Designing Disaster Recovery Plan of Data System for University

Difana Meilani¹, Ikhwan Arief¹, Mulya Habibullah¹

¹Industrial Engineering Department, Faculty of Engineering, Universitas Andalas, Padang, Indonesia
*E-mail: difana@eng.unand.ac.id

Abstract. According to the QS World University Rankings, Andalas University is a 3-star university and is in ranked 12th of the best universities in Indonesia based on the Indonesian Ministry of Research and Higher Education criteria. The university is located in three different areas which are Padang, Payakumbuh, and Dhamasraya. Currently, the university’s Information and Communication Technology Development Unit which is responsible in managing the information and communication technology has no formal documentation of response procedures in an event of an emergency. Being used by some 26,702 students and staffs, the system is potentially corrupted by a few possible disasters like viruses, hackers, and server downs. Therefore it is crucial for the organization to plan a documented security action to protect essential archives and application software in anticipating the catastrophes. This study developed a Disaster Recovery Plan (DRP), as a document to act on accidents which may occur in information system failures. It is a plan for rapid recovery from the disaster or the emergency response so that the organization does not perceive the impact given by the information system failure.

1. Introduction

Recently, organizations are often faced various types of disruptions that could affect to the organizations. The effects of each disruption might be different. Traditionally, Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) as the main contingency plans are carried out separately in different time horizons within organizations. To face disruptive events that may happen, proactive planning of internal and external resources of the organization should be prepared so that the disasters will cope with effectively and efficiently [1],[2]. A disaster is defined as the occurrence of any event that causes a significant disruption in IT capabilities [3].

The disaster recovery plan will provide some activities to do in response to a disaster. This plan will provide effective and efficient ways to recover from any disaster that affect IT system in organizations. Disaster loses can be minimized by having a good disaster recovery plan for every business subsystem and operation within an enterprise. Every business disaster has one or more causes and effects. The causes can be natural, human or mechanical in origin, ranging from simple case such as a tiny hardware or software component’s malfunctioning to universally recognized events such as earthquakes, fire, and flood. Effects of disasters range from small interruptions to total business shutdown for days or months, even fatal damage to the business [4].

Information Technology (IT) system has become vital to every aspect of business [5],[6]. IT Disaster Recovery Plan must contain requirements and steps that need to be taken in response to disaster that affect IT System in University (in this case is Andalas University). The fundamental goal of disaster
recovery plan is allowing basic business functions to resume and continue until system can be restored into its previous disaster functions [7]. This Disaster Recovery Plan is designed to ensure the continuation of vital business processes in the case that a disaster occurs [8]. An effective solution that can be used to solve the problems in IT system. After disaster, the organizations should provide disaster recovery plan to restore all required frame vital business processes [9].

IT disaster recovery plans provides step-by-step procedures for recovering disrupted systems and networks, and help them resume normal operations. The goal of these processes is to minimize any negative impacts to company operations. The IT disaster recovery process identifies critical IT systems and networks; prioritizes their recovery time objective; and delineates the steps needed to restart, reconfigure, and recover them. A comprehensive IT DR plan also includes all the relevant supplier contacts, sources of expertise for recovering disrupted systems and a logical sequence of action steps to take for a smooth recovery [9].

Disaster recovery plan will have an outcome as a disaster recovery plan document. This document will be the primary source in term of emergency when the disaster happened and affect the IT system. The disaster recovery plan documents will provide procedures to restore all the lost in IT system. Therefore, the document should be readable, simple and the instructions are detailed. The purpose of the document must be clearly stated in the introduction, defining the objectives the plan intends to achieve.

Specifically for information technology operations and management, it is namely ISO / IEC 27031. It provides guidance on the concepts and principles behind the role of information and communications technology (ICT) in ensuring business continuity. The International BCM (Business Continuity Management) Standard developed by ISO / TC 223 summarizes the BCM approach to prevent, react and recover from incidents. Activities involved in BCM are incident preparedness, operational continuity management, Disaster Recovery Planning (DRP) and risk mitigation that focus on improving the resilience of the organization and preparing it to react effectively to incidents and recover predetermined timeframes [10], [11].

Andalas University is a 3-star university and it is in ranked 12th of the best universities in Indonesia based on the Indonesian Ministry of Research and Higher Education criteria. The university is located in three different areas which are Padang, Payakumbuh, and Dhamasraya. The university's Information and Communication Technology Development Unit which is responsible in managing the information and communication technology and in providing applications that are used for the academic community. Based on its responsibility, the unit is the center of information and storage of all important files or data that must be maintain so the system of Andalas University runs continuously. Currently, it has no formal documentation of response procedures in an event of an emergency. If a disaster happens, it can cause lost and damage of all information. Furthermore the organization and lecturer system can be paralysis. The purpose of this research is to design a Disaster Recovery Plan for Information and Communication Technology Development Unit of Andalas University.

2. Method

The data and information being collected were related to the problems faced in information systems, especially regarding handling in disasters. In addition, data deals with designing a Disaster Recovery Plan were also being collected. The Data and information regarding the Information and Communication Technology Development Unit were obtained from direct observation, interviews, and discussions with related experts. The stages of the survey were carried out with literature related to this study. Literature studies were carried out by reading theories on books and journals which concern in Disaster Recovery Plan and also collecting information from the online sources through internet.
The method used in this study was ISO 27031. This was chosen since it offers several advantages such as:
1. ISO is a standard with a middle to upper area coverage
2. ISO is suitable for use in IT management
3. The framework can be used to manage technology and information infrastructure in organizations, and ways to provide the best service for users of information technology.
4. The framework is used since it can help them at the highest level of the organization to achieve and fulfill their legal, regulatory and ethical requirements in terms of the use of IT organizations.

The design of DRP began by analyzing the running system and identifying threats that occurred, both from the outside and originating from within. After obtaining a risk assessment one of steps in risk management process then risk analysis is carried out for determining the level of each risk [12]. The risk assessment has been validated and verified by the expert. Determination of risk level is done by using the Failure Mode and Effect Analysis (FMEA) method [13], [14]. Then the Business Impact Analysis (BIA) is carried out. It is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency [15].

BIA is analyzed using qualitative and quantitative approach. The qualitative analysis is for obtaining an assessment from the point of view of the system manager and user regarding the critical assets at the Information and Communication Technology Development Unit of Andalas University. While, the quantitative analysis is for getting assessment from the point of view of the productivity of the existing system and, it is also to sharpen the result of qualitative method. In the quantitative approach, Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are two important parameters of a disaster recovery or data protection plan which are being calculated [16], [17], [18]. These are objectives which can guide enterprises to choose an optimal data backup plan.

Finally, the design of the content of the Disaster Recovery Plan is based on the standard of ISO/IEC 27031. At the end, the validation process is done by the stakeholders at the Information and Communication Technology Development Unit of Andalas University to prove that the DRP document has already fulfilled the needs of the unit.

3. Finding and Result

The Risk Assessment stages based on ISO 27031 are as follows:
1. Identify the potential failure mode.
2. Determine the potential impact on ICT services; the severity of each failure mode.
3. Identify the frequency of failure modes that the organization has prior experience, as well as ease of monitoring and detection of failure modes.
4. Identify indicators that will provide signals or information of failing components.
5. Identify the direct and indirect events that are related, and will change the state of each indicator.
6. Identify existing controls that prevent important components of failure, or can detect those failures.
7. Identify related data sources, and possible methods for detecting changes in indicator values.
8. Identify whether suitable risk reduction or elimination of controls can be applied to prevent such occurrences.

At this stage, risk identification was carried out from the literature which specifically threatens the information systems. The potential risks to the information system from previous research are shown in Table 1.

| No     | Item /Attribute Risk Agent |
|--------|-----------------------------|
|        |                             |
| Indicators / Dimensions | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 | 32 | 33 | 34 |
|-------------------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| Nature / Environment    | Fire | Flood | Earthquake | Lightning | Storm | Dew | Heat radiation | Temperature varies | Dust / dirt | Humidity | Device theft | Information is accessed by unauthorized parties | Leaks of data / internal information of the company / institution | Data and information do not match the facts | Misuse of access rights / User ID | Former users / employees still have access to information | Unauthorized physical access | Data loss | Human error | Risk of human-caused damage such as cybercrime, terrorism, piracy and vandalism | Hardware failure / damage | Server down | Overheat | The network connection is lost | System crash | Overcapacity | Overload | Data corrupt | Backup failure | Failed to update | Poor network quality | Obsolete technology | Risk of damage due to problems | power / voltage |

The risks obtained from the literature were validated and verified by the expert. In this validation and verification, the expert can add, reduce and improve the risk data points to be relevant to the Information and Communication Technology Development Unit of Andalas University. Furthermore, the expert gave the points of the risks relevant to the Information and Communication Technology Development Unit of Andalas University and the causes. Table 2 shows the risks after the validation from the expert.

**Table 2** Risks after Validation
| Indicators / Dimensions | No | Item / Attribute Risk Agent                  |
|-------------------------|----|----------------------------------------------|
| Nature / Environment    | 1  | Fire                                         |
|                         | 2  | Earthquake                                   |
|                         | 3  | Temperature varies                           |
|                         | 4  | Humidity                                     |
|                         | 5  | Device theft                                 |
|                         | 6  | Former users / employees still have access to information |
|                         | 7  | Data loss                                    |
|                         | 8  | Human error                                  |
|                         | 9  | Risk of human-caused damage such as cybercrime, terrorism, piracy and vandalism |
|                         | 10 | Late Data Backup                             |
| Human                   | 11 | Hardware failure / damage                    |
|                         | 12 | Server down                                  |
|                         | 13 | Network connection disconnected ISP          |
|                         | 14 | Data is corrupt                              |
|                         | 15 | Backup failure                               |
|                         | 16 | Failed to update                             |
|                         | 17 | Power / voltage                              |
|                         | 18 | Blacklist from Certain Sites                 |
|                         | 19 | The internal network is disconnected         |

Description of Color:

: The attribute chosen by Expert

: Additional attributes from Expert

**Table 3 Table of Levels for Severity**

| Effect                        | Explanation                                      | Non Productive Time | Level |
|-------------------------------|--------------------------------------------------|---------------------|-------|
| Harmful without changes       | Can harm the server without warning              | > 6 x 24 hours      | 10    |
| Dangerous but there is a warning | Can endanger the server with a warning first       | > 6 x 24 hours      | 9     |
| Very high                     | Failure to completely interfere with the server  | > 4 x 24 hours      | 8     |
| High                          | Failure interferes with 50% of server work       | > 3 x 24 hours      | 7     |
| Medium                        | Failure interferes with 25% of server work       | > 2 x 24 hours      | 6     |
| Low                           | Failure interferes with 10% of server work       | > 24 hours          | 5     |
| Very low                      | Failure affects server work                      | > 12 hours          | 4     |
| Small                         | Failure has a minor effect on the server         | > 6 hours           | 3     |
| Very small                    | Failure has a negligible effect                  | > 3 hours           | 2     |
| There is no                   | Failure has no effect                            | > 0 hours           | 1     |

The level for Occurrence is shown in Table 4

**Table 4. Table of Level for Occurrence**
Probability of failure | Number of Failures Per Year | Possible Failure Rate | Level
---|---|---|---
Very high: inevitable | >500 | > 1 in 2 | 10
| 366 – 500 | 1 in 3 | 9
Height: Repeated failure | 300 – 3365 | 1 in 8 | 8
| 250 – 300 | 1 in 20 | 7
Moderate: failure seasonal | 150 – 249 | 1 in 80 | 6
| 50 – 149 | 1 in 400 | 5
| 10 – 49 | 1 in 2000 | 4
Low | 5 – 9 | 1 in 15000 | 3
| 1 – 4 | 1 in 150000 | 2
Remote: rarely happening | <1 | 1 in 1500000 | 1

The level for Detectability is shown in Table 5

| Detection | Explanation | Level |
|---|---|---|
| Almost impossible | It is almost impossible to check to detect failure | 10 |
| Very few possibilities | Very little possibility for checking large failures | 9 |
| Little possibility | It's less likely to check to detect a failure | 8 |
| Very low | Check has a low chance of detecting failure | 7 |
| Low | Check for possible low detection | 6 |
| Enough | Check will likely detect failure | 5 |
| High enough | Check is likely to detect failure | 4 |
| High | Checking has a great chance of detecting failure | 3 |
| Very tall | Check almost certainly can detect failure | 2 |
| Almost certain | Checking can definitely detect failure | 1 |

After obtaining the level of each FMEA criterion, the Risk Priority Number (RPN) was then being calculated.

Example:
Risk Priority Number = Severity x Occurrence x Detectability
\[
RPN = 7 \times 5 \times 6
\]
\[
= 210
\]

From the value of the RPN, it could be seen that the risk rating has the most potential for failure of the Information and Communication Technology Development Unit of Andalas University. The highest RPN value was the most potential risk. The RPN calculation result is shown in Table 6.
## Table 7. RTO (Recovery Time Objective)

| RTO (Recovery Time Objective) | Description |
|-------------------------------|-------------|
| 0                             | Recovery within 0 hours - 0 days |
| 1                             | Recovery within 24 hours - 1 day |
| 2                             | Recovery within 48 hours - 2 days |
| 3                             | Recovery within 72 hours - 3 days |
| 4                             | Recovery is greater than 72 hours -> 3 days |

The next step is the Business Impact Analysis, which was a step to determine RTO and RPO values for each critical server in the Information and Communication Technology Development Unit of Andalas University. RTO value was needed to see how long the server are cut off during repairing if a disaster occurs that causes the server to be cut off. The RTO assessment is shown in Table 7.

Table 7. RTO Assessment

| No | Item /Attribute Risk Agent | RPN  | Rank |
|----|----------------------------|------|------|
| 1  | Fire                       | 180  | 2    |
| 2  | Earthquake                 | 210  | 1    |
| 3  | Temperature varies         | 125  | 5    |
| 4  | Humidity                   | 100  | 7    |
| 5  | Device theft               | 175  | 3    |
| 6  | Former users / employees still have access to information | 175  | 3    |
| 7  | Data loss                  | 96   | 8    |
| 8  | Human error                | 80   | 9    |
| 9  | Risk of human-caused damage such as cybercrime, terrorism, piracy | 150  | 4    |
| 10 | Late Data Backup           | 100  | 7    |
| 11 | Hardware failure / damage  | 150  | 4    |
| 12 | Server down                | 120  | 6    |
| 13 | Network connection disconnected ISP | 96  | 8    |
| 14 | Data is corrupt            | 80   | 9    |
| 15 | Backup failure             | 96   | 8    |
| 16 | Failed to update           | 80   | 9    |
| 17 | Power / voltage            | 96   | 8    |
| 18 | Blacklist from Certain Sites | 125  | 5    |
| 19 | The internal network is disconnected | 100  | 7    |

While the RPO assessment is to see how much data is allowed to disappear if a disaster occurs. This RPO value is very influential on the backup method of the server that is in the Information and Communication Technology Development Unit of Andalas University. The RPO Assessment is shown in Table 8.

Table 8. RPO Assessment
RPO (Recovery Point Objective)

"RTO is defined as how much user data will be lost. If the system that supports your business process fails, the data can be recovered and how many losses can be received?"

|   |   |   |   |
|---|---|---|---|
| 0 | No data is allowed to be lost |   |   |
| 1 | In the last 8 hours regardless of when the disturbance occurred |   |   |
| 2 | All data entered since the last backup must be re-inputted |   |   |
| 3 | It can take up to one week of lost data to be reconstructed |   |   |

The value of RTO and RPO were determined by distributing questionnaires. The distribution of the questionnaire was filled out by one person from each division, namely the network division, the data collection division, and the multimedia division. The questionnaires were distributed to three people with the aim to obtain accurate data on the state of the Information and Communication Technology Development Unit of Andalas University. To see the criticality of the server, it can be seen from how long the server is cut off. The RTO Value on each the Information and Communication Technology Development Unit of Andalas University Server is shown in Table 9.

Table 9. RTO value on each Information and Communication Technology Development Unit of Andalas University Server

| RTO 0 | RTO 1 | RTO 2 |
|-------|-------|-------|
| Data Base | SIA | E Office | Administrasi |
| SIA |   |   | LP3M |
| Jurnal 1 | FAPERTA | Evaluasi Pendidikan | Akademik |
| Jurnal 2 | Buku | FATETA | Alat Lab |
| UNAND.AC | Development | Feder PDPT | Berkas |
| DNS Server | Fekon | Dosen.Unand | SIA Dikti |
| E Journal | FHUK | E Books | SIKS |
| I-Learn 1 | FIB | Educong | Sister |
| I-Learn 3 | FKM | Eorfernece | UKT |
| Katalog Pustaka | FMIPA | Farmasi | BAPSI |
| Kerja Sama | FTUA | Faterna | Blog |
| LPPM | IKA | FISIB | I-learn Depan |
| LPTIK | JNTE | FJI | Karir |
| Server Pustaka | Litbang Aset | Fkep | PPID |
| Sim Keuangan | LPSE Unand | FKG | Share Point |
| Simpeg | Repo Sitory | FTI | Staf Unand |
| Analytic | Scolar | Galery | Teknik Elektro |
| BIOS | Sim Kehadiran | I-Learn 2 | Teknik Industri |
| Digilib | Simalyar | Intake D3 | Teknik Lingkungan |
| SNMPTN | Journal | Mahasiswa | Teknik Mesin |
|             | Mahasiswa | Teknik Sipil |

The RPO value on each the Information and Communication Technology Development Unit of Andalas University server is shown in Table 10.
Table 10. RPO Value on each Information and Communication Technology Development Unit of Andalas University Server

| RPO 0 | RPO 1 | RPO 2 |
|-------|-------|-------|
| UNAND.AC | I-Learn 1 | FJI | Eorfernece | Kerja Sama |
| Jurnal 1 | Feder PDPT | SNMPTN | Faterna | Development |
| Simpeg | Sister | LPSE Unand | RSP Unand | LPPM |
| Jurnal 2 | I-Learn 3 | Atal Lab | Administrasi | IKA |
| SIA | Katalog Pustaka | Digilib | Karir | Analytic |
| | Sim Keuangan | Journal Mahasiswa | Fekon | Kemahasiswaan |
| | Sim Kehadiran | SIA Dikti | E Books | Galery |
| | Litbang Aset | Simalyar | SIKS | PPID |
| | E Jornal | Scolar | Pasca | Staf Unand |
| | JNTE | LPTIK | FISIB | Seminar |
| Server Pustaka | FIB | Buku | Educonf |
| Data Base SIA | FMIPA | FKG | Teknik Sipil |
| FAPERTA | FATETA | LP3M | Teknik Industri |
| Evaluasi Pendidikan | FKM | Berkas | Teknik Elektro |
| BIOS | Intake D3 | Akademik | Teknik Mesin |
| DNS Server | FHUK | BAPSI | Teknik Lingkungan |
| I-Learn 2 | FTUA | | Share Point |
| Repo Sitory | Fkep | | Dosen.Unand |
| E Office | FTI | | I-learn Depan |
| UKT | Farmasi | | Blog Mahasiswa |

In planning DRP, a backup server location was needed to maintain data security. The location’s indicators is referred to ISO 27031, which is compared to the circumstances of each location. The alternative locations and considerations is shown in Table 11.

Table 11. Alternative Locations and Considerations

| No | Location Considerations | Alternative location |
|----|-------------------------|----------------------|
|    |                         | Padang | Payakumbuh | Dharmasraya |
| 1  | Being in a safe area but within an affordable distance from the location it will serve | √ | √ | √ |
| 2  | Minimum> 40 km from the data center |        | √ | √ |
| 3  | Be outside the mitigation radius |        | √ | √ |
| 4  | Not in the geological fault line |        | | |
| 5  | Small potential risks from disasters | √ | | |
| 6  | Availability of local staff and vendors | √ | | |
| 7  | Availability and quality of electricity / battery | √ | | |
| 8  | Nearby Fiber Routes | √ | √ | |
| 9  | Information technology can function at that location | √ | | |
| 10 | Not prone to conflict and terrorism | √ | | |
| 11 | Tax Incentive | √ | | |

Total | 7 | 10 | 9 |
The design of the DRP document for the Information and Communication Technology Development Unit of Andalas University are based on the ISO/IEC 27031. The standard content that must be in the DRP document has been set at ISO / IEC 27031 as follows; Purpose and scope, Roles and responsibility, Calling Plans, Response and Recovery Plan, Application Recovery Team. The plan must be documented so that competent personnel can use it in the event of an incident. Documentation must define the overall framework in which the recovery plan is prepared, which includes; Overall strategy, Critical services based from RTO and RPO values, Timeline for recovery, Recovery team and their responsibilities before and during the disaster. The plan must be documented so that competent personnel can use it in the event of an incident. The documentation consist of Purpose, Coverage based on the BIA, Availability requirements determined by the business for the availability of services and related technologies, Information security requirements, the appendix. The Appendix consist of Inventory of information systems, applications, and databases; Review of network infrastructure and server names; Inventory of hardware and software system; Service level contracts and agreements. Last the documentation the main ICT supplier. After designing the DRP document, the document validation is carried out. The document was validated by Mr. Hendra Gunawan as chairman of the Information and Communication Technology Development Unit of Andalas University, Mr. Prama Wahyudi as the multimedia division, Mr. Rudi as the network division. The results of the validation by the validator show that the DRP document designed is in accordance with the needs of the unit.

4. Conclusion

This research has developed Disaster Recovery Plan (DRP) documents for data systems in the Information and Communication Technology Development Unit of Andalas University. In the DRP documents consist of quick response procedures and activities in the event of a disaster. This DRP documents will be used in the event of a disaster not for daily operational activities. In the DRP document there is a risk analysis. It analysis what potential destroy the data system by using FMEA method. This DRP documents also have RTO and RPO values that will be used to save the system and the location of backup service which later can be used as a backup server during the repairing of the main server. Suggestions for further research on DRP covers documents and also requiring costs.

5. Acknowledgment

Authors would like to thank the Engineering Faculty of Universitas Andalas for providing publication grant 2019 with contract number 017/UN.16.09.D/PL/2019.

6. References

[1] N. Sahebjamnia, S. A. Torabi, and S. A. Mansouri, “Integrated Business Continuity and Disaster Recovery Planning: Towards Organizational Resilience,” Eur. J. Oper. Res., vol. 242, no. 1, pp. 261–273, 2015.
[2] V. Lozupone, “Disaster Recovery Plan for Medical Records Company,” Int. J. Inf. Manage., vol. 37, no. 6, pp. 622–626, 2017.
[3] E. Andrade, P. T. Endo, R. Lima, E. Andrade, P. T. Endo, and R. Lima, “Disaster Recovery Solutions for IT Systems: A Systematic Mapping Study,” J. Syst. Softw., 2018.
[4] R. B. Duffey, “Power Restoration Prediction Following Extreme Events and Disasters,”
Int. J. Disaster Risk Sci., vol. 10, no. 1, pp. 134–148, 2019.

[5] H. Chae, C. E. Koh, and K. O. Park, “Information Technology Capability and Firm Performance: Role of industry,” Inf. Manag., vol. 55, no. October 2017, pp. 525–546, 2018.

[6] D. Meilani, A. Andiningtias, and D. Fatrias, “Decision Support System For Inventory Control of Raw Material,” in 5th International Conference on Industrial Engineering and Applications (ICIEA), 2018, pp. 2–6.

[7] H. R. Soufi, S. A. Torabi, and N. Sahebjamnia, “Developing a Novel Quantitative Framework for Business Continuity Planning,” Int. J. Prod. Res., vol. 0, no. 0, pp. 1–22, 2018.

[8] Faisal, “The Backup Recovery Strategy Selection to Maintain the Business Continuity Plan,” in International Conference on Disaster Management (ICDM), 2018, vol. 229.

[9] H. Abdel and R. Mohamed, “A Proposed Model for IT Disaster Recovery Plan,” Int. J. Mod. Educ. Comput. Sci., vol. 4, no. April, pp. 57–67, 2014.

[10] M. Niemimaa, J. Järveläinen, M. Heikkilä, and J. Heikkilä, “Business Continuity of Business Models: Evaluating the Resilience of Business Models for Contingencies,” Int. J. Inf. Manage., vol. 49, no. April 2018, pp. 208–216, 2019.

[11] S. A. Torabi, R. Giahi, and N. Sahebjamnia, “An Enhanced Risk Assessment Framework for Business Continuity Management Systems,” Saf. Sci., vol. 89, pp. 201–218, 2016.

[12] R. A. Hadiguna, “Decision Support Framework for Risk Assessment of Sustainable Supply Chain Decision Support Framework for Risk Assessment of Sustainable Supply Chain,” Int. J. Logist. Econ. Glob., no. January 2012, 2012.

[13] S. Vazdani, Gh. Sabzghabaei, S. Dashti, M. Cheraghi, R. Alizadeh, and A. Hemmati, “FMEA Techniques Used in Environmental Risk Assessment,” Environ. Ecosyst. Sci., vol. 1, no. 2, pp. 16–18, 2017.

[14] M. Yazdi, “Improving failure mode and effect analysis (FMEA) with consideration of uncertainty handling as an interactive approach,” Int. J. Interact. Des. Manuf., vol. 13, no. 2, pp. 441–458, 2019.

[15] P. Radanliev et al., “Future Developments in Cyber Risk Assessment for the Internet of Things,” Comput. Ind., vol. 102, pp. 14–22, 2018.

[16] H. E. Miller and K. J. Engemann, “Business continuity management in data center environments,” Int. J. Inf. Technol. Syst. Approach, vol. 12, no. 1, pp. 52–72, 2019.

[17] V. Gupta, P. K. Kapur, and D. Kumar, “Prioritizing and Optimizing Disaster Recovery Solution using Analytic Network Process and Multi Attribute Utility Theory,” Int. J. Inf. Technol. Decis. Mak., vol. 18, no. 1, pp. 65–86, 2019.

[18] E. Andrade and B. Nogueira, “Performability Evaluation of a Cloud-Based Disaster,” J. Grid Comput., vol. 17, no. 3, pp. 603–621, 2018.