**JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)**
**Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi**
**ISSN: 2540-8984**
**Vol. 8, No. 2, Juni 2023, Pp. 407-418**

# E-GOVERNMENT RISK MANAGEMENT ANALYSIS USING PERMENPAN RB NUMBER 5 OF 2020 AT COMMUNICATION AND INFORMATION OFFICE OF XYZ REGENCY

**Ozha Dilatri Niverta[1], Farisya Setiadi[2], Kusuma Adi Achmad[3]**

1. Telkom University, Indonesia
2. Telkom University, Indonesia
3. Telkom University, Indonesia

**Article Info**
**Kata Kunci:** teknologi informasi, ancaman, risiko, SPBE, manajemen risiko

**Keywords:** teknologi informasi, ancaman, risiko, SPBE, manajemen risiko

**Article history:**
Received 6 January 2023
Revised 13 January 2023
Accepted 8 February 2023
Available online 1 June 2023

**DOI :**
https://doi.org/10.29100/jipi.v8i2.3475

* Corresponding author.
Corresponding Author
E-mail address:
ozhadilatri@student.telkomuniversity.ac.id

## ABSTRAK

Teknologi Informasi (TI) sering dimanfaatkan oleh instansi pemerintah untuk mendukung pencapaian tujuan pemerintahan. Semakin tinggi penerapan TI pada instansi pemerintah, maka semakin tinggi pula an-caman dan risiko yang terjadi. Pemerintah Kabupaten XYZ merupakan salah satu instansi pemerintah yang menerapkan Sistem Pemerintah Berbasis Elektronik (SPBE). Penerapan SPBE melalui pemanfaatan TI un-tuk memberikan layanan kepada pengguna SPBE memerlukan manajemen risiko. Pemanfaatan TI berbasis manajemen risiko memudahkan dalam mencapai tujuan, mengurangi risiko, dan melindungi sumber daya TI instansi pemerintah. Penelitian ini bertujuan untuk mengidentifikasi potensi risiko-risiko yang terjadi menggunakan Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (PERMENPAN RB) Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik. Hasilnya menunjukan bahwa terdapat 23 kemungkinan risiko yang terjadi, terbagi menjadi dua kategori, meliputi risiko positif dan risiko negatif. Risiko positif, meliputi kesesuaian layanan SPBE dengan rencana induk SPBE nasional, fleksibilitas arsitektur SPBE, kesesuaian penerapan SPBE dengan visi dan misi serta regulasi terkait, fleksibilitas kerja pegawai, kesesuaian kebutuhan infrastruktur SPBE dan prioritas instansi, ketepatan waktu penyelesaian proyek SPBE, penerapan keamanan informasi (backup data), dan pemuta-khiran proses bisnis dan layanan SPBE. Analisis risiko negatif yang berdampak tinggi adalah minimnya pelatihan TI untuk staf yang diselenggarakan oleh pemerintah daerah. Berdasarkan evaluasi, diperlukan rencana mitigasi penanganan risiko SPBE terkait kurang mahirnya staf dalam mengakses aplikasi, phish-ing, pembobolan website pemerintah daerah, kerusakan komponen perangkat keras, dan ketidaksesuaian ketrampilan TI dan kebutuhan SPBE.

## ABSTRACT

Information Technology (IT) is often used by government agencies to support the achievement of gov-ernment goals, the higher the utilization of IT in government agencies, the higher the threats and risks that occur. The XYZ Regency Government is one of the government agencies that implement the Electronic-Based Government System (e-Government). The implementation of e-Government through the use of IT to provide services to users requires risk management. The use of IT based on risk management makes it eas-ier to achieve goals, reduce risks, and protect IT resources of government agencies. This study aims to identify potential risks that occur using the Regulation of the Minister of Administrative and Bureaucratic Reform Number 5 of 2020 concerning Guidelines for Risk Management of Electronic-Based Government Systems. The results show that there are 23 possible risks that occur, divided into two categories, includ-ing positive risks and negative risks. Positive risks include the suitability of e-Government services with the national e-Government master plan, flexibility of e-Government architecture, conformity of e-Government implementation with the vision and mission as well as related regulations, employee work flexibility, suita-bility of e-Government infrastructure needs and agency priorities, timeliness of e-Government project completion, implementation of information security (data backup), and updating of e-Government business processes and services. A high impact negative risk analysis is the lack of IT training for staff organized by local governments. Based on the evaluation, it is necessary to have a risk mitigation plan for e-Government related to the lack of expertise of staff in accessing applications, phishing, breaking into local government websites, damage to hardware components, and mismatch of IT skills and e-Government needs.

## I. INTRODUCTION

Information technology (IT) has become a very important requirement for organizations to increase their productivity [13]. The development of technology today offers many benefits. Individuals, institutions, and government agencies often use IT to support the achievement of organizational goals. This shows that in Indonesia, the use of IT has become an important part of the sustainability of an organization's business processes. In addition to the rapid development of IT, there are still many vulnerabilities and risks in IT implementation, the higher the application of IT in an organization, the higher the threats and risks that occur [14]. Some organizations are still unable to identify and manage threats and risks that will arise after the company implements IT. Therefore, there is a need for risk management that aims to facilitate the achievement of business goals, reduce risk and protect IT in the company [4].

In response to the development of information technology in Indonesia, the President of Indonesia issued Presidential Regulation (PERPRES) Number 95 of 2018 concerning Electronic-Based Government Systems with the aim of increasing the integration and efficiency of electronic-based government systems. In the implementation of e-government, local governments are required to carry out risk management according to Indonesian National Standards as stated in the Regulation of the Minister of Administrative Reform and Bureaucratic Reform (PERMENPAN RB) Number 5 of 2020 [5].

XYZ Regency is one of the local government agencies that has implemented an Electronic-Based Government System in its government system. E-government is the administration of government that uses information and communication technology to provide services to e-government users. E-government is aimed at realizing effective, efficient, and sustainable governance, as well as quality e-government services [2]. With the development of technology, it will certainly affect the XYZ government which relies on technology as its government system. Therefore, the XYZ Regency government needs to implement risk management to reduce and overcome IT risks that hinder the achievement of organizational goals related to the use of IT itself. Risk management can help develop SPBE so that the services used can work optimally [7].

Therefore, the authors conducted research on e-government risk management in the XYZ Regency Government using the PERMENPAN RB guidelines No. 5 of 2020. The purpose of this study was to take risks that occurred in the XYZ Regency Government by identifying sources of risk, estimating the impact and recommendations for management risk.

As also used in the journal entitled "E-government Operational Risk Management Design in the Risk Category of Infrastructure, Applications, Services, data and information (Case Study of Bandung City Government)", the approach method used both uses qualitative methods and uses both PERMENPAN RB guidelines no. 5 of 2020, but the journal is limited to the focus of the risk categories taken, namely infrastructure, applications, services, data and information only [5]. So in this study the researchers wanted to identify risks based on 16 e-government risk categories. So the results obtained will be different from previous studies.

## II. RESEARCH METHODOLOGY

### A. Research Methodology

The research methodology is a discussion of the theoretical concepts of various methods, advantages and disadvantages, which in scientific work is followed by the selection of the method used [9]. The research method used in this research is qualitative. Qualitative research is a research procedure that produces descriptive data, in the form of writing or speech, and observed behavior. Qualitative research aims to obtain a comprehensive understanding of social reality from the participant's perspective [3]. The stages of research carried out in this study are as follows.

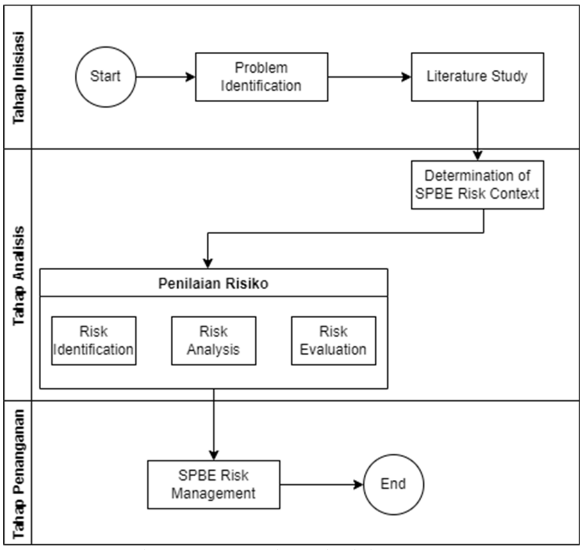

Figure 1 Research Methodology

1. Initiation Stage
   At this stage the research begins by identifying the problem first. Problem Identification is a step in finding and identifying problems that must be investigated more deeply in the phenomenon. These problems will later be measured and linked to theories in accordance with existing research procedures [6]. Then the researcher conducted a literature study to strengthen the research basis. Literature study is a technique used to find ideas or references in research or problem solving by tracing information that has been previously written. In this study, researchers must have broad insight into the object to be studied. Otherwise, in a large-scale demonstration, the research is doomed to fail [8]. The field study used in this research is to conduct interviews and make direct observations of a particular object.
2. Analysis Stage
   At this stage, the researcher analyzed the data that had been collected previously. Next, the researcher determined the context of the e-government, then continued with a risk assessment, where the risk assessment consisted of identifying risks, analyzing risks and evaluating risks [11]. This research was conducted at communication and Information office of XYZ Regency. With the data that has been collected, the analysis process is carried out using the PERMENPAN RB guidelines Number 5 of 2020. The following is the e-government risk management process.

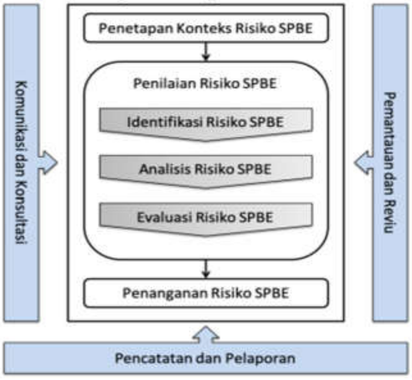

Figure 2 E-Government Risk Management Process

Based on Figure 2, the e-government risk management process can be explained as follows

a. Communication and Consulting
   Communication and consultation is an ongoing iterative process to provide, share or obtain information, and engage in dialogue with stakeholders about e-government risks [1].
b. E-Government Risk Context Determination
   The determination of the e-government risk context aims to determine the basic parameters and scope of the e-government risk application that must be managed in the e-government risk management process [1]. The following are the steps for determining the e-government Risk context.
   1. General Information Inventory
   2. Identification of e-government Targets

3. Determination of the Implementation Structure of E-government Risk Management
4. Identification of Stakeholders
5. Identification of Legislation
6. Determination of E-government Risk Category
7. Determination of E-government Risk Impact Area
8. Determination of E-government Risk Criteria
9. E-government Risk Analysis Matrix
10. E-government Risk Appetite
11. E-Government Risk Assessment

c. E-government risk assessment on the implementation of e-government is carried out through a process of identification, analysis and evaluation of e-government risk. The e-government risk assessment aims to understand the causes, possibilities and impacts of e-government risks that may occur in central and local government agencies [1]. The following are the stages of e-government risk assessment.

1. E-government Risk Identification
   E-government Risk Identification is a process of digging up information about the events, causes, and impacts of e-government Risks [1].
2. E-government Risk Analysis
   E-government risk analysis is the process of assessing the e-government risks that have been identified previously. E-government risk analysis is carried out by determining the control system, the level of possibility and the level of impact of the occurrence of e-government risk [1].
3. E-government Risk Evaluation
   E-government risk evaluation is carried out to determine whether further efforts are needed to address e-government risks, and prioritize the handling of these risks. If there are several e-government risks with the same size, then the way of determining priority is based on expert judgment [1].
4. Monitoring and Review
   Monitoring aims to monitor factors or causes that affect e-government risk and environmental conditions in central and local government agencies. The monitoring results can be used as a basis for readjusting the E-government risk management process. The review aims to control the suitability and accuracy of the implementation of the entire E-government risk management process in accordance with applicable regulations. The review is carried out according to the agreement of each central agency and local government [1].

3. E-Government Risk Management Stage
   At this stage, it is carried out to compile or make recommendations for handling e-government risks. Recommendations can be given to the Bandung city government after verification of conformity. E-government risk management is the process of modifying the causes of e-government risks. E-government risk management is carried out by identifying various options that can be applied and selecting one or more e-government risk treatment options [1]. Next, the recording and reporting process is carried out. Recording and Reporting is designed to communicate e-government risk management activities and outputs, inform decision making, improve the quality of e-government risk management activities, and monitor interactions with stakeholders, including e-government risk management responsibilities and accountability [1].

## B. Data Collection Techniques

Data collection techniques in this study were carried out by conducting data analysis to collect information related to research needs. Furthermore, conducting interviews with informants in order to obtain the information needed to analyze data and make direct observations of a particular object. Then the data obtained from the Communication and Information Office of XYZ Regency was used in the analysis using PERMENPAN RB Number 5 of 2020.

1. Document Analysis

Document analysis is a method or activity to collect information about documents within the XYZ Regency Government related to research needs. The activity carried out is the analysis of documents needed to obtain relevant data and information as design materials in research [1].

2. Interview
   An interview is a face-to-face conversation, in which one party gathers information from the other [15]. The purpose of this interview is to obtain correct information from sources, namely the Head of the Main IT Division and Staff related to e-government in the XYZ Regency Government regarding the Electronic-Based Government System to obtain the required data. Interviews were conducted by the interviewer asking several questions to the informants regarding the e-government risk conditions, questions asked about the description of the incident, causes, impacts, impact areas, level of possibility and level of impact of the risk conditions.
3. Observation
   Observation as a data collection technique has specific characteristics compared to other techniques. Observations made through direct observation to the location, such as the condition of the workspace and work environment, can be used to determine factors that are suitable for interviews and support questionnaires for job analysis [10].
4. Data Needs
   The data used in this study are primary data and secondary data. Primary data is data taken from a study by conducting interviews and direct observations of a particular object. Secondary data is obtained through journals, books and archives both published and unpublished in general [12].

## III. Result and Discussion

### A. Determination of E-Government Risk Context

The determination of the e-government risk context aims to determine the basic parameters and scope of the e-government risk application that must be managed in the e-government risk management process [1]. The stages of establishing the e-government Risk context consist of general information, objectives, risk management implementation structure, list of stakeholders, list of laws and regulations, risk categories, impact areas, probability criteria, impact criteria, risk matrix, risk level, and risk appetite. The following are the steps for determining the e-government Risk context.

1. General Information Inventory
   General Information Inventory aims to provide an overview of work units that implement e-government risk management [1]. The Department of Communication and Information as the Risk Ownership Unit (UPR) of the e-government has the task of implementing the implementation of e-government risk management and has the function of compiling and determining the e-government risk assessment, implementing coordination and operations.
2. Identification of E-government Targets
   Identification of e-government Targets aims to identify the objectives of the e-government as well as indicators and objectives that support the objectives of the work unit that is the e-government UPR [1]. The targets of the e-government UPR include the effectiveness of local government administration, public information disclosure, and the availability of data and information.
3. Determination of E-Government Risk Management Implementation Structure
   Determination of the e-government Implementing Structure aims to identify the work unit responsible for implementing e-government risk management [1]. Communication and information office of XYZ Regency officials are involved as implementers, coordinators and managers of e-government risk management, including heads of offices, secretaries and heads of fields.
4. Identification of Stakeholders
   Identification of Stakeholders aims to obtain information and understand the parties interacting with the e-government UPR in order to achieve the e-government targets [1]. Stakeholders include relevant ministries, regional apparatus for managing ICT, regional apparatus for business process owners, and academics and practitioners.
5. Identification of Legislation
   The identification of laws and regulations aims to understand the powers, duties, duties, functions and legal obligations that must be carried out by UPR e-government [1]. Related policies include PERPRES on e-

government, PERMENPAN RB on e-government Evaluation Guidelines, and PERBUP on implementation of e-government XYZ Regency.

6. Determination of E-Government Risk Category
   The identification of e-government risk categories aims to make the process of identification, analysis, and evaluation of e-government risks comprehensively [1]. The e-government risk category consists of 16 categories including the national e-government master plan, e-government architecture, e-government plan map, business processes, plans and budgets, novation, compliance with regulations, procurement of goods and services, development/development projects, data and information, e-government infrastructure, e-government applications, e-government security, e-government services and e-government human resources.
7. Determination of E-Government Risk Impact Area
   Determination of Impact Areas aims to find out which areas in central and local government agencies are affected by e-government risk [1]. The impact area consists of 7 categories covering finance, reputation, performance, organizational services, ICT operations and assets, law and regulation, and human resources.
8. Determination of E-Government Risk Criteria
   In determining the risk criteria, there are 2 criteria that are determined, namely the probability criteria and the impact criteria. The possible criteria are presented in the following table.

TABLE I
E-GOVERNMENT PROBABILITY CRITERIA

| No | Probability Level | Percentage Likelihood of Occurring in 1 Period |
|---|---|---|
| 1 | Almost didn't happen | Percentage probability of occurrence < 5% in 1 period |
| 2 | Rarely happens Sometimes happens | Percentage probability of occurrence 5% to 10% in 1 period |
| 3 | Often occur | Percentage probability of occurrence 10% to 20% in 1 period |
| 4 | Often occur | Percentage of probability of 20% to 50% in 1 period |
| 5 | It's almost certain to happen | Percentage probability of occurrence > 50% in 1 period |

Based on Table I, the criteria for the likelihood of an e-government risk are the magnitude of the probability of an e-government risk occurring within a certain period. The determination of the criteria may be carried out through a statistical probability percentage approach, the number of times the occurrence of an e-government risk in units of time, or based on expert judgment [1]. After that, it is necessary to inventory the following impact criteria.

TABLE II
E-GOVERNMENT IMPACT CRITERIA

| Impact Area | | Impact Level |
|---|---|---|
| Financial | Positive | Total income increased |
| | Negative | Material loss |
| Reputation | Positive | Stakeholder praise |
| | Negative | There is Negative News |
| Performance | Positive | Achievement of performance targets increased |
| | Negative | Performance drop |
| Organizational Service | Positive | Service acceleration |
| | Negative | Service operation delay |
| ICT Operations and Assets | Positive | Operational acceleration |
| | Negative | Delayed service |
| Law and Regulation | Positive | Increased level of organizational compliance with the law |
| | Negative | Number of lawsuits |
| | Positive | Employee mental physical improvement |

| | | |
|---|---|---|
| Human Resources | Negative | Lack of competent human resources |

Based on Table II, the criteria for the impact of e-government risk are the magnitude of the occurrence of an e-government risk that affects the e-government target [1].

9. E-Government Risk Analysis Matrix and E-Government Risk Level

The Risk Analysis Matrix contains a combination of the likelihood level and the impact level to determine the e-government risk [1]. Determination of the magnitude of e-government risk which is represented in the form of numbers such as the following risk matrix.

TABLE III
E-GOVERNMENT RISK ANALYSIS MATRIX

| Possibility | | Impact Level | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| | | Not significant | Less Significant | Significant Enough | Significant | Very Significant |
| 5 | Almost didn't happen | 9 | 15 | 18 | 23 | 25 |
| 4 | Often occur | 6 | 12 | 16 | 19 | 24 |
| 3 | Happens sometimes | 4 | 10 | 14 | 17 | 22 |
| 2 | Rarely happening | 2 | 7 | 11 | 13 | 21 |
| 1 | Almost didn't happen | 1 | 3 | 5 | 8 | 20 |

Based on Table III, for blue is a risk with a very low level of risk, green is a risk with a low level of risk, yellow is a risk with a moderate level of risk, orange is a risk with a high level of risk, and red is a risk with a very high level of risk.

TABLE IV
E-GOVERNMENT RISK LEVEL

| | Risk Level | Risk Magnitude Range | Color Description |
|---|---|---|---|
| 1 | Very Low | 1-5 | Blue |
| 2 | Low | 6-10 | Yellow |
| 3 | Currently | 11-15 | Green |
| 4 | Tall | 16-20 | Orange |
| 5 | Very high | 21-25 | Red |

Based on Table IV, the selection of the e-government risk level can use 5 e-government risk levels that are adjusted to the complexity of the e-government risk. Each level is represented by color according to the preferences of each Central Agency and Local Government [1].

B. E-Government Risk Assessment

E-Government risk assessment on the implementation of e-government is carried out through a process of identification, analysis and evaluation of e-government risk. The e-government risk assessment aims to understand the causes, possibilities and impacts of e-government risks that may occur in central and local government agencies [1]. The following are the stages of e-government Risk assessment.

1. Risk Identification

Risk Identification is the process of digging up information about the events, causes, and impacts of e-government risks. In this process, risk is divided into two types, namely positive risk and negative risk. In this risk identification process, 9 positive risks and 13 negative risks were identified, with the details as set out in Table V below.

TABLE V
E-GOVERNMENT RISK IDENTIFICATION

| Risk ID | E-Government Risk Type | Incident | Risk Category | Area Impact |
|---|---|---|---|---|
| RP1 | Positive | E-Government services are in accordance with the national master plan in its implementation | National E-Government Master Plan | Performance |
| RP2 | | E-Government architecture is modern and flexible to support smooth business | E-Government Architecture | Performance, Service Organization |
| RP3 | | E-Government implementation has been directed towards achieving E-Government 's vision and mission | E-Government Plan Map | Performance, Service Organization |
| RP4 | | There is a policy flexible work in agencies, which allows staff to work from a location other than in an office building | E-Government Business Process | Performance, Service Organization |
| RP5 | | Preliminary analysis is carried out to ensure the selection of the required infrastructure | Plan and Budget | Financial |
| RP6 | | Most of the staff have complied with existing policies/regulations | Compliance with Regulations | Laws and Regulations |
| RP7 | | E-Government project completed on time | System Development/Development Project | Performance |
| RP8 | | Data backup procedures are applied with a 1x24 hour check | Data and Information | ICT Operations and Assets |
| RP9 | | Services and business processes are continuously updated for the better | E-Government Innovation | Performance, Service Organization |
| RN1 | Negative | There are obstacles in the process of procuring goods and services at the agency | Procurement of goods and services | Performance, Financial |
| RN2 | | The official website has not yet fully provided the information needed by the public. | Data and Information | Reputation, Organizational Service |
| RN3 | | There has been a technical failure such as electricity | E-Government Infrastructure | Performance |
| RN4 | | There was a bug/error when the application was accessed | E-Government App | ICT Performance, Operations and Assets |
| RN5 | | There are some staff who are not proficient in accessing and exploiting the application | E-Government App | Performance, HR |
| RN6 | | *Phishing* which spread to staff computers | E-Government Security | ICT Performance, Operations and Assets |

| Risk ID | E-Government Risk Type | Incident | Risk Category | Area Impact |
|---|---|---|---|---|
| RN7 | | There has been a burglary of the local government's internal web | E-Government Security | ICT Operations and Assets |
| RN8 | | Damaged hardware components | E-Government service | Tik Operations and Assets |
| RN9 | | There is a mismatch between ICT skills and e-government needs. | E-Government HR | Performance, HR |
| RN10 | | Staff with IT background in each field is still lacking | E-Government HR | Performance, Organizational Service, HR |
| RN11 | | Dependence on Main IT staff | E-Government HR | Performance |
| RN12 | | No government provided training for IT staff | E-Government HR | Performance, Organizational Service, HR |
| RN13 | | There has been a natural weather disturbance, namely lightning | Natural disasters | ICT Performance, Operations and Assets |

Based on Table V, identified positive risks and negative risks along with risk categories and areas of impact from these risks. The results obtained from the risk identification process are the results of interviews and direct observations conducted previously, identified risks with an average risk of impacting on performance as well as ICT operations and assets. Next, the following risk analysis process is carried out.

### C. Risk Analysis

At this stage, the risks that have been identified are analyzed for their level of risk. An assessment is made of the frequency of risk occurrences, the magnitude of the impact of the occurrence of the risk, the determination of the risk magnitude and the Risk Level, obtained from a combination of the likelihood level and the impact level using the formula in the e-government Risk Analysis Matrix as described in Tables III and IV. The results of the analysis are described in Table VI below.

TABLE VI
E-GOVERNMENT RISK ANALYSIS

| Risk ID | Possibility | Impact | Amount of Risk | Risk Level |
|---|---|---|---|---|
| RP1 | Almost Definitely Happening | Significant | 23 | Very high |
| RP2 | Often occur | Significant Enough | 16 | Tall |
| RP3 | Often occur | Significant Enough | 16 | Tall |
| RP4 | Rarely happening | Significant Enough | 11 | Currently |
| RP5 | Almost Definitely Happening | Significant | 23 | Very high |
| RP6 | Often occur | Significant | 19 | Tall |
| RP7 | Almost Definitely Happening | Very Significant | 25 | Very high |
| RP8 | Almost Definitely Happening | Significant | 23 | Very high |
| RP9 | Almost Definitely Happening | Significant | 23 | Very high |

| | | | | |
|---|---|---|---|---|
| RN1 | Rarely happening | Not significant Low | 2 | Very low |
| RN2 | Happens Sometimes | Significant | 17 | Tall |
| RN3 | Happens Sometimes | Less Significant | 10 | Low |
| RN4 | Rarely happening | Less Significant | 7 | Low |
| RN5 | Rarely happening | Less Significant | 7 | Low |
| RN6 | Rarely happening | Significant | 13 | Currently |
| RN7 | Rarely happening | Significant | 13 | Currently |
| RN8 | Hardly Happened | Not significant | 9 | Low |
| RN9 | Happens Sometimes | Less Significant | 10 | Low |
| RN10 | Happens Sometimes | Significant Enough | 14 | Currently |
| RN11 | Happens Sometimes | Significant Enough | 14 | Currently |
| RN12 | Happens Sometimes | Significant Enough | 14 | Currently |
| RN13 | Rarely happening | Less Significant | 7 | Low |

Based on Table VI, identified 5 (five) positive risks with a very high level of risk, 3 (three) risks with a high level of risk, and 1 (one) risk with a moderate level of risk. Furthermore, identified 1 (one) negative risk with a high risk level, 1 (one) risk with a moderate risk level, 6 (six) risks with a low risk level and 1 (one) risk with a very low risk level. The identified risks are analyzed for their level of risk. The results of the analysis are as follows.

## D. Risk Evaluation

At this stage, an analysis is carried out to make a decision whether or not further risk management efforts are needed and determine the priority for handling them. Risk management priorities are sorted by the magnitude of the risk. If there is more than one risk that has the same magnitude, the way of determining priority is based on expert judgment. The risk evaluation process is outlined in the following Table VII.

TABLE VII
E-GOVERNMENT RISK EVALUATION

| Risk Level | Risk ID | Decision Risk Management (Yes) |
|---|---|---|
| Very high | RP1, RP5, RP7, RP8, RP9 | - |
| Tall | RP2, RP3, RP6, RN2 | RN2 |
| Currently | RP4, RN6, RN7, RN10, RN11, RN12 | RN6, RN7, RN10, RN11, RN12 |
| Low | RN3, RN4, RN5, RN8, RN9, RN13 | RN3, RN5, RN8, RN9 |
| Very low | RN1 | RN1 |

Based on Table VII, 11 negative risks were identified that needed to be addressed. The prioritized risks are RN2, RN6, RN7, RN10, RN11 and RN12. This risk must be handled as soon as possible so that no adverse event occurs because this risk has a very large risk for the XYZ Service. Risks with a low risk level can be handled directly or postponed because the impact is not too large, and for a risk with a very low risk level, the handling can be delayed because the impact does not significantly affect performance. In this E-Government risk management process, the author sets the E-Government risk treatment options which are described in the following diagram.

### E. E-Government Risk Management

E-Government risk management is the process of modifying the E-Government risk causes to produce an E-Government risk management plan [1].

TABLE VIII
E-GOVERNMENT RISK MANAGEMENT PLAN

| Decision Handling | Risk ID |
|---|---|
| Escalation | RN2, RN3, RN11, RN12, RN13 |
| Transfer | RN4 |
| Mitigation | RN6, FN7, RN8, RN9 RN10 |

Based on Table VIII, there are five risks with risk id RN2, RN3, RN11, RN12 and RN13 with Escalation treatment option, five risks with risk id RN6, RN7, RN8, RN9, and RN10 with Mitigation treatment option and one risk with risk id RN4 with the option of handling Transfer.

### F. Discussion

This study has similarities with the research conducted by Balya Haris Alfajri namely both using the same qualitative method and both using PERMENPAN RB guidelines no. 5 of 2020. The results of research conducted by Balya Haris Alfajri there are 6 positive risks and 10 negative risks, especially in the Application and service risk category, namely there are 4 negative risks, and 80% of negative risks are handled with options for management Escalation, Mitigation, Transfer, Avoidance and risk acceptance [5]. However, this journal is limited to focusing on the risk categories taken, namely infrastructure, applications, services, data, so the researcher wants to identify risks based on 16 e-government risk categories with 9 positive risks and 13 negative risks, the risk category that has the most risk is the source of the risk human resources with a total risk of 4 negative risks. A total of 11 negative risks with handling decisions were handled with the Escalation, Transfer and Mitigation management options.

## IV. Conclusion

XYZ Regency E-Government risk management analysis is based on PERMENPAN RB Number 5 of 2020. The risk assessment process is carried out through 3 processes, namely risk identification, risk analysis, risk evaluation, the results of which are useful as suggestions for risk management for possible risks that occur in the XYZ Department. From the results of risk identification, the XYZ Regency Government has 9 positive risks and 14 negative risks. Positive risk of 1 (one) moderate risk, 3 (three) high level risk and 5 (five) very high level risks Meanwhile, there are 6 (six) low-level risks, 5 (five) moderate-level risks, 1 (one) high-level risk, and 1 (one) very high-level risk.

The prioritized risks at Communication and Information office of XYZ Regency are RN3, RN13, RN11, and RN12. Where this risk must be handled as quickly as possible so that no adverse event occurs because this risk has a very large risk for the XYZ Regency. The results obtained in this study need improvement, because other risks can also occur in the same time frame or in a different time span. Therefore, further research is needed with a different point of view to get better results than before.

## References

[1] Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia, Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik, Jakarta: Direktur Jendral Perundang-Undangan Kementerian Hukum dan Hak Asasi Manusia Republik Indonesia, 2020.

[2] Presiden Republik Indonesia, Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, Jakarta: Menteri Hukum dan Hak Asasi Manusia Republik Indonesia, 2018

[3] Bogdan, R. C., Biklen, S. K., 1992, Qualitative Research for Education: an Introduction to Theory and Methods, Boston: Allyn & Bacon.

[4] Afri, A. A., Fauzi, R., & Mulyana, R. 2020. Perancangan Manajemen Risiko Proyek Pada Spbe Berdasarkan Permen Panrb Nomor 5 Tahun 2020: Studi Kasus Di Pemerintah Kota Bandung. eProceedings of Engineering, 7(2)

[5] Al-fajri, B. Y. H., Fauzi, R., & Mulyana, R. 2020. Perancangan Manajemen Risiko Operasional Spbe/e-gov Pada Kategori Risiko Infrastruktur, Aplikasi, Layanan, Data Dan Informasi Berdasarkan Permen Panrb Nomor 5 Tahun 2020 (studi Kasus: Pemerintah Kota Bandung). eProceedings of Engineering,7(2).

[6] Harisdayanti, D., Fauzi, R., & Mulyana, R. 2020. Perancangan Manajemen Risiko Operasional Pada Spbe/e-government Berdasarkan Permen Panrb Nomor 5 Tahun 2020: Studi Kasus Pemerintah Kabupaten Bandung. eProceedings of Engineering, 7(2).

[7] Chaidir, R. R., Fauzi, R., & Mulyana, R. 2020. Perancangan Manajemen Risiko Operasional Spbe/e-gov Pada Kategori Sumber Daya Manusia, Keamanan Dan Bencana Alam Berdasarkan Permen Panrb No. 5 Tahun 2020: Studi Kasus Di Pemerintah Kota Bandung. eProceedings of Engineering, 7(2).

[8] Danial dan Wasriah. (2009). Metode Penulisan Karya Ilmiah. Bandung: Laboratorium Pendidikan Kewarganegaraan UPI.
[9] Sedarmayanti & Syarifudin Hidayat, Metode Penelitian, Bandung: Mandar Maju, 2002
[10] Sugiyono. (2017). Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung : Alfabeta, CV.
[11] Nisa, K., Fauzi, R., & Mulyana, R. (2020). Perancangan Manajemen Risiko Proyek Pada Spbe/e-government Berdasarkan Permen Panrb Nomor 5 Tahun 2020 (studi Kasus: Pemerintah Kabupaten Bandung). eProceedings of Engineering, 7(2).
[12] Tarigan, K., Abdurrahman, L., & Mulyana, R. (2020). Perancangan Manajemen Risiko Strategis Pada Spbe/e-government Berdasarkan Permen Panrb Nomor 5 Tahun 2020: Studi Kasus Pemerintah Kabupaten Bandung Barat. eProceedings of Engineering, 7(2).
[13] Wardiana, W. (2002). Perkembangan teknologi informasi di Indonesia.
[14] Mildawati, T. (2000). Teknologi informasi dan perkembangannya di indonesia. Ekuitas, 4(1), 101-110.
[15] Fadhallah, R. A., & Psi, S. (2021). Wawancara. UNJ PRESS.