Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6564

Information Security Risk Analysis Using ISO 31000:2018 and ISO 27001:2022

Athiyatul Ulya[1*], Annisa Karima[2], T. Sukma Achriadi Sukiman[3], Anni Zulfia[4], Rafika Rahmawati[5]
[1,2] Faculty of Engineering, Department of Electrical Engineering, Information Systems, Universitas Malikussaleh
[3,4] Faculty of Engineering, Department of Informatics, Informatics Engineering, Universitas Malikussaleh
[5] Faculty of Computer Science, Information Systems, Universitas Pembangunan Nasional Veteran Jawa Timur
[*] athiyatululya@unimal.ac.id

open access

***Corresponding Author**

Article History:
Submitted: 10-08-2025
Accepted: 06-09-2025
Published: 08-09-2025

Keywords:
Information Security; Risk Analysis; ISO 27001:2022; ISO 31000:2018; BPS.

ABSTRACT

Information system risk audits are an important step in ensuring the security, effectiveness, and efficiency of the systems used by organizations. However, the fast advancement of information and communication technologies has made information-security threats more intricate, arising not only from internal sources like employee carelessness but also from external sources such as cyber-attacks, malware, and data-theft. This study aims to analyze information security risks at the Central Statistics Agency (BPS) of Lhokseumawe by referring to two international standards, namely ISO/IEC 27001:2022 and ISO 31000:2018. The research approach used is descriptive qualitative with a case study method. Data collection techniques were conducted through interviews, observations, and document studies. The results of the study indicate that there are still various security gaps, both technical and non-technical, such as weak system authentication, the absence of adequate security policies, and the lack of incident handling procedures. This study successfully compiled a risk register containing 30 types of risks along with their causes, impacts, likelihood levels, and relevant mitigation recommendations. Improvement recommendations include strengthening technical controls, updating information security policies, enhancing human resource capacity, and conducting regular internal audits. The results of this study are expected to serve as a reference for strengthening information security systems in a systematic and standardized manner within the BPS environment.

INTRODUCTION

In this growing digital age, information has become a really important strategic asset for every organization, including government agencies like the Central Statistics Agency (BPS). As the official provider of statistical data at the national and regional levels, the BPS is responsible for managing, storing, and distributing various types of data, including sensitive and confidential data. As an institution mandated to conduct statistical activities at both the national and regional levels, BPS is responsible for managing, storing, and distributing various types of data, including sensitive and confidential data (Xu, Shi, Shi, & You, 2023). The quality and reliability of the data provided by BPS greatly depend on the institution's ability to maintain information security, which includes aspects of confidentiality, integrity, and data availability. However, with the rapid development of information and communication technology, threats to information security have become increasingly complex, both from internal factors such as employee negligence and from external factors such as cyber-attacks, malware, and data theft (Ardiansyah, Ilyas, & Haeranah, 2023). Case studies in several BPS offices, such as the West Kalimantan Provincial BPS, show that not all information assets are managed optimally. Common problems found include the lack of a formal information security management system (ISMS), low awareness of information security among employees, and the absence of standard procedures for handling cyber incidents. This situation not only has the potential to reduce the quality of public services provided by BPS, but also to undermine public confidence in the accuracy and integrity of the statistical data produced (Putri, Mutiah, & Prawira, 2022).

Responding to these challenges, the adoption of international standards is a necessary strategic solution. Two complementary standards in this context are ISO 31000:2018 and ISO/IEC 27001:2022. ISO 31000 provides a general framework for systematically managing risk and integrating it into organizational processes (British Standard Institusion, 2018), while ISO/IEC 27001 sets out the requirements and technical controls for establishing an information security management system (ISMS) (International Standard Organization, 2022). The latest version of ISO/IEC 27001:2022 includes 93 controls divided into four main categories: organizational controls, human controls, physical controls, and technological controls (International Standard Organization, 2022). Empirical research shows that integrating the risk management approach of ISO 31000 with the security controls of ISO 27001 can improve the effectiveness of information risk control in the public sector. This standard has proven effective in helping government organizations manage uncertainty, including cyber risks, with a context-based approach (Aven & Ylönen, 2019).

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6564

This study uses a qualitative approach and aims to evaluate information security risks at the Lhokseumawe City Statistics Agency. By combining ISO 31000:2018 and ISO 27001:2022, this study focuses on identifying potential information security risks, analyzing and evaluating risks, and providing risk control recommendations to enhance the resilience of information systems within the BPS environment. A case study approach was used to obtain a comprehensive overview through the collection of primary data (interviews and observations) and secondary data (documents and literature). These findings are expected to serve as the basis for recommendations to improve information security governance in local governments, while also supporting empirical literature on the integration of the two standards in the public sector context. This research is also expected to strengthen sustainable information security governance, improve data management efficiency, and build public trust in the integrity of the statistical data produced (Wiener, 2021).

LITERATURE REVIEW

Information Security

Information security is an effort to protect information assets within an organization in order to avoid various threats that could cause losses to the organization. The main objectives of information security are to minimize losses, maximize profits, and ensure that a business runs smoothly. These losses can include data and information theft, which will destroy the organization's business. Information or data from an organization may pose threats or vulnerabilities that could harm the organization. An organization must manage its information appropriately in order to avoid and minimize the possibility of criminal threats that may occur now or in the future. If information is not properly protected, it will cause a business to fail and suffer losses. Therefore, in order to minimize these threats, an organization needs to be aware of the need for planning to protect information, which requires the responsibility of every party within the organization (British Standard Institusion, 2018). There are several stages in implementing information security:

a. Identifying various threats that could attack an organization's information sources.
b. Identifying risks that could potentially threaten an organization's information sources.
c. Determining several policies that can support an organization's information security.
d. Implementing controls to monitor risks that are likely to occur.

The purpose of information security awareness is to instill responsibility in every individual within the organization to better protect information, understand how to manage and handle information, and foster a sense of care for the work environment among every individual in the organization. In addition, this awareness will help to foster knowledge and understanding for designing, implementing, and running a program in the organization. An organization that builds clear organizational responsibilities and objectives will represent the proper and correct management of information within the organization in accordance with the original objectives for which the organization was established (British Standard Institusion, 2018).

Risk

Risk is an impact arising from uncertainty regarding the achievement of an organization's objectives (British Standard Institusion, 2018). Impact refers to a deviation from what the organization expects. It is possible that there will be positive impacts that benefit the organization and negative impacts that harm the organization. In 1921, Frank Knight introduced the concepts of risk and uncertainty in his publication (H. Knight, 1921). According to Knight, risk is “unknown outcomes whose odds of happening can be measured or at least learned about.” Meanwhile, uncertainty is “uncertain events that we do not even know how to describe” (H. Knight, 1921). Risk itself has several components, specifically:

a. Event; a situation that causes a change in a series of specific circumstances.
b. Asset; a risk that occurs in a specific object.
c. Outcome; the result of an event that occurs in an object that has an impact on that object or asset.
d. Probability; a risk is an uncertainty that can be estimated. Risks have both good and bad possibilities.

Risk Management

Based on ISO 31000 (standard for risk management in organizations), risk management is: “A set of coordinated activities and methods used to guide organizations in controlling risks that could interfere with the achievement of organizational objectives” (British Standard Institusion, 2018). This definition emphasizes that risk management is not a single activity but an integrated, systematic approach that aligns risk-handling actions with the organization’s strategic, operational, and compliance goals. The standard outlines five core components: (1) establishing the context, (2) risk identification, (3) risk analysis, (4) risk evaluation, and (5) risk treatment, followed by ongoing monitoring and review. By embedding these steps into governance structures, organizations can create a risk-aware culture, improve decision-making, and allocate resources more efficiently (Aven, Risk Assessment and Risk Management: Review of Recent Advances on Their Foundations, 2016).

In the present study, the risk-management process described in the methods section adopts this ISO-based framework, tailoring each phase to the specific objectives, data sources, and analytical techniques of the research while

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6564

maintaining alignment with the standard's principles of integration, structured processes, and continual improvement.

ISO/IEC 31000:2018

Among the globally recognized risk management standards is ISO 31000. ISO 31000:2018 provides a universally applicable set of principles, a framework, and a risk-management process that can be embedded in any organization's governance, strategy, and operations (British Standard Institusion, 2018). The framework emphasizes leadership commitment, integration into organizational processes, and the design of tailored risk-management structures (e.g., risk registers, roles, and resources). The process comprises risk identification, analysis, evaluation, treatment, monitoring, and communication, enabling systematic treatment of threats such as supply-chain disruptions, financial volatility, and cybersecurity incidents (Institute of Risk Management, 2018). In practice, ISO 31000 can be applied in various types of public or private enterprises and is capable of establishing principles and stages for managing risk so that it can be used as a framework in risk management to implement more effective risk management (Gillis, 2025).

ISO 31000 is a risk implementation guide consisting of three elements: principles, framework, and process. In general, ISO 31000:2018 simplifies the 2009 version. This is immediately apparent, among other things, from the name change from "principles and guidelines" to simply "guidelines" and from the reduction in the number of pages from 24 to 16 (British Standard Institusion, 2018). ISO 31000:2018 emphasizes the importance of integrating risk management into all organizational activities, including strategic and operational decision-making and planning processes. This approach is designed to be flexible and adaptable to the specific context and needs of each organization. Through a systematic framework, organizations can proactively identify, analyze, and evaluate risks before they have a significant impact on business objectives. Thus, the implementation of ISO 31000 not only increases organizational resilience, but also provides added value through transparent and data-driven risk management.

ISO/IEC 27001:2012

ISO 27001:2022 is the latest revision of the international standard for information-security management systems (ISMS) and refines the previous standard, covering significant changes relevant to the current dynamics of cyber threats (International Standard Organization, 2022). This standard is designed to ensure that information security is not only the responsibility of the IT department, but also an integral part of the overall governance of the organization. It specifies requirements for establishing, implementing, maintaining, and continually improving an ISMS, with the goal of protecting the confidentiality, integrity, and availability of information assets. The 2022 edition aligns the standard more closely with ISO 27002:2022, which reorganizes the 93 controls into 4 themes: Organizational, People, Physical, and Technological. The latest edition also reduces the total to 93 controls grouped in 11 clauses. With a risk-based approach, ISO/IEC 27001:2022 helps organizations identify potential security risks and establish appropriate controls to manage those risks (IT Governance USA, 2022).

METHOD

This study uses a descriptive qualitative approach that aims to obtain a comprehensive picture of how information security risk management is implemented in government agencies, particularly at the Central Statistics Agency (BPS) in Lhokseumawe. The qualitative approach allows researchers to observe actual conditions in the field, explain the phenomena that occur, and interpret the meaning of organizational behavior in managing information security risks (Creswell, 2014). This research is a case study, as it examines in depth a specific object, namely the BPS of Lhokseumawe as an institution that manages strategic and sensitive data (Yin, 2009). Data and information were obtained from various sources, both primary and secondary, and analyzed with reference to the international standards ISO 31000:2018 and ISO/IEC 27001:2022. The stages of this study refer to the risk management stages issued by ISO 31000:2018 (British Standard Institusion, 2018). The steps taken in this study are shown in Figure 1.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6564

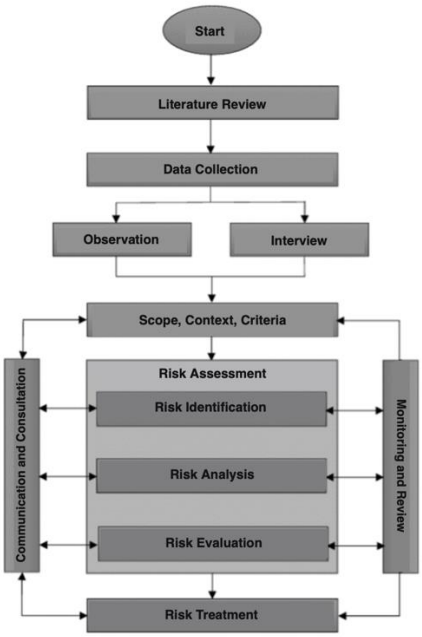

Figure 1. Research Stages

Literature Review

A literature review is the initial step in this research process. In order to acquire a theoretical foundation and conceptual framework for the subject under study, the literature study stage involves analysing data from a variety of reference sources, including pertinent prior research findings. Researchers can discover gaps in prior research, comprehend the most recent advancements in knowledge, and acquire understanding of the ideas, concepts, and techniques that have been applied in comparable contexts by doing a literature review (Pubrica, 2025).

Data Collection

Semi-structured interviews are used in this study's data collection strategy with a select group of informants who are directly involved in system operations, such as the Head of the General Subdivision, information technology personnel, and others who play important roles in information system management and data security within the BPS environment. Taking into account the positions and authority of the informants in relation to information security risk management, the researcher established the interview targets. Semi-structured interviews were selected because they allow researchers to stay focused on the research topic while allowing them to use open-ended questions to delve deeply into informants' experiences and opinions (Creswell, 2014). This method allows researchers to collect data on access regulations, technical difficulties faced by IT personnel, and the state of information system security.

Setting Goals and Context

The goals, scope, and organisational units that will be the focus of the risk management audit are decided upon at this point. While the scope establishes the limits of the processes, activities, and resources to be examined, the objectives and context serve to guide the audit's focus in line with the organization's needs and priorities. Furthermore, determining the pertinent organisational units guarantees a comprehensive and accurate audit (British Standard Institusion, 2018). Setting goals and context at this stage is essential to ensuring that the audit process is in line with organisational risks and that risk assessment can be carried out successfully using predetermined standards. As a result, hazards can be mitigated effectively and suitably, assisting in the accomplishment of the organization's overarching goals (Hopkin, 2018).

Risk Assessment

The subsequent phase of this study involves performing a risk assessment to identify risks associated with information technology assets at BPS Lhokseumawe. At this step, an assessment is made of the potential of hazards arising and their impact on these assets. Risk assessment and evaluation are carried out using a risk evaluation matrix, which categorises risk as low, medium, or high. This risk assessment procedure follows the international standard ISO 31000:2018, which divides risk assessment into three major stages: risk identification, risk analysis, and risk evaluation (British Standard Institusion, 2018).

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6564

Risk Treatment

Following the analysis and evaluation of risks, the next stage is to mitigate risks. At this level, mitigation actions are implemented with the goal of reducing the possibility of hazards occurring or their impact on the organisation. The primary goal of risk treatment is to choose and implement effective risk-management measures based on the priorities established during the evaluation stage (British Standard Institusion, 2018). In this study, risk control is carried out in line with the ISO/IEC 27001:2022, an international standard for information security management systems (ISMS). The ISO/IEC 27001:2022 standard was chosen because it outlines effective security procedures for protecting information assets and managing information security risks in a methodical manner. This risk mitigation stage produces a risk treatment plan document, which includes the risk treatment plan as well as the installation of risk controls that are suited to the organization's needs and conditions. This paper serves as the foundation for developing risk control strategies and regularly reviewing their efficacy (International Standard Organization, 2022).

RESULTS

Organizational Overview

The Central Statistics Agency (BPS) of Lhokseumawe is a vertical agency that reports to the Central Statistics Agency of the Republic of Indonesia. BPS is primarily responsible for delivering accurate, up-to-date, and accountable statistical data to support regional development planning, implementation, and evaluation. In carrying out its duties, the Lhokseumawe BPS regularly compiles official publications such as “Lhokseumawe in Figures,” which contains important information on the geographical, demographic, social, and economic aspects of the region. The BPS of Lhokseumawe also actively contributes theme statistical data, such as poverty rates, unemployment rates, economic growth, regional inflation, and human development indices. These data provide an important foundation for local governments to develop public policies, as well as a reference for decision-making by diverse stakeholders. This institution is committed to promoting data-driven, transparent, and participatory development through census activities, surveys, and the compilation of various sectoral statistics. To promote the efficacy of accurate, relevant, and timely regional statistics, BPS Lhokseumawe comprises of technical and functional departments that support the implementation of its core responsibilities and functions, which include:

a. Social Statistics Section, responsible for collecting and presenting social data such as population, education, health, and poverty.
b. Production Statistics Section, which processes data on the agriculture, industry, energy, construction, and environment sectors.
c. Distribution Statistics Section, which handles data on prices, trade, consumption, transportation, and communications.
d. Regional Balance and Statistical Analysis Section, which is tasked with compiling the Regional Domestic Product (PDRB), conducting sectoral statistical analysis, and supporting data-based policies.
e. Statistical Processing and Dissemination Integration Section, which focuses on data integration, survey result processing, and statistical information services to the public.
f. General Subdivision, which manages personnel, finance, logistics, and general administration.

Data Collection

This study's data was collected utilizing two main methods: in-depth interviews and direct observation. These two methodologies were used together in the work environment of BPS Lhokseumawe to generate an objective and comprehensive picture of the state of information system management, the application of information security rules, and potential threats. This strategy seeks to guarantee that the data gathered is genuine and representative of the actual conditions on the ground, laying a solid foundation for the identification and analysis of risks in following stages (Rachman, Yochanan, Samanlangi, & Purnomo, 2024).

In-depth interviews were conducted with a number of important personnel at BPS Lhokseumawe who are involved in information system management and ICT infrastructure. The informants included the Head of the IT Team of the Lhokseumawe City Statistics Agency, as well as other administrative personnel. The interviews employed a guide with 30 open-ended questions based on the findings of a literature review to investigate perspectives and experiences with information security and risk management.

Risk Identification

Risk identification is carried out to explore various threats and vulnerabilities that could affect the operational sustainability of the information system at the Central Statistics Agency (BPS) in Lhokseumawe. The risk identification process covers critical organizational assets, including

a. Statistical application systems such as the Population Census and Regional Socioeconomic Survey (Susenas) data processing applications.
b. IT infrastructure including physical servers, switches, routers, and user computer devices.
c. Databases that store sensitive and strategic government information.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6564

d. Local area networks (LAN/WAN) used for internal and external connectivity.
e. Human resources (HR) involved in managing and accessing information systems.

The results of this identification are then compiled into a Risk Register, which is a risk management tool used to document important information related to each risk identified during the audit process. This Risk Register not only includes the name of the risk faced but also details: the assets affected, the cause of the risk, the likelihood of the risk occurring, the magnitude of the impact caused, the overall risk classification (low, medium, high), as well as existing controls and mitigation plans to reduce or eliminate the risk. The purpose of risk register is to provide a clear, structured, and systematic overview to management or relevant parties in making strategic decisions and determining priorities in the effective implementation of information security controls. With this risk documentation, the agency can also conduct regular monitoring of developments and changes in risk levels, evaluate the effectiveness of controls or measures that have been implemented, and make continuous improvements in information security governance (International Standard Organization, 2022). Overall, 30 risks were identified, representing distinct areas of vulnerability in information security management. This risk register is presented in Table 1 as part of the research results.

Table 1. Risk Register

ID	Risk	Cause	Impact	Existing Control
R01	Statistical Data Leaks	Permissionless, unencrypted access	Privacy violations, legal sanctions	Standar username-password, manual log
R02	Phishing Attacks	No user safety training	Login data theft, incoming malware	Basic email filter
R03	Server Failure	No daily backups	Data loss, system downtime	Weekly backup, UPS
R04	Brute Force Attack	Weak password, no login limit	Illegal access to the system	Basic login protection
R05	System Vulnerability Exploit	The system is not updated	System intrusion and damage	Patch manual
R06	Social Engineering Attack	Lack of safety education	User leaks credentials	Basic communication SOPs
R07	Backdoor Malware	Application gaps are not secured	Long-term system access without authorization	Antivirus, firewall
R08	Illegal Public VPN/DNS Access	No technical blocking	Unsafe network, bypass filtering	Manual monitoring
R09	Malware from Ads	Accidental ad clicks	System infections, data theft	Ad-blocker, antivirus
R10	Information Security Ignorance	Lack of training & socialization	Overall risk increases	Poster & general appeals
R11	Authentication System Failure	Unstable login system	Services are not accessible	Manual Monitoring
R12	Use of Pirated Apps	Illegal software installation	Malware & law violations	No software policy
R13	Admin Access Not Monitored	No adequate logging	Abuse of admin access	Limited admin rights
R14	Personal Device Use (BYOD)	No BYOD security controls	Malware spread to the network	No BYOD policy
R15	Unauthorized Physical Access to Servers	Server room not secured	Data theft/sabotage	Standard padlocks
R16	Spam and Malicious Emails	No powerful spam filter	Phishing, malware	Basic email filter
R17	Reliance on One Vendor	All systems from a single vendor	Operational disruptions when vendors are in trouble	Annual vendor evaluation
R18	DdoS Attack	Open network without protection	Service outages	Standard Firewall
R19	Unavailability of Emergency SOPs	No incident guide	Panic during incidents, poor handling	General SOP
R20	Lack of System Documentation	The system was developed without documentation	Difficult to manage, knowledge loss	Limited documentation
R21	Data Sync Failed	Separate system	Inconsistencies of critical	Manual sync

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6564

			data	
R22	No periodic security reports	No incident reports	Unmonitored risk	Monitoring of undocumented incidents
R23	Unstructured Data Storage	Unorganized files & DBs	Difficult to find & audit	Separate storage
R24	Unstable Internet Connection	Single Provider	Online work disruption	No Control
R25	New System Without Complete Trial	Launched without QA	Lots of bugs when live	Limited internal testing
R26	Forgot to Log Out by Users	Not logging out of a common device	Unauthorized access by others	No control
R27	Weak Website Security	No HTTPS or CAPTCHA	Vulnerable to bot/hacker intrusion	Partial HTTPS
R28	No Periodic Security Audits	Evaluation only occasionally	Hidden risks go undetected	Sporadic examinations
R29	Unencrypted Backups	Backups are stored without protection	Data stolen in offline conditions	Standard Format
R30	Human Operational System Error	Manual misconfiguration	Operational disruption & downtime	No validation procedure

Risk Analysis and Evaluation

Following a thorough risk identification process, a risk analysis is carried out to evaluate each risk's seriousness using two primary criteria: impact and likelihood. This study tries to categorize risks as low, medium, or high, allowing the organization to identify the most appropriate and effective risk management priorities (British Standard Institusion, 2018). In order to visualise and understand the overall amount of risk, risks are organised into a two-dimensional risk matrix that combines likelihood and impact. This matrix is a method for categorising threats based on severity and urgency. The risk matrix that was employed is as follows:

Table 2. Risk Matrix

	Low Impact	**Medium Impact**	**High Impact**
Low Likelyhood	Low	Low	Medium
Medium Likelyhood	Low	Medium	High
High Likelyhood	Medium	High	High

According to the results of the matrix-based risk assessment, 11 out of 30 detected risks are classified as high risk, 14 risks are classified as medium and 5 risks are classified as low. These risks are in areas with significant to catastrophic consequences and a high possibility of occurrence, necessitating rapid mitigation measures and making them a top priority in their management. The risk mapping is illustrated in Table 3.

Table 3. Risk Assessment

ID	**Risk**	**Cause**	**Impact**	**Likelyhood**	**Impact**	**Risk Level**
R01	Statistical Data Leaks	Permissionless, unencrypted access	Privacy violations, legal sanctions	Medium	High	High
R02	Phishing Attacks	No user safety training	Login data theft, incoming malware	Medium	Medium	Medium
R03	Server Failure	No daily backups	Data loss, system downtime	Low	High	Medium
R04	Brute Force Attack	Weak password, no login limit	Illegal access to the system	Medium	High	High
R05	System Vulnerability Exploit	The system is not updated	System intrusion and damage	Low	Medium	Low
R06	Social Engineering Attack	Lack of safety education	User leaks credentials	Low	Medium	Low
R07	Backdoor Malware	Application gaps are not secured	Long-term system access without authorization	Medium	High	High
R08	Illegal Public VPN/DNS Access	No technical blocking	Unsafe network, bypass filtering	Medium	Medium	Medium
R09	Malware from Ads	Accidental ad clicks	System infections, data theft	High	Medium	High
R10	Information	Lack of training &	Overall risk increases	Medium	Medium	Medium

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6564

	Security Ignorance	socialization				
R11	Authentication System Failure	Unstable login system	Services are not accessible	Medium	Medium	Medium
R12	Use of Pirated Apps	Illegal software installation	Malware & law violations	Low	Low	Low
R13	Admin Access Not Monitored	No adequate logging	Abuse of admin access	Medium	High	High
R14	Personal Device Use (BYOD)	No BYOD security controls	Malware spread to the network	High	Medium	High
R15	Unauthorized Physical Access to Servers	Server room not secured	Data theft/sabotage	Low	High	Medium
R16	Spam and Malicious Emails	No powerful spam filter	Phishing, malware	Medium	Medium	Medium
R17	Reliance on One Vendor	All systems from a single vendor	Operational disruptions when vendors are in trouble	Medium	High	High
R18	DdoS Attack	Open network without protection	Service outages	Medium	High	High
R19	Unavailability of Emergency SOPs	No incident guide	Panic during incidents, poor handling	Low	Medium	Low
R20	Lack of System Documentation	The system was developed without documentation	Difficult to manage, knowledge loss	Medium	Medium	Medium
R21	Data Sync Failed	Separate system	Inconsistencies of critical data	Medium	High	High
R22	No periodic security reports	No incident reports	Unmonitored risk	Medium	Medium	Medium
R23	Unstructured Data Storage	Unorganized files & DBs	Difficult to find & audit	Medium	Medium	Medium
R24	Unstable Internet Connection	Single Provider	Online work disruption	Medium	Medium	Medium
R25	New System Without Complete Trial	Launched without QA	Lots of bugs when live	Low	Medium	Low
R26	Forgot to Log Out by Users	Not logging out of a common device	Unauthorized access by others	Medium	Medium	Medium
R27	Weak Website Security	No HTTPS or CAPTCHA	Vulnerable to bot/hacker intrusion	High	Medium	High
R28	No Periodic Security Audits	Evaluation only occasionally	Hidden risks go undetected	Low	High	Medium
R29	Unencrypted Backups	Backups are stored without protection	Data stolen in offline conditions	Low	High	Medium
R30	Human Operational System Error	Manual misconfiguration	Operational disruption & downtime	High	High	High

Risk Treatment Plan

After conducting risk assessment and mapping, the next step is to develop a Risk Treatment Plan for each risk identified in the Risk Register. This Risk Treatment Plan serves as a guide for the concrete actions that the organization must take to reduce the likelihood and/or impact of existing risks. The risk treatment plan is developed in accordance with the controls outlined in ISO/IEC 27001:2022 Annex A, which are categorized as follows:

a. Organizational Controls
b. Human Resources Controls
c. Physical Controls
d. Technological Controls (Technological)

Each risk is reassessed based on its priority (high/medium), then additional controls or improvements are applied to existing controls. The following are the Risk Treatment Plan for the 30 information security risks identified at the BPS of Lhokseumawe.

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6564

Table 4. Risk Treatment Plan

ID	Risk	Risk Level	Existing Control	Action Plan	Kontrol ISO 27001:2022	Responsible Party
R01	Statistical Data Leaks	High	Standar username-password, manual log	Data encryption, automated log audits	A.8.10 – Encryption	Admin Server
R02	Phishing Attacks	Medium	Basic email filter	Advanced user education & email filters	A.6.3 – Awareness Training	IT Security Staff
R03	Server Failure	Medium	Weekly backup, UPS	Implement daily automatic backups	A.8.13 – Backup	IT Security Staff
R04	Brute Force Attack	High	Basic login protection	2FA, login attempt restrictions	A.8.2 – Authentication	Database Admin
R05	System Vulnerability Exploit	Low	Patch manual	Automation of patches & scannings	A.8.6 – Vulnerability Mgmt	Application Admin
R06	Social Engineering Attack	Low	Basic communication SOPs	Social engineering training & simulation	A.6.3 – Awareness Program	Human Resources
R07	Backdoor Malware	High	Antivirus, firewall	Code audits & periodic scans	A.8.30 – Code Security Review	IT Security Staff
R08	Illegal Public VPN/DNS Access	Medium	Manual monitoring	Block public VPN/DNS, DoH	A.8.23 – Web Filtering	IT Security Staff
R09	Malware from Ads	High	Ad-blocker, antivirus	Automatic ad blocking, education	A.8.23 – Web Filtering	Human Resources
R10	Information Security Ignorance	Medium	Poster & general appeals	Regular security campaigns & training	A.6.3 – IS Awareness	Head of ICT UPT
R11	Authentication System Failure	Medium	Manual Monitoring	Evaluation of the login and recovery system	A.8.2 – Authentication	IT Security Staff
R12	Use of Pirated Apps	Low	No software policy	Software audit and legality socialization	A.5.11 – Software Compliance	IT Support
R13	Admin Access Not Monitored	High	Limited admin rights	Implementation of automated log audits	A.5.15 – Logging	Head of IT and Security
R14	Personal Device Use (BYOD)	High	No BYOD policy	Personal device usage rules	A.5.18 – BYOD Policy	Network Admin
R15	Unauthorized Physical Access to Servers	Medium	Standard padlocks	Install CCTV & biometric access	A.7.4 – Physical Security	Head of IT Infrastructure
R16	Spam and Malicious Emails	Medium	Basic email filter	Advanced filter spam + education	A.8.24 – Email Security	Admin Email
R17	Reliance on One Vendor	High	Annual vendor evaluation	Diversify IT Vendors	A.5.19 – Supplier Relationship	IT Procurement Team
R18	DDoS Attack	High	Standard Firewall	Proteksi DDoS & traffic monitoring	A.8.23 – Network Protection	Network Team
R19	Unavailability of Emergency SOPs	Low	General SOP	Compile & simulate IT incident SOPs	A.5.29 – IS Continuity Plan	Head of Unit
R20	Lack of System	Medium	Limited	Mandatory	A.5.10 –	DevOps

Brilliance
Research of Artificial Intelligence

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6564

	Documentation		documentation	documentation of each system	Documentation Mgmt	Team
R21	Data Sync Failed	High	Manual sync	Otomatisasi sinkronisasi antar sistem	A.7.5 – Availability Controls	Network Team
R22	No periodic security reports	Medium	Monitoring of undocumented incidents	Monthly security reports	A.5.28 – Monitoring & Review	Head of IT Security
R23	Unstructured Data Storage	Medium	Separate storage	Implement a document management system	A.5.10 – Documentation Mgmt	Head of Unit
R24	Unstable Internet Connection	Medium	No Control	Use failover ISP	A.7.5 – Availability Controls	Network Admin
R25	New System Without Complete Trial	Low	Limited internal testing	Implement official UAT & QA	A.8.28 – Testing of Systems	Developer Team
R26	Forgot to Log Out by Users	Medium	No control	Auto-logout & notifications	A.8.2 – Session Controls	Application Admin
R27	Weak Website Security	High	Partial HTTPS	Implement SSL & CAPTCHA	A.8.27 – Web Security	Application Admin
R28	No Periodic Security Audits	Medium	Sporadic examinations	Annual audits by third parties	A.5.29 – IS Review	Head of Unit
R29	Unencrypted Backups	Medium	Standard Format	Automatic backup encryption	A.8.13 – Backup Security	IT Security Staff
R30	Human Operational System Error	High	No validation procedure	Double-check & technical training	A.6.3 – User Awareness	Operational IT Team

DISCUSSION

The primary objective of this study was to conduct a comprehensive information security risk analysis at the Central Statistics Agency (BPS) of Lhokseumawe by integrating the frameworks of ISO 31000:2018 and ISO/IEC 27001:2022. The results reveal a critical state of information security, characterized by a significant number of high-priority risks, foundational but immature technical controls, and a pronounced vulnerability stemming from human factors. The finding that 36.7% (11 out of 30) of identified risks are classified as high-risk is an alarming outcome. This prevalence indicates that the organization's core assets, such as the confidentiality, integrity, and availability of its statistical data, are under substantial threat. This aligns with concerns raised in prior research, such as the study at West Kalimantan BPS (Putri, Mutiah, & Prawira, 2022), which also identified significant gaps in the formalization of Information Security Management Systems (ISMS) within statistical agencies.

Furthermore, this study strongly reinforces the established axiom that technology alone is insufficient without addressing the human element. The identification of high-risk issues directly tied to human error (R30), lack of awareness (R10), and social engineering (R06) highlights that employees remain the most critical vulnerability vector. This finding is consistent with the broader information security literature and is explicitly addressed in ISO/IEC 27001:2022 through controls like A.6.3 (Information security awareness) (International Standard Organization, 2022). The success of the proposed technical and procedural controls is inherently dependent on effective human resource development, including continuous training and simulated phishing campaigns, to foster a culture of security.

Most significantly, this study demonstrates the practical efficacy of integrating ISO 31000:2018 and ISO/IEC 27001:2022. The ISO 31000 framework provided a robust, systematic process for establishing context, identifying, analyzing, and evaluating risks (British Standard Institusion, 2018). This process ensured the audit was comprehensive and grounded in the organization's specific operational reality. Subsequently, ISO/IEC 27001:2022 served as an indispensable toolkit for treatment, providing a validated set of controls (Annex A) to address each identified risk effectively and efficiently (International Standard Organization, 2022). This synergy answers the call for a context-based approach to managing public sector cyber risks, moving from a theoretical model to a practical, actionable risk treatment plan that is both prioritized and standardized (Aven & Ylönen, 2019).

While this study provides valuable insights, its limitations must be acknowledged. The audit was conducted at a single regional office, which may limit the generalizability of the findings to other BPS offices or different public sector institutions, though the methodological framework is universally applicable. Furthermore, the risk assessment inherently involves a degree of subjectivity in scoring likelihood and impact. Future research could build upon this

E-ISSN : 2807-9035
Volume 5, **Number** 2, November 2025
https://doi.org/10.47709/brilliance.v5i2.6564

work in several ways. A longitudinal study tracking the implementation of the proposed recommendations and measuring the change in risk levels over time would provide powerful evidence for the framework's effectiveness. Finally, applying this integrated approach to other government agencies or critical infrastructure sectors would help to further validate and refine the methodology.

CONCLUSION

Several key conclusions emerged from the information security risk management audit undertaken at the Central Statistics Agency (BPS) in Lhokseumawe. First, the identification of 30 risk revealed that the majority of them (11 out of 30) were classed as high risk, posing a threat to the information system's continuity and the trustworthiness of BPS data. In addition, 14 risks were found to be in the medium category and 5 risks in the low category. Second, many existing security mechanisms, such as data encryption, two-factor authentication, and automatic audit logs, are still basic or only existent. Third, user awareness remains a weakness, with high-risk issues discovered owing to human mistake and poor security training.

In response to the risks identified in this study, recommendations have been formulated in line with the controls in Annex A of ISO/IEC 27001:2022. These recommendations cover three main areas: technical enhancements (e.g., implementation of patch management and failover systems), procedural improvements (e.g., creation of back up plans, updating of SOPs and policies), and human resource development (e.g., training and security awareness campaigns). In addition, this study successfully integrated ISO 31000:2018 and ISO/IEC 27001:2022 and proved capable of providing a comprehensive approach, from risk identification and assessment to the development of controls and response plans. This approach helps organizations understand the overall risk context and select the appropriate controls to mitigate threats.

REFERENCES

Ardiansyah, A., Ilyas, A., & Haeranah. (2023). Reformulation Of Statistical Data Sources: Big Data New Data Sources Supporting Future Official Statistics? *Injuruty: Interdiciplinary Journal and Humanity*.

Aven, T., & Ylönen, M. (2019). The strong power of standards in the safety and risk fields: A threat to proper developments of these fields? *Reliability Engineering & System Safety*, 279-286.

Aven, T. (2016). Risk Assessment and Risk Management: Review of Recent Advances on Their Foundations. *European Journal of Operational Research*, 1-13.

British Standard Institusion. (2018). *ISO 31000:2018 - Risk Management Guidelines.* Switzerland: BSI Standards Limited.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* Singapore: Sage Publications.

Gillis, A. S. (2025, June 30). *What is the ISO 31000 Risk Management standard?* Retrieved from Tech Target: https://www.techtarget.com/searchsecurity/definition/ISO-31000-Risk-Management

Hopkin, P. (2018). *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management.* London: Kogan Page Publishers.

H. Knight, F. (1921). Risk, Uncertainty and Profit.

International Standard Organization. (2022). *ISO 27001:2022 - Information Security Management Systems.* Switzerland: BSI Standards Limited.

Institute of Risk Management. (2018). *Standard Deviations A Risk Practitioners Guide to ISO 31000.* Retrieved from The IRM: https://www.theirm.org/media/6884/irm-report-iso-31000-2018-v2.pdf

IT Governance USA. (2022). *SO 27001 and ISO 27002 2022 updates*. Retrieved from IT Governance: https://www.itgovernanceusa.com/iso27001-and-iso27002-2022-updates

Pubrica. (2025). *What Is the Purpose and Importance of Literature Reviews in Research?* England: Pubrica.

Putri, T. S., Mutiah, N. M., & Prawira, D. P. (2022). Analisis Manajemen Risiko Keamanan Informasi Menggunakan Nist Cybersecurity Framework Dan ISO/IEC 27001: 2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat). *Coding: Jurnal Komputer dan Aplikasi*, 237-248.

Rachman, A., Yochanan, E., Samanlangi, A. I., & Purnomo, H. (2024). *Metode Penelitian Kualitatif, Kuantitatif, dan R&D.* Karawang: Saba Jaya Publisher.

Wiener. (2021). Risk Management in the Public Sector: A Systematic Literature Review. . *International Journal of Public Administration, 44*(10), 850-867.

Xu, T., Shi, H., Shi, Y., & You, J. (2023). From data to data asset:conceptual evolution and strategic imperatives in thedigital economy era. *Asia Pacific Journal of Innovation and Entrepreneurship*.

Yin, R. K. (2009). *Case Study Research: Design and Methods* (4th ed.). United State of America: SAGE Publications.