International Journal of Safety and Security Engineering
Vol. 15, No. 7, July, 2025, pp. 1471-1480
Journal homepage: http://iieta.org/journals/ijsse

Risk Assessment of Information System Audit Tools Based on SPBE Risk Management Guidelines

Harnum Annisa Prafitia[1,2*], Nilo Legowo[1]

[1] Information Systems Management Department, BINUS Graduate Program - Master of Information Systems Management, Bina Nusantara University, Jakarta 11480, Indonesia
[2] Research Center for Data and Information Sciences, National Research and Innovation Agency, Bandung 40135, Indonesia

Corresponding Author Email: harnum.prafitia@binus.ac.id

https://doi.org/10.18280/ijsse.150714

Received: 4 June 2025
Revised: 10 July 2025
Accepted: 23 July 2025
Available online: 31 July 2025

Keywords:
risk management, e-government, SPBE, audit tools, ISO 31000, SPBE digital transformation, risk prioritization assessment

ABSTRACT

Many challenges and risks arise in the implementation of the Electronic-Based Government System (SPBE), including the management of Audit Tools. Conducting a risk assessment is crucial. To that end, the Indonesian government has established a framework based on the Minister of Administrative and Bureaucratic Reform Regulation No. 5 of 2020, specifically the SPBE Risk Management Guidelines. In this study, risk management will be conducted on the management of Audit Tools using the SPBE Risk Management Guidelines. The aim is to identify, analyse, and evaluate risks associated with the management of Audit Tools and provide recommendations. This research focuses on eight categories of SPBE technical risks. Twenty-seven risks have been successfully identified, consisting of 6 positive risks and 21 negative risks. Based on the risk assessment, the results of this study indicate that the highest priorities in the risk management of Audit Tools are server downtime, slow access, system development delays, outdated technology, and cyber attacks. An assessment of the maturity of the Audit Tools management information system, which received a score of 2.59, has also been conducted. The recommendation given is the need to create a Disaster Recovery Plan (DRP) and an SOP for Audit account access. Additionally, enhancing the Service Team's capabilities must be implemented to prevent existing risks from recurring.

1. INTRODUCTION

The Indonesian government has already begun taking steps to realize Indonesia's digital transformation. Digital transformation in the government sector is commonly referred to as digital government. The implementation of digital transformation in Indonesia is not just about technology application but also about culture and attitude [1]. The utilization of information and communication technology in providing government services is referred to as the Electronic-Based Government System (SPBE) or e-government [2]. SPBE will significantly improve government efficiency and transparency, as well as bureaucratic accountability [3] This improves the quality of public services to enhance user accessibility [4].

SPBE is implemented to support more efficient and integrated government services [5]. The implementation of this digital transformation has both negative and positive impacts on the organization. Therefore, the organization must prepare all aspects that must be addressed wisely [6]. In the implementation of SPBE, monitoring and evaluation are conducted to assess the improvement of SPBE implementation, one of which is through the SPBE ICT Audit. The process is carried out on all Central Agencies and Regional Governments (IPPD) to encourage them to accelerate their organization's digital transformation. With the enactment of the SPBE Regulation, implementing ICT audits is mandatory for all Central and Regional Government Agencies (IPPD) in Indonesia [7]. The Audit Tools SPBE provides a positive contribution to IPPD in enhancing the maturity and implementation of SPBE and improving IT governance [8].

Before the existence of SPBE, the government's procedure for conducting ICT audits was done manually through interviews between auditors and auditees. With the mandatory implementation of the SPBE ICT Audit, an application called Audit Tools SPBE was created. The SPBE Audit Tools users have been in use from 2021 until June 2024. Every year, the number of IPPDs conducting SPBE Application and Infrastructure Audits continues to increase. This is because implementing the SPBE Application and Infrastructure Audit is an aspect evaluated by PANRB Ministry. By conducting the SPBE Application and Infrastructure Audit, the SPBE index value in each IPPD will be improved. In 2021, there were 13 IPPDs; in 2022, there were 69 IPPDs; in 2023, there were 102 IPPDs; and in 2024, there were 104 IPPDs.

Disruptive incidents often occur during the management process of SPBE Audit Tools. Many incidents disrupt the audit process and coordination in the implementation of the audit, like the server downtime on the server network that prevents users from accessing the application, as seen in Figure 1. The

SPBE Audit Tools themselves have vulnerabilities in terms of information security. This causes losses to the application users, namely auditors and auditees [9].

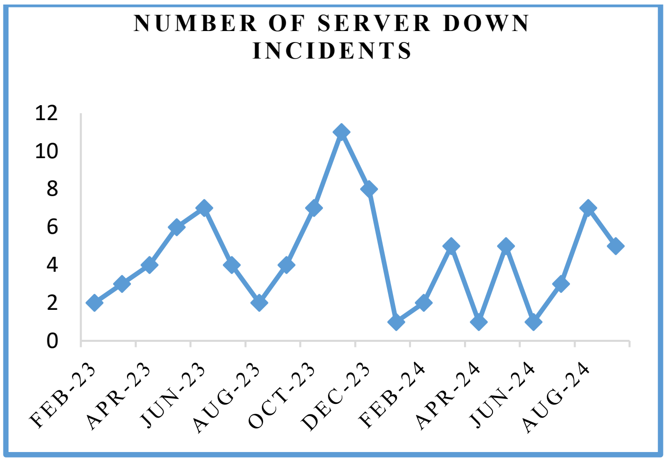

Figure 1. Number of server down incident

The implementation of information systems poses risks during the application process. The risks include database errors, server downtime, access misuse, network hacking, malware attacks, device theft, bandwidth access limitations, infrastructure failures, SQL Injection, Cross Site Scripting (XSS), data negligence, fire floods, and earthquakes [10-13]. These risks also occur in the implementation of information systems in government [14-19].

Therefore, a risk analysis is necessary for the management process of SPBE Audit Tools. Moreover, all IPPDS in Indonesia implement the SPBE Application and Infrastructure Audit. With the implementation of this risk management, it is hoped that no incidents will disrupt the SPBE Application and Infrastructure Audit process. The application of risk management in information technology to achieve organizational goals. The implementation of risk management must use an appropriate roadmap to be effective [20].

In order to address the risks in the implementation of SPBE, the Indonesian Government has established regulations to support its successful execution. The regulation is outlined in the PANRB Ministry Regulation No. 5 of 2020 [21]. This regulation explains guidelines and forms for the risk management process within the scope of government organizations. This guideline is called the SPBE Risk Management Guideline, which is adopted from ISO 31000.

This study developed a risk management framework for the management of SPBE Audit Tools using the SPBE Risk Management Guidelines. Based on the explanation of the problem above, the formulation of the problem in this research is to identify, analyze, and evaluate risks in managing the Audit Tools Application. Then, the identification, analysis, and evaluation of risks will be limited to eight risk categories, which consist of system development or enhancement projects, data and information, SPBE infrastructure, SPBE applications, SPBE security, SPBE services, SPBE human resources, and natural disasters. Implementing risk management will later serve as a recommendation for researchers in the development of SPBE Audit Tools. It is also hoped that the SPBE Application and Infrastructure Audit implementation process will run smoothly for all IPPDs in Indonesia.

2. LITERATURE REVIEW

The SPBE Risk Management Guidelines adopt SNI ISO 31000. This standard is used because it is repetitive in risk management and can assist organizations in strategy formulation, goal achievement, and decision-making. Table 1 presents a comparison between SNI ISO 31000 and Permenpanrb No.5 of 2020 as follows:

Table 1. Comparison of ISO 31000 with Permenpanrb No. 5 of 2020

No	Aspect	SNI ISO 31000	Ministry of PANRB Regulation No.5 of 2020
1	Main Objective	Improving organizational performance by encouraging innovation and providing support in achieving goals.	Integrating all SPBE risks into Central Agencies and Regional Governments (IPPD) tasks and functions in implementing SPBE.
2	Framework	A more flexible framework that can adapt to the organization's context and needs makes adjusting the risk management process easier.	A framework designed for IPPD provides guidelines and risk management work forms.
3	Communicationand Consultation	The process of building risk understanding in decision-making.	The ongoing process of sharing information through regular meetings or FGDs.
4	Context Setting	Determining the scope, internal and external context, and risk criteria.	Consists of inventorying general information, identifying SPBE targets, and determining the structure for risk management implementation.
5	Risk Assessment	There is a risk identification, risk analysis, and risk evaluation process.	The risk identification process is based on risk categories, followed by a risk analysis based on the likelihood and impact of the risk. Risk evaluation refers to risk appetite.
6	Handling on Risk	Selection and implementation of risk management, consisting of mitigation, avoidance, transfer, and acceptance of risk.	Positive risks consist of escalation, exploit, enhancement, share, and acceptance. Negative risks consist of escalation, mitigation, transfer, avoid, and acceptance.
7	Monitoring and Review	Paying attention to the effectiveness of risk management and making adjustments to changes.	Conducted periodically, with the identification of residual risks and further handling.

Risk is the effect of uncertainty in achieving a goal that can have positive, negative, or both impacts [22]. Risk is a combination of the likelihood of an event occurring and the impact of that event [23]. Risk management involves identifying, assessing, and controlling threats to an organization's assets and operations [24]. In the implementation of digital technology, risk management needs to be conducted. The rapid changes in technology make organizations quick to respond and adaptive.

Many risks arise from the transition from manual service systems to electronic ones. Therefore, the government mandates SPBE risk management for all IPPDs. SPBE Risk is the opportunity for events to occur that can affect the success rating of SPBE implementation [21]. A structured procedure is carried out to determine the best solution for SPBE risks, starting from the process, measurement, structure, and culture of SPBE risks. Identification, analysis, control, monitoring, and evaluation of SPBE risks are systematic processes of SPBE Risk Management, as outlined in the SPBE Risk Management Guidelines. The SPBE Risk Management process can be seen in Figure 2.

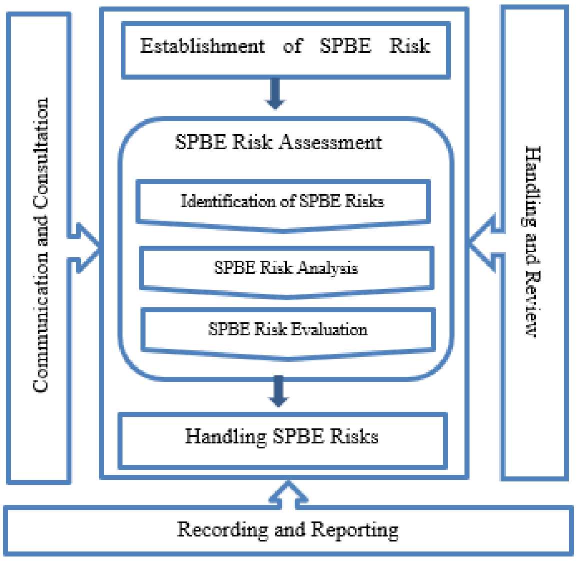

Figure 2. Risk management process

2.1 Establishment of SPBE risk

In establishing the SPBE risk context, the basic parameters and scope of SPBE risk application to be managed will be identified. In this process, the determination of SPBE risk categories, identification of SPBE risk impact areas, establishment of SPBE risk criteria, creation of an SPBE risk analysis matrix, classification of SPBE risk levels, and determination of SPBE risk appetite will be carried out.

2.2 SPBE risk assessment

The following process is risk assessment, which involves identifying, analyzing, and evaluating SPBE risks [7]. The goal is to understand the causes, likelihood, and impact of SPBE Risks in IPPD. The following are the stages of SPBE risk assessment, namely SPBE risk identification, SPBE risk analysis, and SPBE risk evaluation.

Risk identification is divided into two types: positive and negative risks. Positive risks can enhance the success of achieving the goals of SPBE. Meanwhile, negative risks can hinder the achievement of SPBE objectives. Then, a risk analysis is performed by selecting the control system, likelihood level, impact level, risk magnitude, and risk level. The final stage of risk evaluation is to decide whether the risk will be addressed according to the handling priority.

2.3 Handling SPBE risk

Risk prioritization and risk handling plans are determined in the risk management process. The risk management plan is determined by creating risk handling options, risk handling action plans, outputs, and responsible parties.

3. METHODOLOGY

This research examined the risks in managing the SPBE Audit application. The risk management process is applied by applying the SPBE Risk Management Guidelines [21]. The stages of the research are as follows: Figure 3.

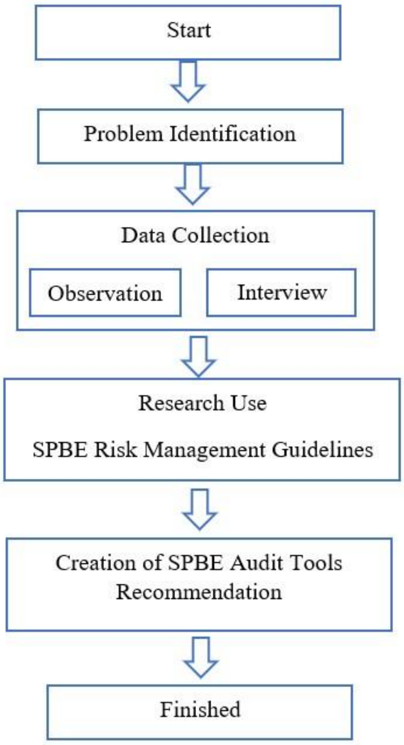

Figure 3. Research methodology

3.1 Problem identification

This research addresses a problem formulation for identifying, analyzing, and evaluating risks in the management of Audit Tools. Additionally, it explores recommendations that can be provided for better management of Audit Tools.

3.2 Data collection

In this research, the data collection process involved conducting observations and distributing questionnaires to the SPBE Audit Tools Application Managers, as follows:

3.2.1 Research instrument

This research uses the SPBE Risk Management Guidelines, which are the government's policy related to SPBE Risk Management. The policy is outlined in PANRB Ministry Regulation No. 5 of 2020. The SPBE Risk Management Guidelines refer to SNI ISO 31000. In this guideline, there is an SPBE Risk Management form as an instrument for conducting research.

3.2.2 Data collection

The data collection process in this research involves conducting observations and interviews. The results of these observations and interviews are used to identify risks occurring in the Audit Tools application. The following are the stages of data collection:

- Observations are conducted by observing the SPBE Application and Infrastructure Audit processes carried out by IPPD. Observations are made by examining the Audit Tools application.

- Interviews are conducted to obtain historical data on risks that have occurred, application data, and recommendations for application development. Interviews are conducted with four members of the Development Team and one member of the Infrastructure and Cybersecurity Team.

3.2.3 Research object

Audit Tools are auxiliary tools in the SPBE audit process conducted for all Indonesian government agencies, starting from the central and provincial levels to district/city levels. Audit Tools are managed by the Application and Infrastructure SPBE Audit Service Team. There are three modules in the SPBE Audit Tools application, namely the planning module, the implementation module, and the reporting module. The usage flow of the Audit Tools is divided according to its users, namely superadmin, auditee, and auditor.

3.3 SPBE risk management guidelines

In this section, the analysis will begin according to the framework used. The first step is to establish the SPBE risk context, followed by the SPBE risk assessment and handling on risk. At risk assessment stage, risk identification, risk analysis, and risk evaluation are carried out. Risk identification was conducted using data obtained from observations and interviews. The identified risks were then transformed into a questionnaire.

Risk identification was conducted using data obtained from observations and interviews. The identified risks were then transformed into a questionnaire. The questions in the questionnaire were based on the SPBE risk categories defined in the SPBE Risk Management Guidelines. The risk assessment process requires the involvement of 5 to 8 full team members [25]. Accordingly, eight members of the Audit Tool Management Team participated in completing the questionnaire. The team comprises members from both the development team and the application services team. They are all familiar with the Audit Tool Application and use it regularly.

3.4 Recommendations

The next stage involves providing recommendations. Recommendations will be provided based on the risk, impact, maturity value, and current conditions. Recommendations will be provided per SPBE risk category.

4. RESULT AND DISCUSSIONS

In this chapter, the application of the SPBE Risk Management Guidelines in the management of SPBE Audit Tools will be discussed according to Figure 3. Here are the results of the implementation:

4.1 Establishment of SPBE risk context

Based on the explanation in the previous section, the first stage in SPBE risk management is establishing the risk context of SPBE. At this stage, it consists of target identification, risk category determination, risk impact areas, risk criteria establishment, risk analysis matrix, risk levels, and risk appetite from the management of SPBE Audit Tools.

In this research, eight categories of SPBE risks will be used, namely, system development or enhancement projects, data and information, SPBE infrastructure, SPBE applications, SPBE security, SPBE services, SPBE human resources, and natural disasters [21]. As for the impact of SPBE risks, it consists of financial, reputational, performance, organizational service, operational and ICT asset, as well as legal and regulatory consequences.

Then risk anlysis matrix (Table 2), it is based on several regulations such as Permenkominfo No.16 of 2022 [26] and BRIN Regulations No.1 of 2024 [27].

Table 2. Risk matrix

Matrix			Impact				
			1	2	3	4	5
			No Signif-icant	Less Signif-icant	Quite Signif-icant	Signif-icant	Very Signi-ficant
Likelihood	5	almost certain to happen	9	15	18	23	25
	4	often occurs	6	12	16	19	24
	3	sometimes happens	4	10	14	17	22
	2	rarely happens	2	7	11	13	21
	1	almost never happens	1	3	5	8	20

Next, determine the risk level of the Audit Tools [21], as follows: Table 3.

Table 3. Risk level

Risk Level	Risk Scoring	Colour Symbol
Very Low	1 - 5	Blue
Low	6 - 10	Green
Medium	11 - 15	Yellow
High	16 - 20	Orange
Very High	21 - 25	Red

The final stage is determining the risk appetite, which aims to show the order of priority in handling risks by considering their positive or negative aspects. For positive risk, the minimum handling value is ≤ 10. Then, for negative risk, the minimum handling value is ≥11, except for human resources and natural disaster categories with a minimum of ≥16.

4.2 SPBE risk assessment

In this section, the Audit Tools Application management risk assessment will be conducted according to the SPBE risk management stages.

4.2.1 Risk identification

The first step is to conduct a risk identification. Risk identification is obtained from the results of observations and interviews. Additionally, it considers previous research on information system risk management in government.

Table 4. Risk identification

Risk Category	Code	Risk
System Development	A.1	Planned system development
	A.2	System development is hindered
Data dan Information	B.1	There is data access
	B.2	No data access
	B.3	Data and information leakage
	B.4	Data and information are not transparent
Infrastructure	C.1	Server down
	C.2	Power outage
	C.3	Network monitoring is inadequate.
	C.4	Slow access
Application	D.1	User satisfaction level is not good.
	D.2	Access to the application besides the auditee and auditor
	D.3	Technology is not updated
	D.4	Users are increasing
Information Security	E.1	Cyber attacks
	E.2	Information security according to policy
	E.3	Physical attack on data center
Service	F.1	Audit Services in accordance with regulations
	F.2	Audit services do not comply with regulations.
	F.3	The slow response of the Audit Service Team
Human Resources -IT	G.1	Quick response Audit Service Team
	G.2	Overloaded tasks on the Management Team
	G.3	The HR capabilities are inadequate.
	G.4	Infrastructure managers are not working.
Natural Disaster	H.1	Fire
	H.2	Flood
	H.3	Earthquake

Based on the risk identification in Table 4, it can be seen that there are 27 identified risks divided into eight risk categories. The risks mentioned above are a combination of positive and negative risks. Some are risks that have occurred in the Audit Tools application.

Then, some risks were also identified in previous research. Such as the risk of data access abuse, server disruptions, power outages, network connection issues, limited IT resources, cyberattacks, and natural disasters [15-17, 19]. Governance and management are also important factors in the successful implementation of SPBE. Therefore, risks related to the governance and management category have also been added.

4.2.2 Risk analysis

The first risk analysis begins by dividing risks into positive and negative risks. The probability value and impact value are obtained from the questionnaire results. The risk value is the result of the matrix of probability values and impact values from Table 2. For the risk level based on the explanation from Table 3.

The analysis in Table 5 reveals that out of the 27 identified risks, six are positive and 21 are negative. As explained earlier, this means that 78% of the identified risks hinder the success of Audit Tools' strategic objectives. The results of the risk analysis, as presented in Table 5, are more clearly illustrated in Figure 4.

From Figure 4 below, it can be seen that there are five high-level risks in positive risks, namely planned system development, data access, information security by policy, audit services by regulation, and rapid response from audit services. This means that the Audit Tool Management Team has followed the existing rules regarding the Development of SPBE Applications. The Audit Tool Management Team follows the planning for implementing the SPBE Audit as described in the SPBE regulations.

Table 5. Risk analysis

Risk Category	Code	Risk Type	Likelihood	Impact Level	Risk Value	Risk Level
System Development	A.1	Positive	3	4	17	High
	A.2	Negative	3	4	17	High
Data and Information	B.1	Positive	4	4	19	High
	B.2	Negative	2	3	11	Medium
	B.3	Negative	1	4	8	Low
	B.4	Negative	2	3	11	Medium
Infra-structure	C.1	Negative	3	4	17	High
	C.2	Negative	2	4	13	Medium
	C.3	Negative	2	4	13	Medium
	C.4	Negative	3	4	17	High
Application	D.1	Negative	3	3	14	Medium
	D.2	Negative	3	3	14	Medium
	D.3	Negative	3	4	17	High
	D.4	Positive	5	4	23	Very High
Information Security	E.1	Negative	2	4	13	Medium
	E.2	Positive	3	4	17	High
	E.3	Negative	2	3	11	Medium
Service	F.1	Positive	4	4	19	High
	F.2	Negative	2	3	11	Medium
	F.3	Negative	2	3	11	Medium
Human Resources -IT	G.1	Positive	4	3	16	High
	G.2	Negative	4	3	16	High
	G.3	Negative	2	3	11	Medium
	G.4	Negative	2	4	13	Medium
Disaster	H.1	Negative	2	4	13	Medium
	H.2	Negative	1	4	8	Low
	H.3	Negative	2	4	13	Medium

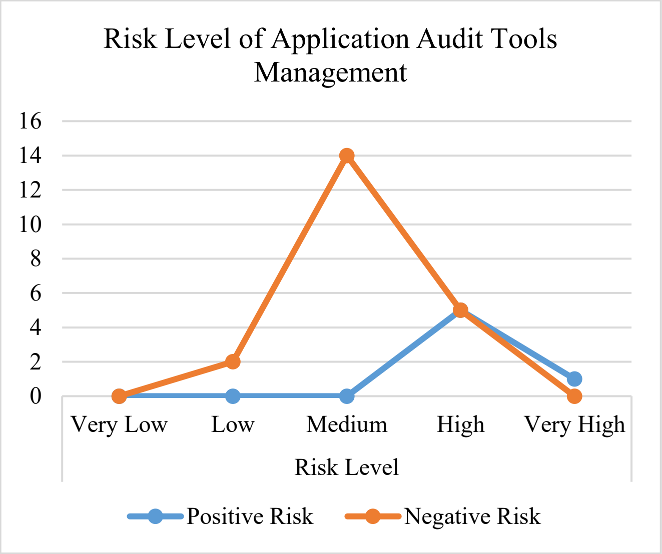

Figure 4. Risk level of audit tools

Then, among the existing positive risks, there is one very high-level risk, which is the increase in users of the Audit Tools Application. This is due to the obligation of all IPPDs to conduct ICT SPBE Audits. Moreover, an API exists between the SPBE evaluation application, Tauval, and the Audit Tools application. Data on the implementation of application and infrastructure audits will be directly retrieved as supporting evidence for the audit execution. The implementation of the SPBE Application and Infrastructure Audit adds value to the SPBE evaluation.

Out of the 21 identified negative risks, there are five high-level risks: system development being hindered, server downtime, slow access, outdated technology, and the Audit Tools Application management team being overloaded. Those five risks are indeed the ones that have been occurring in the management of the Audit Tools Application. As explained above, server downtime and slow access often become obstacles in implementing SPBE Application and Infrastructure Audits. Moreover, if the audit completion deadline is approaching. This will impact the completion of Audit implementation.

Then, regarding negative risks, there are 14 medium-level risks, namely no data access, data and information are not transparent, and power outage. Other risk are network monitoring is inadequate, user satisfaction level is not good, access to the application besides the auditee and auditor, cyber attacks, and physical attack on the data center. Besides that, there is a risk that audit services do not comply with regulations, the slow response of the Audit Service Team, the HR capabilities are inadequate, the infrastructure managers are not working, fire, and earthquake.

The above risks are common in the management of information systems in government. These risks will have a significant impact, namely, on the reputation of Audit Tools. The trust in IPPD decreases due to the many unresolved risks. Then the performance of the Audit Tools management will also decrease. The operation of the application will be disrupted, resulting in a delay to the audit process. The implementation of the SPBE Application and Infrastructure Audit is time-bound.

In the implementation of an audit, data and information are exchanged between the auditee and the auditor. For data access and transparency, data and information must be accessible to both the auditee and the auditor. Audit account access must be ensured not to be leaked, as audit results are highly confidential for IPPD. IPPD's trust is at stake from this data access.

The occurrence of cyber attacks, physical attacks on data centres, fires, earthquakes, power outages, and inadequate network monitoring will disrupt the ongoing Audit. The web application slows down and even becomes inaccessible, which indeed halts the audit process. This affects the application's satisfaction level, especially if it disrupts the supporting data uploaded to the application.

Application and Infrastructure Audit Services must be conducted by applicable regulations. So that the audit implementation runs according to its business process. The ability and speed of the management team's response will significantly impact the timing of the Audit. Therefore, the Service Team on duty must promptly respond to emails from IPPD.

There are two risks at a low level for negative risks, namely, audit data leakage and flooding. Audit data leakage will impact Audit Tools' reputation, leading to a decrease in users and a decline in IPPD's trust. For floods, the management of Audit Tools is already in a flood-free condition. So it has a low level. Here is a summary of the risk levels from the 27 identified risks. In Table 6. below, it is a combination of negative and positive risks.

4.2.3 Risk evaluation

After that, based on risk appetite, it will be determined whether the risk will be addressed or not. From Figure 5, it can be seen that none of the positive risks were addressed. Then, for the negative risks, 6 risks were not addressed and 15 risks will be addressed. The six risks that will not be addressed are audit data leaks, inadequate IT personnel capabilities, non-functional IT personnel, and risks associated with fire, flood, and earthquake.

Table 6. Audit tools risk analysis results

Matrix			Impact				
			1 No Significant	2 Less Significant	3 Quite Significant	4 Significant	5 Very Significant
Likelihood	5	almost certain to happen	🟩	🟨	🟧	🟥	🟥
	4	often occurs	🟩	🟨	🟧 G.2	🟧	🟥
	3	sometimes happens	🟦	🟩	🟨 D.1; D.2	🟧 A.2; C.1; C.4; D.3	🟥
	2	rarely happens	🟦	🟩	🟨 B.2; B.4; E.3; F.2; F.3; G.3	🟨 C.2; C.3; E.1; G.4; H.1; H.3	🟥
	1	almost never happens	🟦	🟦	🟦	🟩 B.3; H.2	🟧

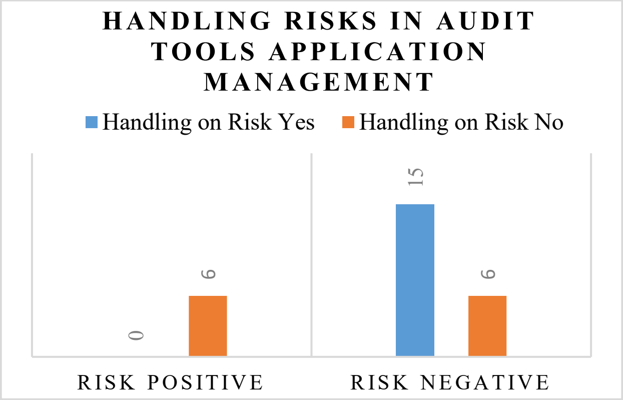

Figure 5. Handling risk

4.3 Handling on risk

For all positive risks, risk acceptance will be carried out. Because all positive risks already have a positive impact on the management of the Audit Tool Application, such as improved reputation, performance, service, and operational efficiency of the Audit Tool. For negative risks, the priority of each risk is determined. The top five risk priorities are server downtime, slow access, hindered system development, outdated technology, and cyber attacks. The risks that will be escalated are system development and technology updates for the Audit Tool Application. Risk escalation is the transfer of risk responsibility to higher authorities. Because the core Audit Tool Management Team currently lacks the necessary human resources for application development, it needs to be transferred to the relevant work unit. Other risks will be mitigated through risk management.

4.4 Maturity level

In addition to implementing risk management according to the SPBE Risk Management Guidelines, this study also includes the measurement of information system maturity [13]. Data from 8 respondents who are the Management Team and users of the Audit Tools, the existing risk categories were analyzed on a scale of 1-5 by all respondents.

The purpose of calculating this maturity value is to assess the organization's maturity in implementing the information system according to the eight risk categories. From Figure 6 above, it can be seen that the target maturity for the risk category is valued at 5. The application category has the highest maturity level at 3.28, followed by the system development category with a score of 3.25. The IT human resources category has a maturity score of 2.91, while the infrastructure category has a score of 2.66. In the service category, the score is 2.46, in the data and information category, the score is 2.41, and in the information security category, the score is 2.25.

The category with the lowest maturity value is natural disasters, which is 1.5. The average maturity score is 2.59. There is a GAP between the target and what has been implemented, which is 2.41. There is a GAP between the target and what has currently been implemented. Therefore, recommendations are needed for the management of Audit Tools. From the results of the risk analysis and risk evaluation, the best handling will be provided for each risk. So that in the future, the maturity of the Audit Tools Application will continue to improve.

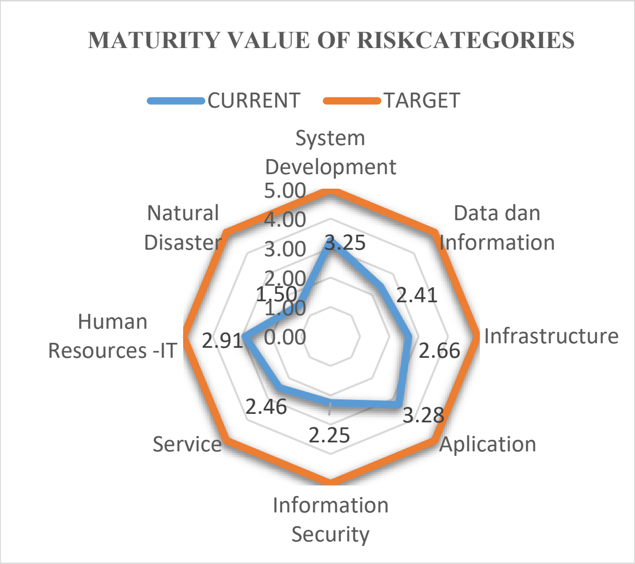

Figure 6. Maturity level of audit tools

4.5 Recommendations

Recommendations will be formulated from the results of risk identification, risk assessment, and risk handling above, as well as the results of interviews with the Audit Tools Development team. Here are the recommendations for the management and development of the Audit Tools Application:

4.5.1 System development

Coordination between the Audit Tools Management Team and the National SPBE Team is necessary in system development. Because the implementation of the SPBE Application and Infrastructure Audit is based on the applicable policies. In addition, good planning is needed to develop audit tools according to the needs of the users, namely the auditee and auditor of each IPPD.

4.5.2 Data and information

In the category of data and information, there are risks related to data and information access, lack of transparency in access, and data and information leaks. To prevent those risks from occurring, the Management Team must create an Audit Account Control SOP. Each IPPD only provides the username and password of the account to the responsible auditee and auditor. For user account access, SSO can be used because it enhances security through the use of additional authentication methods, such as two-factor authentication. Additionally, SSO can simplify account management [3].

4.5.3 Infrastructure

The infrastructure category has risks such as server downtime, slow access, power outages, and an inadequate network. To avoid those risks, it is mandatory to conduct an infrastructure audit annually to assess the capability value of the Audit Tools management infrastructure. Hiring cloud services from third parties has certainly been done, but regular monitoring of cloud usage is necessary. Then, if an incident occurs or there is infrastructure maintenance, the Audit service team must immediately notify the audit website. In addition, coordination between the Audit service team and the infrastructure team must be carried out. This is done to prevent disruption of the services and operations of the Audit Tools.

4.5.4 Application

In the Application category, there are risks related to user satisfaction levels, the number of users, application access, and application technology. To increase the number of users, conducting periodic socialization of the SPBE Application and Infrastructure Audit Implementation to all IPPDs is necessary. In addition, the application socialisation also needs to include information about the risk mitigation plan, so that they are aware of the application's cybersecurity policies [28].

Implementing the SPBE ICT Audit complies with SPBE policy, which needs to be made a culture by all IPPDs. Training on application usage will also increase user satisfaction levels. The features in the application need to be improved and made user-friendly. For example, the additional question feature needs to be reviewed or removed. Because so far, it is still error-prone, and no IPPD auditors have added questions outside the provided question indicators. Then the feature to add audit activities by auditors should be removed. Because its creation is carried out by the Audit Services Team. There are still many other features that need to be maintained and reviewed. The application features need to be periodically improved for user comfort.

4.5.5 Information security

In the information security category, there are risks of cyber and physical attacks on data centers. To prevent such risks, there needs to be an Information Security policy. In addition, it is necessary to conduct a Security Audit every year. The Information Security Team must continue to work according to their duties to prevent cyber and physical attacks. To address the risks to data centre security, organisations can perform real-time backups. Additionally, they should update to the latest monitoring tools [11].

4.5.6 Service

In the service category, there are risks of non-compliance with regulations and slow service response. Therefore, forming a solid service team that can quickly respond to service requests is necessary. The Audit service email needs to be monitored to respond promptly to service requests. In addition, periodic evaluations of the SPBE audit services are necessary. The service website needs to include a help desk and a user manual for the service so that IPPD does not get confused when they want to request an audit account. The preparation of the service SLA must also be carried out.

4.5.7 IT human resources

In the IT HR category, it is necessary to periodically enhance the competencies of the Audit Tools management team. Conducting training sessions as needed, such as Audit services, incident and disaster handling, system/application development, etc. [29]. In addition, personnel placement according to needs must also be carried out. To improve service and performance, increasing awareness among the team must also be done. After that, it is necessary to conduct periodic performance evaluations of the Audit Tools management personnel to ensure operations run smoothly without any incidents occurring.

4.5.8 Natural disaster

In the disaster category, there are fire, flood, and earthquake risks. The presence of cloud in the data center will help avoid those risks. In addition, it is necessary to create a Disaster Recovery Plan so that each personnel member managing the Audit Tools understands how to recover the system in case of a disaster. By conducting monitoring and evaluation of cloud and physical infrastructure, the services and operations of Audit Tools will run smoothly. There is a need to develop earthquake-resistant physical infrastructure and update disaster early warning systems [30].

5. CONCLUSIONS

The mandatory implementation of the SPBE ICT Audit by all IPPDs has led to an increase in the number of users of the Audit Tools Application each year. Audit Tools were developed alongside formulating policies regarding SPBE ICT Audits and the Standards and Procedures for Auditing SPBE Applications and Infrastructure. Of course, many improvements need to be made in both technical and management governance aspects. With the incidents that have occurred, implementing Information System Risk Management in the management of Audit Tools has become necessary. With the existence of the Risk Management Guidelines, the implementation of Risk Management in the Management of Audit Tools becomes more structured and detailed.

From the results of risk management on the management of Audit Tools above, it can be seen that there are 27 identified risks. These risks consist of 6 positive risks and 21 negative risks. In the positive risks, there are five high-level risks, namely planned system development, data access, information security by policies, audit services by regulations, and quick response from audit services. Then, among the positive risks, there is one very high-level risk, which is the increase in users of the Audit Tools Application. There are two low risks for negative risks, namely, audit data leakage and flooding. Then there are 14 moderate risks, namely, no data access, data and information are not transparent, power outage, network monitoring is inadequate, user satisfaction level is not good, access to the application besides the auditee and auditor, cyber attacks, and physical attack on the data center. In addition, there are risks such as audit services not complying with regulations, the slow response of the Audit Service Team, inadequate HR capabilities, infrastructure managers not working, fire, and earthquake. Meanwhile, there are five high risks: system development is hindered, server down, slow access, outdated technology, and the Audit Tools Application management team is overloaded.

For risk management, a priority for handling them is established. The highest priority risks are server downtime, slow access, system development delays, outdated technology, and cyber attacks. There are 13% of risks that need to be escalated and 87% of risks that need to be mitigated. In addition, the maturity of the information system was measured based on eight risk categories used in this study. The average maturity score is 2.59. Therefore, improvements in the management of Audit Tools are necessary, so recommendations for their management are needed. In this study, residual risk is not discussed. In the next research, risk management of Audit Tools governance and management needs to be conducted. Better risk management of Audit Tools and adherence to policies are required. IPPD, which performs the Audit of SPBE Applications and Infrastructure, has also been spared from previous incidents.

DATA AVAILABILITY STATEMENT

The datasets analyzed are not publicly available due to their confidential nature and institutional protocols. This paper considers the data confidentiality restrictions set by the institution.

AUTHOR CONTRIBUTIONS

Harnum Annisa Prafitia: Conceptualization, Methodology, Formal Analysis, Writing – Original Draft. Nilo Legowo: Supervision, Validation, Writing-Review and Editing, Project Administration, Funding Acquisition.

ACKNOWLEDGMENT

The authors express their deepest gratitude to the entire Audit Tools Management Team who have been willing to be interviewed and provide recommendations on the audit Tools. The author also thanks Prof. Dr. Drs. Nilo Legowo, M.Kom, for all his guidance, reviews, feedback, and support in writing this paper. This research is funded by the Indonesian Ministry of Communication and Digital (Komdigi) to the first author as a recipient of the Komdigi Aspiration Scholarship. Thank you for the trust placed in the author.

REFERENCES

[1] Wantiknas. (2024). Arah Transformasi Digital. Wantiknas. http://www.wantiknas.go.id/id/berita/arah-transformasi-digital-indonesia.

[2] Yeremias, T.K., Cahyadi, D., Djunaedi, A. (2024). Modelling E-government maturity determinants at the local level in Indonesia using technology-organization-environment framework. Jurnal Ilmu Sosial Dan Ilmu Politik, 28(1): 17-34. https://doi.org/10.22146/jsp.81803

[3] Pratama, A.D., Abdurrahman, L., Saedudin, R.R. (2024). Implementation of Single Sign On (SSO) technology on the SMART JABAR portal based on the principles of electronic based government system. In Proceedings of the 2024 7th International Conference on Information Science and Systems, pp. 96-104. https://doi.org/10.1145/3700706.3700723

[4] Hardi, R., Nurmandi, A., Purwaningsih, T., Manaf, H.A. (2025). Smart city governance and interoperability: Enhancing human security in Yogyakarta and Makassar, Indonesia. Frontiers in Political Science, 7: 1553177. https://doi.org/10.3389/fpos.2025.1553177

[5] Arisal, A., Setiadi, B., Muslim, I. (2025). Analysis of alternatives methodology for large-scale information system implementation. Bulletin of Electrical Engineering and Informatics, 14(1): 665-675. https://doi.org/10.11591/eei.v14i1.7800

[6] Hadiono, K., Candra, R., Santi, N. (2020). Menyongsong Transformasi Digital. In Proceeding SENDIU 2020. https://www.researchgate.net/publication/343135526_MENYONGSONG_TRANSFORMASI_DIGITAL.

[7] Presiden, R.I. (2018). Perpres No.95 of 2018. Sistem Pemerintahan Berbasis Teknologi (SPBE).

[8] Irzavika, N., Mahda, F.R. (2023). The effectiveness of SPBE application and infrastructure audit tools in enhancing information technology governance using COBIT 2019. In 2023 International Conference on Informatics, Multimedia, Cyber and Informations System (ICIMCIS), Jakarta Selatan, Indonesia, pp. 633-638. https://doi.org/10.1109/ICIMCIS60089.2023.10348973

[9] Widyasuri, A., Priambodo, D.F., Ajhari, A.A., Sunaringtyas, S.U. (2024). Security analysis of audit tools. In 2024 International Conference on Computer, Control, Informatics and its Applications (IC3INA), Bandung, Indonesia, pp. 405-410. https://doi.org/10.1109/IC3INA64086.2024.10732702

[10] Sahibu, S., Sakti, A., Iskandar, A. (2024). Risk management analysis of SMK Telkom Makassar's Integrated Academic Information System in compliance with ISO 31000 standards. Ingénierie des Systèmes d'Information, 29(1): 205-218. https://doi.org/10.18280/isi.290121

[11] Andry, J.F., Liliana, L., Tannady, H., Arief, A.S. (2022). Data centre risk analysis using ISO 31000: 2009 framework. Journal of Physics: Conference Series, 2394(1): 012032. https://doi.org/10.1088/1742-6596/2394/1/012032

[12] Masso, J., Pino, F.J., Pardo, C., García, F., Piattini, M. (2020). Risk management in the software life cycle: A systematic literature review. Computer Standards & Interfaces, 71: 103431. https://doi.org/10.1016/j.csi.2020.103431

[13] Suyasa, G.W.A., Legowo, N. (2019). The implementation of system enterprise risk management using framework ISO 31000. Journal of Theoretical and Applied Information Technology, 97(10): 2669-2683.

[14] Cartens, H., Suawa, S., Prillysca Chernovita, H., Kristen, U., Wacana, S. (2023). Analisis Manajemen Risiko Aplikasi SRIKANDI pada Kantor DISKOMINFO Kota Manado menggunakan ISO 31000. https://ejurnal.unima.ac.id/index.php/edutik/article/view/8562, accessed on Oct. 18, 2024.

[15] 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): 7364-7372.

[16] Linda Lole, K.M., Maria, E. (2020). Analisis manajemen risiko pada aplikasi pegadaian digital service menu tabungan emas menggunakan ISO 31000:2018. Jurnal Sistem Komputer dan Informatika (JSON), 3(3): 319. https://doi.org/10.30865/json.v3i3.3891

[17] Mahardika, F., Agreindra H,M., Fatimah, S.A., Nur F, L.T. (2023). Manajemen risiko teknologi informasi aplikasi e-office ASN menggunakan ISO 31000:2018. Infotekmesin, 14(2): 237-243. https://doi.org/10.35970/infotekmesin.v14i2.1877

[18] Nastiti, A.D., Wulandari, M., Agustiningtyas, S., Radhitya, R., Ahmad, I., Hermawan, W. (2023). Risk management planning of certification authority termination based on ISO 31000: 2018. In 2023 7th International Conference on New Media Studies (CONMEDIA), Bali, Indonesia, pp. 127-131. https://doi.org/10.1109/CONMEDIA60526.2023.10428241

[19] Putri, S.W., Ashari, M., Mardi, M., Fadli, S. (2024). Analisa manajemen risiko pada aplikasi e-smart di

BKPSDM lombok tengah menggunakan iSO 31000. Innovative: Journal of Social Science Research, 4(1): 4614-4627. https://doi.org/10.31004/innovative.v4i1.8323

[20] Berrada, H., Boutahar, J., El Ghazi El Houssaïni, S. (2023). Roadmap and information system to implement information technology risk management. International Journal of Safety and Security Engineering, 13(6): 987-1000. https://doi.org/10.18280/ijsse.130602

[21] Kemenpanrb. (2020). Permenpanrb No.5 of 2020. Pedoman Manajemen Risiko SPBE. https://peraturan.bpk.go.id/Details/143664/permen-pan-rb-no-5-tahun-2020.

[22] SNI ISO 31000. (2018). Risk Management-Guidelines. https://pu.go.id/pustaka/biblio/sni-iso-31000-2018-manajemen-resiko/BKB99K.

[23] Matheu, S.N., Martínez-Gil, J.F., Bicchierai, I., Marchel, J., Piliszek, R., Skarmeta, A. (2025). A flexible risk-based security evaluation methodology for information communication technology system certification. Applied Sciences, 15(3): 1600. https://doi.org/10.3390/app15031600

[24] Radjulan, J.C., Iriani, A., Tambotoh, J. (2024). Evaluation IT governance computer network at central bureau of statistics (BPS) maluku province using COBIT 2019 DSS01 and DSS05 domains. BAREKENG: Jurnal Ilmu Matematika dan Terapan, 18(4): 2779-2794. https://doi.org/10.30598/barekengvol18iss4pp2779-2794

[25] Piper, J. (2018). Risk Management Framework: Qualitative Risk Assessment through Risk Scenario Analysis. NATO Science and Technology Organization. MP-IST-166-07.

[26] Kemenkominfo. (2022). PM Kominfo 16-2022 tentang KUPATIK. https://peraturan.bpk.go.id/Details/255601/permenkominfo-no-16-tahun-2022.

[27] BRIN. (2024). Peraturan BRIN Nomor 1 Tahun 2024 Tentang Standar dan Tata Cara Pelaksanaan Audit Infrastruktur dan Audit Aplikasi SPBE. 2024.

[28] Kioskli, K., Seralidou, E., Polemi, N. (2025). A practical human-centric risk management (HRM) methodology. Electronics, 14(3): 486. https://doi.org/10.3390/electronics14030486

[29] Oktarina, D. (2023). Implementation of an electronic-based government system (SPBE) at the Muaro Jambi regency communication and information service. Sustainability (STPP) Theory, Practice and Policy, 3(2): 133-143. https://doi.org/10.30631/sdgs.v3i2.2083

[30] Sousa, M.L., Tsionis, G. (2025). National seismic risk assessment: An overview and practical guide. Natural Hazards, 1-34. https://doi.org/10.1007/s11069-024-07008-y