Jurnal Teknologi Informasi dan Pendidikan
Volume 16, No. 2, September 2023
https://doi.org/10.24036/jtip.v16i2.724

P.ISSN: 2086 – 4981
E.ISSN: 2620 – 6390
tip.ppj.unp.ac.id

Design of Risk Management in SPBE Infrastructure Based on PAN-RB Ministerial Regulation Number 5 of 2020 (Case Study: XYZ Institution)

Rochmawati[1*]✉, Muhammad Salman[1]

[1] Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Indonesia

*Corresponding Author: rochmawati91@ui.ac.id

Article Information

Article history:

No. 724
Rec. June 08, 2023
Rev. October 10, 2023
Acc. November 10, 2023
Pub. November 13, 2023
Page. 41 – 55

Keywords:

- *SPBE*
- *SPBE Risk*
- *SPBE Risk Management*
- *SPBE Infrastructure*
- *PAN-RB Ministerial Regulation Number 5 of 2020*

ABSTRACT

The arrival of the Industrial Revolution 4.0 not only spurred the acceleration of digitalization in industry and manufacturing, but also brought a broader influence on various sectors, including the government. One of the Government's efforts to support digital transformation is by issuing Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems (SPBE). However, the application of SPBE in Central Agencies and Regional Governments can create several risks that have an impact on the achievement of SPBE goals. Therefore, the Ministry of State Apparatus Empowerment and Bureaucratic Reform (PAN-RB) issued a PAN-RB Ministerial Regulation Number 5 of 2020 which contains SPBE Risk Management Guidelines that need to be implemented by SPBE organizers in managing SPBE risk in their respective institutions, including XY Work Unit. The XY Work Unit is one of the work units in the XYZ Institute responsible for carrying out tasks and functions in the IT field. SPBE risk assessment has been conducted on the SPBE Infrastructure in XY Work Unit. As a result, 47 negative SPBE risks were identified and 26 negative SPBE risks were above the SPBE Risk Appetite threshold hence SPBE Risk Management Recommendations were then planned based on PAN-RB Ministerial Regulation Guidelines Number 5 of 2020.

How to Cite:

Rochmawati, M. Salman. (2023). "Design of Risk Management in SPBE Infrastructure Based on PAN-RB Ministerial Regulation Number 5 of 2020 (Case Study: XYZ Institution)". Jurnal Teknologi Informasi Dan Pendidikan, 16(2), 41-55.

1. INTRODUCTION

The Internet, which began to enter Indonesia in the early 1990s, has made major changes in various areas of life in society [1] [2] [3]. The rapid development of the Internet has begun to change the paradigm of society in communicating and exchanging information towards the digital era. Now, the advent of the Industrial Revolution 4.0 has not only accelerated the digitalization of industry and manufacturing, but also had a broader impact on various sectors, including government. “Revolution” is a term to describe major and radical change where economic systems and societal structures undergo significant changes because of new inventions and emerging technologies [4]. The phrase "Industry 4.0" was initially used during the Hannover Fair in April 2011 [5]. The German government uses this phrase to refer to the utilization of technology aid in moving the industrial field (smart factories) to the next level [6]. Schwab (2016), however, pointed out that the fourth industrial revolution is not only about “smart factories”, but has a far broader reach [4]. Technological megatrends will reshape the industrial and social sectors, as well as governments and agencies, education, transportation, logistics, and other fields [4].

As a government administrator, the Government of the Republic of Indonesia must be able to adapt and follow the flow of change by utilizing advances in communication and information technology to organize good governance. To answer these challenges, the Government of the Republic of Indonesia began to pioneer digital transformation by issuing Presidential Instruction Number 3 of 2003 concerning National Policy and Strategy for the development of e-government [7]. Through the implementation of e-government, the Government wants to take advantage of advances in communication and information technology to eliminate bureaucratic barriers and form a network of work systems and processes that enable government agencies to work in an integrated manner to simplify access to all information and public services [7]. Presidential Instruction Number 3 of 2003 mandates Ministers, Heads of Institutions, and Heads of Regions to carry out e-government development in accordance with their duties, functions, authorities, and resource capacities [8].

However, the results of a study on the implementation of e-government or Electronic-Based Government Systems (SPBE) conducted in 2018 showed that the development of SPBE in Central Agencies and Local Governments is still at a relatively low level of maturity [8]. The problem arises due to several factors, such as the absence of a SPBE governance system, the application of SPBE in government administration and public services that is not yet optimal, the uneven coverage of ICT infrastructure, and the lack of civil servants with ICT skills [8]. Therefore in 2018, the Government of the Republic of Indonesia issued Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems which regulates SPBE Governance, SPBE Management, ICT Audit, SPBE organizers, SPBE acceleration and SPBE monitoring and evaluation [8]. According to Presidential Decree Number 95 of 2018, an Electronic-Based Government System is one of the state's efforts in administering government by utilizing information and communication technology to provide services to SPBE users [8]. SPBE was created to realize clean, effective, transparent and accountable governance as well as quality and reliable public services [8].

Implementation of Electronic-Based Government Systems in Central Agencies and Regional Governments is not without obstacles [9] [10]. The complexity of the bureaucracy and government structure as well as the rapid development of digital technology in the current Industrial Revolution 4.0 era can create a number of risks that will hinder the optimal and comprehensive implementation of SPBE in the government sector. Meiyanti *et al*. (2018) categorized the obstacles to implementing SPBE into six categories: IT infrastructure, managerial issues, digital culture, budgeting, laws & regulations, and human resources [11]. Arief and Abbas (2021) found three other obstacles in their literature review, namely political, geographical, and cultural aspects [9]. These various obstacles and risks that arise must be managed properly so that they do not become threats that can endanger the Central Agency and Regional Government as SPBE organizers [10] [12].

In order to address these issues, the Ministry of State Apparatus Empowerment and Bureaucratic Reform (PAN-RB) issued Ministerial Regulation Number 5 of 2020 about SPBE Risk Management Guidelines which adopts standards and provisions from ISO 31000:2018 [13] and Cobit 5 for Risk [14] which are then adapted to the prevailing governance arrangements in Indonesia [12]. COBIT (Control Objective for Information and Related Technology) is a standard and framework for IT governance developed by ISACA and ITGI, a nonprofit that specializes in IT governance [15]. It also serves as a set of widely recognized measurements for IT management procedures [15]. This guideline was created to serve as a guide for Central Agencies and Regional Governments in preparing SPBE risk management in their environment [12]. PAN-RB Ministerial Regulation No. 5 of 2020 regulates the SPBE Risk Management Framework, which contains basic components to assist the integration of SPBE Risk Management in the organization, the SPBE Risk Management Process, which contains the stages of preparing SPBE Risk Management, SPBE Risk Management Structure, which contains the parties authorized and responsible for SPBE Risk Management, and the implementation of a Risk Awareness Culture in the organization [12].

XYZ Institute, as one of the government organizations of the Republic of Indonesia, has the duty and function to carry out digital transformation through the implementation of SPBE in accordance with Presidential Regulation No. 95 of 2018 on Electronic-Based Government Systems.. To support the implementation of SPBE in these institutions, it is necessary to design a SPBE Governance and Management system that adopts the characteristics of the institution. XY Work Unit, one of the work units in XYZ Institute, is responsible for carrying out tasks and functions in the IT field within the organization. However, based on the results of the Focus Group Discussion (FGD), until now the XY Work Unit does not yet have SPBE Risk Management guidelines so that the work unit has difficulty identifying, preventing and providing management of risks that occur. In addition, with the SPBE Risk Management guidelines, work units can map the current conditions, identify sources of risk as well as weaknesses and strengths they have, close security gaps, and carry out handling according to the priority of risks that may and will occur. Based on the results of the FGD with the XY Work Unit, the SPBE Risk Assessment will be carried out on 3 (three) elements, namely SPBE Infrastructure, SPBE Applications, and SPBE Security. However, of these three elements, this research only focuses on designing Risk Management for the SPBE Infrastructure in the XY Work Unit based on PAN-RB Ministerial Regulation Number 5 of 2020.

2. RESEARCH METHOD

This study uses a qualitative method approach that focuses on quality and in-depth observations so as to produce a more comprehensive study [3] [16]. Through qualitative research, in-depth information can be explored and open to various responses [17]. In practice, this research was divided into several stages as depicted in Figure 1.

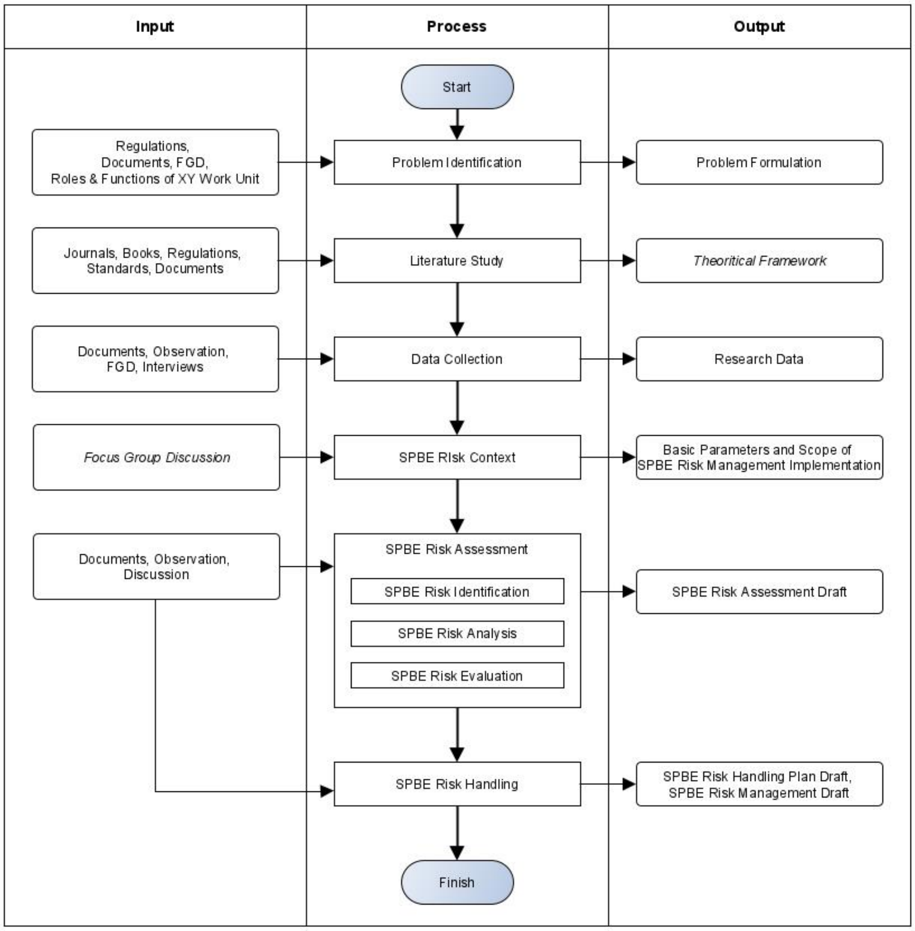
Input
Process
Output
Start
Regulations, Documents, FGD, Roles & Functions of XY Work Unit
Problem Identification
Problem Formulation
Journals, Books, Regulations, Standards, Documents
Literature Study
Theoritical Framework
Documents, Observation, FGD, Interviews
Data Collection
Research Data
Focus Group Discussion
SPBE RIsk Context
Basic Parameters and Scope of SPBE Risk Management Implementation
Documents, Observation, Discussion
SPBE Risk Assessment
SPBE Risk Identification
SPBE Risk Analysis
SPBE Risk Evaluation
SPBE Risk Assessment Draft
SPBE Risk Handling
SPBE Risk Handling Plan Draft, SPBE Risk Management Draft
Finish

Figure 1. Research Stages

2.1. Problem Identification

Problem identification is carried out to define problems that will become the focus of research obtained from the results of analysis of the needs of work units related to the SPBE Infrastructure based on existing documents, applicable regulations, Focus Group Discussions (FGD), as well as the duties and functions of the XY Work Unit.

2.2. Literature Study

At this stage a literature study is carried out to determine with what steps the problem will be solved and solved by studying references from various sources such as books, journals, international standards, regulations, and work unit documents to produce a theoretical framework that will become a guide in conducting research.

2.3. Data collection

At this stage data collection was carried out through interviews, Focus Group Discussion (FGD), direct observation, discussion, and review of existing documents.

2.4. SPBE Risk Context

The results of the Focus Group Discussion are used to identify the fundamental parameters and scope of SPBE risk, which will later serve as a reference when compiling a risk assessment, to determine the SPBE risk context [12].

2.5. SPBE Risk Assessment

SPBE risk assessment stages are divided into three, namely SPBE risk identification, SPBE risk analysis, and SPBE risk evaluation [12] [18]. The SPBE risk identification process is carried out to obtain information regarding the types of SPBE risks, the forms of events and their causes, the categories of SPBE risks that occur, as well as the impacts and areas affected by SPBE risks in the XY work unit [19]. SPBE risk analysis is carried out to assess the control system that exists in XY work unit, the level of possibility, the level of impact, as well as the magnitude of the SPBE risk and its level [19]. SPBE risk evaluation is made to determine if further SPBE risk management is needed [19]. The SPBE risk assessment stages are obtained from the results of direct observation, document review, and repeated discussions with the Head of the XY Work Unit, the Head of the Sector, and the IT staff who are responsible for the SPBE Infrastructure of the XYZ Institute.

2.6. SPBE Risk Handling

At this stage, the selection of SPBE risk management options is carried out, making action plans, implementation schedules and determining the responsible unit for each action plan made [20].

3. RESULTS AND DISCUSSION

This chapter contains the Risk Management Design for the SPBE Infrastructure in the XY Work Unit based on the Minister of Administrative and Bureaucratic Reform Regulation Number 5 of 2020 as mandated by the Indonesian Government.

3.1. SPBE Risk Context Determination

The SPBE Risk Context Determination process for Work Unit XY is divided into the following steps [12]:

3.1.1 General Information Inventory

An inventory of general information is carried out to identify information regarding the XY Work Unit as the SPBE Risk Owner Unit (UPR) such as the name of the SPBE UPR, the duties and functions of the SPBE UPR on the implementation of SPBE in the XYZ Institute, as well as the period of implementation of SPBE Risk Management in the XY Work Unit.

3.1.2 SPBE Target Identification

SPBE Target Identification is designed to provide information about the goals to be achieved and the indicators to be used in implementing SPBE at XYZ Institute. This information contains the following elements:

a. SPBE UPR targets, filled with XY Work Unit targets related to SPBE. The SPBE UPR target is derived from the strategic objectives of the XYZ Institute and is made in accordance with the duties and functions of the XY Work Unit, namely as a work unit that carries out tasks and functions in the field of data and information.

b. The SPBE target, in this case, is filled in with the target of the XY Work Unit related to the SPBE and is obtained from the XY Work Unit's Key Performance Indicator (KPI) document.

c. The SPBE Performance Indicator is filled in with the Main Performance Indicator of the XY Work Unit listed in the KPI document.

d. The SPBE Performance Target is filled with the value/measurement of the SPBE Performance Indicator obtained from the XY Work Unit KPI document draft.

3.1.3 SPBE Risk Management Implementation Structure

Based on the FGD results, it was determined that the XY Work Unit is the SPBE Risk Owner Unit, which will develop and implement SPBE Risk Management. The SPBE Risk Management Implementing Structure includes the SPBE Risk Owner Unit, SPBE Risk Owner, SPBE Risk Coordinator, and SPBE Risk Manager.

3.1.4 Identification of Stakeholders

Stakeholder identification is needed to find out which parties interact with the XY Work Unit and influence the achievement of the SPBE targets, where these parties can come from internal work units, external work units, government, or non-government agencies. Based on the FGD results, 8 stakeholders have been identified, namely the Head of XYZ Institution, the Chief Secretary, Echelon I & II Leaders, XYZ Institution employees, XY Work Unit, third parties, institution partners, and the National SPBE Coordination Team.

3.1.5 Identification of Regulations

Identification of regulations must be carried out so that the XY Work Unit understands the authorities, duties and functions, responsibilities, as well as legal regulations that need to be implemented and obeyed. The regulations upon which the SPBE Risk Management Guideline is based are: a) Law of the Republic of Indonesia No. 19 of 2016 on Amending Law No. 11 of 2008 concerning Electronic Information and Transactions, b) Presidential Regulation No. 95 of 2018 concerning Electronic-Based Government Systems, c) PAN-RB Ministerial Regulation No. 5 of 2020 about SPBE Risk Management Guideline, d) Presidential Regulation about XYZ Institution, e) XYZ Institution Regulations concerning the Organization and Work Procedures, f) Vision, Mission, Strategic Goals and Key Performance Indicators of XYZ Institution for 2022-2024, and g) Implementation of SPBE in XYZ Institution.

3.1.6 SPBE Risk Categories

According to PAN-RB Ministerial Regulation Number 5 of 2020, there are 16 SPBE risk categories that have been determined so that the process of identifying, analyzing, and evaluating SPBE risks can be carried out comprehensively.

3.1.7 SPBE Risk Impact Areas

It is necessary to determine the SPBE Impact Areas to see which areas or parts of the XY Work Unit or XYZ Institute are affected by the SPBE risk. Referring to the SPBE Risk Management Guidelines belonging to the Ministry of PAN – RB and based on the results of the FGD, the XY Work Unit determined that there were 7 impact areas consisting of: a) financial, b) reputation, c) performance, d) organizational services, e) operational and ICT assets, f) laws and regulations, and g) human resources.

3.1.8 SPBE Risk Criteria

The determination of SPBE risk criteria is carried out to measure how likely a risk is to occur and its impact on achieving the XY Work Unit's targets. In determining the SPBE

Possible Risk Criteria, the XY Work Unit uses 5 types of probability levels as well as the probability percentage approach and the probability of events occurring in one year as shown in Table 1

Table 1. SPBE Risk Criteria

No	Likelihood level	Percentage of Occurrence in One Year	Frequency of Occurrence in One Year
1.	Very Unlikely	X ≤ 0,1%	X < 2
2.	Unlikely	0,1% < X ≤ 10%	2 = X ≤ 12
3.	Moderate	10% < X ≤ 20%	12 < X ≤ 18
4.	Likely	20% < X ≤ 50%	18 < X ≤ 24
5.	Very Likely	X > 50%	X > 24

The SPBE Risk Impact Criteria is a combination of the SPBE Risk Impact Area and Impact Level. The XY Work Unit uses 5 levels of impact, namely Not Significant, Less Significant, Moderately Significant, Significant, and Very Significant.

3.1.9 SPBE Risk Analysis Matrix and Risk Level

The SPBE risk analysis matrix is obtained from the results of an assessment of the likelihood level and impact level that have been predetermined and represented in numerical form (SPBE Risk Amount) as in Table 2.

Table 2. SPBE Risk Analysis Matrix

			Impact Level				
	Risk Analysis Matrix 5 x 5		1 Not Significant	2 Less Significant	3 Moderately Significant	4 Significant	5 Very Significant
Likelihood Level	5	Very Likely	9	15	18	23	25
	4	Likely	6	12	16	19	24
	3	Moderate	4	10	14	17	22
	2	Unlikely	2	7	11	13	21
	1	Very Unlikely	1	3	5	8	20

The SPBE Risk Amount is then grouped in the form of SPBE Risk Levels and each level contains a range of SPBE Risk Amount values. Based on the results of the FGD, the range of values for each label was determined as follows:

Table 3. SPBE Risk Level

No.	Risk Level	Risk Value Range	Color Description
1.	Very Low	1 – 5	Blue
2.	Low	6 – 10	Green
3.	Medium	11 – 15	Yellow
4.	High	16 – 19	Orange
5.	Very High	20 – 25	Red

3.1.10 SPBE Risk Appetite

SPBE's risk appetite is made to be a minimum threshold reference for risks that must be addressed. If the SPBE Risk Amount has exceeded or equal to the predetermined risk appetite value, then the risk must be handled, applicable both to negative risks and positive risks. Meanwhile, based on the results of the FGD meeting, the risk appetite for SPBE belonging to the XY Work Unit is as follows:

Table 4. SPBE Risk Possible Criteria

No	SPBE Risk Categories	Minimum Threshold for risk to be handled (Negative SPBE Risk)
1.	Data and Information, SPBE Infrastructure, SPBE Application, SPBE Security, SPBE Service	11
2.	SPBE Architecture, SPBE Road Map, Planning &Budgeting, Business Process, Innovation, Regulatory Compliance, Procurement of Goods and Services, System Development/ Projects, SPBE Human Resources, Natural Disaster	16

3.2. SPBE Risk Assessment

3.2.1. SPBE Risk Identification

SPBE Risk Identification is carried out to gather information regarding events/predictions of events that will occur (hereinafter referred to as SPBE Risk), causes, types of SPBE risks, SPBE risk categories, impacts, and areas of impact in accordance with the SPBE Risk Context which has been defined in Section 3.1. The SPBE Risk Assessment results are obtained through an iterative discussion process, either through meetings or direct discussions with the Head of Division and/or IT staff in the XY Work Unit.

Table 5 shows the results of the SPBE risk assessment at the XYZ Institute Data Center and Intra Network which are arranged based on handling priority. There are 47 Negative SPBE Risks which are divided into 15 SPBE Risks in the XYZ Institute Data Center (N.1 – N.15) and 32 SPBE Risks in the XYZ Institute Intra Network (N.16 – N.47). 26 Some of the SPBE risks are above the SPBE Risk Appetite value so that they must be handled further and recommendations for SPBE Risk Management are made.

3.2.2. SPBE Risk Analysis

SPBE Risk Analysis is conducted to determine the control system, the likelihood, and the impact of SPBE Risk. The determination of the control system is based on the results of observations and discussions with the SPBE risk owner, as well as the determination of the level of likelihood and level of impact, as shown in Table 5.

3.2.3. SPBE Risk Evaluation

After the SPBE risk analysis is completed and the Magnitude value of each SPBE Risk is obtained, the next stage of the risk assessment process is the SPBE Risk Evaluation. At this stage the researcher together with the person in charge of SPBE Risk discusses and decides whether it is necessary to carry out further handling of the SPBE Risk that has been analyzed and determines the priority of the risks. SPBE Risk Prioritization in this study is determined by prioritizing the risks that have the largest SPBE Risk Magnitude value first. From the research results, there are 6 SPBE risks with a very high level, 20 SPBE risks with a medium level and are above the threshold/risk appetite so that SPBE risk handling needs to be done, 1 SPBE risk with a medium level that is below the SPBE risk appetite, 7 SPBE risks with a low level, and 13 SPBE risks with a very low level so that the risk is accepted and no risk handling is made.

Table 5. SPBE Risk Assessment on XYZ Institute Data Centers and Intra Networks

No.	Category	Likelihood	Impact	Risk Value	SPBE Risk Handling (Yes/No)	Risk Priority	SPBE Risk Handling Options
N.1	Planning&Budgeting	2	5	21	Yes	1	Risk Mitigation
N.39	SPBE Infrastructure	2	5	21	Yes	2	Risk Mitigation
N.2	SPBE Infrastructure	1	5	20	Yes	3	Risk Mitigation
N.3	SPBE Infrastructure	1	3	20	Yes	4	Risk Mitigation
N.5	SPBE Infrastructure	1	5	20	Yes	5	Risk Mitigation
N.16	Planning&Budgeting	1	5	20	Yes	6	Risk Mitigation
N.13	Human Resources	2	4	14	Yes	7	Risk Mitigation
N.14	SPBE Infrastructure	3	3	14	Yes	8	Risk Mitigation
N.24	SPBE Infrastructure	3	3	14	Yes	9	Risk Mitigation
N.42	SPBE Infrastructure	3	3	14	Yes	10	Risk Mitigation
N.46	SPBE Service	3	3	14	Yes	11	Risk Mitigation

N.47	SPBE Service	3	3	14	Yes	12	Risk Mitigation
N.11	SPBE Infrastructure	2	4	13	Yes	13	Risk Mitigation
N.12	SPBE Infrastructure	2	4	13	Yes	14	Risk Mitigation
N.15	SPBE Infrastructure	2	4	13	Yes	15	Risk Mitigation
N.22	SPBE Security	2	4	13	Yes	16	Risk Mitigation
N.17	SPBE Infrastructure	2	3	11	Yes	17	Risk Transfer
N.20	SPBE Infrastructure	2	3	11	Yes	18	Risk Mitigation
N.26	SPBE Infrastructure	2	3	11	Yes	19	Risk Mitigation
N.27	SPBE Infrastructure	2	3	11	Yes	20	Risk Mitigation
N.33	SPBE Infrastructure	2	3	11	Yes	21	Risk Mitigation
N.35	SPBE Infrastructure	2	3	11	Yes	22	Risk Acceptance
N.38	SPBE Infrastructure	2	3	11	Yes	23	Risk Mitigation
N.41	SPBE Infrastructure	2	3	11	Yes	24	Risk Mitigation
N.43	Human Resources	2	3	11	Yes	25	Risk Mitigation
N.45	SPBE Service	2	3	11	Yes	26	Risk Mitigation
N.25	Planning&Budgeting	2	3	11	No	27	-
N.6	SPBE Infrastructure	1	4	8	No	28	-
N.9	SPBE Infrastructure	1	4	8	No	29	-
N.18	Natural Disaster	1	4	8	No	30	-
N.29	Natural Disaster	1	4	8	No	31	-
N.37	Natural Disaster	1	4	8	No	32	-
N.8	SPBE Infrastructure	2	2	7	No	33	-
N.10	SPBE Infrastructure	2	2	7	No	34	-
N.4	SPBE Infrastructure	1	3	5	No	35	-
N.7	SPBE Infrastructure	1	3	5	No	36	-
N.28	SPBE Infrastructure	1	3	5	No	37	-
N.30	SPBE Infrastructure	1	3	5	No	38	-
N.31	Human Resources	1	3	5	No	39	-
N.32	SPBE Infrastructure	1	3	5	No	40	-
N.36	SPBE Infrastructure	1	3	5	No	41	-
N.44	Human Resources	1	3	5	No	42	-
N.19	Human Resources	2	2	4	No	43	-
N.21	SPBE Infrastructure	2	2	4	No	44	-
N.23	SPBE Infrastructure	2	2	4	No	45	-
N.34	Human Resources	2	2	4	No	46	-
N.40	Human Resources	2	2	4	No	47	-

3.3. SPBE Risk Handling Recommendations

Based on the results of the SPBE risk evaluation, there are 26 SPBE risks that require further handling. Therefore, recommendations for handling SPBE risks are made as shown in Table 6.

Table 6. SPBE Risk Handling Recommendations in the XY Work Unit

No.	Risk Priority	SPBE Risk Handling Options	SPBE Risk Handling Action Plan	Person in Charge
N.1	1	Risk Mitigation	Create a Disaster Recovery Center	Infrastructure Section
N.39	2	Risk Mitigation	1. Conduct equipment inventory 2. Planning for equipment renewal needs	XY Work Unit

			3. Procurement of devices	
N.2	3	Risk Mitigation	Create a Disaster Recovery Center	Infrastructure Section
N.3	4	Risk Mitigation	Create a Disaster Recovery Center	Infrastructure Section
N.5	5	Risk Mitigation	1. CCTV installation design and strengthening of data center entry security (using biometrics) 2. Create Data Center SOP; or 3. Utilization of a third-party cloud service	Infrastructure Section
N.16	6	Risk Mitigation	1. Develop an Internet procurement needs plan 2. Ensure the Internet procurement process goes well	XY Work Unit
N.13	7	Risk Mitigation	Human resources training	Infrastructure Section
N.14	8	Risk Mitigation	Monitoring and alerting system development	Infrastructure Section
N.24	9	Risk Mitigation	Check and monitor bandwidth on a regular basis	Infrastructure Section
N.42	10	Risk Mitigation	1. Conduct equipment inventory 2. Planning for equipment renewal needs	XY Work Unit
N.46	11	Risk Mitigation	1. Develop an IT Service SLA 2. Set IT service performance targets;	XY Work Unit
N.47	12	Risk Mitigation	Monitor and report on IT services on a regular and periodic basis	XY Work Unit
N.11	13	Risk Mitigation	1. Capacity management plan 2. Third-party Annual Technical Support (ATS) activities on data center equipment	XY Work Unit
N.12	14	Risk Mitigation	Recovery of applications and supporting hardware	Infrastructure Section
N.15	15	Risk Mitigation	1. Communication line recovery 2. Monitoring and alerting system recovery	Infrastructure Section
N.22	16	Risk Mitigation	1, Network security training for IT staff 2. Dissemination of information and building a culture of information security awareness	XY Work Unit
N.17	17	Risk Transfer	Bandwidth testing and monitoring by vendors and infrastructure section on a regular basis	Infrastructure Section
N.20	18	Risk Mitigation	1. Conduct equipment inventory 2. Planning for equipment renewal needs	XY Work Unit
N.26	19	Risk Mitigation	Check and monitor network devices on a regular basis	Infrastructure Section
N.27	20	Risk Mitigation	Check and monitor network devices on a regular basis	Infrastructure Section
N.33	21	Risk Mitigation	1. Conduct equipment inventory 2. Planning for equipment renewal needs	XY Work Unit
N.35	22	Risk Acceptance	1. Conduct evaluation and needs analysis 2. Dissemination of information to user	XY Work Unit
N.38	23	Risk Mitigation	Coordination with the relevant and responsible parties	Related Parties
N.41	24	Risk Mitigation	Implementation of related SOP	Regional IT Service Team
N.43	25	Risk Mitigation	Analyze and plan for IT Service Human Resource needs	XY Work Unit

N.45	26	Risk Mitigation	Adopt IT service management system application support	XY Work Unit

4. CONCLUSION

After conducting research related to the Risk Management on the SPBE Infrastructure based on the PAN-RB Ministerial Regulation Number 5 of 2020, the following conclusions and suggestions are obtained:

a. The Risk Management Design for the SPBE Infrastructure in the XY Work Unit is prepared based on the SPBE Risk Management Guidelines issued by Ministry of PAN-RB which adopts the standards and provisions from ISO 31000:2018 and COBIT 5 for Risk and then adjusted to the prevailing governance arrangements in Indonesia.

b. The design of Risk Management on the SPBE Infrastructure in the XY Work Unit is prepared based on six stages of Problem Identification, Literature Study, Data Collection, Determination of SPBE Risk Context, SPBE Risk Assessment, and SPBE Risk Management.

c. Based on the results of the risk assessment on the SPBE Infrastructure, 50 negative SPBE risks were identified, of which 29 SPBE risks required further treatment based on the priorities that had been made. There are 6 risks with a very high level, 24 risks with a medium level, 7 risks with a low level, and 13 risks with a very low level.

d. Based on the results of preparing Recommendations for Handling Risks on SPBE Infrastructure, 27 SPBE Risks will be mitigated, 1 SPBE Risk will be transferred, and 1 SPBE Risk will be accepted as a consequence.

ACKNOWLEDGEMENTS

The research leading to this result has received funding from National Research and Innovation Agency (BRIN) under SAINTEK scholarship program.

REFERENCES

[1] D. Hill and K. Sen, The Internet in Indonesia's New Democracy, New York: Routledge, 2005.

[2] M. Lim, Contesting Media Power: Alternative Media in a Networked World, Maryland: Rowman & Littlefield Publishers, Inc., 2003.

[3] R. Hendra and M. Hanita, "The Implementation of Cyber Incident Management Frameworks in Indonesia," *Jurnal Teknologi Informasi dan Pendidikan,* vol. 13, no. 2, pp. 9-16, 2020.

[4] K. Schwab, The Fourth Industrial Revolution, Switzerland: World Economic Forum, 2016.

[5] B. Vogel-Heuser and D. Hess, "Guest Editorial Industry 4.0–Prerequisites and Visions," *EEE Transactions on Automation Science and Engineering,* vol. 13, no. 2, pp. 411-413, 2016.

[6] K.-D. Thoben, S. Wiesner and T. Wuest, ""Industrie 4.0" and Smart Manufacturing – A Review of Research Issues and Application Examples," *Int. J. of Automation Technology,* vol. 11, no. 1, pp. 4-16, 2017.

[7] Indonesia, *Instruksi Presiden Republik Indonesia Nomor 3 Tahun 2003 tentang Kebijakan dan Strategi Nasional Pengembangan E-Government,* Jakarta: Pemerintah Republik Indonesia, 2003.

[8] Indonesia, *Peraturan Presiden Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik,* Jakarta: Kementerian Sekretariat Negara, 2018.

[9] A. Arief and M. Y. Abbas, "Kajian Literatur (Systematic Literature Review): Kendala Penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE)," *PROtek: Jurnal Ilmiah Teknik Elektro,* vol. 8, no. 1, pp. 1-6, 2021.

[10] F. S. Tazkiyyah, L. Abdurrahman and R. Mulyana, "Perancangan Manajemen Risiko Operasional SPBE/e-Government pada Kategori Data dan Informasi, Infrastruktur, Aplikasi, Pengadaan Barang dan Jasa, Keamanan, Arsitektur, dan Sumber Daya Manusia Berdasarkan Permen PANRB No. 5 Tahun 2020 Studi Kasus: Pemkab Ba," in *e-Proceeding of Engineering*, Bandung, 2020.

[11] R. Meiyanti, B. Utomo, D. I. Sensuse and R. Wahyuni, "e-Government Challenges in Developing Countries: A Literature Review," in *6th International Conference on Cyber and IT Service Management (CITSM 2018)*, Medan, 2018.

[12] Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi, *Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik,* Jakarta: Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi, 2020.

[13] International Organization for Standardization, ISO 31000 : 2018 Risk Management - Guidelines, Geneva: ISO, 2018.

[14] ISACA, COBIT 5 for Risk, Illinois: ISACA, 2013.

[15] Harleni and Marisa, "Sistem Informasi Akademik (SIAKAD) STIKES Perintis Padang," *Jurnal Teknologi Informasi dan Pendidikan,* vol. 11, no. 2, pp. 44-48, 2018.

[16] N. Matondang, B. Hananto and C. Nugrahaeni, "Analisis Tingkat Kesiapan Pengamanan Sistem Informasi (Studi Kasus UPN Veteran Jakarta)," *Jurnal Teknologi Informasi dan Pendidikan,* vol. 12, no. 1, pp. 1-4, 2019.

[17] W. D. Perreault and E. J. McCarthy, Essentials of Marketing: A Global-Managerial Approach Tenth Edition, New York: McGraw-Hill, 2006.

[18] Mahkamah Agung, *Keputusan Sekretaris Mahkamah Agung Republik Indonesia Nomor: 4475/SEK/SK/VII/2019 tentang Pedoman Manajemen Risiko di Lingkungan Mahkamah Agung dan Badan Peradilan di Bawahnya,* Jakarta: Mahkamah Agung Republik Indonesia, 2019.

[19] Kementerian Pertanian Republik Indonesia, *Keputusan Inspektur Jenderal Kementerian Pertanian Nomor B.1527/KPTS/PW.110/G/06/2021 tentang Pedoman Teknis Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik Lingkup Kementerian Pertanian,* Jakarta: Kementerian Pertanian Republik Indonesia, 2021.

[20] Pemerintah Kabupaten Grobogan, "Laporan Akhir Manajemen Risiko SPBE Daerah Kabupaten Grobogan," Pemerintah Kabupaten Grobogan, Grobogan, 2021.