JURNAL AKSI
Akuntansi dan Sistem Informasi
http://aksi.pnm.ac.id

Information Technology Risk Analysis and Mitigation Using ISO 31000 and House of Risk (HOR) for SIAK in Western Seram Regency

Christine Mayasamy Pentury [1], Johan Jimmy Carter Tambotoh[2]

[1] [2] System Information Department, Faculty of Technology Information, Satya Wacana Christian University

ARTICLE INFO

ABSTRACT

SIAK stands for population administration information system. It is a computerized system that was established according to administrative service regulations to organize the population administration system in Indonesia, more precisely in the Western Seram Regency. Given the critical function of this application in aiding in identifying regional demographic statistics, it is vital to examine potential dangers while also identifying mitigation measures that may be performed to avoid them. ISO 31000 was utilized in the study to map potential hazards for subsequent reduction using the House of Risk (HOR) methodology. According to the findings of this research, there is one danger that falls into the high category, namely the unstable network. Additionally, based on the results of risk mitigation identification, two mitigation steps are identified that can mitigate 60% of existing risks, namely the construction particular resistant to natural disasters for critical equipment storage and collaboration with internet providers to ensure stable internet and network connections.

INTRODUCTION

Rapidly evolving and sophisticated information technology and information systems provide dependable options to assist various organizations tasks. The function of information technology applications has evolved into an unavoidable requirement and a resource on which users may depend to address a variety of difficulties. The Population Administration Information System (or Sistem Informasi Administrasi Kependudukan – SIAK) is a web-based information system that built on procedures and specific standards for population administration system. Its purpose to organize the administrative system in the field of the population to achieve administrative order and assist Regional Government officers, particularly those at the Population and Civil Registration Office in Western Seram Regency. In terms of population growth, the development of population administration plays a significant role in making sure that the law is clear and protecting people's individual rights. Protective measures come in the form of public services, such as birth certificates and the Population Identification Number (NIK), as well as documents like the Identity Card (KTP), the Family Card (KK), and the Civil Registration Certificates. The rights and basic needs of citizens will be protected by these administrative services, which can help people get important documents that show who they are, how long they have been alive, and other things. The state must do these things because they are essential and must be done (Dwiyanto, 2010).

The regional governments are responsible for recording population statistics in an area through the population administration information system, which begins with the village and sub-district as the starting point for population data collection. Additionally, the data would be saved in a database that is connect to the internet network on a national scale. Additionally, the SIAK, which is deployed through the internet network, is harmed by the network's sluggish speed. Apart from these impediments, the SIAK program may operate effectively and in compliance with the established regulations. The shortcomings of traditional data processing may be mitigated with online data management. SIAK provides numerous benefits, including the ability to use the results of statistical data calculation and management to develop and improve policies, strategies, and programs for the implementation and implementation of development in the fields of quality, quantity, and population mobility, as well as other development interests (Munarja, 2014).

SIAK plays a critical role mainly because of sensitivity of the data gathered and inventoried, such as demographic statistics, which is crucial information that cannot be accessible by everyone. Web services eliminate the need for direct data access between applications and the database. Due to the mediation procedure through a web service, the database was not immediately accessible to the outside world. If there is a security hole from the application side, the database cannot be accessed directly. Thus, population data is generally secure in this procedure when compared to apps that link directly to the database.

Nevertheless, every application must be subjected to a multitude of potential risks that might cause the application to perform sub optimally or even crash. A variety of internal and external variables to the program might pose a threat to the application's security. The SIAK application is no different; the application, like any other, maybe subjected to potential dangers that may occur in its environment. Based on these issues, more study is required to detail the many potential hazards as well as the importance of each risk to the firm. The ISO 31000 approach, which is commonly utilized for this purpose, is frequently used to examine the risks that may develop. When identifying and categorizing risks, this strategy has been extensively employed in many past research. Several studies have used this method, including Christian and Sitokdana (2022), who conducted a risk analysis of ABC Bank, Manuputty et al. (2022), who conducted a risk analysis on the operational aspects of information technology at PT. Schlumberger Geophysics Nusantara, Ayuningtyas & Tanaem (2022), who conducted a risk analysis of asset security risk management at the Secretariat of the Salatiga City DPRD, and Nuris et al. (2021) which conducted a risk analysis of software development projects, Putri & Syafi'i (2022) who conducted a risk study at PT J&T.

However, the ISO 31000 approach generates very simple outputs and suggestions that are prone to bias; even the recommendations themselves are highly complicated and require a significant cost to implement by the corporation or linked entity. This is because each risk will need a unique risk management strategy. Thus, some researchers prefer to combine the ISO 31000 method with other quantitative methods, such as Hardianto & Dharmawan's (2021); Aprianto et al. (2020); Butarbutar & Tanaamah's (2021) research, which combined ISO 31000 with Cobit 5 and FMEA, Asmarawati & Pangeran (2021); Nugriho & Pangeran (2021); Safitri & Pangeran (2020); Monica & Pangeran (2020) study, which combined ISO 31000 with Balanced Scorecard, and Pribadi & Ernastuti's (2020) research, which combines ISO 31000 with FMEA.

Thus, the approach utilized in this research is not restricted to two methods but incorporates the ISO 31000 analysis findings for additional quantitative calculations to generate to for effective mitigation measures while overcoming ISO 31000's inherent complexity. As a result, this research integrates ISO 31000 with the House of Risk (HOR). HOR, which was initially introduced and Geraldin (2009), is a regenerative technique for risk analysis. The program employs the FMEA (Failure Mode and Effects Analysis) concept to quantify risk and the House of Quality (HOQ) model to identify risk agents that must be prioritized first, followed by the most prioritized action-mitigate the possible hazards caused by risk agents (Purwaningsih et al. 2021; Ikhsan et al. 2021; Utomo & Setiawan, 2021; Munawir et al. 2021).

Furthermore, this paper will be organized as follows. After the introduction, it will be continued with the material and method, then continued with the results and discussion, followed by conclusions and recommendations.

MATERIALS AND METHOD

This study employs mixed method approach, that this technique used when concerns about outcomes and processes need to be investigated, and involves a mix of quantitative and qualitative methods in one study (Figure 1).
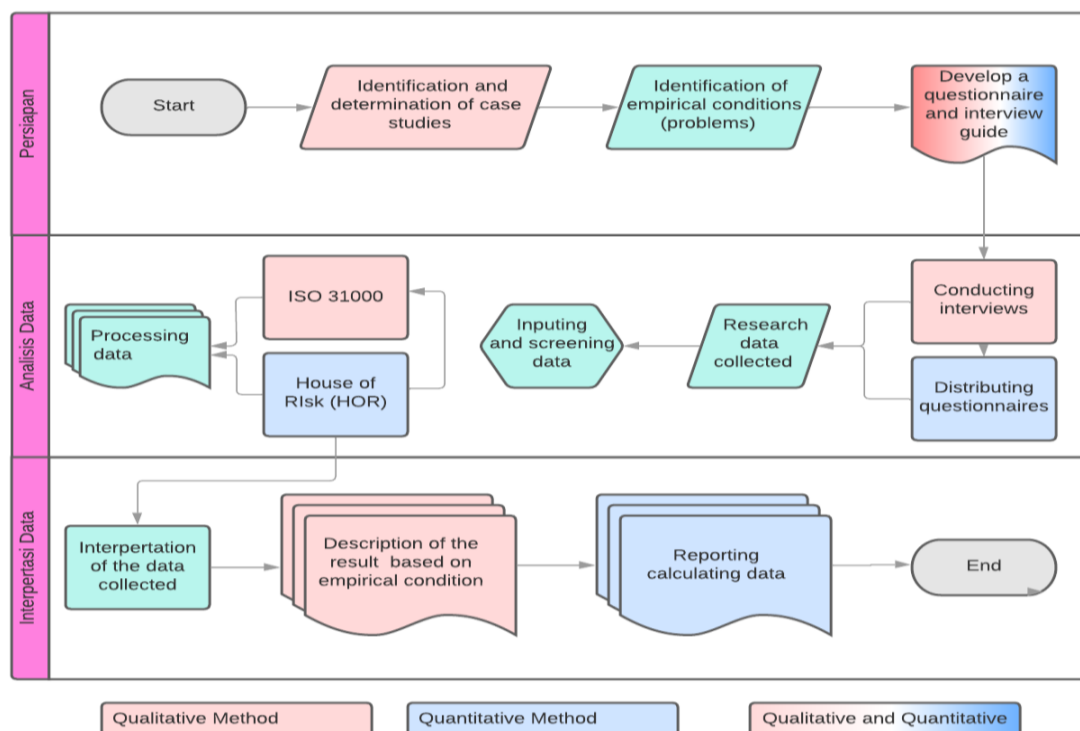

Figure 1. Methodology approach

Data Collecting and Sample

At this stage, data collection was accomplished via various methods, including conducting interviews with the operator and 11 personals and leaders at the population and civil register office in West Seram Regency who utilized directly involved with the SIAK application. The second objective was to spend two months observing business operations and the usage of SIAK software at the population and civil register office in West Seram Regency. Then, utilized data from the SIAK application at West Seram Regency's population and civil register office, the third step is to determine what procedures have transpired.

Analysis Method
ISO 31000

ISO 31000 is a standard produced by the International Organization for Standardization (ISO) with the goal of providing universal risk management concepts and practises. According to the International Organization for Standardization (ISO 31000:2009), the risk management process consists of two phases. The first step is risk assessment, which is the process of identifying hazards that might jeopardise the company's ability to achieve its business objectives. There are three steps in the risk assessment stage: risk identification, risk analysis, and risk evaluation. Risk identification is the process of identifying potential risks that could jeopardise the company; risk analysis is the process of determining risks that could prevent the company from achieving its business objectives; and risk evaluation is the process of categorising each potential risk based on its severity level in accordance with established criteria. The next step is risk treatment, during which the researcher narrows down the previously considered dangers. As a result, the potential dangers and their effect might be increased or decreased.

House of Risk (HOR)

The HOR model underpins risk management with a prevention-oriented approach, meaning minimizing the possibility of risk agents occurring. As a result, the first step is to identify risk occurrences and agents. Typically, a single agent may generate many risk events. Adapting the FMEA technique, the risk assessment used is the Risk Priority Number (RPN), which is composed of three factors: chance of occurrence, severity of the resulting effect, and detection. The HOR approach gives probability values to risk agents and severity values to risk events. Due to the possibility of a single risk agent triggering several risk events, it is important to aggregate the risk agent's risk potential.

Priority should be given to adapting the House of Quality (HOQ) model to determine risk agents as a preventative step. Each risk agent is granted an A rating based on its ARPj value. Thus, if a corporation has many risk agents, it might begin by selecting the agent with the highest potential to create a risk event. The model with two distributions is referred to as the House of Risk (HOR), and it is a variant of the House of Quality (HOQ) model (Pujawan & Geraldin, 2009).

1. HOR 1 is used to establish the degree of priority for risk agents that must be administered as a preventative intervention.

   Stages in HOR1 include:
   1) Identify the hazards that may arise in Ei (risk events).
   2) Rate the severity of the danger on a scale of 1 to 5. Each risk's intensity is indicated by Si. In this study, severity measure by value of impact on Table 5.
   3) Identify risk agents and analyse their probability. Risk agents (Aj) and occurrence (Oj) (Table 10).
   4) Create a correlation matrix for each risk agent. Rij (connection) 0 (no correlation), 1, 3, and 9 (low, moderate, and strong) correlation.

Then compute ARP (Aggregate Risk Potential) using the equation:

$$ARP_j = O_J \sum_i S_I R_{IJ} \quad \text{.. (1)}$$

2. HOR 2 is a top priority when it comes to implementing activities that are deemed effective. HOR2 attempts to determine mitigation strategies for supply chain risks in the following stages:
   1) Pick high-risk agents to follow up on HOR2 (Pareto Diagram for ARPj). The specified risk agents are displayed in the left and right columns (ARPj value).
   2) Identify potential risk-prevention activities. This row of HOR2 (Preventive Actions PAk) (Table 11).
   3) Correlate each preventative activity with each risk agent (Ejk). Ejk 0 shows no connection, whereas Ejk 1, 3, and 9 imply low, medium, and strong association. EJK also indicates the efficacy of mitigation strategies in minimising risk agent emergence.

   4) Calculate each action's TEk using the formula:
   $$TE_k = \sum ARP_j E_{jk} \ \forall k \quad \text{... (2)}$$

   5) Rate the difficulty of each mitigation action (Difficulty Dk) using a Likert scale or other measure that represents the financial capacity or other resources required.

   6) Calculate the TEk/Difficulty Dk ratio using the formula:
   $$ETD_k = D_k TE_k \quad \text{... (3)}$$
   7) Determine each action's Priority Rank (Rk), with 1 being the highest ETD.

RESULTS AND DISCUSSION

ISO 31000

The risk assessment stage, or risk assessment, is the first step in accordance with the ISO 31000 principles for risk management analysis. Three steps will be carried out at this stage: risk identification, risk analysis, and risk assessment. These three procedures must be completed in order to proceed to the next step. Identifying potential risks to SIAK caused by a variety of elements such as nature/environment, people, systems, and infrastructure. And don't forget that each potential danger would be assigned a unique identifier (Table 1).

The risk identification approach identified 18 potential hazards arising from natural/environmental, human, system, and infrastructural variables that might harm the business.

Then, the identified risks are evaluated for their effect on the business. Thus, the effect of each potential risk may be detected throughout this procedure (Table 2).

Following identifying potential risks and their associated consequences, the risk analysis process begins. A table of probability criteria and a table of impact criteria are included in this method as a reference for the risk analysis process. Table 3 contains the likelihood criterion or the computed probability value. The likelihood evaluation is split into five categories, each of which indicates the probability of a risk occurring during a certain time period. Table 4 contains the effect values that would occur if the potential risks materialised in the business. Five impact factors are used in the evaluation. The five criteria range from having no influence to having the greatest impact on the company's success. The discovered risks will be included into the specified impact value one by one for each effect.

Table 1. Identification of potential risks

Code	Potential Risk	Categorize
R001	Earthquake	
R002	Flooding	
R003	Thunder	Nature
R004	Heavy Wind	
R005	Landslide	
R006	Hurricane	
R007	Lack of competence and knowledge	
R008	Human error	
R009	Limited number of operator	Human Factor
R010	No job description	
R011	Absent (Lazinesss)	
R012	Server down	
R013	Power outage	
R014	Inadequate computers	
R015	System maintenance	System and Infrastructure
R016	Restriction access	
R017	LAN connection down	
R018	Unstable network	

Table 2. The impact of potential risks identification

Code	Potential Risk	Impact
R001	Earthquake	Damaging to the infrastructure and the service was stopped.
R002	Flooding	Damaging infrastructure that disrupts all related activities.
R003	Thunder	Damaging digital devices
R004	Heavy Wind	Damaging digital devices and connection
R005	Landslide	Damaging infrastructure and connection
R006	Hurricane	Damaging all operations
R007	Lack of competence and knowledge	Error in services
R008	Human error	System error
R009	Limited number of operator	Delay in service time
R010	No job description	Problem in connections and system services
R011	Absent (Lazinesss)	Error left unhandle
R012	Server down	System become inaccessable
R013	Power outage	All system are down
R014	Inadequate computers specs	Slower services
R015	System maintenance	Delay in all services
R016	Restriction access	Disruption of system flow
R017	LAN connection down	System offline
R018	Unstable network	Distuption of overall services

Table 3. Likelihood criteria

Likelihood		Description	Frequency
Value	Criteria		
1	Rare	Risk almost never occurs	>5 times per year
2	Unlikely	Risk is rare	2-5 times per year
3	Possible	Risks happen sometimes	1-2 times per year
4	Likely	Risk often occurs	7-12 times per month
5	Certain	The risk is sure to happen	1-6 times per month

Table 4. Impact criteria

Impact		Description
Value	Criteria	
1	Insignificant	The risk does not interfere with existing business processes and the company's activities
2	Minor	The risk slightly hinders the company's activities
3	Moderate	The risk of hindering some of the company's activities
4	Major	The risk starts to disrupt service processes and hampers almost all company activities
5	Catastrophic	The risk is very disruptive to overall service processes and stops the company's activities

By establishing the likelihood and effect numbers, the next step is to examine each potential risk individually. The chance and effect values for each of the 18 potential hazards are calculated one by one using the table referenced above, which is shown in Table 5.

The risk evaluation stage is the final phase in the risk assessment stage. A reference is employed in this procedure in the form of a risk assessment matrix. The matrix is split into three risk categories: low, medium, and high. The risk possibilities identified in the previous phase using probability and impact values will be distinguished again using the current matrix. The risk categories in Table 6 have been mapped according to their probability and effect.

Table 5. Assessment of possible risk with likelihood and impact

Code	Potential Risk	Likelihood	Impact
R001	Earthquake	2	5
R002	Flooding	2	5
R003	Thunder	3	4
R004	Heavy Wind	2	4
R005	Landslide	1	5
R006	Hurricane	1	5
R007	Lack of competence and knowledge	4	4
R008	Human error	4	4
R009	Limited number of operator	2	3
R010	No job description	2	3
R011	Absent (Laziness)	2	3
R012	Server down	2	4
R013	Power outage	2	5
R014	Inadequate computers	2	3
R015	System maintenance	3	3
R016	Restriction access	1	4
R017	LAN connection down	2	5
R018	Unstable network	3	5

Table 6. Risk evaluation matrix

Likelihood			1	2	3	4	5
	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*

Table 7. Risk evaluation matrix based on likelihood and impact

Likelihood			1	2	3	4	5
	Certain	5					
	Likely	4				R007 R008	
	Possible	3			R015	R003	
	Unlikely	2			R009 R010 R011 R014	R004 R012	R18 R001 R002 R013 R017
	Rare	1				R016	R005 R006
Impact			*1*	*2*	*3*	*4*	*5*
			Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*

House of Risk (HOR)

Each potential risk will be added into the risk assessment matrix based on its probability and effect, using the mapping from the preceding risk evaluation matrix table. Each probable danger is put into parameters in the identity risk assessment matrix table according to the probability and effect criteria established before. Then, after entering all possible hazards into the risk assessment matrix in tables 6, the 18 potential risks are classified as high, medium, or low risk based on probability and impact criteria.

The results of the risk evaluation process can be seen in table 7, which is from 18 possible 17 (Earthquake, Flooding, Thunder, Heavy Wind, Landslide, Hurricane, Lack of competence and knowledge, Human error, Limited number of operators, No job description, Absent (Lazinesss) , Server down, Power outage, Inadequate computers, System maintenance, Restriction access, LAN connection down) which is included in the medium level of risk. Whereas, 1 risk namely unstable network which is included in the high level of risk. Furthermore, the results of ISO 31000 will be used as a reference for the House of Risk (HOR) process. Where, for the severity value on the HOR, the impact value in table 5 is the source for calculating the HOR1.
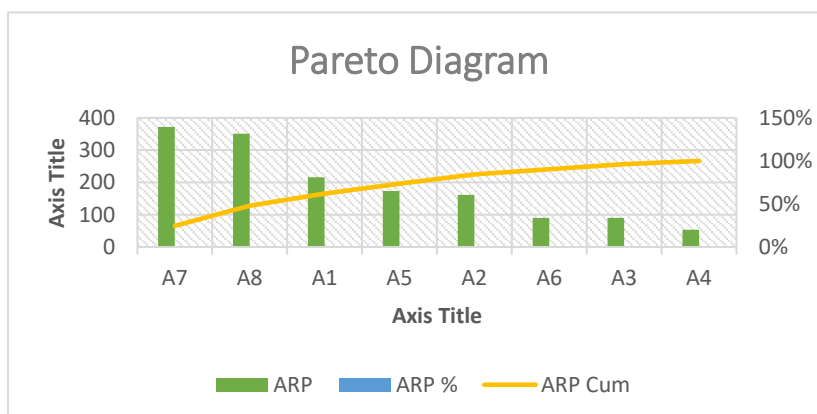

Figure 2. Diagram Pareto

The Aggregate Risk Potential (ARP) value for each risk source may be determined from the calculation results at the HOR1 stage (Table 5). The greatest value is at risk with code A7 (Unstable connection), followed by A8 (lack of system infrastructure); A5 (inadequate equipment); A9 (inactive role of NGOs, research institutions, and universities); and A1 (low active involvement of NGOs, research institutions, and universities) (Geographical location). As seen in Figure 2, these four dangers account for 74% of the risks associated with the usage of the SIAK application in Western Seram Regency (Table 8). The HOR2 stage of the (HOR) strategy focuses on identifying financially feasible measures and committed to being done to address increasing supply chain risk sources (Pujawan and Geraldin, 2009). The HOR2 calculation findings in Table 9 and Table 11 indicate that the most cost-effective and efficient risk reduction approach is PA1 in this scenario is to construct a specific chamber resistant to natural catastrophes for the storage of critical equipment, followed by PA4 which is to collaborate with internet providers to ensure the stability of internet connections and networks.

Table 8. HOR1

Risk Categorize	Risk Events	A1	A2	A3	A4	A5	A6	A7	A8	Severity of Risk Events	Value
Nature	R001	3								S1	5
	R002	3								S2	5
	R003	6								S3	4
	R004	6								S4	4
	R005	3								S5	5
	R006	3								S6	5
Human Factor	R007		9							S7	4
	R008									S8	4
	R009		6							S9	3
	R010			9						S10	3
	R011			6		6				S11	3
System and Infrastructure	R012					6				S12	4
	R013					9	9			S13	5
	R014				9			6		S14	3
	R015								6	S15	3
	R016								6	S16	4
	R017							9	6	S17	5
	R018							6	9	S18	5
Occurrence		2	3	2	2	2	3	4	3		
ARP		216	162	90	54	174	135	372	351		
Priority rank of agent		3	5	7	8	4	6	1	2		

Table 9. Preventive actions

Code	. Preventive actions
PA1	Build a designated room that is resistant to natural disasters to place crucial equipment
PA2	Procurement of supporting devices that have reliable specifications
PA3	Installing a connection that is far from the possibility of force majeure
PA4	Cooperating with internet providers so that internet and network connections can be stable

Table 10. Risk Agents

Code	Risk Agents	Occurrence
A1	Geographical location	2
A2	Lack of adequate human resources	3
A3	Insufficient management and organization	2
A4	Inadequate infrastructure	2
A5	Insufficient equipment	2
A6	Unstable power sources	3
A7	Unstable connection	4
A8	Lack of system infrastructure	3

Table 11. Table HOR2

	Risk Agent	PA1	PA2	PA3	PA4	ARP	
A8	Lack of system infrastructure	6	6		6	351	ARP8
A1	Geographical location	9		9	6	216	ARP1
A7	Unstable connection	9	6	9	6	372	ARP7
A5	Insufficient equipment		9		6	174	ARP5
TE	Total effectiveness of proactive action	7398	5904	5292	6678		
D	Difficulty performing action	3	5	4	3		
ETD	Effectiveness to difficulty ratio of action	2.466	1.181	1.323	2.226		
R	Rank of proactive action	1	3	4	2		

CONCLUSIONS AND SUGGESTION

Users may rely on information technology apps to help them solve several problems, as well as an inescapable need. Procedures and standards are adhered to in the Population Administration Information System (SIAK), which is a web-based system. For the sake of administrative order and to help Regional Government officials, those at the Population and Civil Registration Office in Western Seram Regency, it has been designed to organise the administrative system in the population field. It is important to assess possible risks and develop mitigation steps that may be taken to minimise them, given the application's crucial role in producing area demographic information. The House of Risk (HOR) technique was used in the research to identify possible risks that may be reduced using ISO 31000. This study found that the unstable network poses a serious threat, putting it in the "high" hazard category.

Construction of infrastructure and facilities to handle large volumes of data fast, including computers, operators, and their associated equipment, as well as the SIAK Server and e-KTP Recording and Printing Equipment. In conjunction with Telkom, for the internet network. This infrastructure affects not only the performance of operators, but also the level of happiness in the surrounding community. Organizers and implementation agencies may work together as a single unit to handle population administration data with the help of SIAK, which is an information system that makes use of modern information and communication technology. Service beneficiaries, in this context, are the focus of the Population Administration Information System's administration. This system's success or failure is directly tied to how well users perceive the advantages they get because of SIAK. Ensuring that data and information about the outcomes of population registration and civil registration on a national and regional scale are accurate, complete, current, and easily accessible; realising systemically exchanged data through a single identifying system while guaranteeing confidentiality.

REFERENCES

Aprianto, K., Endroyono, E., & Nugroho, S. M. S. (2021). Analisis Manajemen Risiko SPBE Menggunakan COBIT 5 For Risk dan ISO 31000: 2018 di Kabupaten Magetan (E-Government Risk Management Analysis Using COBIT 5 For Risk and ISO 31000: 2018 in Magetan Regency). JURNAL IPTEKKOM (Jurnal Ilmu Pengetahuan & Teknologi Informasi), 23(2), 107-122.

Asmarawati, S. G., & Pangeran, P. (2021). ISO 31000-Based Risk Management and Balanced Scorecard to Improve Company Performance: A Case Study at Indonsian YNK Tour and Travel Company. International Journal of Multicultural and Multireligious Understanding, 8(3), 376-388.

Ayuningtyas, M., & Tanaem, P. F. (2022). Information Technology Asset Security Risk Management at the Secretariat of the Salatiga City DPRD Using ISO 31000. Journal of Information Systems and Informatics, 4(1), 92-105.

Butarbutar, N., & Tanaamah, A. R. (2021). Analisis Manajemen Risiko Menggunakan COBIT 5 Domain APO12 (Studi Kasus: Yayasan Bina Darma). Journal of Information Systems and Informatics, 3(3), 352-362.

Christian, H. C., & Sitokdana, M. N. (2022). Analisis Risiko Teknologi Informasi pada BANK ABC Menggunakan Framework ISO 31000. JATISI (Jurnal Teknik Informatika dan Sistem Informasi), 9(1), 745-755.

Dwiyanto, Agus. 2010. Manajemen Pelayanan Publik: Peduli, Inklusif, dan Kolaboratif. Yogyakarta: Gadjah Mada University Press.

Hardianto, F. A., & Dharmawan, Y. S. (2021). Manajemen Risiko TI ISO 31000 Dengan Cobit 5 Dan FMEA (PT. XYZ). Jurnal SITECH: Sistem Informasi dan Teknologi, 4(2), 133-146.

Ikhsan, H. M., & Eko Setiawan, S. T. (2021). Upaya Mitigasi Kebencanaan Di Kabupaten Sragen, Indonesia Dengan Menggunakan Pendekatan Quantitative Risk Assessment Dan House Of Risk Fase 2 (Doctoral dissertation, Universitas Muhammadiyah Surakarta).

Munarja, M. T. (n.d.). Pemanfaatan Data Siak Dalam Layanan Data Dan Informasi Administrasi Kependudukan di Kabupaten Gunungkidul. Dukcapil Gunungkidul. Retrieved April 17, 2022, from https://dukcapil.gunungkidulkab.go.id/2014/06/18/pemanfaatan-data-siak-dalam-layanan-data-dan-informasi-administrasi-kependudukan-di-kabupaten-gunungkidul/

Manuputty, G. P., Azis, A. A., & Pratami, N. A. N. (2022). Analisis Manajemen Risiko Berbasis Iso 31000 Pada Aspek Operasional Teknologi Informasi PT. Schlumberger Geophysics Nusantara. E-Prosiding Akuntansi, 3(1).

Monica, E. G., & Pangeran, P. (2020). The Integration of Balanced Scorecard and ISO 31.000 Based Enterprise Risk Management Process to Mitigate Supply Chain Risk: Case Study at PT Anugerah Bintang Meditama. International Journal of Multicultural and Multireligious Understanding, 7(10), 616-628.

Munawir, H., Astuti, F. T., Setiawan, E., & Sufa, M. F. (2021). Mitigation of Halal Risk in the Production Process of Processing Beef Using the FMEA Method in UMKM Dendeng Sapi Asri. Warta LPM, 24(4), 779-787.

Nugroho, R. L., & Pangeran, P. (2021). Application of ISO 31000-Based Risk Assessment to Improve Balanced Scorecard Performance at Shofa Pharmacy. International Journal of Multicultural and Multireligious Understanding, 8(2), 251-263.

Nuris, A. M., Maharani, A., & Rachmadita, R. N. (2021). Analisis Risiko Proyek Pengembangan Perangkat Lunak Menggunakan Kerangka Kerja ISO 31000. Jurnal Metris, 22(02), 73-81.

Pribadi, H. I., & Ernastuti, E. (2020). Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000: 2018 Dengan FMEA (Studi Kasus PT Pertamina). JSINBIS (Jurnal Sistem Informasi Bisnis), 10(1), 28-35.

Pujawan, I. N., & Geraldin, L. H. (2009). House of risk: a model for proactive supply chain risk management. Business Process Management Journal.

Purwaningsih, R., Ibrahim, C. N., & Susanto, N. (2021). Analisis Dan Mitigasi Risiko Rantai Pasok Pada Pengadaan Material Produksi Dengan Model House of Risk (Hor) Pada Industri Pulp. MIX: Jurnal Ilmiah Manajemen, 11(01), 349337.

Putri, A. A., & Syafi'i, D. I. I. (2022). Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi Kasus: Aplikasi J&T Express Indonesia). Aisyah Journal Of Informatics and Electrical Engineering, 4(1), 1-9.

Safitri, R., & Pangeran, P. (2020). Balanced Scorecard and ISO 31000, Risk Management Integration to Improve Performance: Case Study at Indonesian Credit Union. International Journal of Multicultural and Multireligious Understanding, 7(6), 527-538.

Utomo, W. S. T., & Eko Setiawan, S. T. (2021). Mitigasi Bencana Banjir Di Kota Surakarta Dengan Metode House Of Risk (HOR)(Studi Kasus: Kota Surakarta) (Doctoral dissertation, Universitas Muhammadiyah Surakarta).