Contents lists available at: https://e-journal.unair.ac.id

AJIM (Airlangga Journal of Innovation Management)

Journal homepage: https://e-journal.unair.ac.id/AJIM

Analysis of Risk Management Using E-Office Application with ISO 31000:2018 in National Public Procurement Agency (NPPA/LKPP)

Gunawan Syarifah Arif[1] Yustika Erliani[2] Anita Ratnasari[3]

[1,2,3] Department of Information System, Faculty of Computer Science, Universitas Mercu Buana, Indonesia

ARTICLE INFO

Paper Type:
Research Paper

Keywords:
NPPA, Government Procurement, E-Office, Risk Management, ISO 31000:2018

Article History
Received: 7 April 2024
Revised: 6 June 2024
Accepted: 23 June 2024
Available online: 30 June 2024

ABSTRACT

The National Public Procurement Agency (NPPA/LKPP) has implemented the E-Office application to streamline work activities for both civil servant (ASN) and non-ASN employees, encompassing personnel data, attendance, correspondence, and other administrative functions. This research aims to identify and analyze the risks associated with the LKPP E-Office application. This study utilized a qualitative methodology, adhering to the ISO 31000:2018 risk management framework, to conduct in-depth interviews and observations within the LKPP setting. The aim was to gather comprehensive data to support stakeholders in making well-informed and precise policy decisions about the E-Office application. Through this research, 32 distinct risks were identified and categorized into high, moderate, and low levels based on their potential impact. This study developed specific mitigation strategies to address and minimize the effect of identified risks. By adopting these strategies, the research aims to enhance the reliability and security of the E-Office application. Improved risk management practices will lead to a more resilient and secure system. As a result, boosting administrative efficiency and data management capabilities within NPPA/LKPP. Furthermore, this research not only brings to light the critical areas that require immediate attention but also outlines a strategic roadmap for mitigating these risks. This approach ensures the sustainable and efficient operation of the E-Office application. The outcomes of this study are anticipated to offer substantial benefits to stakeholders, creating a more secure and efficient administrative environment.

*Corresponding author: 41821110037@student.mercubuana.ac.id

Cite this article as: Arif, G.S., Erliani, Y., Ratnasari A. (2024). Analysis of Risk Management Using E-Office Application with ISO 31000:2018 in National Public Procurement Agency (NPPA/LKPP). *Airlangga Journal of Innovation Management, 5(2), 260-277.* https://doi.org/10.20473/ajim.v5i2.56656

Introduction

The National Public Procurement Agency of Indonesia (NPPA) known as LKPP had responsibilities of developing, formulating, and establishing government procurement policies. To aid in the implementation of its responsibilities, LKPP utilizes the E-Office application. The LKPP E-Office application was important in supporting the daily activity of employees. Moreover, it also ensures the smooth functioning and tasks of LKCP as a primary focus. As an office management system, the app provides important features such as absences, staff data, stamping, activity agendas, and other administrative components. The use of this application ranges from senior officials to external parties, making it the core of the LKPP's operational efficiency (Rahmadini et al., 2023). However, technological advances carry certain risks that need to be identified and managed effectively. These risks involve data security, potential application failure, and incoherence of development policies with user needs (Santoso & Kusuma, 2023). The study aims to identify the risks that may arise from the use of E-Office LKPP applications and find recommendations to mitigate such risks.

In implementing risk management, no risk management measurements have been carried out using the ISO 31000:2018 framework on the LKPP E-Office application. ISO provides guidelines and principles related to risk management that can provide a solid foundation for risk assessment and mitigation (Candra et al., 2019; Nuryitmawan, 2022). Therefore, risk management analysis is important, and follow-up based on the given risk treatment to minimize the impact of possible risks (Wardhana et al., n.d.). Several previous studies have provided valuable insights related to the implementation of the standard work procedure of ISO 31000:2018 in risk management analysis in various organizational contexts. Research at Grandhika Medan Hotel highlighted the importance of improved socialization and training related to information security risk management to employees. The recommendations included better coordination with stakeholders in managing information security risks (Syahnur et al., 2022). In a separate study conducted at the Trial State Court of Class 1 B, researchers identified 14 potential risks impacting the SIPP applications. These findings underscore the intricate nature of the risks encountered in the judicial context, emphasizing the necessity for targeted risk management strategies (Pangestu et al., 2021).

In another study focusing on the risk management of hospital management information systems (SIMRS) at XYZ Hospital, high-level risks such as virus attacks and power outages were identified. Additionally, the study uncovered 13 medium-level risks, including data entry failures, disconnections, and human errors. The study provided recommendations for risk treatment aimed at preventing these potential risks (Mendo et al., 2023). Lastly, research on the MyPertamina app identified 19 risks, with three classified as high-level risks. These included data breaches, corrupted data, and issues with application updates. This study highlighted the complexity of managing risks within the MyPertamina application using ISO 31000:2018 as a guideline (Liperda & Nieng, 2023).

This research aims to offer valuable insights to the leadership of LKPP for policy formulation concerning the development and maintenance of E-Office applications. By thoroughly understanding the associated risks, LKPP can implement appropriate measures to ensure operational continuity and enhance efficiency in public service delivery. Adopting an ISO-based approach to risk management will also bolster confidence in the reliability and security of the LKPP E-Office applications.

Literature Review

Risk Management

Risks are an integral aspect of all construction projects, potentially impacting the delivery of projects negatively in terms of time, cost, and quality (Osipova, 2015). Therefore, managing these risks is a critical component of a successful project (Rahman et al., 2022). Risk management involves a structured approach to identifying, analyzing, responding to, and monitoring potential risks (Qosim et al., 2023). However, properly managing risks in international EPC (Engineering, Procurement, and Construction) projects presents significant challenges (Pratiwi et al., 2022).

Because of the dynamic variables affected by the changing international environment, risks in global construction markets are complex (Loestefani et al., 2022). The interdependent nature of the EPC processes creates a need for managing project risks by considering the interactions among different stakeholders (Taroun, 2014). Joint efforts by all the involved parties are needed to deal with risks in a cooperative manner by sharing valued information and resources (Zakik et al., 2022).

The risk management processes largely depend on the information available Hastak and Shaked (2000), and coherent information was important to enhance the systematic and proactive efforts for early warning, effective negotiation, and timely problem resolution (Chan et al., 2010; Zou et al., 2010). Thus, EPC contractors must develop partnering relationships with project participants, and aim to facilitate integrated risk management processes by incorporating external information derived from the partners (Tang et al., 2007);(Ryandono et al., 2019).

ISO 31000:2018.

ISO 31000:2018 is an internationally recognized standard that provides guidelines for managing risks in various organizational contexts. It offers comprehensive instructions to identify, assess, control, and mitigate risks that could hinder the organization from achieving its objectives. Emphasizing a risk-based approach to decision-making, ISO 31000 encourages organizations to gain a deep understanding of existing risks and implement effective strategies to manage them. The standard outlines key principles, frameworks, and processes essential for organizations to minimize the adverse effects of risks and capitalize on potential opportunities (Sahira et al., 2020).

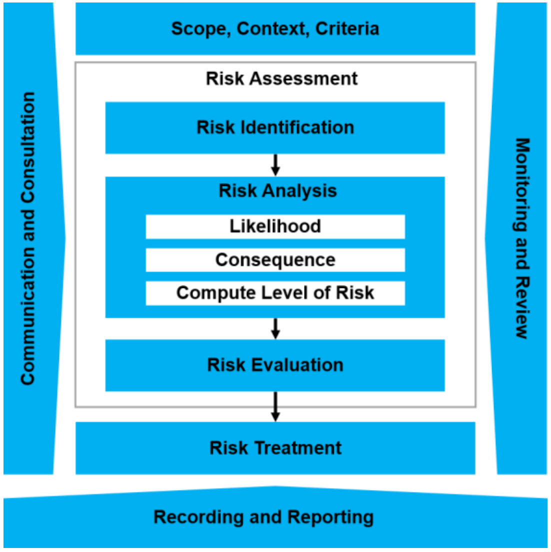


Figure 1. Risk Management Process
Source: Hutchin (2018)

The core principle of ISO 31000:2018 underscores that risk results from the uncertainty that impacts objectives. Poorly managed risks could escalate into problems, crises, or even catastrophic events (Wardhana, 2022). These principles are intended to guide both individuals and organizations in effectively managing risks. The principles articulated in SNI ISO 31000:2018 represent a fundamental cornerstone in the discipline of risk management. Eight principles should be considered and used as a reference when formulating a framework and risk management process (Hopkin, 2018).

1. Integrated: Risk management should be an integral part of the entire business process of the organization, not separate from a particular division or department.

2. Structured and Comprehensive: Risk management should be implemented structurally and systematically by covering all aspects and operations of an organization. A draft Risk Management Framework is required as a guideline for implementation practices.
3. Adaptation: Implementation of risk management must be adapted to the internal and external context of the organization, taking into account unique needs and characteristics.
4. Inclusive: The implementation of risk management must involve all stakeholders, ensuring the involvement of those involved following their respective scope of work and responsibilities.
5. Dynamic: Risk can appear, change, or even disappear from time to time. Therefore, risk management must be able to anticipate, detect, and respond to such changes. The organization is expected to be sensitive to the risks that may arise so that its effectiveness is not compromised.
6. Best Information Available: The application of good risk management should be based on relevant information from the past and present, as well as expectations to be achieved in the future. Organizations should consider all the limitations and uncertainties associated with such information and expectations.
7. Human and Cultural Factors: Competence in risk management is inherent in human or human resources (HRM) within an organization. This principle emphasizes that the human and cultural factors carried by individuals within an organization can be part of risk control or, on the contrary, become the cause of risk.
8. Connectivity Improvement: The application of good risk management must be continuously improved based on learning and experience. The goal of the synergy improvement is to ensure that risk management and process capabilities remain relevant to the current condition in an organization and can be used in the future. These improvements involve improved stakeholder capacity, adequate resource availability, and the reliability of the infrastructure that supports the risk management process.

ISO 31000:2018 consists of three main components: principles, frameworks, and processes. The principles apply universally, while the framework only applies to one organization. Risk management processes apply to certain types of risk, and the organization must have a risk-conscious human resource, obtained through an understanding of these standards (Ryandono et al., 2022).

This standard emphasizes that risk management is an inherent competence of the individual. This is because the perception of risk can vary between individuals. As a guideline, ISO 31000:2018 ensures that organizations have a common language and understanding related to risk management.

LKPP E-Office Application

The e-Office Application of the Government Procurement Policy Institution (LKPP) is a digital platform designed to improve efficiency, transparency, and accountability in office administration and procurement management processes in the LKPP environment. The digital transformation implemented through the e-office application replaces conventional paper-based models with information technology-based systems, creating a more modern, integrated, and adaptive working environment.

The form of digital transformation in the LKPP e-Office application includes a variety of absence features, stamping such as a note of service, letter of service and assignment, employment data, and internal publication to activity agenda. The e-Office application facilitates various processes including electronic document management, scheduling, activity tracking, team collaboration, and summarizing staff activities. As a result, it transforms traditional work methods into efficient and rapid. It also provided easier and quicker access to information for users.

Furthermore, accountability is prioritized as a fundamental principle within the LKPP e-Office application. By leveraging information technology, every transaction and activity within the application is digitally traceable, thereby reducing the risks associated with errors and data loss.

Methodology

This study utilized diverse qualitative data collection methods to gain a profound understanding of risk management within the LKPP E-Office application. The qualitative approach allowed for an in-depth exploration of the complex and nuanced aspects of the risks involved (Ryandono et al., 2020). Methods such as detailed interviews and direct observations yielded rich, comprehensive data that provided insights into the specific challenges and vulnerabilities faced by the system. This methodological choice ensured that the analysis was firmly rooted in the actual experiences and perspectives of both users and administrators of the E-Office application, thereby facilitating a more accurate identification and assessment of risks.

This study collected the data by interviewing various stakeholders knowledgeable about the LKPP environment. These stakeholders included the head of LKPP's Data and Information Center (Pusdatin), personnel responsible for managing data and information, and IT infrastructure experts. The interview was conducted to understand the basic principles of operational practices, perspectives on risk management, insights into existing risks, and the effectiveness of implemented mitigation measures within LKPP.

Observation of activities related to the management of E-Office applications LKPP and the condition of the infrastructure of the server of the e-Office application. This observation allows researchers to understand how the content management process is implemented in practice and to observe the information technology conditions used to support the LKPP E-Office application. It helps researchers identify potential problems and risks that may arise.

In-depth literature study of the ISO 31000:2018 standard. This study used a literature review to understand the basic framework of risk management adopted by LKPP and find key points relevant to analyze their information security risk management. It helps us in linking practice in the field with the international standards in force.

Results and Discussion

The flow diagram of the research performed will be carried out according to the following picture:

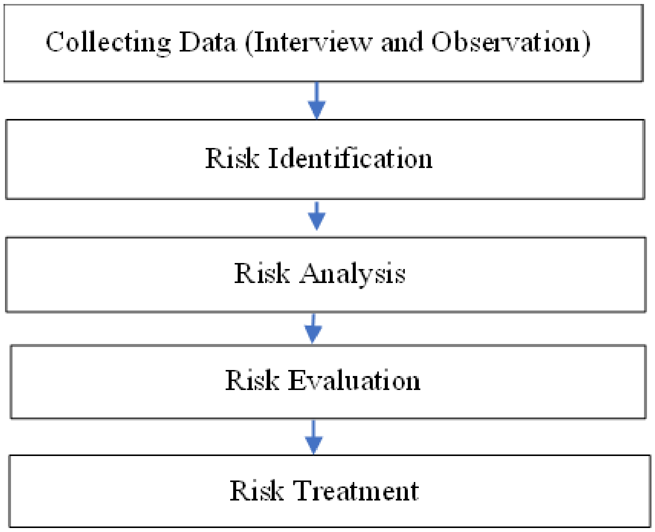


Figure 2. Research Flow Diagram

Source: Arranged by authors

The apps of E-Office Risk Management analyze risks by involving several stages. Those stages were data collection through interviews and observations, risk identification, risk analysis, and risk evaluation.

Risk Identification

The first phase, the research begins with data collection using the methods of interviews and observations Andaru & Adi (2024). Through the interviews, the researchers asked identified sources, namely the head of the Data and Information Centre (Pusdatin), the head of the Public and Public Relations Bureau, infrastructure staff, as well as human platoon. The interview was conducted to obtain a direct condition of how LKPP manages the E-Office application. In addition, the research was also carried out with observation of the process of management of the content of the e-Office applications and the condition of the E-Office application infrastructure directly. By combining both of these methods, researchers can collect complete data about the day-to-day practices related to the Management of E-office applications of LKPP.

At this stage, research is focused on asset identification of official identity data, printing data, absence data, publication data, LKPP agenda data, E-Office LKPP applications, and servers.

Table 1. Asset identification in LKPP E-Office Application

Component	Asset
Data	1. ID Staff 2. Mailing Data 3. Presentation Data 4. Public Data 5. LKPP Agenda Data
Software	E-Office LKPP Application
Hardware	Server

The research continued with the identification of possible risks. At this stage, it was carried out identifying various potential risks that may arise in the management of the E-Office LKPP application that covers natural/environmental factors, humans, systems, and infrastructure.

Table 2. Identification of Possible Risks on LKPP E-Office Applications

Factor	Id	Risk Event
Environment	R01	Flood
	R02	Earthquake
	R03	Lightning
	R04	Fire
	R05	Power outage
	R06	Dust/Dirt
Human	R07	Denial of Service
	R08	Not following procedure
	R09	Abuse of Access Rights
	R10	Man in the Middle Attack

Infrastructure and system	R11	Data/Hardware Theft
	R12	UI design is difficult to understand
	R13	Not knowing the operation of e-office
	R14	Data not updated successfully
	R15	Organization change
	R16	Server Down
	R17	Backup Failure
	R18	Data Corrupt
	R19	Over Capacity
	R20	Access Overload
	R21	Web Service Down
	R22	Network Connection Broken
	R23	Unstable Network Connection
	R24	System Crash
	R25	System Update failed
	R26	Memory Ram full
	R27	Slowly application
	R28	Genset is not working properly
	R29	System not integrated
	R30	Rats/other animals
	R31	Login Failure
	R32	Virus Attack

After identifying the possible risk acquired, the research continues with the identification of the risk impact. At this stage, it is done by evaluating the impact of risk that may occur if the potential risk obtained occurs.

Table 3. Risk Impact of LKPP E-Office Applications

Id	Risk Possibility	Impact
R01	Flood	Damaging hardware, servers, and physical documents, as well as causing interference in operations.
R02	Earthquake	Damaging hardware and physical structures, causing system failures and data loss.
R03	Lightning	Potential hardware and server damage due to Lightning shutdown, causing downtime.
R04	Fire	Hardware, physical documents, and servers were damaged. It also caused heavy data loss.
R05	Power Outage	Caused downtime, loss of unsaved data, and interruption of operations.
R06	Dust	Damaging hardware and causing problems in device functionality.
R07	Denial of Service	Operational disorder.

R08	Un-procedure	Data loss or corruption due to improper execution of procedures, as well as potential downtime.
R09	Abuse of access rights	The risk of unauthorized access to data and information that may result in leakage or misuse.
R10	Man in the Middle Attack	Potential risk of leakage of classified information or sensitive data.
R11	Data Theft/ Hardware Theft	Loss of data or hardware potentially creates a security gap.
R12	UI design is difficult to understand	Decreases user productivity and increases the risk of error in use.
R13	Can't Operate E-Office	Decreases the efficiency of use and increases the risk of error.
R14	Data Failed to Update	The risk of bad decision-making due to a lack of state-of-the-art data.
R15	Change Management	Changes to the approval system of service documents involving the organization's leadership
R16	Server Down	Downtime, unavailable data and applications.
R17	Backup Failure	Loss the ability to recover data in case of failure or damage.
R18	Data Corrupt	Loss of data integrity, which can lead to loss of information.
R19	Over Capacity	Decreased system performance and potential failure.
R20	Overload Access	Poor system performance and reduced responsiveness.
R21	Web Service Down	Unable to access web services and e-Office applications.
R22	Network Down	Loss of connectivity and access to data.
R23	Unstable Connection	Disruption in operation and potential data loss.
R24	System Crash	Comprehensive system failure with downtime consequences and data loss.
R25	Failed to update system	Vulnerable security potential and incompatibility with the latest technology.
R26	Memory Ram Full	Poor application performance and risk of system failure.
R27	Slow Application	Long running data appearance process.
R28	Genset is not working properly	Risk of backup power failure during power outages.
R29	Unintegrated system	Lack of coordination and exchange of information between systems can hinder efficiency.

R30	Mice/ Other animals	Physical damage to hardware and hygiene risks.
R31	Login Failed	Resistant to security gaps and performance issues.
R32	Virus attack	It damages data, hardware, and can cause system failure.

Risk analysis

After identifying possible risks and impacts, the next step is a risk analysis. At this stage, an analysis is carried out of the potential risks that have been previously identified. In this phase, two criteria tables, namely probability and impact, are used as a reference for the risk analysis phase. The probability table, which consists of five criteria, refers to the amount of possible risk.

Table 4. Criteria values on each probability

Possibility		Description	Frequency of Events in a Year
Value	Criteria		
1	Rare	Risk is rare	x < 2 Times
2	Unlikely	Risk is unlikely to happen	2 ≤ x ≤ 5 Times
3	Possible	Risk is possible to happen	6 ≤ x ≤ 9 Times
4	Likely	Risk is likely to happen.	10 ≤ x ≤ 12 Times
5	Certain	Risk is certain to happen	> 12 Times

Next, the impact value table consists of the possible impact of the LKPP E-Office application. The impact assessment table uses five criteria, structured based on the smallest impact on office performance to the greatest impact.

Table 5. Risk impact values

Impact	Value	Description
Very small	1	Risk does not interfere with business activities and processes on the instance
Smaller	2	Activity on the instance is slightly inhibited, but does not interfere with core activity on instance
Medium	3	The risk interferes with the course of business processes at the agency, so business activity is slightly impaired.
Heavy	4	These risks hinder the entire course of business processes at the agency.
Very heavy	5	Risk of interrupting the course of existing business processes completely and stopping the activity of the agency altogether

After determining the probability values in Table 4 and the impact in Table 5, the next step is to assess the risk probability that has been previously identified. Out of the 32 possible risks that have been identified, probability and impact values are determined, which have been shown in Table 4 and Table 5. Table 6 showed a probability risk assessment.

Table 6. Possibility and Impact Assessment

Id	Risk Possibility	Possibility	Impact
R01	Flood	1	5
R02	Earthquake	3	5
R03	Lightning	1	2
R04	Fire	1	5
R05	Power Outage	2	4
R06	Dust	1	1
R07	Denial of Service	1	4
R08	Un-procedure	5	5
R09	Abuse of access rights	1	3
R10	Man in the Middle Attack	1	3
R11	Data Theft/ Hardware Theft	1	3
R12	UI design is difficult to understand	1	2
R13	Can’t Operate E-Office	2	2
R14	Data Failed to Update	1	2
R15	Change Management	2	2
R16	Server Down	2	5
R17	Backup Failure	2	4
R18	Data Corrupt	1	3
R19	Over Capacity	1	3
R20	Overload Access	1	2
R21	Web Service Down	2	3
R22	Network Down	2	4
R23	Unstable Connection	2	3
R24	System Crash	1	4
R25	Failed to update system	2	2
R26	Memory Ram Full	1	2
R27	Slow Application	2	2
R28	Genset is not working properly	1	3
R29	Unintegrated system	1	2
R30	Mice/ Other animals	1	2
R31	Login Failed	2	2
R32	Virus attack	2	4

Risk Evaluation

The final risk assessment process is the risk evaluation that is performed at the risk assessment stage. Table matrix reference was essential to be used to evaluate risk based on the ISO 31000 framework guidelines. Table 7 showed three risk levels namely low, medium, and high. The table is a risk assessment matrix that had been adjusted to the risk level based on probability and impact.

Table 7. Risk Matrix

Possibility	Certain	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Possible	3	Low	Medium	Medium	Medium	High
	Unlikely	2	Low	Low	Medium	Medium	Medium
	Rare	1	Low	Low	Low	Medium	Medium
	Impact		1	2	3	4	5
			Very Small	Smaller	Medium	Heavy	Very Heavy

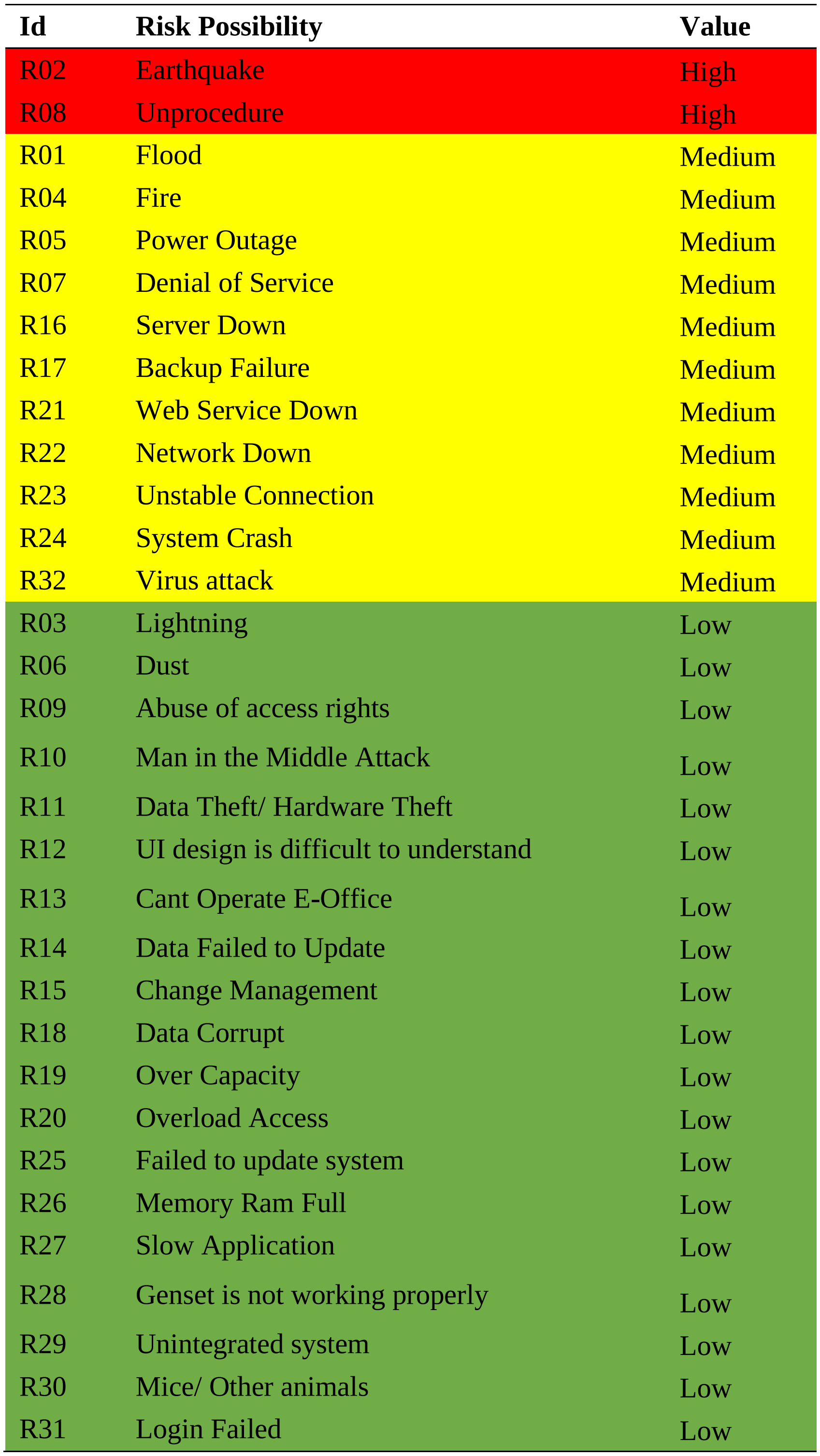
At this stage, the probability risk that has been given a value for probability and impact will be entered into the risk matrix table according to the mapping contained in the table. Table 8 below shows the results of probability risks that had been entered in the matrix table.

Table 8. Risk Assessment Matrix

Possibility	Certain	5	🟨	🟨	🟥	🟥	R08
	Likely	4	🟨	🟨	🟨	🟥	🟥
	Possible	3	🟩	🟨	🟨	🟨	R02
	Unlikely	2	🟩	R13 R15 R25 R27 R31	R21 R23	R05 R17 R22 R32	R16
	Rare	1	R06	R03 R12 R14 R20 R26 R29 R30	R09 R10 R11 R18 R19 R28	R01 R24	R01 R04
	Impact		1	2	3	4	5
			Very Small	Smaller	Medium	Heavy	Very Heavy

The results obtained are subsequently grouped according to the 32 possible levels of risks in high, medium, and low levels.

Table 9. Risk assessment



Id	Risk Possibility	Value
R02	Earthquake	High
R08	Unprocedure	High
R01	Flood	Medium
R04	Fire	Medium
R05	Power Outage	Medium
R07	Denial of Service	Medium
R16	Server Down	Medium
R17	Backup Failure	Medium
R21	Web Service Down	Medium
R22	Network Down	Medium
R23	Unstable Connection	Medium
R24	System Crash	Medium
R32	Virus attack	Medium
R03	Lightning	Low
R06	Dust	Low
R09	Abuse of access rights	Low
R10	Man in the Middle Attack	Low
R11	Data Theft/ Hardware Theft	Low
R12	UI design is difficult to understand	Low
R13	Cant Operate E-Office	Low
R14	Data Failed to Update	Low
R15	Change Management	Low
R18	Data Corrupt	Low
R19	Over Capacity	Low
R20	Overload Access	Low
R25	Failed to update system	Low
R26	Memory Ram Full	Low
R27	Slow Application	Low
R28	Genset is not working properly	Low
R29	Unintegrated system	Low
R30	Mice/ Other animals	Low
R31	Login Failed	Low

In Table 9 above this is expected to be used as a policy consideration in the operation of E-Office LKPP applications.

The risk assessment for the operation of E-Office LKPP applications categorizes various potential risks based on their likelihood and impact, serving as a crucial guide for policy considerations. High-risk scenarios within the E-Office LKPP include seismic events (R02) and procedural anomalies (R08), posing substantial threats that necessitate robust mitigation strategies to ensure the continuity and resilience of operations. Medium-risk scenarios encompass a spectrum of issues such as floods (R01), fires (R04), power outages (R05), denial-of-service attacks (R07), server downtime (R16), backup failures (R17), interruptions to web services (R21), network disruptions (R22), unstable connections (R23), system crashes (R24), and virus attacks (R32). These risks require comprehensive contingency plans and proactive measures to minimize their potential impact on the E-Office LKPP system.

Low-risk scenarios involve various concerns including lightning strikes (R03), dust accumulation (R06), misuse of access rights (R09), man-in-the-middle attacks (R10), data or hardware theft (R11), challenges with user interface design (R12), operational downtime (R13), failures in data updates (R14), issues with change management (R15), data corruption (R18), overcapacity (R19), access overload (R20), failures in system updates (R25), RAM limitations (R26), sluggish application performance (R27), malfunctioning generators (R28), lack of system integration (R29), interference from animals (R30), and login failures (R31). While these risks are less likely or may have lower impacts, they still warrant attention and should be managed through appropriate risk management practices.

Each risk is given a distinct identifier to facilitate systematic tracking and management of these potential issues. This risk assessment had a role as a foundational tool for developing policies that enhance the security, efficiency, and reliability of the E-Office LKPP applications. This assessment followed the ethic of risk management stated by (Hutchins, 2018) as well as following procurement done by (Hald et al., 2021).

Risk Treatment

This phase is the final phase in which the risk control of the E-Office LKPP application is carried out on all risks both high, medium, and low levels of Table 9 sorted according to their urgency, then the risk treatment is made according to the urgency of the risk in Table 10.

Table 10. Risk Treatment

ID	Risk Treatment
R02	Use shock-resistant hardware or consider using cloud data storage to reduce the risk of physical data loss
R08	Monitoring and periodic evaluation of SOP implementation
R01	Using waterproof infrastructure for sensitive hardware
R04	Installation of smoke detection and automatic extinguishing systems, and storage of data separately from the fire hazard area.
R05	Ensure the backup generator or backup power line is running properly.
R07	Consider using anti-DDoS services provided by cloud service providers.
R16	Create clear and periodically tested server-down procedures.
R17	Consider using an automated and scheduled backup solution to reduce the risk of backup failure.
R21	Consider using cloud services that offer high availability and failure tolerance.
R22	Considering using reliable network provider services and having redundant infrastructure.
R23	Monitoring and evaluation of good network equipment and performing scheduled maintenance.
R24	Create and test a comprehensive system crash recovery plan to deal with severe system failure.

R32	Educate users about cyber security practices such as avoiding opening suspicious email attachments or downloading from untrusted sources.
R03	Periodically backup data to anticipate damage that may be caused by lightning.
R06	Perform routine cleaning of the hardware and physical environment around the IT equipment.
R09	Implement strict security policies to regulate user access to the system.
R10	Uses data encryption to protect information transmitted between user and server.
R11	Install the latest physical security systems such as door locks, surveillance cameras, and alarms to protect the hardware.
R12	Perform regular UI/UX evaluations to ensure the user interface is intuitive and easy to understand.
R13	Training and educating users on how to use e-Office applications effectively.
R14	Permanent monitoring and follow-up of operational reporting
R15	The Service Management Unit will update the service status once an official letter has been issued.
R18	Perform periodic data backups to ensure that stored data copies can be restored if data is corrupted or lost.
R19	Monitor system capacity periodically and make capacity increases or adjustments as needed.
R20	Use a traffic management system to manage and limit the number of requests received by the server.
R25	Ensure the testing phase in the development system runs according to the procedure
R26	Monitor memory usage periodically and perform cleaning or optimization if necessary.
R27	Ensure data query runs efficiently
R28	Routine maintenance and periodic testing of the generator to ensure the availability of backup power.
R29	Use standard open communication interfaces and protocols to facilitate integration between different systems.
R30	Implement physical and technical measures to protect hardware and system environment from damage or interference caused by animals.
R31	Performing a bug check on the sign-in system

The risk treatment plan for E-Office LKPP applications incorporates proactive measures drawn from industry best practices. Strategies for managing high-risk events like earthquakes (R02) were using shock-resistant hardware and leveraging cloud data storage to mitigate physical data loss, following FEMA guidelines (Abrahams et al., 2021; Pankow et al., 2021). Addressing procedural irregularities (R08) involves continuous monitoring and evaluation of standard operating procedures (SOPs), aligning with PMI's emphasis on procedural compliance (Singh & Williams, 2021). Mitigating flood risk (R01) entails implementing waterproof infrastructure solutions, which align with IFRC recommendations for protecting critical assets during flood events. Managing fire risk (R04) includes installing smoke detection systems and ensuring data storage away from fire-prone areas, adhering to NFPA standards for comprehensive fire protection (LaMalva & Medina, 2022). Preparation for power outages (R05) focuses on maintaining operational backup generators, following Uptime Institute practices to ensure uninterrupted operations during power failures.

To mitigate denial-of-service attacks (R07), it is recommended to utilize anti-DDoS services provided by cloud providers, a strategy endorsed by CSA to reduce the impact of attacks (Saravanan & Bama, 2020). Preventing server downtime (R16) involves developing and testing robust downtime procedures following ITIL guidelines to minimize service disruptions (Shidqi et al., 2023). Automated backup solutions (R17) are advised to prevent backup failures, aligning with NIST recommendations for ensuring data reliability (Möller, 2023). For addressing web service downtime (R21) and network disruptions (R22), implementing high-availability cloud services and reliable network infrastructure is critical, supported by AWS and TIA standards for resilient service delivery (Zeng & Bao, 2023).

Regular monitoring and maintenance of network equipment (R23) are essential to prevent unstable connections, following Cisco's guidelines for proactive network management (Shukla et al., 2023). Comprehensive plans for system crash recovery (R24) align with Microsoft's best practices in disaster recovery planning to minimize downtime and data loss. Educating users about cybersecurity practices (R32) to prevent virus attacks reflects CIS strategies for enhancing user awareness and system security (Rains, 2023). These treatments for medium and low-risk issues, such as lightning (R03), dust (R06), abuse of access rights (R09), and UI/UX improvements (R12), emphasize ongoing monitoring, training, and adherence to best practices to enhance the security, efficiency, and reliability of E-Office LKPP applications.

Conclusion

Based on the result above, it can be concluded that there were 32 risks impacting business processes. These include 2 high-level risks (Earthquakes and Unprocedural issues), 11 moderate-level risks (e.g., Flood, Fire, Power Outage, Denial of Service, Server Down), and 19 low-level risks (e.g., Lightning, Dust, Abuse of access rights, Data Theft, UI design issues). To address these risks, the following treatments are recommended:

1. High-risk treatments: Use shock-resistant hardware or cloud data storage, and regularly monitor SOP implementation.
2. Moderate-risk treatments: Employ waterproof infrastructure, smoke detection systems, data storage away from fire hazards, anti-DDoS services, automated backups, reliable network services, and educate users on cyber security.
3. Low-risk treatments: Backup data, maintain hardware cleanliness, enforce strict security policies, use data encryption, perform regular UI/UX evaluations, train users, monitor system capacity, and conduct routine maintenance.

This study hoped to be used as a guideline for the Government Procurement Policy Agency to implement these risk management strategies effectively, minimizing potential risks.

Author’s Contribution

The author conceptualizes the research, designs the research methodology, collects and analyzes the data, and interprets the findings. Arif did the Literature review, while Yuliana did data collection, and Ratnasari did data curation. In addition, the authors take full responsibility for the intellectual content, accuracy of data analysis, and adherence to ethical considerations in conducting this research. This manuscript has undergone several revisions and editing processes, all of which were carried out by the authors themselves

Acknowledgments

Thank you to the instructor lecturer, the LKPP government agency, and the family who have supported this research as the final task to obtain a Bachelor of Computer in Information Systems Studies Program of the Faculty of Computer Science of Mercu Buana University of Jakarta.

Declaration of Competing Interest

The author declares that the research was conducted without external funds which could be construed as a potential conflict of interest.

Funding

This study did not receive any funding.

References

Abrahams, L., Abrahams, L., Van Pay, L., Sattar, S., Johnson, K., McKittrick, A., Bartels, L., Butcher, L. M., Rubinyi, L., & Mahoney, M. (2021). *NIST-FEMA Post-Earthquake Functional Recovery Workshop Report*. US Department of Commerce, National Institute of Standards and Technology.

Andaru, R. G., & Adi, T. J. W. (2024). Risk Analysis of E-Procurement Process of EPC Construction Project Based On Risk Management. *Jurnal Indonesia Sosial Teknologi*, *5*(3), 1286–1295.

Candra, R. M., Sari, Y. N., Iskandar, I., & Yanto, F. (2019). Sistem Manajamen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000: 2018. *Jurnal CoreIT*, *5*(1), 19–28.

Chan, D. W. M., Chan, A. P. C., Lam, P. T. I., & Wong, J. M. W. (2010). Empirical study of the risks and difficulties in implementing guaranteed maximum price and target cost contracts in construction. *Journal of Construction Engineering and Management*, *136*(5), 495–507.

Hald, K. S., Wiik, S., & Larssen, A. (2021). Sustainable procurement initiatives and their risk-related costs: A framework and a case study application. *Measuring Business Excellence*, *25*(2), 230–243.

Hastak, M., & Shaked, A. (2000). ICRAM-1: Model for international construction risk assessment. *Journal of Management in Engineering*, *16*(1), 59–69.

Hopkin, P. (2018). *Fundamentals of risk management: understanding, evaluating and implementing effective risk management*. Kogan Page Publishers.

Hutchins, G. (2018). *ISO 31000: 2018 enterprise risk management*. Greg Hutchins.

LaMalva, K. J., & Medina, R. A. (2022). Building Codes and the Fire Regulatory Context of Smart and Autonomous Infrastructure. In *Handbook of Cognitive and Autonomous Systems for Fire Resilient Infrastructures* (pp. 117–138). Springer.

Liperda, R. I., & Nieng, U. A. S. (2023). Analisis Manajemen Resiko Aplikasi Mypertamina Dengan Menggunakan Iso 31000. *INFOTECH Journal*, *9*(2), 361–370.

Loestefani, V., Poan, R., Suwitorahardjo, B., & Wardhana, A. K. (2022). Service Quality and Product Quality as An Influence on Customer Loyalty at Naturalis Koffie. *FIRM Journal of Management Studies*, *7*(2), 211–236.

Mendo, A. Y., Singh, S. K., Yantu, I., Hinelo, R., Bokingo, A. H., Dungga, E. F., Juanna, A., Wardhana, A. K., Niroula, B., & Win, T. (2023). Entrepreneurial leadership and global management of COVID-19: A bibliometric study. *F1000Research*, *12*(31), 31.

Möller, D. P. F. (2023). NIST Cybersecurity Framework and MITRE Cybersecurity Criteria. In *Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices* (pp. 231–271). Springer.

Nuryitmawan, T. R. (2022). Determinants of the intention to participate in waqf: altruism, trust, and religiosity. *Airlangga Journal of Innovation Management*, *3*(2), 199–211.

Osipova, E. (2015). Establishing cooperative relationships and joint risk management in construction projects: Agency theory perspective. *Journal of Management in Engineering*, *31*(6), 5014026.

Pangestu, R. H., Cahyono, A. D., & Tanaem, P. F. (2021). Analisis Manajemen Resiko Aplikasi SIPP di Pengadilan Negeri Salatiga Kelas 1B Mengunakan ISO 31000. *Journal of Computer and Information Systems Ampera*, *2*(1), 43–57.

Pankow, K. L., Rusho, J., Pechmann, J. C., Hale, J. M., Whidden, K., Sumsion, R., Holt, J., Mesimeri, M., Wells, D., & Koper, K. D. (2021). Responding to the 2020 Magna, Utah, earthquake sequence during the COVID-19 pandemic shutdown. *Seismological Research Letters*, *92*(1), 6–16.

Pratiwi, A. C., Wardhana, A. K., & Rusgianto, S. (2022). Application of Vector Error Correction Model on Macroeconomic Variables toward Changes in the Composite Stock Price Index. *Daengku: Journal of*

Humanities and Social Sciences Innovation, *2*(2), 219–229.

Qosim, N., Ratnasari, R. T., Wardhana, A. K., Fauziana, H., & Barkah, T. T. (2023). Eight Years of Research Related to the Green Sukuk in the Global Stock Exchange Market to Support the Implementation of SDG: A Bibliometric Review. *Journal of Islamic Economic and Business Research*, *3*(2), 161–180.

Rahmadini, A., Wolor, C. W., & Faslah, R. (2023). ANALISIS EFEKTIVITAS PENGGUNAAN E-OFFICE PADA PT XXX. *JURNAL ILMIAH RESEARCH AND DEVELOPMENT STUDENT*, *1*(2), 187–198.

Rahman, I., Ratnasari, R. T., & Wardhana, A. K. (2022). Effect of Certificate of Bank Indonesia Sharia and Indonesian Bank Seven Days Repository Rate to Inflation Ratio in Indonesia During Covid-19 Pandemic. *Economic Education and Entrepreneurship Journal*, *5*(1), 157–174.

Rains, T. (2023). *Cybersecurity Threats, Malware Trends, and Strategies: Discover risk mitigation strategies for modern threats to your organization*. Packt Publishing Ltd.

Ryandono, M. N. H., Mawardi, I., Rani, L. N., Widiastuti, T., Ratnasari, R. T., & Wardhana, A. K. (2022). Trends of research topics related to Halal meat as a commodity between Scopus and Web of Science: A systematic review. *F1000Research*, *11*(1562), 1562.

Ryandono, M. N. H., Permatasari, S. A., & Wijayanti, I. (2019). Business behavior in an islamic perspective: Case study of muslim woman entrepreneurs in Ikatan Wanita Pengusaha Indonesia (IWAPI). *12th International Conference on Business and Management Research (ICBMR 2018)*, 154–159.

Ryandono, M. N. H., Wijayanti, I., & Kusuma, K. A. (2020). Determinants of Investment In Islamic Crowdfunding. *Muqtasid: Jurnal Ekonomi Dan Perbankan Syariah*, *11*(1), 70–87.

Sahira, S., Fauzi, R., & Santosa, I. (2020). Analisis Manajemen Risiko Pada Aplikasi E-office Yang Dikelola Oleh Pt Telkom Indonesia Menggunakan Standar Iso/iec 27005: 2018. *EProceedings of Engineering*, *7*(2).

Santoso, T. B., & Kusuma, A. (2023). The Development of the Usage of Blockchain for Waqf and Zakat Globally: A Bibliometric Study. *International Journal of Mechanical Computational and Manufacturing Research*, *13*(3), 83–91.

Saravanan, A., & Bama, S. S. (2020). Multi-Model Anti-Ddos Framework For Detection And Mitigation Of High Rate Ddos Attacks In The Cloud Environment. *International Journal Of Scientific & Technology Research*, *9*(03), 4503–4511.

Shidqi, S. A., Adha, F., Novendri, A., Artanti, F. W., Widadi, W. P. M., Subarkah, F., & Tarwoto, T. (2023). Analysis of Information Technology Service Management Using ITIL V3 Domain Service Operation at Company XYZ. *International Journal of Informatics and Information Systems*, *6*(4), 159–168.

Shukla, A., Patel, J., Panzade, K., & Sardana, H. (2023). *Cisco Cloud Infrastructure*. Cisco Press.

Singh, H., & Williams, P. S. (2021). A Guide to the Project Management Body of Knowledge: PMBOK (®) Guide. *Project Management Institute*.

Syahnur, E. A., Hibrizi, M. N. F., Lesmana, R. K., & Irawan, M. D. (2022). Analisis Manajemen Risiko Keamanan Informasi di PT. Adhi Commuter Properti Medan Menggunakan Standart ISO 31000: 2018 (Studi Kasus Hotel Grandhika Medan). *Balance: Jurnal Akuntansi Dan Manajemen*, *1*(3), 330–338.

Tang, W., Qiang, M., Duffield, C. F., Young, D. M., & Lu, Y. (2007). Risk management in the Chinese construction industry. *Journal of Construction Engineering and Management*, *133*(12), 944–956.

Taroun, A. (2014). Towards a better modelling and assessment of construction risk: Insights from a literature review. *International Journal of Project Management*, *32*(1), 101–115.

Wardhana, A. K. (2022). JANJI (WA’AD) SEBAGAI JARING PENGAMAN PADA TRANSAKSI KEUANGAN DAN BISNIS SYARIAH. *Jurnal Keislaman*, *5*(1), 124–132. https://doi.org/https://doi.org/10.54298/jk.v5i1.3412

Wardhana, A. K., Ratnasari, R. T., & Fauziana, H. (n.d.). *ISLAMIC INVESTMENT IN INDONESIA BEFORE AND DURING PANDEMIC OF COVID-19: A BIBLIOMETRIC STUDY INVESTASI*

SYARIAH DI INDONESIA SEBELUM DAN SELAMA PANDEMI COVID-19: STUDI BIBLIOMETRIK.

Zakik, Z., Kamil, A., Prasetyo, A. S., Ryandono, M. N. H., & Wijayanti, I. (2022). Economic development on Madura Island through halal tourism: A business feasibility study. *Al-Uqud: Journal of Islamic Economics*, *6*(2), 289–303.

Zeng, X., & Bao, S. (2023). The Communication and Security Technology of IoT. In *Key Technologies of Internet of Things and Smart Grid* (pp. 211–299). Springer.

Zou, P. X. W., Chen, Y., & Chan, T.-Y. (2010). Understanding and improving your risk management capability: Assessment model for construction organizations. *Journal of Construction Engineering and Management*, *136*(8), 854–863.