Jurnal Mantik, 5 (2) (2021) 1087-1095

Published by:Institute of Computer Science (IOCS)

Jurnal Mantik

Journal homepage: www.iocscience.org/ejournal/index.php/mantik/index

Information Technology Risk Analysis in The Personnel Management Information System (SIMPEG) at the Salatiga City Education Office

Natasya Ribka Malonda[1], Augie David Manuputty[2]

[1,2]Information Systems, Faculty of Information Technology, Satya Wacana Christian University, Salatiga

E-mail: 682017070@student.uksw.edu, augie.manuputty@uksw.edu

ARTICLEINFO

Article history:
Received: 10/07/2021
Revised: 20/07/2021
Accepted: 01/08/2021

Keywords: Risk Analyst, Risk Management, ISO31000

ABSTRACT

The Personnel Management Information System is an information system owned by the Education Office that is useful for managing ASN personnel data in Salatiga City. SIMPEG is used as a reference for decision-making for agencies, for example in promotions, as well as joint salary increases. However, in the world of risk management, no matter how good the system is, there is always the possibility of risks that can threaten and disrupt the business processes that run in the use of the information system. Therefore, a risk analysis of IS/IT resources is needed that supports the management of the personnel management information system in the Education Office. By applying the ISO 31000:2018 framework, it is hoped that this risk analysis can minimize the possible risks that exist. The results of this risk analysis are in the form of recommendations for risk actions that are needed according to the priority level of risk from the risk data that has been analyzed. So it is hoped that in the future the Education Office can apply the recommendations for risk actions that have been analyzed in this study.

1. Introduction

The development of technology today is so rapid, information technology is an important asset for the development of companies and agencies. Therefore, almost all companies and agencies apply IS/IT in every existing business process, every company and agency is competing to optimize their IS/IT development.[1]. However, with the more optimal information technology assets, there will always be the possibility of risks that can threaten a company or agency, especially for those who already have their own system.[2].

These risks cannot be avoided, and will certainly hinder the achievement of the goals of the company or agency. However, every risk can certainly be minimized by implementing good IS/IT risk management and management, so that existing information technology assets can work optimally, and can make existing business processes more effective and efficient. Companies that can be classified as successful, must realize how important risk management is related to planning and implementing IS/IT[3]. Not only from fixating on one particular sector. In the world of Management, everything that is carried out in an organization or company must always be accompanied by threats and risks. Risk always overshadows every activity undertaken to prevent an organization or company from achieving their goals as well as their vision and mission, therefore a risk control is needed to be able to help an organization or company to handle any existing risks and be able to realize the goals of the organization or company.[4].

The Salatiga City Education Office is one of the government agencies engaged in education in the city of Salatiga. The Salatiga City Education Office has optimized the use of IS/IT by implementing the Personnel Management Information System or more commonly known as SIMPEG, which is useful for recording and managing every employee who works for the agency, especially for every ASN (state civil apparatus) so that it can be organized in an organized manner. maximum. This Personnel Management Information System is another language of ERP in a company, so that this Personnel Management Information System is integrated with various sectors such as payroll, attendance, employment, and so on in the Salatiga City Education Office, so that SIMPEG is used as a reference for decision-making for agencies towards ASN, such as for example as a reference for promotions, joint salary increases, and requests for employee leave. However, it is undeniable that the Personnel Information System certainly has the possibility of risk threats that can disrupt

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

existing business processes. It can be seen visually from some of the risks that the agency still cannot overcome, such as human error, server downtime, and several other risks. So we need an evaluation of risk management by identifying risks, conducting risk assessments, and conducting risk analysis so as to produce appropriate recommendations to minimize risk. as well as employee leave applications. However, it is undeniable that the Personnel Information System certainly has the possibility of risk threats that can disrupt existing business processes. It can be seen visually from some of the risks that the agency still cannot overcome, such as human error, server downtime, and several other risks. So we need an evaluation of risk management by identifying risks, conducting risk assessments, and conducting risk analysis so as to produce appropriate recommendations to minimize risk. as well as employee leave applications. However, it is undeniable that the Personnel Information System certainly has the possibility of risk threats that can disrupt existing business processes. It can be seen visually from some of the risks that the agency still cannot overcome, such as human error, server downtime, and several other risks. So we need an evaluation of risk management by identifying risks, conducting risk assessments, and conducting risk analysis so as to produce appropriate recommendations to minimize risk. It can be seen visually from some of the risks that the agency still cannot overcome, such as human error, server downtime, and several other risks. So that an evaluation of risk management is needed by identifying risks, conducting risk assessments, and conducting risk analysis so as to produce appropriate recommendations to minimize risk. It can be seen visually from some of the risks that the agency still cannot overcome, such as human error, server downtime, and several other risks. So we need an evaluation of risk management by identifying risks, conducting risk assessments, and conducting risk analysis so as to produce appropriate recommendations to minimize risk.

The purpose of this study is to minimize the possible risks that are happening or will occur and to provide appropriate recommendations for the Salatiga City Education Office regarding existing risks and risks that can arise at any time. This risk analysis is carried out using an approach using the ISO 31000:2018 method. ISO 31000:2018 is a standard guide for an organization or company to build a foundation for a risk management process[5]. This foundation includes planning, accountability of employees, assets and activities used to manage risk in the Education Office. In managing this risk, a risk assessment is required which has been regulated in ISO 31000:2018 in order to be able to see the risk value of each identified risk.[6].

Based on previous research conducted by Driantami, Suprapto and Perdanakusuma in 2018 regarding risk management using ISO 31000:2009 with the NIST 800-30 framework with a case study: PT Matahaari Department Store Sales System Malang Town Aquare Branch. From the research conducted, there are three important points that can be drawn, among others: (1) For risk management using the ISO 31000 framework requires a more technical framework such as NIST 800-30. (2) By using ISO 31000, the risk value is seen with three levels, namely low, medium, and high. (3) Appropriate control recommendations such as risk reduction for the risk of human error (errors in operating the system), risk avoidance for the risk of authorization password theft, and risk reduction for the risk of unstable connections[7].

Then also research conducted by Rilyani, Firdaus and Jatmiko in 2015 conducted an information technology risk analysis using ISO 31000 with a case study: I-Ggracial Telkom University. After carrying out a series of risk management processes, the results of the risk level in the i-Gracias system are obtained. Risks that are at a high level are risks that have a high probability and impact value. In the i-Gracias system, the risk that has the highest risk value is Database Server Down. The impact if this risk occurs is that all i-Gracias services cannot run, so it is necessary to handle this risk quickly.[8].

Another research related to ISO 31000 was written by Francisca Lady Nice with the title "Information Technology Risk Analysis at the National Aeronautics and Space Institute (LAPAN) on the SWIFTS website using ISO 31000" in 2016. This research focuses on the SWIFTS website. From this research, the results of the risk level that have a high probability and impact value are assets, both software data, hardware, human resources and procedures related to the SWIFtS system which are considered to be able to interfere with the LAPAN business process itself. So that a review is needed by the head of the LAPAN IT Division and the application of the recommended risk treatment[9].

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

2. Method

Fig 1. Research Method

Researchers approach using qualitative research methods. Qualitative research is research that is used to investigate, find, describe, and explain the quality that is measured or described through a quantitative approach in a natural case study and by utilizing various natural methods.[10].

One of the methods used in this research is Case Study Research, which focuses on only one case study object. The application of this case study research method is intended so that researchers can focus on a more in-depth research object so that researchers can collect the data needed to be more centralized.[11].

In managing risk management in the application of the Personnel Information System at the Salatiga City Education Office, researchers use the ISO 31000 framework. Where ISO 31000 focuses on risk management. In its development, ISO 31000 is also officially recognized as a risk management standard in up to 40 countries around the world. In this study, the method used by the researcher was carried out in various stages[12]. This stage is in line with the ISO 31000 framework, where by conducting research, in finding all kinds of valid data and information and used for research on the Personnel Management Information System at the Education Office of Salatiga city by using an approach from the researcher to internal parties in this research by interviews to explore primary data sourced from resource persons, namely employees at the Salatiga City Education Office. In collecting data for this study, namely by conducting interviews with sources, namely the IT department of the agency.

That way, researchers can determine a risk assessment or Risk Assessment. This risk assessment is a method that is widely used in companies and organizations to determine risk. In carrying out a risk assessment there are several stages:[13].

a. Risk Identification

Risk identification is an identification of all possible risks by collecting valid data and information[14].

b. Risk Analysis (Risk Analyst)

Conducted to find out the various levels of risk that have been found, which threaten the development of the Personnel Information System at the Salatiga City Education Office

c. Risk Evaluation

Risk evaluation is a process to compare the level of risk levels in accordance with predetermined risk criteria. These risk levels are ordered from the lowest to the highest risk level[15].

Furthermore, entering the stage of Risk Treatment (Risk Treatment) in this stage risk management is carried out, namely by selecting one or more ways to overcome the risks that have been found and implementing the application of risk management.[16]. Once implemented, the effectiveness of risk management can be assessed whether the level of risk can be tolerated or not, if risk management cannot be tolerated, it will result in new risk management.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

3. Results and Discussions

3.1 Risk Assessment

This stage is the risk assessment stage at the Salatiga Education Office. The risk assessment process for this Personnel Information System application consists of 3 stages, namely: risk identification, risk analysis, and risk evaluation.

3.2 Risk Identification

a. Asset identification

At this stage, it is necessary to identify assets for the application of the Personnel Information System such as data assets, software assets, and hardware assets. At this stage it is more focused on data assets, software and hardware.

Table 1.
Asset Identification

Information System Components	Asset
Data	Personal Data, Group Data, Rank Data, Education Data
Software	Personnel Information System Application
Hardware	Personal computers

b. Identify possible risks

After identifying the assets, it is necessary to identify possible risks that can threaten the Personnel Information System. Possible risks can be grouped based on 3 factors, namely; natural/environmental factors, human factors and system and infrastructure factors. Which can be seen in table 2. below.

Table 2.
Identification of Possible Risks

Factor	ID	Possible Risk
Natural	R001	Flood
	R002	Earthquake
	R003	Fire
	R004	Lightning
Man	R005	Human error
	R006	Abuse of access rights
	R007	Data theft and leaks
	R008	Hardware theft
	R009	Hacking
	R010	User Interface that is difficult to understand
	R011	*Vandalism*
	R012	New employees who don't really understand the workflow of the system
System and infrastructure	R013	Bad network connection
	R014	Hardware damage
	R015	Server down
	R016	Corrupt data
	R017	Overheat
	R018	Double Backup
	R019	System error
	R020	Power outage

At this stage, it was identified that there were 20 possible risks originating from the three factors, namely: nature/environment, human, system and infrastructure.

c. Identification of Impact Possible Risk

At this stage, the risk impact identification is carried out from the possible risks to determine the causal correlation that can occur from the possible risks. Can be seen in table 3

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Table 3.
Identification of Possible Risk Impacts

Factor	ID	Possible Risk	Impact
Natural	R001	Flood	damage to infrastructure and disrupt business processes
	R002	Earthquake	disrupting business processes
	R003	Fire	damage to infrastructure and disrupt business processes
	R004	Lightning	damage to infrastructure
Man	R005	Human error	
	R006	Abuse of access rights	User access rights can be abused
	R007	Data theft and leaks	Data can be misused by other parties
	R008	Hardware Theft	Financial loss
	R009	Hacking	The system can be bugged and compromised
	R010	User Interface that is difficult to understand	Users may experience difficulties in understanding and operating the system
	R011	*Vandalism* (damaging facilities such as computer equipment)	Financial loss and cause the device to be damaged
	R012	New employees who don't really understand the workflow of the system	The data settlement process is not timely
System and infrastructure	R013	Bad network connection	Users will have difficulty accessing the system
	R014	Hardware damage	Inhibiting business processes and users will find it difficult to access the system
	R015	Server down	Unable to access system and database
	R016	Corrupt data	User cannot see valid data
	R017	Overheat	May cause hardware damage due to temperature rise
	R018	Double Backup	May cause data loss
	R019	System error	Users will have difficulty in running the system
	R020	Power outage	Business process activities cannot run

3.3 Risk Analysis

At this stage the possibility of risk in the previous risk identification stage is assessed using the Likelihood criteria table. In the Likelihood table there are 5 criteria based on the frequency of occurrence of possible risks.

Table 4.
Likelihood Criteria

Mark	*Likelihood* Criteria	description	Frequency of occurrence
1	Rare	This risk almost never occurs	>2 Years
2	Unlikely	This risk is rare	12 years old
3	possible	This risk happens sometimes	7 – 12 Months
4	Likely	This risk often occurs	4 – 6 Months
5	Certain	The risk is bound to happen	13 months

Then in table 5 below is a table of impact values or impacts that occur from possible risks in the application of the Personnel Information System. In this impact assessment table, they are grouped into 5 criteria and grouped based on the impact of the least influential to the most influential impact.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Table 5.
Impact Criteria

Impact Mark	Impact Criteria	Information
1	Insignificant	Does not interfere with activities
2	Minor	The company's activities are a bit hampered
3	Moderate	Causing disruption to business processes
4	Major	Inhibits almost all activities
5	Catasirophic	Company activities stop

After obtaining the Likelihood criteria in table 4, and the Impact criteria in table 5. Then the next step is to assess the possibility of risk based on tables 4 and 5.

Table 6.
Assessment of Likelihood and Impact

Factor	ID	Possible Risk	Likelihood	Impact
Natural	R001	Flood	1	4
	R002	Earthquake	2	2
	R003	Fire	1	5
	R004	Lightning	2	3
Man	R005	Human error	4	3
	R006	Abuse of access rights	2	2
	R007	Data theft	1	2
	R008	Hardware theft	1	3
	R009	Hacking	1	3
	R010	User Interface that is difficult to understand	2	1
	R011	*Vandalism* (damaging facilities such as computer equipment)	1	3
	R012	New employees who don't really understand the workflow of the system	4	2
System and infrastructure	R013	Bad network connection	4	4
	R014	Hardware damage	2	4
	R015	Server down	4	4
	R016	Corrupt data	1	4
	R017	Overhead	4	1
	R018	Double Backup	1	2
	R019	System error	3	4
	R020	Power outage	3	3

From table 6 above, you can find the value of the possible risks in the table *Likelihood* and Impact. After finding the value of Likelihood and Impact, then enter the risk evaluation stage.

3.4 Risk Evaluation

At the last stage, namely risk evaluation, a risk evaluation process will be carried out from the possible risks that have been analyzed in the previous stage. The results of the analysis will be entered into a risk evaluation matrix based on the guidelines in the ISO 31000 framework. The evaluation matrix is divided into 3 risk levels, namely: Low, Medium, and High.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

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
			Insignificant	Minor	Moderate	Major	Catastrophic

The next stage is to enter each possible risk identity into the risk evaluation matrix according to the Likelihood criteria and Impact criteria.

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

After entering the possible risks into the evaluation matrix based on Likelihood and Impact, in the next stage the 20 possible risks will be grouped into high, medium and low levels.

Table 9.
Grouping of Risks Based on Levels

ID	Possible Risk	Likehood	Impact	Risk Level
R013	Bad network connection	4	4	High
R015	Server down	4	4	High
R001	Flood	1	4	Medium
R003	Fire	1	5	Medium
R004	Lightning	2	3	Medium
R005	Human error	4	3	Medium
R012	New employees who don't really understand the workflow of the system	4	2	Medium
R014	Hardware damage	2	4	Medium
R016	Corrupt data	1	4	Medium
R017	Overhead	4	1	Medium
R019	System error	3	4	Medium
R020	Power outage	3	3	Medium
R002	Earthquake	2	2	Low
R006	Abuse of access rights	2	2	Low
R007	Data theft	1	2	Low
R008	Hardware theft	1	3	Low
R009	Hacking	1	3	Low
R010	User Interface that is difficult to understand	2	1	Low
R011	*Vandalism* (damaging facilities such as computer equipment)	1	3	Low
R018	Double Backup	1	2	Low

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

In the stages of the risk evaluation process above, there are 20 possible risks that have been analyzed and grouped based on the level of risk. There are 2 possible risks that are categorized into high risk levels, namely: R013 and R015. Then there are 10 possible risks that are categorized into medium risk levels, namely: R001, R003, R004, R005, R012, R014, R016, R017, R019 and R020. And there are also 8 possible risks that are categorized into low risk levels, namely: R002, R006, R007, R008, R009, R010, R011, and R018.

3.5 Risk Treatment

After carrying out the risk identification process regarding assets that are in the application environment of the Personnel Information System, then the next stage will be the Risk Treatment or risk treatment. In this stage, it provides risk actions against possible risks that have been grouped based on the risk level in table 9. In table 10, it is expected to minimize the possible risks that can occur for the application of the Personnel Information System owned by the Salatiga City Education Office.

Table 10.
Proposed Risk Treatment

ID	Possible Risk	Risk Level	Risk Action
R013	Bad network connection	High	Replace with a new ISP (Internet Service Provider)
R015	Server down	High	Perform scalable checks on the database
R001	Flood	Medium	Placing infrastructure tools in a place that is safe from flooding
R003	Fire	Medium	Prepare fire extinguishers
R004	Lightning	Medium	Installing a lightning rod
R005	Human error	Medium	Conduct training to users
R012	New employees who don't really understand the workflow of the system	Medium	Make system work SOPs and conduct training for new employees
R014	Hardware damage	Medium	Provide insurance on existing hardware assets
R016	Corrupt data	Medium	Perform regular backups
R017	Overheat	Medium	Provide a room that has AC (Air Conditioner) and add fans to all hardware
R019	System error	Medium	Increase bandwidth, perform system updates, and update antivirus.
R020	Power outage	Medium	Provide an electric generator set with a power that suits your needs. Then set up Uninterruptible Power Supply (UPS)
R002	Earthquake	Low	Provide a safe enough place to place the devices
R006	Abuse of access rights	Low	Provide access restrictions on each device
R007	Data theft	Low	Install CCTV, alarms, and sensors in every room
R008	Hardware theft	Low	Install CCTV, alarms, and sensors in every room
R009	Hacking	Low	Using a private network and increasing the security of the system
R010	User Interface that is difficult to understand	Low	Change the appearance of the user interface to make it more simple and functional
R011	*Vandalism* (damaging facilities such as computer equipment)	Low	Give a compensation warning to every user
R018	Double Backup	Low	Make SOP backups and perform backups on a scale.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

4. Conclusion

Based on the IS/IT risk analysis research using ISO 31000:2018 on the Personnel Information System application owned by the Salatiga City Education Office, starting from the risk assessment stage, risk identification, risk analysis, risk evaluation, to the risk treatment stage.

From these stages, this risk analysis obtained 20 possible risks that could at any time interfere with the performance of the Personnel Information System application or disrupt the business processes contained in the Salatiga City Education Office. After this research is conducted, it is hoped that this research can be used by the Salatiga City Education Office as a guideline or policy to minimize the possible risks that can occur, so as not to disrupt the Personnel Information System application system.

5. References

[1] A. Using and F. Cobit, "INFORMATION TECHNOLOGY ON BUSINESS STRATEGIES (Case Study of PT. BRI, Tbk) Adityawarman Diponegoro University ABSTRACT Strategic alignment between Information Technology (IT) and business has become CIOs and CEOs primary concern nowadays. This shows ," vol. 1, pp. 166–177.

[2] FM Hutabarat and AD Manuputty, "Information Technology Risk Analysis of PT Visionet Data Internasional's VCare Application Using ISO 31000," *J. Computing.*, vol. 2, no. 1, pp. 52–65, 2020, doi:10.33557/binacomputer.v2i1.792.

[3] S. Wiyono and AR Tanaamah, "Analysis of IS/IT Performance at PDAM Salatiga City Using the IT Balanced Scorecard Framework," *J. Buana Inform.*, vol. 8, no. 4, pp. 181–192, 2017, doi:10.24002/jbi.v8i4.1442.

[4] Y. Erlika, MI Herdiansyah, and AH Mirza, "Analysis of IT Risk Management at Bina Darma University Using ISO31000," *J. Ilm. information. Glob.*, vol. 11, no. 1, 2020, doi:10.36982/jig.v11i1.1073.

[5] NM Sirait and A. Susanty, "Operational Risk Analysis Based on Enterprise Risk Management (ERM) Approach in Companies," *eng. eng. Online J.*, vol. 5, no. 2012, p. 4, 2016.

[6] GW Lantang, AD Cahyono, and N. Ngalumsine, "Analysis of Information Technology Risk in Sap Applications at Pt Serasi Autoraya Using Iso 31000," *Sebatik 2621-069X*, vol. 23 No. 1, pp. 36–43, 2019, doi: 1410-3737.

[7] I. Lanin, "The New ISO 31000:2018 Risk Management Standard," *IBFG Institute*, 2018. https://ibfgi.com/risk-management-31000/ (accessed Apr. 12, 2018).

[8] A. Novia Rilyani, YA Firdaus W ST, and DS Dwi Jatmiko, "Information Technology Risk Analysis Based on Risk Management Using ISO 31000 (Case Study: 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.

[9] FL Nice and RV Imbar, "Analysis of Information Technology Risk at the National Institute of Aeronautics and Space (LAPAN) on the SWIFTS Website Using ISO 31000," *J. Inform. and Sis. inf.*, vol. 2, no. 2, pp. 1–11, 2017.

[10] RM Candra, YN Sari, I. Iskandar, and F. Yanto, "Information Technology Asset Security Risk Management System Using ISO 31000 : 2018," vol. 5, no. 1, pp. 19–28, 2019.

[11] A. Rahmawati and AF Wijaya, "Information Technology Risk Analysis Using ISO 31000 in ITOP Applications," *J. SITECH Sist. inf. and Technol.*, vol. 2, no. 1, pp. 13–20, 2019, doi:10.24176/sitech.v2i1.3122.

[12] HTI Driantami, Suprapto, and AR Perdanakusuma, "Information Technology Risk Analysis Using ISO 31000 (Case Study: Sales System of PT Matahari Department Store Malang Town Square Branch)," *J. Pemb. Technol. inf. and Computer Science.*, vol. 2, no. 11, pp. 4991–4998, 2018.

[13] DE Adi and N. Susanto, "Risk Management Analysis of Procurement Activities in Newspaper Printing," *J. Metris*, vol. 18, pp. 113–118, 2017.

[14] PP Thenu, AF Wijaya, and C. Rudianto, "Analysis of Information Technology Risk Management Using Cobit 5 (Case Study: Pt Global Infotech)," *J. Computing.*, vol. 2, no. 1, pp. 1–13, 2020, doi:10.33557/binacomputer.v2i1.799.

[15] DL Ramadhan, R. Febriansyah, and RS Dewi, "Analysis of Risk Management Using ISO 31000 on Smart Canteen SMA XYZ," *JURIKOM (Journal of Ris. Computer)*, vol. 7, no. 1, p. 91, 2020, doi:10.30865/jurikom.v7i1.1791.

[16] GW Lantang, AD Cahyono, and MNN Sitokdana, "Analysis of Information Technology Risk in SAP Applications at Pt Serasi Autoraya Using Iso 31000," *Sebatik*, vol. 23, no. 1, pp. 36–43, 2019.