IJEEMCS : International Journal of Electrical Engineering, Mathematics and Computer Science
Vol. 1, No.4 December 2024
e-ISSN: 3048-1945, p-ISSN : 3048-1910, Page 01-15
DOI: https://doi.org/10.62951/ijeemcs.v1i4.92
Available online at: https://international.arteii.or.id/index.php/IJEEMCS

Analysis Management Risk Technology Information on CV. Aren Jaya Use ISO 31000:2018

Muhamad Rizky [1*], Faaza Bil Amri [2]
[1,2] Sistem Informasi, Universitas Islam Negeri Syarif Hidayatulah, Indonesia
mr.rizkyy2019@gmail.com [1*], faaza.bilamri19@mhs.uinjkt.ac.id [2]

Address: Jl. Ir H. Juanda No.95, Ciputat, Kec. Ciputat Tim., Kota Tangerang Selatan, Banten 15412
Email correspondence: mr.rizkyy2019@gmail.com

Abstract. *CV. Aren Jaya is an AC service provider located in South Tangerang. In 2017 this shop began to develop by opening new and used AC sales services, AC installation services, used washing machine sales services and washing machine service services. In carrying out the company's business process activities, of course there will always be possible risks and potential risks that can threaten and disrupt business process activities. The need for a risk analysis of existing IS/IT resources in the company, using the ISO 31000:2018 method related to risk management. The purpose of this study is to minimize all possible risks that are currently being experienced or will also occur and provide appropriate recommendations regarding risks that may occur at any time. The research method used in the risk analysis uses the ISO 31000:2018 framework. The results of this risk analysis are in the form of an analysis of the possibility of existing risks, evaluations and risk mitigation plans so that they can produce improvements to existing risks. The final result of the research produces risk recommendations, so the company can adjust to the priorities of the existing risk level, so that it does not interfere with business activities at CV. Arena Jaya.*

Keywords: *Risk, Analysis, Management, ISO*

1. INTRODUCTION

Progress technology innovative the more push company For the more compete as well as develop. A good company That in field manufacturing and services so that Can compete and develop, can done with maintain quality product, do innovation in products and always guard satisfaction consumers. But the most important thing in success a company is own quality product. It is very possible happen if company do error Good from aspect design product until the production process. (AA Ulfa And T. Immawan, 2021).

Speak related business, of course No regardless and also faced with future risks faced. Risk This No only appear Because existence internal factors of the company, but also from factor external the company that sues company so that more care will risk those. Risks No only appear in companies big, but also risky appear in companies small. (D.Hendarwan, 2022).

Risk appear result in existence uncertainty. If the level uncertainty This high, then can impact negative on the company. Risk This Can interpreted as events that will happen faced by individuals and company as well as Can cause loss. For That required a efforts to be able to reduce or minimize possibility and consequence from a risk. (JO Yoewono And AH Prasetyo, 2022).

Received Oktober 20, 2024; Received Oktober 28, 2024; Accepted November 05 2024;
Online Available November 06 2024

Management risk become very crucial especially in conditions COVID-19 pandemic at the moment this. The COVID-19 pandemic can called as one of the example from *inherent risk* global scale and has give very big impact related aspects in life. Not only only on the aspect health but also spread most aspect others, such as economic, psychological, social, political and others. Under normal conditions only Lots company feel difficulty in manage the risks it has. Especially in conditions pandemic like moment this, company naturally have a distant challenge more large and required to be able to more be careful in face existing risks. (K. Vincent, 2021).

Every level in the company This responsible answer to management risk, starting from planning, supervision, and control to possible risks happens in the company. Management risk interpreted as a series from procedure and methodology used For identify, measure, monitor as well as control risks that arise from activity business. (AA Hapsari, 2018).

Founded on year 2016, CV Sugar Palm J aya Thisis a service AC service located Tangerang city South. On year 2017 shop This start develop by opening a new and used AC sales service, AC installation services, used washing machine sales services andservice service machine wash. In the year 2019 CV. Sugar Palm Jaya This open branch in Semarang area with services offered same as the one in the center. The development of information technology at this time at the company CV sugar palm Jaya Which has operate process his business with Good And balanced especially in the field of information technology that it has. CV sugar palm Jaya Already have your own website, the website you own functioning as a medium of information related services provided, photos activities and information For contact person For can use service. CV. Sugar Palm Jaya also always try For increase quality product as well as its services with do checking product, check condition service tools and also do maintenance system. However naturally Certain always There is possibility risk as well as potential risks that can occur threatening and disturbing business process activities. Of course need do analysis of potential risks up to the stage of risk management evaluation at CV. Sugar Palm Jaya by identifying assets and potential risks, risk analysis, and risk evaluation. Therefore, risk management is needed that is able to manage the company's IS/IT asset risks, using the ISO 31000:2018 method related to *risk management.* Where risk management is a management effort in preventing the risk of the company's operational activities by implementing evaluation, analysis, and risk mitigation plans.

A number of study previous related Usage ISO 31000:2018 in analysis management risk. Research using ISO 31000:2018, resulting in that This management, regardless of the

type of supervision carried out, is an element of the risk management framework and the principles of risk management are the basis of management operations. (J. Ząbek, 2018). Provision of resources and documentation of risk management are the most important management tasks related to risk management. Research using ISO 31000:2018, the results are show that OSRA-BN can help For support Lots from ISO 31000:2018 principles and models are very useful For analysis and evaluation risk as well as communication. (T. Parviainen, 2021).

Research using ISO 31000:2018, resulted in 2 possible low level risks, 11 possible risks with medium levels and 4 high-level risks. From these results, the DISKOMINFO of Salatiga City requires special attention related to frequent power outages, *server down,* frequent internet connection breaks, and lightning strikes. (MI Fachrezi, 2021). Research using ISO 31000:2018, the results of the study showed that there are *top five* risks that must be mitigated because they have high and medium risks, including: external risks, namely the number of business competitors, financial risks, namely unstable prices for equipment and materials, risks K3, namely the occurrence of work accidents, human resource risks, namely lack of personnel/workforce, and *technical risks,* namely work being hampered due to power outages.

Research using ISO 31000:2018, generates risk possibilities with various levels. It is concluded that IT CV. XY has not been able to meet the requirements of the ISO 31000:2018 standard, because from several stages of observation, interviews, and assessment of the risk itself, there are still many risk findings that have not been resolved by the company.

Research using the ISO31000:2018 framework, resulting in 23 possible risks in the PDS gold savings menu application. Of the 23 possible risks, there is one risk at a high risk level, namely data leakage, six risks at a medium level and 16 risks at a low level.

The purpose of this research is to minimize all possible risks that are currently being experienced or will occur and to provide appropriate recommendations for CV. Sugar Palm Jaya related to the risks that may occur at any time. This risk analysis is carried out using an approach using the ISO 31000:2018 method.

2. RESEARCH METHODS

Research Method

Method research in case management risk at CV. Sugar Palm Jaya done use framework ISO 31000:2018, Which where principle and These guidelines from ISO 31000 are suitable for used in risk management and is recognized internationally international. Risk management is a pattern of risk identification, risk analysis, to risk evaluation so that generate recommendations on risk management. In Figure 1 is method his research.

Stage First need Implemented Assessment Risk. Evaluation risk This done with use systematic method, so that it will produce results that can determine whether in on CV. Sugar Palm Jaya there are risks that are acceptable or not. Following This There are several stages of assessment risk, that is:

a. *Risk Identification* (Identification) Risk)

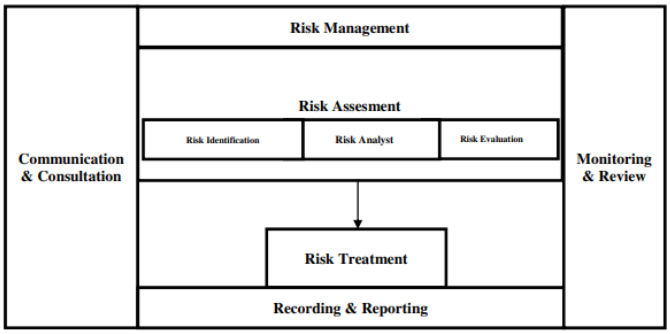
Efforts to gather useful information to find out what risks there are possibility appear in activities - activities operational Which done by company.

b. *Risk Analyst* (Analysis Risk)

Analysis risk This in the form of factors What just Which influence evaluation, characterization and management risk Which relate with infrastructure IS/IT in company.

c. *Risk Evaluation* (Evaluation Risk)

The last risk evaluation is the process of assessing risk, where the risk has between the lowest risk level to the highest risk level, an analysis will be carried out in the form of risk grouping according to risk level. The purpose of this risk evaluation is to obtain process risk taking based on results analysis risk. Which can to be continued with do *risk treatment* (risk treatment) will list one or more options to address the risk, so that it can be implemented Handling risk.



Picture 1. Method Study

Data Collection Methods

Data collection process, conducted by means of an interview with the owner of *CV.Aren Jaya*, the results of this interview are intended to be able to knowing IT assets, knowing constraints, and what are the ongoing problems at *CV.Aren Jaya*, so that can concluded How *risk treatment* Which appropriate And can used For minimize risk. In addition, observation method by researchers aims to find out directly what business processes are worth implementing in design system Which will be done. Next used literature study method through the official website *of CV.Aren Jaya* done by researchers who aims to add information What only those who haven't complete at stage interview about *CV. Aren Jaya.*

3. RESULTS AND DISCUSSION

Identification Risk

a. Asset Identification

At the stage This given a list of assets owned by CV. Aren Jaya from side technology information (IT) which got it from process interview Which done to party company. In table 1 is asset Which owned by CV. Aren Jaya in field IT:

Table 1. Identification of IT Assets CV. Aren Jaya

IS/IT Components	Asset
Data	Document important Company
Hadwarare	Computer
Software	Devices Supporter operational
Server	Server Database Server Web Service

b. Identification Possibility Risk

After identification assets on CV. Aren Jaya, step next done identification possibility risk. Done through grouping based on factors that emerge as in the factor nature, human resource factors, and factor systems and infrastructure. Identification possibility risk can seen in table 2.

Table 2. Identification Possibility Risk

ID	Factor	Risk
R001	Natural	Fire
R002		Natural disasters
R003		Dust / dirt
R004		Theft device
R005		Information accessed by unauthorized parties authorized

R006	Man	Data and information No in accordance fact
R007		Abuse right access /User ID
R008		Former user / employee Still own access information
R009		Data loss
R010		Human error
R011		Cybercrime and piracy
R012		Maintenance no scheduled
R013		Program documentation is not available complete
R014		Hardware failure / damage
R015		Server down
R016		Overheat
R017	Systems and Infrastructure	Connection network disconnected
R018		System crash
R019		Overcapacity
R020		Overload
R021		Datacorrupt
R022		Backup failure
R023		Not good quality network
R024		Technology using
R025		Power outage
R026		CCTV does not functioning with Good
R027		Generator is broken

c. Identification Impact Risk

After done stage identification risk, some possibility risk found from a number of factor like factor environment, nature, and systems and infrastructure that can potential threaten performance business, then the need done analysis the impact obtained from the risk that has been identified. In table 3 it can be seen identification impact the risks.

Table 3. Identification Impact Risk

Id	Risk	Impact
R001	Fire	Damage facilities and infrastructure company loss material hinder activity company
R002	Natural disasters	Damage facilities and infrastructure company
R003	Dust / dirt	Devices become fast hot
R004	Theft device	Loss financial
R005	Information accessed by unauthorized parties authorized	important data about a company that is spread out
R006	Data and information No in accordance fact	System become less valid
R007	Abuse right access /User ID	Leakage of company data

R008	Former user / employee Still own access information	Possibility corporate data leak
R009	Data loss	Loss of employee data and record keeping wages employee
R010	Human error	Cause accident work work process hampered
R011	Cybercrime and piracy	important data about the lost company
R012	Maintenance no scheduled	Weakening performance system
R013	Program documentation is not available complete	Become difficult when need information system
R014	Hardware failure / damage	Reduce amount asset company and reduce performance
R015	Server down	Inhibiting ongoing business processes walk in field marketing The applications contained within company be error / not can walk with Good
R016	Overheat	Application software in progress used become slow / error
R017	Connection network disconnected	Communication hampered marketing process decrease
R018	System crash	Existing SOPs No can walk with Good
R019	Overcapacity	System become lamb
R020	Overload	Impact on server performance which becomes slow
R021	Datacorrupt	The company is at a loss
R022	Backup failure	Absence data update lost previous data
R023	Not good quality network	Slowing down work processes in the company
R024	Technology using	Work process slow down company become difficult For developing and not follow trend
R025	Power outage	Loss operational company interfere with the work process of the server quality server menu
R026	CCTV does not functioning with Good	Monitoring work processes in the company become not enough effective decrease level security
R027	Generator is broken	Bother activity company

Analysis Risk

Stage This analysis process is carried out risk with method determine mark from possibilities the risks that have been identified at the stage previously. In this process use table criteria differentiated *likelihood* into five criteria from How many the amount possibility risks that occur during the period time certain. *Likelihood* Table Can seen in Table 4.

Table 4. Values on Likelihood [12]

Likelihood		Description	Frequency of Criteria Values Incident
Mark	Criteria		
1	Rare	Very rare risk happen	>2 years
2	Unlikely	Risk seldom happen	12 years old
3	Possible	Risk Enough often happen	7 - 12 months
4	Likely	Risk often happen	4 - 6 months
5	Certain	Risk always happen	1 - 6 months

Then implemented stage evaluation from impact or *impact* that occurs on the object case to possibility the risk that occurs. In the criteria evaluation impact This differentiated through how much big the impact that will caused For influence performance. The value of impact This Can seen in the table *impact* in Table 5.

Table 5. Impact Criteria Values [12]

Impact		Description
Mark	Criteria	
1	Insignificant	Risk No disturbing activities and business processes in the agency
2	Minor	Activities at the agency A little hampered, but No disturbing core activities in the agency
3	Moderate	Risk the disturbing the course of business processes in the agency, so that activity business A little hampered
4	Major	Risk the hinder almost all over the course of business processes in an agency
5	Catastrophic	Risk bother the course of existing business processes in a way comprehensive and stop activity agency in total

From the criteria *Likelihood* in table 4 and criteria *impact* on table 5. Next is give evaluation to possibility risk based on tables 4 and 5.

Table 6. Likelihood and Impact Assessment

Id	Risk	Likelihood	Impact
R001	Fire	1	5
R002	Natural disasters	1	5
R003	Dust / dirt	4	2
R004	Theft device	2	3
R005	Information accessed by unauthorized parties authorized	2	3
R006	Data and information No in accordance fact	3	4
R007	Abuse right access /User ID	2	3
R008	Former user / employee Still own access information	1	4
R009	Data loss	3	5
R010	Human error	4	5

R011	Cybercrime and piracy	1	5
R012	Maintenance no scheduled	3	5
R013	Program documentation is not available complete	4	4
R014	Hardware failure / damage	3	5
R015	Server down	2	5
R016	Overheat	2	4
R017	Connection network disconnected	4	5
R018	System crash	4	5
R019	Overcapacity	3	5
R020	Overload	3	5
R021	Datacorrupt	2	5
R022	Backup failure	3	5
R023	Not good quality network	4	4
R024	Technology using	4	2
R025	Power outage	4	5
R026	CCTV does not functioning with Good	2	4
R027	Generator is broken	1	4

From table 6 above, it was found values *likelihood* and *impact* to possibility the risks that have been identified. Until Then will found mark from *Likelihood* and *Impact*, after That done evaluation risk.

Evaluation Risk

Stage end is evaluation risk, namely conduct the evaluation process to all possibility the risk that was previously has done analysis from stages previously. Until Then produced analysis risk in order to be able to categorized as 3 risk levels namely : *Low, Medium, and High.*

Table 7. Evaluation Matrix Risk [15]

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
			Inspiring	Minor	Moderate	Major	Catastrophic

Ratio grouping based on risk level or risk level starts from the highest until lowest, thing the explained in table 7. So that later each Id from possibility risk will entered into the matics evaluation risk in accordance with criteria *Likelihood* and Impact criteria.

Table 8. Matrix Evaluation Risk Based on *Likelihood* And *Impact*

Likelihood							
	Certain	5					
	Likely	4		R003 R005 R024		R013 R023	R010 R017 R018 R025
	Possible	3				R006	R009 R012 R014 R019 R020 R022
	Unlikely	2			R004 R007	R016 R026	R015 R021
	rare	1				R008 R027	R001 R002 R011
		Impact	1	2	3	4	5
			Inspiring	Minor	Moderate	Major	Catastrophic

Table 8 yields calculation *Likelihood* and *Impact* there are 27 possibilities risks that can occur grouped with ratio. After that will grouped has adapt with level 27 possibilities risk the into the *high*, medium and *low* levels.

Table 9. Grouping Risk Based on Levels

ID	Risk	Likelihood	Impact	Risk Level
R001	Fire	1	5	Medium
R002	Natural disasters	1	5	Medium
R003	Dust / dirt	4	2	Medium
R004	Theft device	2	3	Medium
R005	Information accessed by unauthorized parties authorized	2	3	Medium
R006	Data and information No in accordance fact	3	4	Medium
R007	Abuse right access /User ID	2	3	Medium
R008	Former user / employee Still own access information	1	4	Medium
R009	Data loss	3	5	High
R010	Human error	4	5	High
R011	Cybercrime and piracy	1	5	Medium
R012	Maintenance no scheduled	3	5	High
R013	Program documentation is not available complete	4	4	High

R014	Hardware failure / damage	3	5	High
R015	Server down	2	5	Medium
R016	Overheat	2	4	Medium
R017	Connection network disconnected	4	5	High
R018	System crash	4	5	High
R019	Overcapacity	3	5	High
R020	Overload	3	5	High
R021	Datacorrupt	2	5	Medium
R022	Backup failure	3	5	High
R023	Not good quality network	4	4	High
R024	Technology using	4	2	Medium
R025	Power outage	4	5	High
R026	CCTV does not functioning with Good	2	4	Medium
R027	Generator is broken	1	4	Medium

Table 9 above, the sequence of risk evaluation, has 27 possible suspected risks that have been analyzed and categorized according to their risk levels. There are 12 risks with high levels, namely R013, R023, R010, R017, R018, R025, R009, R012, R014, R019, R020 R022. Then there are 15 risks with medium levels, namely: R003, R005, R024, R004, R007, R006, R016, R026, R008, R027, R015, R021, R001, R002, R011.

Treatment Risk

After analysis risk above, then to be continued with enter the stage *Risk Treatment* or treatment risk. In the stages This done giving proposal related action risk from risks that have been grouped based on the risk level of table 9.

Table 10. Proposal Treatment Risk

ID	Risk	Risk Level	
R001	Fire	Medium	Do provision tool fire extinguisher fire around building company and place part important.
R002	Disaster natural	Medium	Provide a safe place to be able to keep documents and devices important thing
R003	Dust / dirt	Medium	Do cleaning regularly related document and device when seen dirty
R004	Theft device	Medium	Do CCTV installation and holding security guard

R005	Information accessed by unauthorized parties authorized	Medium	Limit right access to user
R006	Data and information No in accordance fact	Medium	Do checking related to data and information This is valid and can be used
R007	Abuse right access /User ID	Medium	Limit right access to user
R008	Former user / employee Still own access information	Medium	Do deletion right access to ex employee
R009	Data loss	High	Perform regular data backups as required standard
R010	Human error	High	Do HR training
R011	Cybercrime and piracy	Medium	Do Change server passwords regularly.
R012	Maintenance no scheduled	High	Do scheduling appropriate and ensure implementation can implemented.
R013	Program documentation is not available complete	High	Do recording documentation What only one must there is. Then done checking whether Already complete in accordance notes completeness documentation
R014	Hardware failure / damage	High	Do repairs to hardware and perform evaluation related reason damage / failure Can happen.
R015	Server down	Medium	Perform server maintenance routinely and on schedule.
R016	Overheat	Medium	Do maintenance in a way scheduled and place the hardware accordingly with recommended temperature.
R017	Connection network disconnected	High	Do checking related to ISP and network at CV.Aren Jaya
R018	System crash	High	Do repairs at the time Already found error system after perform maintenance

R019	Overcapacity	High	Do addition at capacity more memory big Power capacity. It is also necessary to do checking memory routinely.
R020	Overload	High	Do Monitoring on the server for ensure in condition all in condition Good
R021	Datacorrupt	Medium	Perform regular data backups.
R022	Backup failure	High	Do check on usage memory used in the database, so that it is known that memory This Already fullness or Still Can used. Then do maintenance in a way periodically and ensure that it continues implemented according to the schedule that has been made.
R023	Not good quality network	High	Do replacement more network Good.
R024	Technology worn	Medium	Do purchase update if Still allows. Then can do purchase device new If old device already No can used
R025	Power outage	High	Providing Generators
R026	CCTV does not functioning with Good	Medium	Perform routine maintenance.
R027	Generator is broken	Medium	Performing Service for repair and know which part is problematic.

In table 10 above This expected Can For minimize possibility risk What only one will happened to CV. Sugar Palm Jaya.

4. CONCLUSION

From research related analysis risk using ISO 31000:2018 which has been implemented implemented on CV. Sugar Palm Jaya which includes a number of stages like evaluation risk, identification risk, analysis risk, evaluation risk and at what stage treatment

risk. There are 27 risks that cause CV. Sugar Palm Jaya in his business process become obstructed.

Based on study 2 possibilities found risk, with levels *High* as many as 12 such as data loss, human error, *maintenance* No scheduled, program documentation is not complete, hardware failure / damage, connection network disconnected, system crash, *overcapacity, overload, backup failure*, less the good thing is quality Network and electricity off. Then 15 risks found with levels *medium*, which includes fire, disaster nature, dust / dirt, theft device, information accessed by unauthorized parties authorities, data and information No in accordance facts, abuse right access /user ID, former user/ employee Still own access information, *cybercrime* and piracy, *server down, overheat, datacorrupt*, technology obsolete, CCTV is not functioning with good and the generator is broken.

After implemented study This expected Can used as CV guidelines. Sugar Palm Jaya for minimize possibility risks that can occur caused by various type matter as per what has been explained on with done implementation treatment risk from table 10. As perform regular data backups when *datacorrupt*, do *maintenance* in a way routine, when CCTV is not functioning with good and doing HR training when human error occurs, so that the business process company This Can walk with good and smooth.

BIBLIOGRAPHY

AA Ulfa And T. Immawan, "Risk Management Analysis Using Iso 31000 At Machining Process (Case Study: Ab Company)," Jurnal Ilmiah Teknik Industri, Pp. 42–52, 2021.

D.Hendarwan, "Implementation of Risk Management with the ISO 31000:2018 Approach in the Implementation of Corporate Strategy," Adminika Journal, Vol. 8, No. 1, Pp. 58–73, 2022.

JO Yoewono And AH Prasetyo, "Risk Management Design And Process At PT Surya Selaras Cita," Muara Jurnal Ilmu Ekonomi dan Bisnis, Vol. 6, No. 1, Pp. 56–72, 2022.

K. Vincent, "Design and Implementation of Risk Management at CV. Comformindo to Become a Sustainable Business," Vol. 1, No. 1, Pp. 2120–2126, 2021.

AA Hapsari, "The Influence of Corporate Governance on Risk Management in Indonesian Banking," *J. Muara Ilmu Ekon. Dan Bisnis*, Vol. 1, No. 2, P. 1, 2018, Doi: 10.24912/Jmieb.V1i2.936.

J. Ząbek, "The Role Of The Organization's Leadership In Risk Management According To Norm Iso 31000: 2018," *Zesz. Nauk. Małopolskiej Wyższej Szk. Econ. W Tarnowie*, No. 3 (43), Pp. 117–126, 2019, Doi: 10.25944/Znmwse.2019.03.117126.

T. Parviainen, "Implementing Bayesian Networks For Iso 31000:2018-Based Maritime Oil

Spill Risk Management: State-Of-Art, Implementation Benefits And Challenges, And Future Research Directions," *J. Environ. Manage.*, Vol. 278, 2021, doi: 10.1016/J.Jenvman.2020.111520.

MI Fachrezi, "Information Technology Asset Security Risk Management Using ISO 31000:2018 Diskominfo Kota Salatiga," *Jatisi (Journal of Tech. Inform. And Information Systems)*, Vol. 8, No. 2, Pp. 764–773, 2021, Doi: 10.35957/Jatisi.V8i2.789.

PASitanggang And FASitanggang " Analysis of Risk Management Implementation Based on SNI ISO 31000:2018 (Case Study: Spare Parts for Second Personal Computers in Jambi)," Scientific Journal of Economics and Business Vol. 13, No. 1, Pp. 12–19, 2022, Doi: 10.33087/Eksis.V13i1.293.

KB Mahardika, AF Wijaya, and D. Cahyono, "Information Technology Risk Management Using ISO 31000: 2018 (Case Study: CV. Xy)," Sebatik Journal, Vol. 2018, pp. 277–284, 2018.

K. Mey, L. Lole, and E. Maria, "Risk Management Analysis on Pegadaian Digital Service Application Gold Savings Menu Using ISO 31000:2018," *J. Sist. Comput. and Inform. Page 319−*, Vol. 324, No. 3, 2022, Doi: 10.30865/Json.V3i3.3891.

W. Harefa, "Risk Management Analysis Using the ISO 31000:2018 Framework in Warehouse Information Systems," *Jatisi (Journal of Information Technology and Information Systems)*, Vol. 9, No. 1, Pp. 407–420, 2022, Doi: 10.35957/Jatisi.V9i1.1478.

DL Ramadhan, R. Febriansyah, and RS Dewi, "Risk Management Analysis Using ISO 31000 at Smart Canteen SMA XYZ," *Jurikom (Jurnal Ris. Komputer)*, Vol. 7, No. 1, P. 91, 2020, Doi: 10.30865/Jurikom.V7i1.1791.

M. Miftakhatun, "Analysis of Information Technology Risk Management on Ecofo Website Using ISO 31000," *J. Comput. Sci. Eng.*, Vol. 1, No. 2, Pp. 128–146, 2020, Doi: 10.36596/Jcse.V1i2.76.

LEHutagalung., "Risk Management Analysis Of Hospital Management Information System (Simrs) In Xyz Hospital Using ISO 31000," TeIKa Journal pp. 23–33, 2022.