JURNAL TEKNOINFO
Volume 17, Nomor 1, Januari 2023, Page 140-147
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

IDENTIFICATION OF POTENTIAL AND PLANNING FOR DISASTER RECOVERY USING THE ISO/IEC 24762 STANDARD AT XYZ UNIVERSITY

Devi Yurisca Bernanda[1)], Yanthi Charolina[2)], Ozmar Azhari[3)], Cynthia Pangrestu[4)], Johanes Fernandes Andry[5)]

[1,2,3,4,5]Faculty Technology and Design/Information System Department, University of Bunda Mulia
[1,2,3,4,5]Jl. Lodan Raya No. 2 Ancol, Jakarta Utara 14430, Indonesia
Email: [1]bernanda@bundamulia.ac.id, [2]11580@lecturer.ubm.ac.id, [3]11582@lecturer.ubm.ac.id, [4]cynthiahia74@gmail.com, [5]jandry@bundamulia.ac.id

Abstract

XYZ University is a college that annually accepts large numbers of students and has tens of thousands of students. This organizations has an obligation to maintain information and maintain the existence of information against various risks of accidents, whether intentional or unintentional. With the possibility of a risk in the form of a disaster which is a threatening and disruptive event, a disaster can cause loss of organizational data so that risk management is needed that can control it. The progress of information technology development has made technology a means to assist disaster recovery plans in tertiary institutions. The Disaster Recovery Plan is a strategic step to restore the system due to the impact of disasters, both natural and non-natural disasters. Disaster Recovery Plan (DRP) is a set of documents that defines every activity, action, and procedure that must be carried out related to disaster recovery, continuing delayed business processes in a short time and can save existing assets. The research was conducted using the ISO / IEC 24763: 2008 standard. The results obtained are in the form of Risk Recapitulation Based on Literature, then the severity and detection levels are obtained through FMEA analysis which is assessed at levels 1-10, and with business impact analysis the RTO and RPO results are obtained.

Keyword: *Disaster recovery plan, Risk management, ISO / IEC 24763: 2008*

1. INTRODUCING

In this era of information technology, organizations rely heavily on their operational support for information technology services. Information technology is developing faster than technology for physical processing [1]. Information technology is currently one of the basic needs used in almost all sectors. Information technology is a set of tools that help work with information and perform tasks related to information processing [2]. Information and Communication Technology (ICT) plays an important role in society [3] to help accelerate users in obtaining information needs. In the field of disaster management, information technology involves various aspects and disciplines. The need for data is increasing to make data a high-value asset, so the risk of data corruption results in inaccessible data which can happen at any time. It is inconceivable if important data of an organization were lost due to a disaster. Higher education is an organization that also entrusts all important information to information technology devices. Information is data that has been arranged so that it provides meaning and value for the recipient. Every student wants maximum satisfaction from every service found on campus [4], [5]. [6]. Information services are provided not only for academic aspirations within the university but also for alumni from these colleges and the general public [7]. Therefore, there are preparations to follow up on the conditions that will occur so that decisions can be made to be able to decide what plans will be taken to maintain the sustainability of the university.

Currently, company has several campuses with different geographic locations. Every year, XYZ University students and students reach tens of thousands. With this data, of course, Organizations has an obligation to maintain information and maintain the existence of information about various risks of accidents, whether intentional or unintentional, one of which is natural disasters. Information technology infrastructure can be interpreted as the foundation of information technology capabilities, which includes all businesses in the form of reliable services [8]. Information technology infrastructure is also referred to as information technology resources consisting of the basic physical techniques of hardware, software, telecommunications technology, data, and core applications. Institutions really needs infrastructure facilities to manage information for students and other parties in need. Where at this time the information system becomes the foundation of activities that will be accessed by users anytime and anywhere. Online-based information systems are

JURNAL TEKNOINFO
Volume 17, Nomor 1, Januari 2023, Page 140-147
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

built by relying on computer network infrastructure and data centers to help the performance of a system to run properly.

Information systems are systems created by humans to achieve a goal. Therefore, the general interest of the IS field is all aspects of the development, dissemination, implementation, use, and impact of IS in organizations and society [9]. Every system has components that work together to achieve specific goals. Existing information Risks that can occur include internal risk, facility risk, and data system risk. The amount of data that must be stored is a problem that causes organizations to prepare themselves in the event of a disaster, where a disaster that occurs directly in the information system will result in a risk to the data system. This data system risk affects the network, software applications and hardware which can impact the many departments that use the information system. Every disaster that occurs can affect the information system. The consequences of these disaster risks include loss of data, loss of IT functions or certain programs, and loss of access to certain systems or data. In addition, disasters that occur in an information system can also cause daily activities to stop due to information loss. This will be detrimental and will hinder university activities. Therefore, data protection is very important for the sustainability of the information system. Because most of the system users are often not ready to face such events and do not have a definite plan to deal with unexpected events that can be devastating. This is a necessity for an organization to plan a safeguard action against important components of the organization to anticipate disasters.

Disaster recovery planning is defined as an anticipatory planning process for unpredictable events and no organization knows when it occurs and its impact on the continuity of existing business processes [10], [11]. Disaster recovery plan is also defined as planning that focuses on information systems to restore target operating systems, applications, and computer facilities in alternative locations in an emergency [12]. DRP is implemented with the aim of becoming an organization's ability to face disasters or to survive disasters. Handling and management of possible risks that occur at XYZ University can be started by measuring risks with several stages, namely risk identification, and strategy determination against possible risks. In this paper, the focus of DRP discussion is emphasized on DRP related to saving information technology systems and infrastructure from disaster threats. business continuity itself is an activity carried out by an organization to ensure that critical business functions can remain available to consumers, suppliers and other interested parties [13]. The purpose of DRP is continuity or the ability of an organization to survive in the face of disasters (The process of preparing DRP includes analysis, planning, DRP creation, periodic testing and revision based on current business conditions) [14]. The impact of disasters on organizations can be in the form of direct damage (direct damage to equipment and buildings), inaccessibility (inaccessible facilities), utility outage (unavailability of supporting infrastructure such as electricity, water, and so on), transportation disruption, communication disruption, evacuation, and workers, absenteeism [15]. ISO / IEC 24762: 2008 can be used for all organizations, for example for personal, government, non-government, and commercial businesses [16]. The result of the analysis is a business impact report that describes the potential risk to an organization. The existing risks will be analyzed based on the existing business impact [17].

2. RESEARCH METHODS

Research methodology is a method used to solve research problems systematically. It is very important for someone who is doing research to know not only research methods or techniques but also research methodology. Researchers also really need to understand the assumptions underlying various techniques and need to know the criteria to decide that certain techniques and procedures will be applied to a particular problem [18]. Based on Figure 1. Research Workflow, the first step here is to read theory through books and journals related to the DRP and collect data and knowledge from the global. Then for the formulation of problems in disaster management planning for the information system managed by XYZ University obtained will be used as a basis for carrying out this research. The next step is validation and verification to experts, verification of risk data, namely risk data obtained based on expert opinion or experts at XYZ University. In this case, the expert can increase or decrease the risk data collected (based on literature). for risk data validation, namely ensuring the existing risk data is verified so that risk data is obtained in accordance with the conditions. Where then the collection of risk data from the literature is a process of identifying and assessing risks using the FMEA method in the document being reviewed. then performed a Business Impact Analysis (BIA). a processes that allow for systematic of identifying, evaluating possibility impact of disruptions to serious management executions due to disasters, accidents, or emergencies [19].

JURNAL TEKNOINFO
Volume 17, Nomor 1, Januari 2023, Page 140-147
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

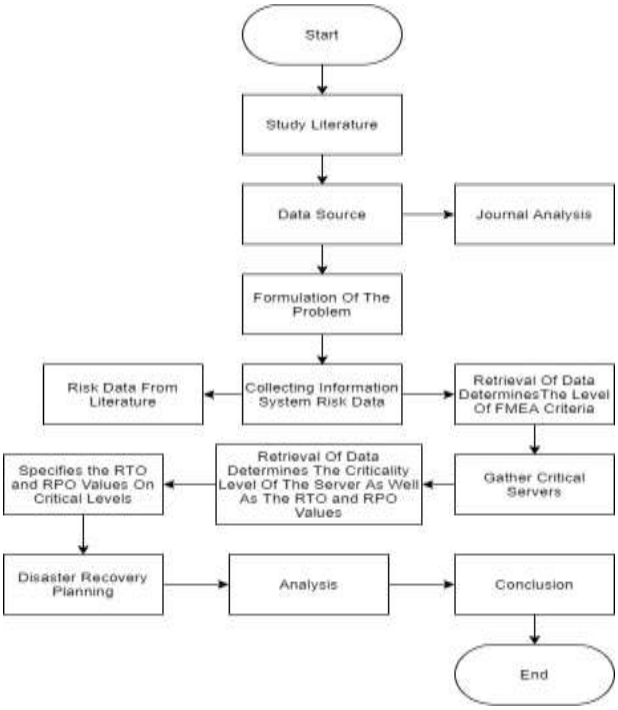

Figure 1. Research Workflow [18].

The BIA analysis was successful. qualitative and quantitative methods. Qualitative analysis was conducted to obtain an evaluation of the opinion of system managers and users of important assets in the information technology development unit and the distribution of XYZ universities. at the same time, quantitative analysis is used to evaluate the productivity of the existing system. and at the same time improve the results of qualitative methods. In terms of quantitative methods, the objective is point recovery (RPO) and for the purpose of recovery time or damages (RTO) are two important parameters of a recovery plan whether it is disaster calculation or data protection. Then it will be analyzed, and final conclusions will be made.

3. RESULT AND DISCUSSIONS

3.1 Risk Identification

In this stage, potential risks are identified to the XYZ University data system. This risk identification has two stages, namely collecting risk data from literature and validating and verification to experienced experts in the field of information systems. Risk identification is carried out by looking at disaster indicators or types of disasters that have great potential and can occur at any time that can threaten the information system. The summary results of previous research regarding potential risks in information systems can be seen in Figure 1. Research Workflow. From this recapitulation, the risks that will be used in this study can be taken, which can be seen in Table 1. Risk Indicator

Based on table 1 of risk indicators, in the table, there are 3 categories, namely disaster indicators, potential disasters, and the risks they cause. From the first category, there is an indicator disaster where there are natural disasters and human disasters, each of which has the potential to occur at XYZ University, the first is a natural disaster with potential disasters such as floods, fires, earthquakes, Explosion, dust, and when -Time may occur Storms. The second is human disasters. There are potential disasters that can occur, namely abuse of access rights, loss of data, wrong data and information, theft of equipment.

Then from natural disasters and human disasters, of course, there are risks that occur if these disasters hit XYZ University. For natural disasters that have 6 potential disasters, namely flooding with the risk that is caused is Cause electrical short circuit and damage to infrastructure (Hardware), fire with the risk is Causing electrical short circuit and damage to other infrastructure is the Destruction of buildings and infrastructure therein, the presence of dust on a PC or

JURNAL TEKNOINFO
Volume 17, Nomor 1, Januari 2023, Page 140-147
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

CPU can certainly be a disaster if dust gets into it, dust creates a risk, namely Faulty hardware and does not rule out that at any time a storm can occur with the risk caused is Causing electrical short circuit and damage to other infrastructure. Furthermore, there is a human disaster with 4 potential disasters that can occur, namely Misuse of access rights which can cause the risk of disseminating information and all-important data, loss of data can cause risks such as Important data is scattered and Leaking data into unauthorized hands, Incorrect data and information causes invalid. data and finally device theft which of course causes loss of the device and causes loss.

Table 1. Risk Indicator

Disaster Indicators	No	Potential Disaster	Risk
Natural Disaster	1	Flood	Cause electrical short circuit and damage to infrastructure (Hardware)
	2	Fire	Causing electrical short circuit and damage to other infrastructure
	3	Earthquake	Destruction of buildings and infrastructure therein
	4	Explosion	Causing electrical short circuit and damage to other infrastructure
	5	Dust	Faulty hardware
	6	Storm	Causing electrical short circuit and damage to other infrastructure
Human Disaster	7	Abuse of access rights	Disseminate information and all-important data
	8	Loss of data	Important data is scattered and Leaking data into unauthorized hands
	9	Incorrect data and information	Invalid data
	10	Device theft	Lost Device

Based on Table 2. Risks Based on Literature, in the table, there are 3 categories, namely disaster indicators, potential disasters, and the risks they cause. In this table for the first category of disaster indicators, namely System and Infrastructure which has 10 potential disasters that can occur at any time and cause a lot of damage, potential disasters are Network connection problems, Server down, Temperature varies, Hardware failure/damage, System Error, Overcapacity, Overload, Electrical voltage, Data corrupt and Backup failure.

Furthermore, there are risks arising from these disasters. First, this network connection problem creates a risk that Data cannot be sent and cannot access the system. Second, there is a server down which can be caused by a down server, which is a website that cannot be accessed. The third is Temperature varies, this causes the temperature that is too hot can cause damage to hardware. The fourth is Hardware failure/damage, here the risk is data not encapsulated. The fifth is System Error with the risk that the website is difficult for users to access. The sixth is Overcapacity with the risk of Data not encapsulated. The seventh is Overload with the risk of not encapsulated data. The eighth one is Electrical voltage with the risk of short circuit and unable to access the system. the ninth is Data corrupt and the last one is Backup failure which creates the risk of loss of data.

3.2 Risk Analysis Based on The FMEA Method

The research was conducted by collecting data through the FMEA method to determine the risk rating with the most potential in XYZ University. This method is done by giving a level on 2 assessment criteria, namely severity and detectability. Where each criterion has 10 levels. The level of severity used in this study can be seen in Table 3 Level of Severity, where this Table shows the effects that occur due to disasters and the consequences obtained from the severity of the disaster. This section also shows Non-Productive Time, namely working time that is not used to complete work or is referred to as the duration, each of the effects described in the table and then measured to get an assessment with a level. Table 4 Incidence rate describes the levels for detection where at the first detection it is almost impossible with the possibility of detection by the control, that is, it is closed not possible for the check to detect a mistake at level 10.

The second level of detection is a very little possibility with the possibility of detection by the control is very small the possibility for checks to detect failure is at level 9. The third level of detection is the least possibility where the possibility of detection by the control is less likely for the check to detect a failure at level 8. The fourth level is very low with the possibility of detection by the control, namely Checking has a good chance low for detecting failure is at level 7. The fifth level is low with the possibility of detection by control, namely checking the low probability of detection is at level 6. Furthermore, the sixth level of detection is sufficient with the possibility of detection by control Checks that are likely to detect failures that are at level 5.

JURNAL TEKNOINFO
Volume 17, Nomor 1, Januari 2023, Page 140-147
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

Table 2. Risks Based on Literature

Disaster Indicators	No	Potential Disaster	Risk
System and Infrastructure	1	Network connection problem	Data cannot be sent and cannot access the system
	2	Server down	Website that cannot be accessed
	3	Temperature varies	The temperature that is too hot can cause damage to hardware
	4	Hardware failure / damage	Data not encapsulated
	5	System Error	Website is difficult for users to access
	6	Overcapacity	Data not encapsulated
	7	Overload	Data not encapsulated
	8	Electrical voltage	Short circuit and unable to access the system
	9	Data corrupt	Loss of data
	10	Backup failure	Loss of data

Table 3. Level of Severity

Description Of Levels	Explanation Of Difficulties	Non Productive Time	Level
Severity at Dangerous level and without warning	The severity that occurs can harm the server without warning	> 7 x 24 hours	10
Dangerous level severity but there is a warning	The severity that occurs can harm the server with advance warning	> 6 x 24 hours -> 7 x 24 hours	9
Very high-level severity	The severity that occurs results in a failure that completely disrupts the server	> 5 x 24 hours -> 6 x 24 hours	8
High level severity	The severity that occurs causes a Failure that disrupts 50% of server work	> 4 x 24 hours -> 5 x 24 hours	7
Intermediate severity	The severity that occurs causes a Failure that disrupts 25% of server work	> 3 x 24 hours -> 4 x 24 hours	6
Low level severity	The severity that occurs causes a damage that disrupts 0.1 of server work	> 1 days -> 3 x 24 hours	5
Very low-level severity	The severity that occurs causes a failure that affects the working of the server	> 12 hours -> 24 hours	4
Small level severity	The severity that occurs results in a Fail that has a minor effect on the server	> 7 hours -> 12 hours	3
Very low-level severity	The severity that occurs results in a failure which has a negligible effect	> 240 minutes -> 420 minutes	2
No severity	The severity that occurs results in failure, that is, it has no effect	> 0 minutes -> 240 minutes	1

The next level is high enough where Checks are most likely to detect failures that are at level 4. Then high where Checks have a great chance of detecting failures that are at level 3. After that, it is very high where Checks can almost certainly detect failures that are at level 2, the latter is almost certainly where Examinations can detect failures at level 1.

JURNAL TEKNOINFO
Volume 17, Nomor 1, Januari 2023, Page 140-147
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

Table 4. Incidence rate (Occurrence)

Detection	Possible Detected	Level
The severity of this level is almost impossible	It's closed not possible for a check to detect a damage	10
The severity of this level is very unlikely	It is unlikely that the check will detect a failure	9
The severity of this level is unlikely	The check is unlikely to detect a failure	8
The severity of this level is very low	Checks have a weak chance of detecting damage	7
Low level severity	Low detection probability checks	6
Medium severity	The check will likely detect failure	5
The severity of this level is quite high	The check is most likely to detect a damage	4
High level severity	Checks have a high chance of detecting failure	3
The severity of this level is Very high	Checks can almost certainly detect failures	2
Almost sure	Definite checks can detect failure	1

Based on Table 4 incidence rate (Occurrence), where there are 3 categories, namely detection, Possible detected, and level. Detection, namely the severity of this level is almost impossible, the severity of this level is very unlikely, the severity of this level is unlikely, the severity of this level is very low, Low-level severity, medium severity, The severity of this level is quite high, High-level severity, The severity of this level is Very high dan Almost sure. Furthermore, there is Possible detected, the first one, the severity of this level is nearly not possible with it is nearly not possible for a check to detect a damage, which is at level 10. The second severity of this level is very unlikely with It is unlikely that the check will detect a failure which has a level of 9. The third the severity of this level is very unlikely with the check is unlikely to detect a failure on level 8 the fourth he severity of this level is very low with Checks having a low chance of detecting failure at level 7.

Table 5. Assessment

Function	Potential failure	Severity (a)	Potential cause	Occurrence (b)	Prevention	Detection (c)	Detection	RPN (a*b*c)
DRP	Disaster	10	Fire	8	Fire Extinguisher	Fire alarm	2	160
	Data loss		Earthquake	3	None	None	10	300
	Data Corruption		Explosion	9	None	None	10	900
	Hardware failure		Theft	4	Security	Safety alarm	1	40
	Software failure		Flood	3	None	None	10	300

The fifth is Low-level severity with Low detection probability checks at level 6. The sixth is medium severity with the check will likely detect failure is at level 5. The seventh the severity of this level is quite high with the check is most likely to detect a failure at level 4. The eighth is High-level severity with Checks has a high chance of detecting failure at level 3. The ninth severity of this level is Very high with Checks that can almost certainly detect failures at level 2 and finally Almost sure with Definite checks can detect failure is at level 1.

Based on Table 5 Assessment, shows several categories, namely Function Requirement, Potential failure, Severity (a), Potential cause, Occurrence (b), Prevention, Detection (c), det, det here are the values for detection (c) and RPN (a * b * c). In a potential failure, there is a disaster, data loss, data corruption, hardware failure, software failure. Potential causes are fire, earthquake, explosion, Theft, and flood. Where describes a disaster that has a high chance of occurring and is likely to damage the system, infrastructure at XYZ university. RPN or Risk Priority Number is used in the FMEA because RPN provides a risk priority number obtained from the multiplication of Severity, Occurrence, and Detection.

JURNAL TEKNOINFO
Volume 17, Nomor 1, Januari 2023, Page 140-147
ISSN: 1693-0010(Print), ISSN: 2615-224X(Online)
Available online at https://ejurnal.teknokrat.ac.id/index.php/teknoinfo/index

3.3 Risk Business Impact Analysis

Business Impact Analysis can be seen from the value of Recovery Time Objective (RTO) and Recovery Point Objective (RPO) which previously collected data on critical servers. RTO is how long the user tolerates a loss before getting it back. RTO at XYZ University is used to find out how much data loss might occur and how long the existing system or website cannot be accessed. Table 6 RTO the time used for recovery.

Table 6. RTO

Recovery Time Objective	
0	To - recovery within 0 minutes - 0 minutes
1	To - recovery within 1 days – more or less 24 hours
2	To - recovery within 2 days – more or less 48 hours
3	To - recovery within 3 days – more or less 72 hours
4	To - recovery is greater than 3 days - more 72 hours

Meanwhile, the RPO assessment is used to see how much data is allowed to be lost if a disaster occurs. For this RPO value, it greatly affects the backup method of the server at this company. Table 7 RPO value where in the event of a system failure, how much time is used to recover data.

Table 7. RPO

Recovery Point Objective	
0	No data can be lost
1	In the past 0.25 days regardless of when the there is a disturbance
2	without exception all data entered since the most recent backup must be able to be inputted
3	It could be that it will take up to 1 week for the data to be lost

3.4 Disaster Recovery Plan

Designing a disaster recovery plan requires determining an alternative location for the backup server location. This is because if a crash occurs on the main server, the data on the main server has previously been backed up to a backup server that is located different from the main server. The next location consideration is the location of the reserve must be outside the mitigation radius (volcano, tsunami, frequent flooding). The next consideration is the availability and quality of electricity / battery power, the closest fiber line, IT/IS that have purpose in that location, and is not prone to conflict.

4. CONCLUSION

Base on research described, it can be concluded that a disaster recovery plan for an organization is a plan that focuses on information systems to restore target operating systems, applications, and computer facilities. The purpose of a disaster recovery plan is so that organizations can deal with disasters or survive disasters. From the research conducted, this organization does not have a clear plan and mechanism for dealing with disasters, especially those related to disasters in business processes such as hardware and software failures or infrastructure disruptions such as power outages, fire, and others. From the research conducted, the researcher gave the result in the form of a Disaster Recovery Planning (DRP) document which contains guidelines for implementing the disaster recovery phase using ISO / IEC 24762: 2008 standards.

Based on the table 7, authors suggest XYZ university conduct an RPO 11:00 pm - 05:00 am to back up data so that the data is kept safe and stored, in addition, according to the author, if the university gets a big problem such as a natural disaster it can take months. to be able to recover and if what happens are minor problems it will take 8 hours to 3 days to fix them so that people will be able to give their trust. Authors suggest for backup strategy for the system for daily: Do a full backup for the first time, then do a daily backup for differential backup. Differential backup at institutions is another type of backup in which data files that have undergone changes after a full backup are supported instead of backing up all files again. Duplicating data only on new data or data that has undergone changes. In this backup, the data obtained is not tagged. Periodic backups are made of files that have been modified or added to the database. This method has the advantage of a fast backup process and a smaller backup size. For monthly: Performs an Incremental Backup to

synchronize files that have been modified. Backup data that is duplicated on data that has not been backed up, if there is a difference in the capacity of the data, then only the difference in the capacity of the data will be duplicated. Backups are done at regular intervals.

REFERENCES

[1] W. F. Cascio and R. Montealegre, "How Technology Is ChangingWork and Organizations," Annu. Rev. Organ. Psychol. Organ. Behav. 3:349–75. 2016. doi: 10.1146/annurev-orgpsych-041015-062352.
[2] S. Juntorn, S. Sriphetcharawut and P. Munkhetvit, Effectiveness of Information Processing Strategy Training on Academic Task Performance in Children with Learning Disabilities: A Pilot Study, Occupational Therapy International (1):1-13, 2017. doi: 10.1155/2017/6237689
[3] J. Steyn "Some Key Concepts of The Role Of ICT In Societies," Conference: Panel discussion: ICT and Diversity of Information Societies. IADIS2011, 2020.
[4] C. Darawong and M. Sandmaung, "Service quality enhancing student satisfaction in international programs of higher education institutions: a local student perspective," Journal of Marketing for Higher Education, 2019, 29(6):1-16. doi: 10.1080/08841241.2019.1647483, 2003.
[5] D. Y. Bernanda, A. Yohanes, J. Surya Seputro, and J. F. Andry, "Analisis Sistem KRS Online Terhadap Kepuasan Mahasiswa Universitas XYZ Menggunakan Metode UTAUT, Jurnal TEKNOINFO, Vol. 13, No. 2, 124-130, 2019.
[6] Marlina, Y. P. Santoso, Kelvin, and J. F. Andry, "Analisis Pengaruh Website Fashion Macadamia House Terhadap Kepuasan Konsumen dengan Metode Webqual 4.0, Jurnal TEKNOINFO, Vol. 13, No. 2, 2019, 63-70.
[7] I. Snijders, L. Wijnia, R. Rikers, and S. M. M. Loyens "Alumni loyalty drivers in higher education," Social Psychology of Education, 22(3):607-627, 2019. doi: 10.1007/s11218-019-09488-4.
[8] A. S. Kumar, and J. U. M. Reddy, "Service Reliability Impact on Business with Reference to Three Star Hotels" in Hyderabad" International Journal of Engineering and Management Research 09(05):135-140, 2019. doi: 10.31033/ijemr.9.5.19.
[9] S. Alter, "Work system theory: overview of core concepts, extensions, and challenges for the future," J. Assoc. Inf. Syst., p. 72, 2013.
[10] N. Trifonova, A. Proshkina, A. Bezrukov, A. Korolev, and A. Paren, "Sustainability and Business Continuity Management for Production System in the Energy Sector in the Face of Increasing Uncertainty and Risk: Who Determines?," Proceedings of the International Scientific and Practical Conference "Young Engineers of the Fuel and Energy Complex: Developing the Energy Agenda of the Future" (EAF 2021).
[11] C. Martino, and J. F. Andry, Testing Aplikasi Business Activity Monitoring Pada Internet Service Provider Menggunakan ISO 25010, Jurnal TEKNOINFO, Vol. 14, No. 1, 35-40, 2020.
[12] S. Snedaker, Business continuity and disaster recovery planning for IT professionals. Newnes, 2013.
[13] S. Benn, R. Abratt and B. O'Leary, Defining and identifying stakeholders: Views from management and stakeholders, South African Journal of Business Management 47(2):1-11, 2016. doi: 10.4102/sajbm.v47i2.55.
[14] A. Awasthi, "IT Infrastructure -Business Continuity Plan Implementation and Maintenance," Journal of Information Technology 11(2):275, 2021.
[15] M. Titko, J. Havko, and J. Studena, "Modelling Resilience of the Transport Critical Infrastructure Using Influence Diagrams," Komunikacie 22(1):102-118, doi: 10.26552/com.C.2020.1.102-118, 2020.
[16] G. Harangozo, and G. Zilahy "Cooperation between business and non-governmental organizations to promote sustainable development," Journal of Cleaner Production 89, 2015. doi: 10.1016/j.jclepro.2014.10.092.
[17] A. Setiawan, A. Wibowo, and A. H. Susilo, "Risk analysis on the development of a business continuity plan," Conference: 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), 2017. doi: 10.1109/CAIPT.2017.8320736
[18] M. Zizovic, M. Albijanic, V. Jovanović, and M. Zizovic. Kothari, A New Method of Multi-Criteria Analysis for Evaluation and Decision Making by Dominant Criterion, Informatica 30(4):819-832, doi: 10.15388/Informatica.2019.231, 2019.
[19] H. E. Miller dan K. J. Engemann, "Using reliability and simulation models in business continuity planning," Int. J. Bus. Contin. Risk Manag., vol. 5, no. 1, hal. 43, 2014.