activities have stopped
	R17	Backup failure	Can affect in data loss
	R18	Unstable network connection	Difficult to access the system
	R19	Software error	Difficult to access the system
	R20	Damage hardware	Difficult to access the system

3.2.4 Risk Analysis

The next stage is risk analysis. At this stage, an assessment of the possible risks that have been previously identified is carried out using the Likehood and Impact tables where there are 5 criteria each.

Tabel 4. Likehood Criteria

LIKEHOOD		DESCRIPTION	FREQUENCY
VALUE	**CRITERIA**		
1	**Rare**	Risk almost never occurs	>2 Years
2	**Unlikely**	Risk is rare	1-2 Years
3	**Possible**	Risk sometimes occurs	7-12 Month
4	**Likely**	Risk is happening	4-6 Month
5	**Certain**	Risk often occurs	1-3 Month

Then in table 5 below is a table of the value of the impact or impact that occurs from possible risks on the CV Website. Mega Komputama. In the table below, the impacts are grouped into 5 criteria ranging from the least disruptive impact to the most influential impact on all CV activities. Mega Komputama.

Tabel 5. Impact Criteria

Impact		Description
Value	**Criteria**	

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

After determining the value of the probability (likehood) and impact (impact), an assessment of the possible risks that are around the assets related to the CV Website can be carried out. Previously identified Mega Komputama. The results of the assessment of the possible risks can be seen in table 6.

Tabel 6. Assessment of Likehood and Impact

Factors	ID	Possible Risk	Likehood	Impact
Nature	R1	Earthquake	1	5
	R2	Volcano eruption	1	5
	R3	Lightning	2	3
	R4	Flood	1	2
	R5	Fire	2	5
Human	R6	Human Error	3	2
	R7	Data leak	1	2
	R8	Access abuse	2	2
	R9	User interface is difficult to understand	2	2
	R10	New employees who don't understand the system workflow	2	2
	R11	Device or data theft	1	1
	R12	Lack of quantity and quality of human resources	1	2
Systems and Infrastructure	R13	Server down	2	5
	R14	Overheat	3	3
	R15	Data corrupt	2	2
	R16	Power outage	5	4
	R17	Backup failure	2	2

	R18	Unstable network connection	5	3
	R19	Software error	4	3
	R20	Damage hardware	2	3

After conducting a risk management analysis through a table of possible risks, it can be concluded that in the criteria of rarely almost never happening there are 6 possible risks, namely earthquakes, volcanoes, floods, data leaks, theft of devices or data, lack of quantity and quality of human resources. In the criteria for possible risks, there are rarely 9 possible risks, namely lightning, fire, misuse of access, elusive user views, new employees who do not understand system workflows, server down, data corrupt, failed backups, hardware damage. In the criteria for possible risks that sometimes occur, there are 2 possible risks, namely human error, and overheating. In the criteria for possible risks, there is often 1 possible risk, namely software error. And in the criteria for possible risks, there are 2 possible risks, namely power outages, and bad networks.

The results of the risk analysis in the Impact table found that the impact did not interfere with there was 1 possible risk, namely theft of devices or data. As a result, business activities are slightly disrupted, there are 9 possible risks, namely flooding, human error, data leakage, misuse of access, elusive user views, new employees who do not understand system workflows, lack of quantity and quality of human resources, corrupt data, and failed backups. The impact results in disruption in business activities there are 5 possible risks, namely lightning, overheating, bad network, software errors, and hardware damage. The impact hampers all business activities there is 1 possible risk, namely a power outage. And the impact resulted in business activities stopped there are 4 possible risks, namely earthquakes, volcanoes, fires, and server downs.

3.3 Risk Evaluation

The next stage is the risk evaluation stage. Possible risks that have been previously identified and analyzed are included in the risk evaluation matrix based on the Criteria of Probability (Likehood) and Impact. The evaluation matrix is divided into 3 risk levels, namely: Low, Medium, and High.

1. Low, usually depicted in green indicating that the likelihood of such risk does not cause a high risk and the risk is negligible.

2. Medium, usually depicted in yellow indicating that the possible risk requires special attention to anticipate its severity.
3. High, usually depicted in red which indicates that the possible risk is dangerous and should be anticipated immediately.

Table 7. Risk Evaluation Matrix

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**
			Insigficant	Minor	Moderat	Major	Catastrophic

The next step is to include each identity of possible risks into the risk evaluation matrix according to the Likehood criteria and the Impact criteria based on the risk level from high, medium to low.

Table 8. Risk Evaluation Matrix Based on Likehood and Impact

Likelihood	Certain	**5**			R18	R16	
	Likely	**4**			R19		
	Possible	**3**		R6	R14		
	Unlikely	**2**		R8, R9, R10 R15, R17	R3, R20		R5, R13
	Rare	**1**	R11	R4, R7, R12			R1, R2
	Impact		**1**	**2**	**3**	**4**	**5**
			Insigficant	Minor	Moderat	Major	Catastrophic

Based on the Likehood and Impact criteria the possible risks can be categorized as in table 8. After entering the possible risks into the evaluation matrix based on Likehood and Impact, in the next stage, the 20 possible risks above are grouped into high, medium, and low levels.

Table 9. Grouping Risks by Tiers

ID	Possible Risk	Likehood	Impact	Risk Level
R16	Power outage	5	4	High
R18	Unstable network	5	3	High

	connection			
R1	Earthquake	1	5	Medium
R2	Volcano eruption	1	5	Medium
R3	Lightning	2	3	Medium
R5	Fire	2	5	Medium
R6	Human Error	3	2	Medium
R13	Server down	2	5	Medium
R14	Overheat	3	3	Medium
R19	Software error	4	3	Medium
R20	Damage hardware	2	3	Medium
R4	Flood	1	2	Low
R7	Data leak	1	2	Low
R8	Acses abuse	2	2	Low
R9	User interface is difficult to understand	2	2	Low
R10	New employees who don't understand the system workflow	2	2	Low
R11	Device or data theft	1	1	Low
R12	Lack of quantity and quality of human resources	1	2	Low
R15	Data corrupt	2	2	Low
R17	Backup failure	2	2	Low

In the risk evaluation stage, there are 20 possible risks that have been analyzed and grouped based on their risk level. There are 2 high risk levels, namely R16 and R18, 9 possible risks are included in the medium risk level, namely R1, R2, R3, R5, R6, R13, R14, R19, R20 and 9 possible low risk levels, namely R4, R7, R8, R9, R10, R11, R12, R15, R17. The higher the likelihood and severity, the higher the risk treatment required.

3.4 Risk Treatment

At the risk treatment stage, all possible risks are around the CV Website. Mega Komputama will be given proposals in treating it to minimize the possibility of losses and the emergence of these risks that make the CV Website. Mega Komputama can run optimally. Risk treatment proposals are prepared based on known risk levels, namely high to low levels.

ID	Possible Risk	Risk Level	Risk Treatment
R16	Power outage	High	Provide electric generator sets and prepare Uninterruptible Power Supply (UPS)
R18	Unstable network connection	High	Reducing traffic on the network or by changing the ISP (Internet Service Provider)
R1	Earthquake	Medium	Provide server backup in a safe place
R2	Volcano eruption	Medium	Provide server backup in a safe place
R3	Lightning	Medium	Installing lightning protection
R5	Fire	Medium	Provide fire extinguisher and server backup
R6	Human Error	Medium	Conduct the training for employees
R13	Server down	Medium	Perform periodic database checks
R14	Overheat	Medium	Reduce the intensity of hardware usage
R19	Software error	Medium	Perform periodic software and antivirus updates
R20	Damage hardware	Medium	Check and clean hardware regularly
R4	Flood	Low	Placing the device in a high or flood-safe place
R7	Data leak	Low	Change passwords and perform regular maintenance and provide double protection to the system
R8	Access abuse	Low	Provide user restrictions on each device and system
R9	User interface is difficult to understand	Low	Simplify the user interface to make it easier to understand, provide guidance on the use of the system
R10	New employees who don't understand the system workflow	Low	Provide standards in the process of recruiting new employees and providing guidance or training to new employees related to SOPs and system workflows.

R11	Device or data theft	Low	Install CCTV in all corners of the room, provide unique passwords and change passwords regularly.
R12	Lack of quantity /quality of human resources	Low	Provide standards on recruitment and conduct training or mentoring for new employees
R15	Data corrupt	Low	Perform regular backups and antivirus updates
R17	Backup failure	Low	Ensure device storage is not full.

4 CONCLUSSION

Based on SI / IT risk analysis research using ISO 31000: 2018 on cv website. Mega Komputama Salatiga starts from the stage of risk assessment, risk identification, risk analysis, risk evaluation to the stage of risk treatment. From these stages, the results of the analysis show that there are 20 possible risks that at any time can interfere with the performance of the Mega Komputama Website and interfere with the business processes contained in the CV. Mega Komputama Salatiga, 2 of them have a high risk level, namely power outages and poor networks, 9 possible risks have a medium risk level, namely earthquakes, volcanoes eruptions, lightning, fires, human error, server down, overheating, software errors, hardware damage. Then there are 9 possible risks with a low risk level which include flooding, data leakage, access abuse, elusive user views, new employees who do not understand system workflows, device or data theft, lack of quantity and quality of human resources, corrupted data, and failed backups. With this research, it can be used as a tool for CV parties. Mega Komputama in carrying out risk management and minimizing the possibility of risks that occur using proposed risk treatments such as conducting periodic maintenance, installing double protection on the system, providing electricity generators and others. Especially on the possibility of risk with a high-risk level so that business activities and CV websites. Mega Komputama is not disturbed.

REFERENCES

[1] N. V. Richardo and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi Pada Toko Surabaya Cabang Surakarta," J. Inf. Syst. Informatics, vol. 3, no. 1, pp. 13–30, 2021, doi: 10.33557/journalisi.v3i1.84.

[2] T. Ramdhany and R. A. Krisdiawan, "Analisis Risiko Sistem Informasi

Penjualan Berbasis Iso 31000 - Risk Management Di Pt. Remaja Rosdakarya," pp. 1–7, 2018, [Online]. Available: https://journal.uniku.ac.id/index.php/jejaring/article/view/1220.

[3] 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.

[4] S. A. Atmojo and A. D. Manuputty, "Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi AHO Office," JATISI (Jurnal Tek. Inform. dan Sist. Informasi), vol. 7, no. 3, pp. 546–558, 2020, doi: 10.35957/jatisi.v7i3.525.

[5] A. Rahmawati and A. F. Wijaya, "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi ITOP," J. SITECH Sist. Inf. dan Teknol., vol. 2, no. 1, pp. 13–20, 2019, doi: 10.24176/sitech.v2i1.3122.

[6] 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.

[7] L. Muniroh, Y. Rahayu, A. Sirojun, M. N. Rabbani, and E. Yusril, "Analisis Level Risiko Pada Garuda Jaya Garment Menggunakan Iso 31000," Manajerial J. Manaj. dan Sist. Inf., vol. 19, no. 1, pp. 13–23, 2020.

[8] D. Junianti and C. Fibriani, "Analisis Resiko Aplikasi Sistem Informasi Pengelolaan Data Umat Menggunakan ISO 31000 (Studi Kasus: Gereja Katolik Santo Paulus Miki Salatiga)," J. Comput. Inf. Syst. Ampera, vol. 2, no. 2, pp. 107–128, 2021, doi: 10.51519/journalcisa.v2i2.68.

[9] I. P. A. E. Pratama and M. T. S. Pratika, "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, 2020.

[10] H. I. Pribadi and E. Ernastuti, "Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000:2018 Dengan FMEA (Studi Kasus PT Pertamina)," J. Sist. Inf. Bisnis, vol. 10, no. 1, pp. 28–35, 2020, doi: 10.21456/vol10iss1pp28-35.

[11] K. B. Mahardika, A. F. Wijaya, and D. Cahyono, "Manajemen risiko teknologi informasi menggunakan iso 31000 : 2018 (studi kasus: cv. xy)," SEBATIK, vol. 2018, pp. 277–284, 2018.

[12] "ISO 31000:2018(en), Risk management — Guidelines." https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en.

[13] M. I. Fachrezi, "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan Iso 31000:2018 Diskominfo Kota Salatiga," JATISI (Jurnal Tek. Inform. dan Sist. Informasi), vol. 8, no. 2, pp. 764–773, 2021, doi: 10.35957/jatisi.v8i2.789.