American Journal of Computer Science and Technology
2022; 5(3): 170-177
http://www.sciencepublishinggroup.com/j/ajcst
doi: 10.11648/j.ajcst.20220503.13
ISSN: 2640-0111 (Print); ISSN: 2640-012X (Online)

Risk Management Information Technology Based on ISO 31000:2018 at Institute of Philosophy and Creative Technology, Ledalero

Maria Florentina Rumba[1, *], Robertus Mirsel[1], Fransiskus Xaverius Sabu[2]

[1]Philosophy Faculty, Institute of Philosophy and Creative Technology, Ledalero, Indonesia

[2]Library Bureau, Institute of Philosophy and Creative Technology, Ledalero, Indonesia

Email address:

floreleydodemand@gmail.com (M. F. Rumba)

[*]Corresponding author

To cite this article:

Maria Florentina Rumba, Robertus Mirsel, Fransiskus Xaverius Sabu. Risk Management Information Technology Based on ISO 31000:2018 at Institute of Philosophy and Creative Technology, Ledalero. *American Journal of Computer Science and Technology*. Vol. 5, No. 3, 2022, pp. 170-177. doi: 10.11648/j.ajcst.20220503.13

Received: July 6, 2022; **Accepted**: July 29, 2022; **Published**: August 5, 2022

Abstract: Risk is defined as a state of uncertainty, where an undesirable situation occurs and causes a loss for an agency. Therefore, risks need to be managed properly. Risk management is all activities to manage risks or threats that can occur in an agency. One of the standard risk management tools is the ISO 31000:2018. There have been many studies that present how to analyze IT risk management in an agency using the ISO 31000:2018 framework with various methods. From the many articles on risk management in an institution or organization, this framework becomes a reference for analyzing IT risk management in higher education institutions. This research is a case study conducted at the Institute of Philosophy and Creative Technology (IPCT) at Ledalero. The IT risk management analysis work process used is ISO 31000:2018. The methods used in this study were interviews given to the head of the IT division, direct observation, and an open questionnaire given to all work units at IPCT. The purpose of this research is to identify IT assets, identify risks and their impacts, analyze, and treatment risks. The results of this study indicate that the risk impact of 28 elements which is the elaboration of 3 main factors, namely 2 elements are in the Low-Medium category with a scale (0.36-0.42), 5 elements are included in the Medium-Low category with a scale range (0.25-0.34), 7 elements are included in the Minimum-Low category with a scale range ((0.00-0.14), and the most are in the Low-Low category with a scale range (0.15-0.24) which is as many as 14 elements.

Keywords: Risk Management, Information Technology, ISO 31000:2018

1. Introduction

Besides making a higher education institution able to compete, the application of Information Technology is mainly aimed at supporting teaching and learning activities at the institution. As one of the private higher education institution Institute of Philosophy and Creative Technology (IPCT) at Ledalero has utilized information technology/information system (IT/IS) in supporting the operational performance of the institution. Information technology is defined as computers and office equipment that collect and process information [1]. To evolve over time, companies need to automate business processes, apply advanced information technology and appropriate new management methods [2]. With the use of IT, it is necessary and important to pay attention to the risks causing negative impacts.

Risk, the root cause of dangerous incidents, is a combination of the probability of occurrence of harm as well as the severity of that harm [3-6]. As expressed by S. V. Aleksandrova, V. A. Vasiliev, and M. N. Aleksandrov [7], one of the key changes in the ISO standards of the new generation is the introduction of a systematic approach to risk. As every activity involves risks at any level, organizations of all sectors and sizes would rather manage hem in order to set better strategies and make proper decisions [8].

Risk management is part of this key challenge and is linked to many domains for IT and non-IT issues [9]. In the context of

scientific and professional research several processes have also been introduced for risk management from various disciplines and industrial sectors [10]. ISO 31000:2018 is one of the standard risk management tools. ISO 31000:2018 consists of risk management principles, risk management frameworks and processes that have been adopted by many countries and national risk management standards. As quoted from Aniskina and Sorokin, that risk management is an iterative process and helps organizations to determine a strategy, achieve goals and make decisions based on a risk assessment and standard ISO 31000:2018 [11]. Risk management is part of process management so that the agency or institution has a deeper view of risk. Risk management, however, is a complex function facing multiple challenges [12]. The goal of the risk management is to increase the probability and reach of the potential positive events [13]. The objective of IT risk management is to protect Information Technology assets such as data, hardware, software, personnel and facilities from all external (e.g., natural disasters) and internal (e.g., technical failures or unauthorized access) threats so that the costs of losses resulting from the realization of such threats are minimized [14].

The purpose of risk management is to protect and create value [15]. What risks should be managed? [16]. Many studies have reviewed about managing risk in institutions or companies using process management based on ISO 31000:2018, among others are Wicaksono's "Applying ISO:31000:2018 as Risk Management Strategy on Heavy Machinery Vehicle Division" [17]; Urbanek, Adamec, Schullerova, and Kohoutek's work ""Risk identification of implementation of ITS to real traffic" [18]; Intelligent Information System using What If analysis based on ISO 31000:2018; Rampini, Takia, and Berssaneti's "Critical success factors of risk management with the advent of ISO 31000 2018 - Descriptive and content analyzes" [19]; de Oliveira, Marins, Rocha, and Salomon's work "The ISO 31000 standard in supply chain risk management" [20]; and Syahputri and Kitri's "Enterprise Risk Management Analysis of Group XYZ Based on ISO 31000:2018 Framework" [21]. Another work in risk management is Gutandjala, A. Gui, S. Maryam, and V. Mariani's article "Information System Risk Assessment and Management (Study Case at XYZ University)" [22]; Parviainen's et al. "Implementing Bayesian networks for ISO 31000:2018-based maritime oil spill risk management: State-of-art, implementation benefits and challenges, and future research directions" [23], that can support decision-making processes when risks are complex and data is scarce; and Kapsa's "Risk management in biogas plants based on new norm ISO 31000:2018" [24], which suggests the integration of SQuaRE measurement framework with the ISO 31000 process with the goal of evaluating balance and completeness in a dataset as risk factors of discriminatory outputs of software systems.

This study analyzes information technology risk management in a higher education institution. As expressed by Rosado, Moreno, Sánchez, Santos-Olmo, Serrano, and Fernández-Medina [25], that organizations, regardless of their size, must be aware of the importance of the IT risks and how they should be managed. The conducted research shows that the level of IT risk is constantly growing [26]. Therefore, it is important to do this. The purpose of this study was to analyze information technology risk management in tertiary institutions with a case study at the IPCT. To produce an appropriate risk evaluation report, the following questions will serve as a reference in analyzing risk management, namely what is risk management, why risk management exists, how to identify, analyze and assess risk, and how to handle or control risk. Currently IPCT has not used certain standards in dealing with problems/risks that may arise from internal or external factors. The results of the research can be used as a reference for handling and or minimizing the risks or threats that may arise. Therefore, this research is important to find out how to manage risk using the ISO 31000:2018 framework.

2. Method

2.1. Case Selection

From several studies, it shows that there are not many studies on the analysis of information technology risk management in universities. Universities are higher education institutions that should have adequate information technology infrastructure. Apart from being a means of supporting academic activities, it also shows the quality of a higher education institution. With the right management of information technology, it can provide value that leads to a competitive advantage for universities to be able to compete with other universities. One aspect of information technology management is risk management that can arise at any time. Risk management is important so that the information technology division has certain references or standards to be able to identify risks and their impacts. The goal is to minimize the impact of the risks that may arise. In that way, the IT division will be better able to deal with every possible risk, handle risks, and in the end business processes in universities continue to run optimally as they should be.

2.2. Data Collection

This research is quantitative research. It's phase begins with data collection which is carried out through interviews, observations, and questionnaires. Interviews were conducted with the head of the IT division to find out the rules or SOPs used as a reference in information technology governance. Observations were made to observe directly the information technology infrastructure and information systems used. Questionnaires are used to collect relevant information and confirm how to manage risks and impacts that may arise.

2.2.1. Information Technology Risk Management Process in Higher Education

This risk management process carried out in this study is based on the ISO 31000:2018 risk management process as shown in Figure 1.

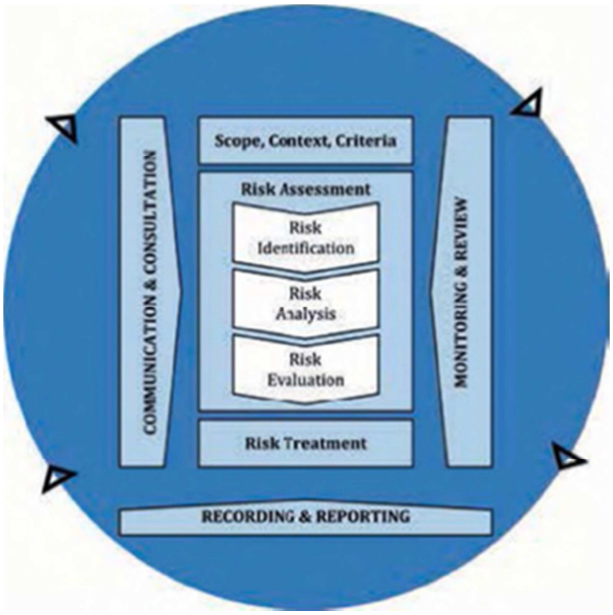

Figure 1. *ISO 31000:2018 Risk Management Process [27].*

According to Ramly and Osman [28], the main purpose of risk assessment is to determine whether the risk level is acceptable according to risk appetite. Risk level is commonly determined through the combination of consequences and likelihood.

2.2.2. Risk Identification

Risk analysis is a process of identifying, evaluating, and prioritizing risk using a series of models and theories [29]. Stoneburner, Goguen, and Feringa [30], explain that identifying risk for an IT system requires a keen understanding of the system's processing environment. The person or persons who conduct the risk assessment must therefore first collect system-related information, which is usually classified as follows: hardware, software, system interfaces (internal and external connectivity), data and information, persons who support and use the IT system, system mission, system and data criticality (e.g., the system's value or importance to an organization), and system and data sensitivity. Analysis is carried out on risks originating from the external and internal environment [31].

Risk identification in this study refers to Stoneburner, Goguen, and Feringa, who explain that risk threats can be seen from 3 aspects, namely natural aspects such as earthquakes, floods, tornadoes, and landslides; human aspects such as hackers, crackers, computer criminals, terrorists, industrial espionage, and institutional internal factors; and environmental aspects such as long term system failure, and pollution [30]. For this study, we included 28 risk probabilities with details of 4 elements from natural factors (R1, R2, R3, R4), 6 elements from human factors (R5, R6, R7, R8, R9, R10), and 17 elements from environmental factors.

2.2.3. Risk Analysis

Risk analysis of the nature and characteristics of risk, includes the level of risk, sources of risk, the likelihood of consequences, events, scenarios, controls, and their effectiveness [32]. A risk analysis aims to determine the relationship between possible risks and their impacts. The mapping of possible risks and impacts used as a reference in this research are Author, Hallows, Wideman, and A. Jolyon's work, "Information Systems Project Management, Second Edition How to Deliver Function and Value in Information Technology Projects" [33] and Elzamly and Hussin's article "An enhancement of framework software risk management methodology for successful software development" [34], as shown in Table 1. The three possibilities and their scale are also confirmed by V. Burkov, I. Burkova, S. Barkalov, and T. Averina [35] that the most popular is a three-point scale (low, medium, high risk).

Based on the Table 1 below, in this study we grouped the risk into 3 categories: Low with a value range of 0.00 – 0.34; Medium category with a value range of 0.35 – 0.70; and the High category with a value range of 0.71 – 1.00.

Table 1. *Categorization Of Degree of Risk.*

Range	Probability	Impact		
		High	Medium	Low
0,7-1,0	High	Extreme	High	Medium
0,3-0,7	Medium	High	Medium	Low
0,0-0,3	Low	Medium	Low	Minimal

2.2.4. Risk Evaluation

The risk assessment step aims to support decision making based on the results of risk analysis [36]. In this study, a risk evaluation was carried out to determine the impact of the risk. The results of the evaluation will provide an overview of how big the impact of the risks/threats posed, which will become a reference in determining which are the priorities to be handled.

2.2.5. Risk Treatment

J. Masso, F. J. Pino, C. Pardo, F. García, and M. Piattini [37] and I. Lavrnić, A. Bašić, and D. Viduka [38] explained that this process is meant to remove the risk, or to change the probability and/or its consequences. In this study, the evaluation results serve as a guide in determining whether the impact of the risk requires handling or mitigation. According to B. Barafort, A. L. Mesquida, and A. Mas, the purpose of risk evaluation is to support decisions [9].

3. Result and Discussion

3.1. Result

As an institution that manages higher education, to support academic activities, each work unit/bureau of IPCT is equipped with information technology devices (computer sets, printers, scanners, web cams, and CCTV), which are supported by adequate internet network infrastructure. In addition to hardware assets, IPCT has software assets which are divided into 2 groups, namely content management system (CMS) based software and learning management system (LMS) based software. The data from all these applications are connected and stored in storage media on the server computer.

The analysis is carried out to measure whether the impact hampers the operational activities of academics, or causes financial losses to the institution. The results of the analysis become a benchmark in determining the level of risk: whether the risk is potentially Low, Medium, or High, according to the values listed in table 1.

Table 2. *Risk Likelihood.*

Risk Code	Likelihood	
	Statement	**Score**
R1	An earthquake occurred	0.56
R2	The occurrence of floods and landslides	0,34
R3	A hurricane occurs	0.46
R4	Occur fire	0.44
R5	Hacking, Social engineering, system intrusion, break-ins, or Unauthorized System Access	0.61
R6	Computer Crime occurs (cyber stalking), fraudulent act (impersonation and interception), Information bribery, Spoofing, and system intrusion.	0.54
R7	Bom/terrorism occurs, attacks on systems (e.g. denial of service or service blocking), and system disruptions.	0.40
R8	Economic exploitation, information theft, social engineering, unauthorized system access (such as access to confidential, proprietary, and/or technology-related information)	0.49
R9	Vandalism	0.41
R10	Former Employees still have access to the system	0.19
R11	Back up Failure	0.32
R12	Technology is not uptodate	0.38
R13	Server down	0.36
R14	CCTV is not working properly	0.25
R15	Unscheduled maintenance	0.42
R16	Web Service not working suddenly	0.32
R17	System Overcapacity	0.34
R18	Data Corupt	0.41
R19	Overheat	0.41
R20	Network connection lost	0.60
R21	Company information data leak	0.25
R22	Virus Attack	0.46
R23	Incomplete program documentation	0.37
R24	Program not completed on time	0.41
R25	Genset not working well	0.61
R26	The program does not meet the needs	0.27
R27	Human Error	0.53
R28	The occurrence of environmental pollution due to electronic waste	0.35

Table 3. *Risk Impact.*

Risk	Impact	
Code	**Statement**	**Score**
R1	Resulting in damage to infrastructure and school facilities and infrastructure, loss of institutional data	0.48
R2	Resulting in damage to the infrastructure of the institution's facilities and infrastructure, loss of systems and data.	0.51
R3	Resulting in damage to infrastructure, institutional infrastructure, delays in communication and academic services.	0.49
R4	Resulting in damage to infrastructure, school infrastructure, loss of school data.	0.50
R5	Resulting in hacking or burglary of institutional data and information by other parties	0.58
R6	Resulting in the burglary of data and information and the system is taken over by unauthorized parties	0.54
R7	As a result, the system cannot be accessed, the system is blocked, or communication and internet connection are cut off	0.54
R8	Which results in financial losses for the Institution	0.43
R9	Resulting in damage and financial loss to the institution	0.45
R10	Resulting in the institution's data and information being accessed by unauthorized parties	0.50
R11	Resulting in Failure to access the server and the cessation of system operation	0.40
R12	As a result, the Institution does not develop and does not follow technological trends, consumer interest is reduced, and there is no competitive advantage offered	0.41
R13	Resulting in the system on the server being an error / unable to run properly	0.36
R14	Resulting in a reduced level of security and less effective monitoring of work processes	0.47
R15	Resulting in frequent errors in applications and weakening the capacity of personal computers	0.51
R16	Resulting in possible loss of data from the system connected to the server	0.43
R17	Resulting in server performance slowing down and the system unable to accommodate new data	0.44
R18	Experiencing data loss	0.51
R19	Resulting in less than optimal hardware performance, due to hardware damage that must endure continuous hot temperatures	0.55
R20	The network connection is lost and communication is hampered so that the activities of the bureau/work unit connected to the server are disrupted	0.50
R21	There was a leak of company information data which resulted in a lot of important data about the Institution being lost and causing financial losses	0.35
R22	A virus or trojan attack occurs which causes system damage	0.54

Risk Code	Impact Statement	Score
R23	Incomplete program documentation which makes it difficult to deal with errors	0.55
R24	The purchased program was not completed on time so that the Institution lost financially?	0.41
R25	The generator is not functioning properly which paralyzes the activities of the Institution	0.70
R26	The program purchased is not in accordance with the needs which results in financial losses for the Institution	0.45
R27	Errors made by staff that resulted in academic administrative services not running optimally	0.60
R28	Resulting in changes in the environmental ecosystem	0.49

In this study, we grouped the level of possible risk and impact into 3 categories, namely Low with a value range of 0.00 – 0.34, the Medium category with a value range of 0.35 – 0.70, and the High category with a value range of 0.71 – 1.00. The results of data processing show that there are 8 risks in the Low category, namely R2, R10, R11, R14, R16, R17, R21, and R26; 20 risks fall into the Medium category, namely R1, R3, R4, R5, R6, R7, R8, R9, R12, R13, R15, R18, R19, R20, R22, R23, R24, R25, R27, R28. And there is no risk that falls into the High category. Meanwhile, the impact measurement results show that all impacts are at the Medium level. This means that risks or threats may occur and the impacts are still in the moderate category. To evaluate the impact of the risks, it is necessary to evaluate using the following formula:

$$\text{Risk Impact} = \text{Likelihood} \times \text{Consequence} \quad (1)$$

This is done so that it will be easy to determine whether from the results of the evaluation risk treatment or risk mitigation will be carried out. From the calculation results, it is found that the impact ranges are categorized as follows: Extreme-High (0.91-1.00); High-High (0.81-0.90); Medium-High (0.71-0.80); High-Medium (0.61-0.70); Medium-Medium (0.51-0.60); Low-Medium (0.35-0.50); Medium-Low (0.25-0.34); Low-Low (0.15-0.24); and Minimum-Low (0.00-0.14). Over all the evaluation results are shown in table 4.

Table 4. *Risk Evaluation.*

Prob. Range	Prob.	Impact		
		High	Medium	Low
0.71-1.00	High	Extreme 0.91-1.00)	High (0.61-0.70)	Medium (0.25-0.34) R1 (0.27); R6 (0.27); R20 (0.30); R22 (0.25); R27 (0.32).
0.35-0.70	Medium	High (0.81-0.90)	Medium (0.51-0.60)	Low (0.15-0.24) R2 (0.17); R3 (0.23); R4 (0.22); R7 (0.21); R8 (0.21); R9 (0.18); R12 (0.16); R15 (0.22); R17 (0.18); R18 (0.21); R19 (0.23); R23 (0.20); R24 (0.17); R28 (0.17).
0.00-0.34	Low	Medium (0.71-0.80)	Low (0.35-0.50) R5 (0.36); R25 (0.42).	Minimal (0.00-0.14) R10 (0.09); R11 (0.13); R13 (0.13); R14 (0.12); R16 (0.14); R21 (0.08); R26 (0.12).

The evaluation results show that the risk impact is only at 4 levels as follows:

1) Low-Medium Risk Impact Category

Data in Table 3 shows that two elements could be included in this category, namely: first, the possibility of hacking, social engineering, system intrusion, break-ins, or unauthorized system access with the impact of causing hacking or burglary of institutional data and information by other parties. These risks/threats are caused by human factors. Second, it is possible that the generator set is not functioning properly with the impact of crippling the activities of the Institute. This risk/threat is also caused by human factor.

2) Medium-Low Risk Impact Category

Table 3 also shows that there are 5 elements that could be categorized as Medium-Low Risk Impact, namely: 1). The possibility of earthquake occurrence that may cause damage to infrastructure and school facilities and infrastructure, and the loss of institutional data. This risk/threat is caused by nature. 2). Possible risks of computer crime (such as cyber stalking), fraudulent acts (such as impersonation and interception), information bribery, spoofing, and system intrusion, which have an impact on data and information burglary, and the system taken over by unauthorized parties. This risk/threat is caused by humans. 3). Possible risk of network connection loss which results in communication delays and the disruption of the activities of the bureau/work unit connected to the server. 4). Possible risk of virus or trojan attack causing system damage. 5). Risk of human errors or errors made by staff which results in academic administrative services not running optimally. This risk/threat is caused by the internal environment of the Institution. Elements 3, 4, 5 are caused by internal factors of the Institution.

3) Low-Low Risk Impact Category

There are 14 elements in the low-Low Risk Impact category, namely: 1). threats/risks caused by natural factors, such as floods, landslides, tornadoes, and fires, which can cause damage to school facilities and infrastructure, loss of systems and data, and delays in communication and academic services. 2). Threats/risks caused by both external and internal human factors, such as bomb/terrorist attacks, attacks on system (including denial of service or service blocking), system disturbances, economic exploitation, information theft, social engineering, unauthorized system access (such as access to confidential, proprietary, and/or technology-related information), vandalism, (which results in the inaccessibility of a system), blocked system, or the interruption of communication and internet connection being, as well as financial damage and loss to the Institution. 3). Threats/risks caused by internal factors of the Institution, both infrastructure and systems. These include out-of-date technology,

unscheduled maintenance, overcapacity, data corruption, overheating, incomplete program documentation, program not completed on time, and environmental pollution due to electronic waste.

4) Minimal-Low Risk Impact Category

Table 3 shows that there are 7 elements of risk in this category, including former employees still having access to the system, back up failure, server down, CCTV malfunction, web service shutting down suddenly, company information data leak, and programs not in accordance with needs. The source of threats/risks from these elements is the Institution's internal environmental factors.

Overall, it is concluded that the probability of risk occurring is at a moderate level with a value range of 0.35 – 0.70, and the risk impact is in the Low category. Thus, until now IPCT, especially the IT division, has been able to manage IT/IS properly.

3.2. Discussion

The previous studies on risk management based on ISO 31000:2018 [39] have viewed risk from the strategic, operational, financial, compliance, reputational, innovation, as well as environmental aspects, along with the risk factors and their impacts. Risk evaluation uses scale range from 1 to 5. Level 1 is categorized as "very light", which means: risk does not lead to noticeable consequences); Level 2 is categorized as "light" which means the consequences of risk are minor, but its appearance has a negative impact on the consumer); Level 3 is "average" which means the risk leads to a marked decrease in the effectiveness of the organization); level 4 is "significant", which means risk leads to the impossibility of the organization to perform its functions; and Level 5 is "critical" which means risk poses a threat to people's lives and health.

Gutandjala et al. [22] identify risks that impact the areas of reputation and customer confidence, finance, productivity, safety and health, and fines and legal penalties with 3 risk impact measurement scales used --Low, Moderate, and High. Meanwhile, Syihabuddin, Suryanto, and Salman in their article "Risk Management in Data Centers Using ISO 31000 Case Study : XYZ Agency", classify risks as "rare risks": <50%; "impossible to happen": 5% - <20%; "moderate chance of occurrence": 20% - <50%; "maybe": 50% - 80%; and "almost certain to happen: 80% - <100%." [40]. Risks are grouped into 10 risks that have impacts on the operational and security sectors.

4. Conclusion and Recommendation

4.1. Conclusion

IPCT is one of the Catholic Colleges located in Sikka Regency, Flores, East Nusa Tenggara. In terms of implementing IT/IS, IPCT has not yet implemented certain standards in managing risk. This research is a case study of this Institute. The results of this study indicate that the risk impact of 28 elements which is the elaboration of 3 main factors, namely 2 elements in the Low-Medium category with a scale (0.36-0.42), 5 elements in the Medium-Low category with a scale range (0.25-0.34), 7 elements in the Minimal-Low category with a scale range (0.00-0.14), and the rest in the Low-Low category with a scale range (0.15-0.24) which is as many as 14 elements. The results of this study become a reference for institutions, especially staff in the IPCT's IT/IS division to understand the importance of recognizing possible risks or threats and their respective impacts, and become more professional in managing risks. To support all business processes, risks to information technology must be managed wisely and should be an integral part of the management of the institution.

4.2. Recommendation

Based on the conclusions above, this study recommends that the staff of the IT/IS division of IPCT need to understand risk possibilities and their impacts and apply risk management system in their daily operation. Furthermore, though this study found that risk possibilities and risks impacts were between low and medium levels, however, it is important to keep them at most at moderate level, if not at low level by identifying which of the human, natural and environmental factors are more likely to occur and increase risk possibility and impacts.

References

[1] D. Deng, "Risk Perception and Acceptance of Information Technology Application Based on Numerical Simulation," Proc. - 2016 Int. Conf. Smart City Syst. Eng. ICSCSE 2016, pp. 277–280, 2017, doi: 10.1109/ICSCSE.2016.0081.

[2] S. A. Grishaeva and V. I. Borzov, "Information security risk management," Proc. 2020 IEEE Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol. IT QM IS 2020, pp. 96–98, 2020, doi: 10.1109/ITQMIS51053.2020.9322901.

[3] X. Wang, J. Xu, M. Zheng, and L. Zhang, "Aviation Risk Analysis: U-bowtie Model Based on Chance Theory," IEEE Access, vol. 7, pp. 86664–86677, 2019, doi: 10.1109/ACCESS.2019.2926210.

[4] G. Xie, G. Zeng, Y. Liu, J. Zhou, R. Li, and K. Li, "Fast Functional Safety Verification for Distributed Automotive Applications during Early Design Phase," IEEE Trans. Ind. Electron., vol. 65, no. 5, pp. 4378–4391, 2018, doi: 10.1109/TIE.2017.2762621.

[5] G. Xie et al., "Reliability enhancement toward functional safety goal assurance in energy-aware automotive cyber-physical systems," IEEE Trans. Ind. Informatics, vol. 14, no. 12, pp. 5447–5462, 2018, doi: 10.1109/TII.2018.2854762.

[6] T. J. Leung and J. Rife, "Refining fault trees using aviation definitions for consequence severity," IEEE Aerosp. Electron. Syst. Mag., vol. 32, no. 3, pp. 4–14, 2017, doi: 10.1109/MAES.2017.150171.

[7] S. V. Aleksandrova, V. A. Vasiliev, and M. N. Aleksandrov, "Information systems and technologies in quality management," Proc. 2020 IEEE Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol. IT QM IS 2020, pp. 173–175, 2020, doi: 10.1109/ITQMIS51053.2020.9322959.

[8] E. Lima, A. L. Lorena, and A. P. Costa, "Structuring the Asset Management Based on ISO 55001 and ISO 31000: Where to Start," Proc. - 2018 IEEE Int. Conf. Syst. Man, Cybern. SMC 2018, pp. 3094–3099, 2019, doi: 10.1109/SMC.2018.00524.

[9] B. Barafort, A. L. Mesquida, and A. Mas, "ISO 31000-based integrated risk management process assessment model for IT organizations," J. Softw. Evol. Process, vol. 31, no. 1, pp. 1–15, 2019, doi: 10.1002/smr.1984.

[10] V. Laine, F. Goerlandt, O. V. Banda, M. Baldauf, Y. Koldenhof, and J. Rytkönen, "A risk management framework for maritime Pollution Preparedness and Response: Concepts, processes and tools," Mar. Pollut. Bull., vol. 171, no. July, 2021, doi: 10.1016/j.marpolbul.2021.112724.

[11] N. N. Aniskina and A. V. Sorokin, "Risk management in running erp-based process model of integrated group of companies," Proc. 2020 IEEE Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol. IT QM IS 2020, no. Figure 1, pp. 180–183, 2020, doi: 10.1109/ITQMIS51053.2020.9322891.

[12] O. Rodríguez-Espíndola, S. Chowdhury, P. K. Dey, P. Albores, and A. Emrouznejad, "Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing," Technol. Forecast. Soc. Change, vol. 178, no. February 2021, p. 121562, 2022, doi: 10.1016/j.techfore.2022.121562.

[13] K. Buganová and J. Šimíčková, "Risk management in traditional and agile project management," Transp. Res. Procedia, vol. 40, pp. 986–993, 2019, doi: 10.1016/j.trpro.2019.07.138.

[14] A. Rot, "Enterprise Information Technology," Encycl. Supply Chain Manag., vol. II, pp. 1–7, 2016, doi: 10.1081/e-escm-120050486.

[15] F. A. Alijoyo, "Risk Management Maturity Assessment based on ISO 31000 – A pathway toward the Organization's Resilience and Sustainability Post COVID-19: The Case Study of SOE Company in Indonesia," pp. 125–142, 2021, doi: 10.33422/3rd.icmef.2021.02.134.

[16] I. I. Livshitz, P. A. Lontsikh, N. P. Lontsikh, E. Y. Golovina, and O. M. Safonova, "The effects of cyber-security risks on added value of consulting services for IT-security management systems in holding companies," Proc. 2020 IEEE Int. Conf. "Quality Manag. Transp. Inf. Secur. Inf. Technol. IT QM IS 2020, pp. 119–122, 2020, doi: 10.1109/ITQMIS51053.2020.9322883.

[17] A. Y. Wicaksono, "Applying ISO:31000:2018 as Risk Management Strategy on Heavy Machinery Vehicle Division," Int. J. Sci. Eng. Inf. Technol., vol. 4, no. 2, pp. 198–202, 2020, doi: 10.21107/ijseit.v4i2.6871.

[18] M. Urbanek, V. Adamec, B. Schullerova, and J. Kohoutek, "Risk identification of implementation of ITS to real traffic," Transp. Res. Procedia, vol. 45, no. 2019, pp. 787–794, 2020, doi: 10.1016/j.trpro.2020.02.093.

[19] G. H. S. Rampini, H. Takia, and F. T. Berssaneti, "Critical success factors of risk management with the advent of ISO 31000 2018 - Descriptive and content analyzes," Procedia Manuf., vol. 39, pp. 894–903, 2019, doi: 10.1016/j.promfg.2020.01.400.

[20] U. R. de Oliveira, F. A. S. Marins, H. M. Rocha, and V. A. P. Salomon, "The ISO 31000 standard in supply chain risk management," J. Clean. Prod., vol. 151, pp. 616–633, 2017, doi: 10.1016/j.jclepro.2017.03.054.

[21] H. Y. Syahputri and M. L. Kitri, "Enterprise Risk Management Analysis of Group XYZ Based on ISO 31000:2018 Framework," Asian J. Account. Financ., vol. 2, no. 3, pp. 1–12, 2020, [Online]. Available: http://myjms.moe.gov.my/index.php/ajafin.

[22] I. I. Gutandjala, A. Gui, S. Maryam, and V. Mariani, "Information System Risk Assessment and Management (Study Case at XYZ University)," Proc. 2019 Int. Conf. Inf. Manag. Technol. ICIMTech 2019, vol. 1, no. August, pp. 602–607, 2019, doi: 10.1109/ICIMTech.2019.8843748.

[23] T. Parviainen, F. Goerlandt, I. Helle, P. Haapasaari, and S. Kuikka, "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, no. October 2020, 2021, doi: 10.1016/j.jenvman.2020.111520.

[24] K. Kapsa, "Risk management in biogas plants based on new norm ISO 31000:2018," Transp. Econ. Logist., vol. 77, pp. 59–72, 2018, doi: 10.26881/etil.2018.77.06.

[25] D. G. Rosado, J. Moreno, L. E. Sánchez, A. Santos-Olmo, M. A. Serrano, and E. Fernández-Medina, "MARISMA-BiDa pattern: Integrated risk analysis for big data," Comput. Secur., vol. 102, p. 102155, 2021, doi: 10.1016/j.cose.2020.102155.

[26] T. Królikowski and A. Ubowska, "TISAX - Optimization of IT risk management in the automotive industry," Procedia Comput. Sci., vol. 192, pp. 4259–4268, 2021, doi: 10.1016/j.procs.2021.09.202.

[27] I. R. Management, "A Risk Practitioners Guide to ISO 31000 : 2018," Inst. Risk Manag., p. 20, 2018.

[28] E. F. Ramly and M. S. Osman, "Development of Risk Management Framework - Case Studies," Int. Conf. Ind. Eng. Oper. Manag., no. 2015, pp. 2542–2551, 2018.

[29] P. Jain, H. J. Pasman, S. Waldram, E. N. Pistikopoulos, and M. S. Mannan, "Process Resilience Analysis Framework (PRAF): A systems approach for improved risk and safety management," J. Loss Prev. Process Ind., vol. 53, pp. 61–73, 2018, doi: 10.1016/j.jlp.2017.08.006.

[30] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems Recommendations," Comput. Secur. Div. Inf. Technol. Lab. Natl. Inst. Stand. Technol. Gaithersbg., p. 54, 2002.

[31] H. Chung, S. P. Cho, and Y. Jang, "Standardizations on IT risk analysis service in NGN," Int. Conf. Adv. Commun. Technol. ICACT, pp. 410–413, 2014, doi: 10.1109/ICACT.2014.6778992.

[32] Maniah and S. Milwandhari, "Risk Analysis of Cloud Computing in the Logistics Process," Proceeding - 2020 3rd Int. Conf. Vocat. Educ. Electr. Eng. Strength. Framew. Soc. 5.0 through Innov. Educ. Electr. Eng. Informatics Eng. ICVEE 2020, pp. 3–7, 2020, doi: 10.1109/ICVEE50212.2020.9243247.

[33] B. Author, J. Hallows, M. Wideman, I. Author, A. Jolyon, and A. Jolyon, "Information Systems Project Management, Second Edition How to Deliver Function and Value in Information Technology Projects," Inf. Syst., pp. 1–8, 2007.

[34] A. Elzamly and B. Hussin, "An enhancement of framework software risk management methodology for successful software development," J. Theor. Appl. Inf. Technol., vol. 62, no. 2, pp. 410–423, 2014.

[35] V. Burkov, I. Burkova, S. Barkalov, and T. Averina, "Project Risk Management," Proc. - 2020 2nd Int. Conf. Control Syst. Math. Model. Autom. Energy Effic. SUMMA 2020, pp. 145–148, 2020, doi: 10.1109/SUMMA50634.2020.9280817.

[36] U. R. De Oliveira, L. Aparecida Neto, P. A. F. Abreu, and V. A. Fernandes, "Risk management applied to the reverse logistics of solid waste," J. Clean. Prod., vol. 296, 2021, doi: 10.1016/j.jclepro.2021.126517.

[37] J. Masso, F. J. Pino, C. Pardo, F. García, and M. Piattini, "Risk management in the software life cycle: A systematic literature review," Comput. Stand. Interfaces, vol. 71, no. March 2019, p. 103431, 2020, doi: 10.1016/j.csi.2020.103431.

[38] I. Lavrnić, A. Bašić, and D. Viduka, "Risk assessment of a solar attack according to ISO 31000 standard," Eng. Rev., vol. 41, no. 1, pp. 120–128, 2021, doi: 10.30765/ER.1566.

[39] X. L. Pavlova and S. O. Shaposhnikov, "Risk management for university competitiveness assurance," Proc. 2019 IEEE Conf. Russ. Young Res. Electr. Electron. Eng. ElConRus 2019, pp. 1440–1443, 2019, doi: 10.1109/EIConRus.2019.8657275.

[40] A. Syihabuddin, Y. Suryanto, and M. Salman, "Risk Management in Data Centers Using ISO 31000 Case Study : XYZ Agency," 1st STEEEM 2019, vol. 1, no. 1, pp. 341–352, 2019.