DISASTER RECOVERY PLANNING FOR IT/IS OF HOSPITALITY INDUSTRY USING NIST SP 800-34 REV.1 METHOD

JOHANES FERNANDES ANDRY[1], NADIA KAREPOWAN[2], HENDY TANNADY[3*]

[1,2]Department of Information System, Universitas Bunda Mulia, Indonesia

[3*]Department of Management, Universitas Multimedia Nusantara, Indonesia

E-mail: [1]jandry@bundamulia.ac.id, [2]nadianataliaaa23@gmail.com, [3*]hendytannady@umn.ac.id

ABSTRACT

The object of this study is a hotel that is in great demand by visitors and continues to develop its business processes. This hotel has made use of the information system to support activities in the hotel which can make it easier for employees. It is the responsibility of the hotel to have a strategy so that the assets and information in the hotel can be safe from accidents, whether intentionally or unintentionally. However, in practice, this hotel still does not have a strategy related to recovery steps in the event of a disaster that can damage assets that can hinder business processes at the hotel. Therefore, as a preventive solution to minimize disaster losses in hotels, disaster recovery is necessary. Diasaster Recovery Planning (DRP) is a structured, documented strategic approach with an approach to dealing with disasters or incidents that can occur at any time. This research was conducted using NIST SP 800-34 Rev. 1 which is one of the methods often used in DRP. The results of the research contain service recovery recovery with disaster actions. Furthermore, there are three information systems that have medium level impact, namely the booking information system and the reports. And what has a low level of impact is the check in and check out information system. Preparation of a Disaster Recovery Plan adapted to the existing situation and conditions, so that planning and handling can be carried out appropriately.

Keywords: *Disaster Recovery Planning, NISP 800-34 Rev.1, Hotel, Information System*

1. INTRODUCTION

Hotel of this study is one of the most popular visitors, both local visitors and visitors who come from outside the city or abroad. This hotel is in great demand because it offers attractive facilities and always follows the existing trends. In addition, even though the offers provided are so many and attractive, this hotel still provides affordable rental prices and can be said to be cheaper when viewed from the various facilities provided. To maximize the success of business processes at the hotel, this hotel utilizes information systems and technology to support operational activities so that business processes can run efficiently and effectively [1]. This hotel has several information systems to support existing business processes.

In order for the continuity of business activities at the hotel to be maintained, the hotel realizes that it is necessary to implement well-structured and well-organized control measures [1]. This control effort is about preventive measures that can serve as guidelines for the hotel to minimize the negative impacts that can occur if a disaster or accident is hit either accidentally or intentionally [2] .

Currently, many organizations have utilized technology and information systems to support business processes in order to run more efficiently and effectively, however, many organizations have not prepared efforts to prevent disasters that can occur at any time, resulting in substantial losses in the event of a disaster [3]. This is what Hotel management avoids and encourages the organization to provide a prevention strategy for the possibility of a disaster that could occur [2].

Strategic planning for the possibility of natural disasters as well as those caused by humans can be done with one of them using DRP or Disaster Recovery Planning. DRP is a type of contingency plan that contains organizational preparation and response in the event of a disaster, both natural and man-made [3].

With the existence of DRP in an organization, it is useful as a form of anticipation of possible disasters, resulting in delays in the provision of information technology services due to loss or damage after a disaster occurs [4]. The occurrence of delays in information technology services will of course affect business activities in an organization [5]. Apart from that, DRP also helps in making decisions. With the existence of DRP, an organization does not need to take a long time to make decisions if a disaster occurs which could result in an incorrect solution because it is carried out spontaneously and not structured [6].

Seeing the various benefits that an organization can feel with the existence of DRP, this study aims to compile the DRP for the hotel. This DRP preparation can be done by applying one of the existing frameworks [6][7]. This research uses the framework of the NIST SP 800-34 which is a standardization document issued by the National Institute of Standards and Technology (NIST) which aims to provide guidance and also considerations in the preparation of plans related to information system contingencies [7].

In this research, the preparation of the DRP will be guided by the NIST SP-800 -34 framework which begins with the identification process and also a risk assessment with the aim of being able to identify risk patterns that can threaten the sustainability of business activities. This is followed by a structured guide that produces recovery steps resulting from the results of the risk identification analysis at the hotel. With the preparation of DRP using the NIST SP 800-34 framework, it is hoped that it can become a guide and guideline in responding when a disaster occurs as a preventive measure that can minimize losses. In addition, the results of this study are also expected to improve the quality of existing governance in hotels in the future.

2. THEORY

This chapter will describe several theories that become the basis and references needed by researchers to be able to carry out research related to DRP using the NIST SP 800-34 Rev.1 method.

2.1 Disaster Recovery Plan (DRP)

DRP or Disaster Recovery Plan is a reference that contains procedures that aim to solve problems that result in loss of information system resources in an organization or company due to a disaster, to provide backup strategies or operations when the main system stops, and also to manage the data recovery process [8]. with the aim of minimizing the losses suffered by the organization or company [9]. The advantages of having a Disaster Recovery Plan include [10]: (1) It can reduce the possibility of economic loss due to disasters, (2) Increase organizational stability, (3) Provide an orderly and measurable recovery plan, (4) Avoid dependence on a concentrated group of personnel, (5) Protect the assets of the organization, including the safety of its personnel.

2.2 NIST SP 800-34 Rev.1

The NIST SP 800-34 Contingency Planning Guide for Federal Information Systems is one of many standardization-related documents issued by the National Institute of Standards and Technology (NIST) [11]. NIST SP 800-34 is a framework that will provide recommendations, direction and also considerations in the formulation of information system contingency plans for formation in NIST SP 800-34 which focuses on immediate handling steps after an organization disruption occurs [12]. Temporary measures such as relocation as well as operating the system to alternative locations or also carrying out information system functions using manual methods are also included in the contingency plan [13]. NIST SP 800-34 describes the process related to contingency planning in 7 steps, namely as follows [14]: 1) Developing a Continuity Planning Policy 2) Conducting a Business Impact Analysis 3) Identifying Preventive Controls 4) Creating a Contingency Strategy 5) Developing a Contingency Plan 6) Testing the Plan , Training, and Exercises 7) Maintenance Plan.

2.3 Business Impact Analysis (BIA)

Business Impact Analysis is the stage in making a Disaster Recovery Plan (DRP) which has a goal to know which business process is a business processes which are actually vital in an organization or company as well as for know about the impact that will be experienced by the organization or company if there is a disruption or disaster in the IS / IT support these business processes [15][16]. Apart from that this BIA also used in making a decision management of the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each business function or service process [17]. Business Impact Analysis (BIA) aims to helps an organization or company understand the impact originating or resulting from a disaster that did not expected, for example a computer network infrastructure down so the service couldn't be used either for access to information and email services, IS / IT and so forth [18][19]. So it takes a period tolerable time if a system service paralyzed by the disaster [20].

3. METHODOLOGY

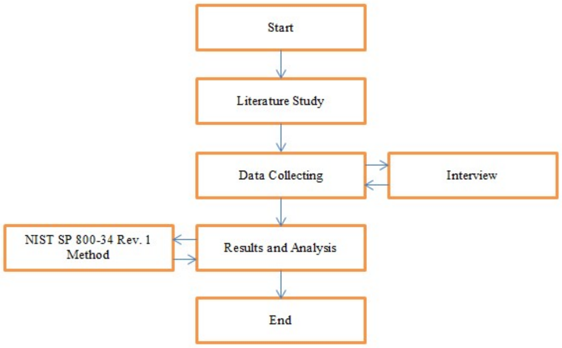

Figure 1: Research Methodology

The following will describe an explanation regarding the methodology in this study, including [21]:

1) Study of literature. This stage is the stage for finding and studying material related to research from various references in order to help researchers carry out research according to predetermined goals.

2) Data collection. This stage is the stage of data collection which is the data from where the researcher is carried out. In this study, the data collection process was carried out by conducting direct interviews and by telephone with one of the owners.

3) Results and Discussion. This stage is the stage for analyzing, identifying and finding solutions to the research being carried out. This DRP study was designed using the NIST SP 800-34 Rev.1 method, which is the most widely used method. After analyzing using this method, a solution or strategy will be generated that can overcome the problems studied in this study.

4. RESULT AND ANALYSIS

In this chapter, the researcher will describe the explanation of the design carried out regarding the design of disaster recovery in hotels. This hotel has used IT / IS in carrying out its daily operational activities. It uses several information systems to support the implementation of operational activities at the hotel. The following are some information systems, including:

Employee and Staff Attendance Management Information System, Information System to Manage Room Data, Information System to Manage Guest Data, Room Check Information System, Room Reservation Information System, Check in Information System, Check out Information System, Reports Information System.

By implementing IT/IS, it requires a computer network infrastructure that can integrate IT / IS applied to hotels. In 2017, the servers at hotel were hit by lightning which resulted in the damage of several computers. To overcome the damage caused by disasters, both natural disasters and disasters caused by humans, it is necessary to design a risk management procedure that is able to mitigate the risks that may occur. Therefore, the Disaster Recovery Plan (DRP) is a design document that must be owned by every organization, which aims to minimize losses that can occur due to the disaster.

4.1 Risk Identification and Assessment

This stage focuses on threats that can affect existing hotel assets to support or support the implementation of services or operational activities. This risk identification and assessment is needed so that it can determine the classification related to the impact and also the cause of a disaster or disturbance that could potentially occur. In addition, it can be useful in determining the optimal or appropriate steps to mitigate potential risks that may harm the hotel. The risk that can occur in the hotel building either as a whole or also only part of the hotel building can certainly damage and destroy the assets of some hotel assets. For example, prolonged power outages, earthquakes, floods, fires, volcanic eruptions, server damage, virus attacks, and others.

Based on data obtained from an interview with one of the owners, the most frequent problem is the occurrence of a power cut and a lightning strike on the hotel server which resulted in obstruction of service and hotel operational activities. In addition, the problem for hotels is the lack of human resources and strategies for dealing with disasters or disruptions that can occur at any time, impacting the hotel business process. This Risk Identification and Assessment stage is the very first stage of the Disaster Recovery Plan procedure. This Risk Identification and Assessment is used to determine what threats have the potential to pose a risk to assets. The following is a description of threats that can pose a risk to hotel assets and important data, which are described in Table 1. Risk Identification and Assessment.

4.2 Business Impact Analysis (BIA)

Business Impact Analysis or BIA is a very important process in making DRP. Before compiling BIA, it is necessary to study what services are available at hotels to support the implementation of business processes. After the mapping is done, it can enter the stage of making BIA. BIA is one of the stages in making a Disaster Recovery Plan (DRP) which is carried out with the aim of seeing which processes are vital business processes in hotels and also to see the impact that will occur on the hotel at the time of the incident. disaster or disruption of IT / IS supporting hotel operations.

Table 1: Identification of Threats and Risks

Threat	Description	Risk
Lightning	Lightning strikes can cause damage to the LAN or electrical network and existing electronic devices.	Operational activity is interrupted and may damage LAN, power lines or electronic devices.
Floods	Floods can cause damage to hotel facilities and infrastructure.	Inventory damage, customer inconvenience, absenteeism of employees and staff as well as obstruction of the implementation of operational activities using IS.
Earthquake	An earthquake that exceeds 5 on the Richter scale can cause damage to infrastructure in hotel buildings.	Termination of hotel operations, stakeholder accidents and damage to hotel inventory.
Volcanic Eruption	Ash from erupting mountains can disrupt activities at the hotel.	Termination of operational activities, employee absences, customer inconvenience
Fire	Fires can occur due to human error or errors in electric currents.	Damage to hotel facilities, stakeholder accidents, customer inconvenience.
Electrical Interference	Electrical disturbances can occur for example due to damage from the center or other errors.	Cessation of operational activities using information systems and customer inconvenience.
Serverdown	The server is damaged due to the downtime of the existing server.	There was a failure to the server.
Worms attack, malware, viruses and etc.	Attacks of worms, malware, and the like can occur at any time, for example when sending or receiving email.	Loss of data, Obstruction of operational activities using information systems
Cyber threat	Cyber threats can occur at any time due to a security hole in the network system.	Damage to the reputation, cessation of operational activities, data leakage and data theft.

In addition, BIA is also used for the purpose of retrieving the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each existing business function or service process. DRP will always liaise with RTOs and RPOs. RTO is the duration or time related to how long operational activities or activities in an organization can run like returning after an accident or disaster. Making an RTO is very important because the duration or time required for the recovery process will be better for the organization. Meanwhile, RPO is a disaster recovery time or the maximum time that can be tolerated when data loss occurs or when an accident or disaster occurs.

Then what must be done is to determine the IT / SI which has a high and low critical level based on regulations and the level of the organization's reputation. Based on the results of interviews conducted regarding the determination of the critical level of information systems or services available at hotel, the following are categories of the impact of disruption or disasters on the hotel business which will actually be in Table 2. Mapping of IT / IS Services.

Table 2: Mapping of IT or IS Services

Information Systems	Impact If SI Down	Impact Level
Manage Room Data	Room data cannot be managed or updated.	High
Manage Guest Data	Guest data cannot be managed or updated.	Medium
Room Checks	Cannot check rooms through the system.	High
Booking	Cannot input process data cannot input data from customer checkin room reservations.	Medium
Check in	Cannot input the check-in process data from the customer.	Low
Check out	Unable to update checkout data from customers.	Low
Reports	cannot access or view	Medium

	existing data reports	

The next stage is to determine the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) of each IT/IS service with the aim of analyzing the business impact. RTO is related to the time available to restore an interrupted system, whereas RPO is the amount of data loss that can be tolerated. The following is an overview of RTO and RPO identification which can be seen in Table 3.

There are two information systems that have high level impact, there are three information systems that have medium level impact and the remaining two information systems that have low level impact. The management room data information system has a high level of impact because if this information system cannot be operated or is hampered by disruption or disaster, the hotel cannot serve hotel visitors who want to rent rooms because the room data update process cannot be updated so that it cannot perform services which relates to room data which results in the hotel being unable to serve hotel visitors who want to stay at the hotel. Furthermore, the information system that has a high level of impact is the room checks information system. This information system has something to do with the previous information system, namely manage room data. If manage room data IS cannot be executed, the hotel cannot serve visitors because the room data has not been updated. Likewise with room checks IS, if this IS is hampered, the hotel cannot process visitors who come because they cannot find out which rooms are empty at that time if the IS is obstructed or experiencing interference.

Table 3: Identification of Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

Information Systems	Recovery Time Objective	Recovery Point Objective	Impact Level
Manage Room Data	1-12 Hours	1-12 Hours	High
Manage Guest Data	1-24 Hours	1-24 Hours	Medium
Room Checks	1-12 Hours	1-12 Hours	High
Booking	1-24 Hours	1-24 Hours	Medium
Check in	1-24 Hours	1-24 Hours	Low
Check out	1-24 Hours	1-24 Hours	Low
Reports	1-24 Hours	1-24 Hours	Medium

At the medium level impact, first there is IS manage guest data. This IS is included in the impact medium level because guest data can still be done later if the IS is running as normal after the disturbance occurs. The second IS which is included in the medium impact level is the booking IS, this SI is the medium level impact because if the IS is a problem, the customer can make the booking process in other ways, one of which can be done by contacting the hotel contact. The latest IS included in medium impact levels are IS reports. The reason why this SI is at a medium level impact is because the process of manage reports can still be done after a disruption occurs so that it does not really hamper the operational process at the hotel.

Furthermore, IS which includes low level impact is IS Check-in. This does not mean that it is not too important, but this IS can still be tolerated if there is a disturbance because the check-in process can be done manually and later processed again when the IS is running normally. Likewise with IS Checkout, it can be done manually first and can be processed again after the problem has been resolved.

4.3 Identification of Preventive Controls

The preventive control process is based on the results of the risk identification and assessment process. From the results of the hotel that can generate risks to hotel assets. Of the various risks identified in that phase, all of them are the responsibility of the Information Technology Division. This contingency strategy is made including determining a strategy related to backup and also determining the alternative location of each of the existing services.

4.4 Contingency Strategy Development

This contingency strategy includes determining a strategy related to backups and also determining the alternative location of each of the existing services. Backup Strategy - The recommendation for the backup strategy given is related to the method, frequency and type of backup that can be done which is based on considerations regarding the amount of lost data that can be tolerated when there is a disruption or damage to the service. Alternative Locations - Recommendations regarding the selection of an alternative location strategy should be based on the cost ability of the hotel and consider the amount of lost data that could occur due to damage or disruption. The realization of alternative location procurement can be realized in three ways, namely preparation for a more strategic location cooperation with other companies or hire vendors.

4.5 Development of a Contingency Plan

In the NIST SP 800-34 method, there are 3 elements in the contingency plan, namely the activation phase, the recovery phase and also the reconstitution phase. Recommendations related to contingency plans are expected to be carried out in stages, so that development can continue to be carried out by the hotel. Supporting Information - There are several things that have been determined and determined in terms of developing this contingency plan, namely as follows Reserve staff, Roles and Responsibilities and Gathering point. Recovery Phase - This phase will start when DRP has been activated and has been announced to all components in the hotel. This activity will be more focused on restoring service capabilities, repairing damage and also running existing service operations through alternative strategies. The following is a description of recovery strategies related to potential natural or human-induced disasters, which are listed in Table 4. Recovery Process. Reconstitution Phase - This phase is the phase where the recovery process has been completed. This phase focuses more on validation related to the recovery process and also on DRP deactivation.

Table 4: Recovery Strategy

Distraction	**Obstacles**	**Recovery Process**
Lightning	Damage to the power grid or LAN.	Prepare a team that can repair and replace or spare tools.
Floods	Floods can cause damage to hotel facilities and infrastructure.	Providing a special team in charge of saving facilities and infrastructure. Important assets can be placed in a higher place.
Earthquake	An earthquake that exceeds 5 on the Richter scale can cause damage to infrastructure in hotel buildings.	Provide a special team to save important assets and improve the quality of the building infrastructure.
Electrical Interference	Services and operational activities are hampered or cannot be executed.	Provide sufficient electricity and fuel generator.
Volcanic Eruption	Ash from erupting mountains can disrupt activities at the hotel.	Prepare building infrastructure that is free from ash from mountain eruptions
Fire	Damage to hotel assets and stakeholder accidents resulting in operations halting.	Prepare a rescue team for both hotel assets and stakeholders.
Server down	The server experienced a certain problem, causing the server to go down.	Provide a backup server so that operations are not hampered.
Worms attack, malware, viruses and etc.	The operating system becomes slow and data loss.	Using an antivirus that guarantees and always backups data regularly.
Cyber threat	There is a data leak by irresponsible parties and there is a security hole in the computer network.	Change passwords regularly and tighten safeguards.
Information System Disruption	The information system or database has an error so that it cannot be accessed.	Provide a dedicated internal team that can perform information system backups, checks and repairs on coding programs and databases.

The various activities that need to be carried out in this reconstitution phase namely DRP deactivation, Data Backup, Data Validity Testing, Testing the Validity of the Function, Cleanup and Documentation. Event detected as a disturbance can be categorized as a disaster and requires DRP activation. Actually, not all disruptions that will disrupt the operation of the system's operational services can be categorized as a disaster.

5. CONCLUSION

Based on the results of the analysis carried out, the conclusions obtained regarding the preparation of the DRP that have been carried out are the final result of this research is a Disaster Recovery Plan document which contains procedures for the Disaster Recovery Plan which can be used as input for the hotel in making and implementing a recovery plan after a disaster. Disaster Recovery Plan is prepared by identifying disasters and business process conditions. Out of seven information systems owned by hotel management, there are two information systems that have a high level of impact, namely the manage room data information system and the room checks information system. Furthermore, there are three information systems that have medium level impact, namely the booking information system and the reports. And what has a low level of impact is the check in and check out information system. Preparation of a Disaster Recovery Plan adapted to the existing situation and conditions, so that planning and handling can be carried out appropriately. Recommendation for further research is strongly suggest to use the method to another kind of industries like oil and gas or manufacture industries, so that the result could give bigger perspective about the impact of method toward various industries.

REFERENCES:

[1] M. Uddin and A. Abdul, “Virtualization Implementation Model for Cost Effective & Efficient Data Centers,” Int. J. Adv. Comput. Sci. Appl., vol. 2, no. 1, 2011, doi: 10.14569/ijacsa.2011.020110.

[2] H. S. R. R. Dr. Utkarsh Seetha, “Data Center Establishment to run the IT System in Power Utilities,” Glob. J. Comput. Sci. Technol., vol. 13, no. 1, 2012.

[3] N. Dhanujati and A. S. Girsang, “Data Center-Disaster Recovery Center (DC-DRC) for High Availability IT Service,” Proc. 2018 Int. Conf. Inf. Manag. Technol. ICIMTech 2018, no. September, pp. 55–60, 2018, doi: 10.1109/ICIMTech.2018.8528170.

[4] P. Jones, D. Hillier, and D. Comfort, “Data centres in the UK: property and planning issues,” Prop. Manag., vol. 31, no. 2, pp. 103–114, 2013, doi: 10.1108/02637471311309418.

[5] T. Daim, J. Justice, M. Krampits, M. Letts, G. Subramanian, and M. Thirumalai, “Data center metrics: An energy efficiency model for information technology managers,” Manag. Environ. Qual. An Int. J., vol. 20, no. 6, pp. 712–731, 2009, doi: 10.1108/14777830910990870.

[6] A. Alaraifi, A. Molla, and H. Deng, “An exploration of data center information systems,” J. Syst. Inf. Technol., vol. 14, no. 4, pp. 353–370, 2012, doi: 10.1108/13287261211279080.

[7] J. Shropshire and C. Kadlec, “Developing the IT disaster recovery construct,” J. Inf. Technol. Manag., vol. 20, no. 4, 2009.

[8] H. N. Prasetyo, N. Supriatna, A. P. Raharjo, and W. Wikusna, “Information Technology Disaster Recovery Plan (IT-DRP) Model-Based on NIST Framework in Indonesia,” IJAIT (International J. Appl. Inf. Technol., vol. 3, no. 01, p. 34, 2020, doi: 10.25124/ijait.v3i01.2317.

[9] M. Swanson, P. Bowen, A. W. Phillips, D. Gallup, and D. Lynes, “Contingency Planning Guide for Federal Information Systems.,” NIST Spec. Publ. 800-34 Rev. 1, no. May, p. 150, 2010.

[10] Marianne Swanson, Pauline Bowen, Amy Wohl Philips, Dean Gallup, and David Lynes, “Contingency planning guide for information technology systems: Recommendations of the National Institute of Standards and Technology,” vol. 1, pp. 1–117, 2010.

[11] M. J. Shallcross, “HathiTrust is a Solution recommendations made by,” 2009.

[12] N. Tariku, “Information Technology Disaster Recovery Plan (ITDRP) Framework For Banks in Ethiopia Information Technology Disaster Recovery Plan Framework for Banks in Ethiopia,” pp. 0–11, 2020.

[13] P. Somasekaram, “A Component-based Business Continuity and Disaster Recovery Framework,” Uppsala Univ., no. March, 2017.

[14] Kurniasari, F., Lestari, E. D., Tannady, H. Pursuing Long-Term Business Performance: Investigating the Effects of Financial and Technological Factors on Digital Adoption to Leverage SME Performance and Business Sustainability—Evidence from Indonesian SMEs in the Traditional Market. Sustainability 2023, 15, 12668. https://doi.org/10.3390/su151612668

[15] Tannady, H., & Andry, J. F. (2023). The Sustainable Logistics: Big Data Analytics and Internet of Things. International Journal of Sustainable Development & Planning, 18(2).

[16] Andry, J. F., Liliana, L., Chakir, A., & Tannady, H. (2023, November). Online voucher e-commerce testing using ISO 9126 model. In AIP Conference Proceedings (Vol. 2693, No. 1). AIP Publishing.

[17] Tannady, H., Lestari, R., Renwarin, J. M., Nurjanah, S., & Destari, D. (2023, July). Service quality analysis on packaging terminal services at Tanjung Priok Port. In AIP Conference Proceedings (Vol. 2798, No. 1). AIP Publishing.

[18] Madyatmadja, E. D., Liliana, L., Andry, J. F., & Tannady, H. (2020). Risk analysis of human resource information systems using COBIT 5. Journal of Theoretical and Applied Information Technology, 98(21), 3357-3367.

[19] Mishra, V. P., Krushnasamy, V. S., Akram, F., Tannady, H., & Pathak, N. K. (2023). An Operative Encryption Method with Optimized Genetical method for Assuring Information Security in Cloud Computing. International Journal of Intelligent Systems and Applications in Engineering, 11(8s), 276–284.

[20] Amanullah, M., Mishra, V. P., Mayavan, L., Tannady, H., Kulkarni, N., & Kolandaisamy, R. (2023). An Effective Double Verification-

Based Method for Certifying Information Safety in Cloud Computing. International Journal of Intelligent Systems and Applications in Engineering, 11(8s), 268–275.

[21] Madyatmadja, E. D., Alexander, J., Andry, J. F., & Tannady, H. (2022, July). Evaluation of applied service strategy using ITILv3 framework-A case study on a machinery company. In AIP Conference Proceedings (Vol. 2453, No. 1). AIP Publishing.