*IJECBE* (2024), **2**, **3**, 395–413
Received (8 July 2024) / Revised (8 July 2024)
Accepted (11 July 2024) / Published (30 September 2024)
https://doi.org/10.62146/ijecbe.v2i3.81
https://ijecbe.ui.ac.id
ISSN 3026-5258

**International Journal of Electrical, Computer and Biomedical Engineering**

RESEARCH ARTICLE

# Design and Analysis of Information Security Risk Management Based on ISO 27005: Case Study on Audit Management System (AMS) XYZ Internal Audit Department

Diar Eka Risqi Hidayatullah,† Raisiffah Kunthi,‡ and Ruki Harwahyu*†

†Department of Electrical Engineering, Universitas Indonesia, Depok, Indonesia
‡Fakultas Ilmu Komputer, Universitas Indonesia, Depok, Indonesia
*Corresponding author. Email: ruki.h@ui.ac.id

**Abstract**

Information security is an important aspect and supported by a report issued by the Internal Audit Foundation entitled Risk in Focus 2024 Global Summary. The biggest risk that will be faced in 2024 is Cybersecurity and Data Security with a score of 73% for the global average. Based on a report issued by International Business Machine (IBM) entitled Cost of a Data Breach Report 2023, takes an average of 204 days to find out about a data leak by an affected agency or organization, and takes 73 days to overcome the data leak. To realize this digitalization, an Audit Management System (AMS) system was implemented which can accommodate the audit process starting from the Planning, Execution and Reporting stages as well as follow-up process for recommendations process. Using AMS is not without risks, access to AMS can be done without a Virtual Private Network (VPN). In this research, a risk assessment was carried out based on the ISO/IEC 27005:2022 standard by proposing a method for calculating consequences based on the data classification in the system and a method for calculating possibilities based on business processes that have an impact on system vulnerabilities and risks that need to be mitigated. ISO/IEC 27002:2022 will be used to anticipate risks. Results of the risk examination revealed that there were 24 risks with 1 very high-level risk, 3 high level risks, 8 medium level risks, 11 low level risks, and 1 very low-level risk in the XYZ internal audit department.

**Keywords:** Audit Management System, Risk Assessment, Information Security Risk, ISO 27005

## 1. Introduction

Information security is an important aspect that needs to be maintained by organizations. In its application, information security is aimed at protecting organizational assets in the form of information against possible threats. This is supported by a report issued by the Internal Audit Foundation entitled Risk in Focus 2024 Global Summary which states that the biggest risk that will be faced in 2024 is Cybersecurity and Data Security with a score of 73% for the global average [1].

Based on the Personal Data Protection Law (PDP) which been applied on 17 October 2022, it is stated that personal data controllers are obliged to carry out an assessment of the impact of personal data protection if the processing of personal data has the potential for high risk to the personal data subject [2]. With the existence of the PDP Law, all agencies and organizations that have business processes or data in which they process personal data need to adjust and preventive measures so as not to violate the PDP Law.

XYZ company has several business lines that process data in the system. Diverse business processes and applications that do not comply with security standards cause different levels of confidentiality categories according to the level of sensitivity of the data inputted in each business process of XYZ company. This requires a special categorization for applications that process data with a certain level of confidentiality. Based on information obtained from the interview results, it is known that one of the applications used in one of XYZ company's business lines has experienced a cyber attack incident in the form of a ransomware attack.

Ransomware attacks are malicious software designed to encrypt data in a system or device and prevent its owner from accessing the data. The ransomware attack also resulted in data damage to one of XYZ company's business lines. This threat not only attacks applications used to process sensitive data resulting in high-risk personal data leaks but also threatens institutions due to disruption of services at XYZ company. Due to the ransomware incident, XYZ company took recovery steps by re-inputting all data into the system. Data recovery after the ransomware attack took quite a long time. Various system recovery efforts are made so that the system can function as before.

Based on a document issued by The Institute of Internal Auditors (IIA) entitled The IIA's Three Lines Model, the task of internal audit is to ensure accountability and report to the board of directors and maintain independence from management responsibility, communicate suggestions to management and directors that are independent and objective to support organizational achievements in order to encourage and facilitate continuous improvement, as well as reporting any non-conformities to the board of directors and implementing preventive actions according to the problems being faced [3].

In the long-term information technology plan, XYZ's internal audit department has plans to digitalize audit business processes and follow-up on recommendations. Audit Management System (AMS) is an application that can accommodate the end-to-end audit process and carry out follow-up actions for recommendations issued by external auditors. The AMS implementation process is carried out by a vendor who is an authorized partner in Indonesia and collaborates with a certified third party so that

risks related to assets in the form of hardware and networks have been accommodated by the third party. All the needs of XYZ's internal audit department and a User Acceptance Test (UAT) was carried out before AMS Go-Live.

The use of AMS is not without risks, it is not uncommon for auditors to need sensitive and confidential data such as company financial reports or even logs of incidents that occur in an application. With the highly sensitive information in the AMS, special treatment and risk measurement methods are needed that can be adjusted to the potential impact of the data input into the AMS if it falls into the hands of irresponsible parties.

Based on a report issued by International Business Machine (IBM) entitled Cost of a Data Breach Report 2023, the average loss experienced by companies that experienced it was 4.45 million dollars. Apart from financial losses, the point of concern in the report issued by IBM is that it takes an average time or what is called Mean Time To Identify (MTTI) 204 days to find out if there is a data leak experienced by the affected agency or organization, and it takes 73 days to overcome or Mean Time To Contain (MTTC) (see Figure 1). If mapped based on the source of the threat, it is known that vulnerabilities that are zero-day or newly discovered as well as vulnerabilities that are already known but have not been patched on the system have quite high MTTI and MTTC, namely 272 days and 253 days in total to identify and overcome data leaks that occur in agency or organization (see Figure 2) [4].

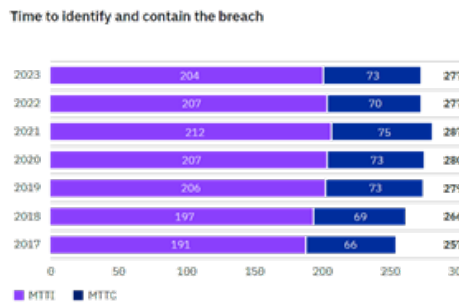


**Figure 1.** Time Required to Identify and Address Data Leaks

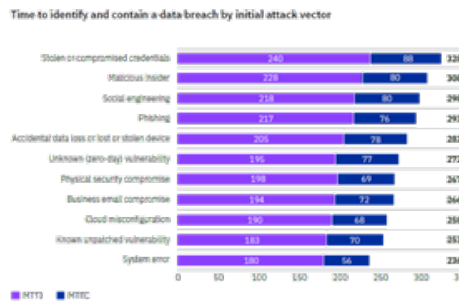


**Figure 2.** Time Required to Identify and Address Data Leaks Based on Attack Vector

Based on the report issued by IBM, the author proposes that adjustments are needed in the information security risk management process. In this research, a risk assessment was carried out based on the ISO/IEC 27005:2022 standard as a reference for designing information security risk management supported by ISO/IEC 27002:2022 as a standard for anticipating risks that occur.

The results of this research are expected to be able to map the risks that exist in AMS used by XYZ's internal audit department and the likelihood and consequences received if the threat occurs. The results of the mapping will be adjusted to the risk acceptance criteria owned by XYZ's internal audit department to get a more detailed picture regarding which risks should be mitigated and accepted by management.

## 2. Literature Study

### *2.1 Audit*

Audit is a process for collecting and examining evidence in the form of information to report any differentiation that occurs between the information obtained and the criteria that have been created and determined, where this audit activity is carried out by someone who is independent and has competence in their field. An audit is also a process that is carried out in a structured manner, and the results of the audit must be informed to parties who have an interest in the agency or organization [5].

Internal audit is an independent activity, evaluating entities, processes or resources objectively using appropriate criteria, and providing space for consultation to increase value and optimize the performance of an agency or organization. These activities will help the agency or organization achieve the desired goals by conducting evaluations where the results of the evaluation will be used to improve the risk management process, internal control and governance within the agency or organization [6].

### *2.2 Risk*

Risk can also be interpreted as the possibility of a loss event occurring. If a threat shows weakness, then a loss event will occur. Based on the ISO 31000:2018 guideline, risk can be defined as an effect that occurs due to uncertainty in objectives [7].

Risks can be categorized into several parts. This is possible if we look at the risks from the impacts caused. There are five risk categories [8]:

a. Strategic risk is a risk related to the goals of an agency or organization. Strategic risk is the risk with the highest level because it can result in the emergence of other risks.
b. Reputational risk is a risk related to the reputation and image of an agency or organization. Reputational risk is usually a risk that has a close correlation with business processes in an agency or organization. Apart from that, this risk may occur if the agency or organization is unable or fails to manage this type of risk. other risks effectively.
c. Financial risk is a risk related to the financial condition of an agency or organization.

d. Compliance risk is a risk related to reputation or rules within an agency or organization where this compliance risk is caused by an agency or organization's non-compliance with applicable regulations, laws, standards and ethics.
e. Operational risk, which is a risk related to the system running in an agency or organization, which consists of human resources, processes running internally, and the technology used.


**Figure 3.** Principles in Risk Management

Risk management is an activity carried out in a coordinated manner within an agency or organization to direct and manage risks. In Figure 3 there are 8 risk management principles which are the basis for managing risk. These principles are very important things to consider when designing and determining the risks that exist in an agency or organization [7]:

a. Integrated - Risk management is something that is combined and related to all existing processes in an agency or organization.
b. Structured and Comprehensive - Risk management is a structured and comprehensive activity, so that it has an impact on consistent and comparable results.
c. Customized - Customization of the framework used in the risk management process is carried out so that it can be adapted to the external and internal context and objectives of the agency or organization.
d. Inclusive - Risk management must involve stakeholders appropriately and regularly to result in increased awareness and an informed risk management process.
e. Dynamic - Risk management is always undergoing adjustments because over time there may be risks that change, either increasing or disappearing, so risk management is expected to be able to overcome, carry out early detection, recognize and respond to incidents quickly and accurately.
f. Best Available Information - Risk management requires sources of historical information and current conditions, as well as future expectations so that it can carry out accurate calculations regarding the limitations and uncertainties between that information and expectations. Information must be timely, clear and available to relevant stakeholders.

g. Human and Cultural Factors – Risk management calculates human resource factors and habits and culture at every level within the agency or organization.
h. Continual Improvement – Risk management supports continuous improvement based on learning and experience gained over time.

### *2.3 Information Security*

Information security is an effort made by an agency or organization to protect information from various threats that come from internal and external to ensure that business processes can continue and minimize risks that occur and increase returns on investment in the business carried out. There are three main components that are the basis of information security, namely Confidentiality, Integrity, and Availability [9].

Confidentiality where information can only be accessed and obtained by authorized parties so that it can be used according to its function and avoid misuse by unauthorized parties. Integrity, where this component ensures that the information obtained is not changed and is not deleted by unauthorized parties. Availability means that information must be able to be accessed and used when needed by parties who have an interest in the information.

The risk assessment process purpose is to evaluate things that could go wrong, the likelihood of occurrence in incident, and the impact which can be harm the organization if incident occur. Information security risk assessment process ranks IT assets based on prioritization of the assets and relating it with levels of associated risk and potential damage that could occur. The purpose is to optimize IT resource that organization have with prioritizing potential incident and impact for organization. It is also helps organization benchmark their current security practices against industry standards [10].

Commonly the information security risk management and control frameworks used are ISO/IEC 27005:2022, NIST SP 800-30 Revision 1, and ISO 27002:2022. ISO/IEC 27005:2022 is the latest standard issued by the International Organization for Standardization (ISO) and the International Electronical Commission (IEC) and replaces ISO/IEC 27005:2018, where this standard is a reference for carrying out information security risk management processes. The application of ISO/IEC 27005:2022 is not limited to specific agencies or organizations but can be used by all agencies or organizations so that a risk management process can be carried out to safeguard risks so that they do not endanger the assets of the agency or organization [11].

ISO/IEC 27005 are one of ISO/IEC 27000 series that consist of various standards in IT security, cybersecurity and privacy protection that are vital for companies and organizations. ISO/IEC 27005 is implementation of the information security risk requirements specified in ISO/IEC 27001 that enables organizations to form an information security committee to make information security policy. The focus of information security risk management will further be discussed on ISO/IEC 27005 [12].

Figure 4 illustrates the information security risk management process contained in ISO/IEC 27005:2022 [11].

a. Context Establishment which consists of 4 important components, namely considerations taken by the organization, identifying the main needs of interested groups, conducting risk checks, and establishing and always updating risk security criteria.
b. Risk Assessment, which in this context consists of 3 parts, namely identifying risks that may occur, analyzing the risks that have been identified, and evaluating the results of the analysis.
c. Risk Treatment, in this context, determines what steps the agency or organization needs to take to overcome the results of the risk assessment process.
d. Communication and Consultation where it is necessary to communicate with external and internal parties in an agency or organization, and the steps to be taken if these risks occur.
e. Documented Information where all information related to the information security risk management process in the agency or organization must be documented.

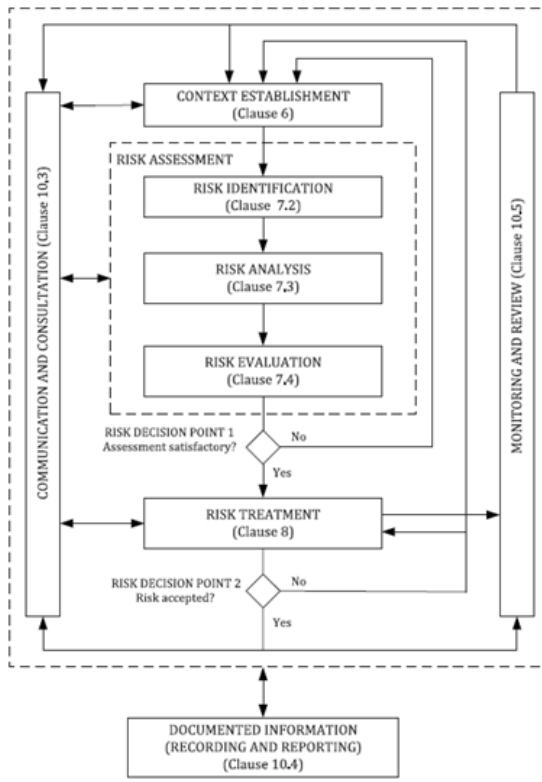


**Figure 4.** Risk Management Process in ISO/IEC 27005:2022

NIST SP 800-30 is one of the frameworks used as a reference in carrying out risk assessments such as ISO/IEC 27005:2022.

NIST SP 800-30 can be used to conduct risk assessment of informational system in organization as complement of NIST SP 800-39 guidance. NIST SP 800-39 provide guidance for an integrated, organization-wide program for managing information security risk to organizational operations. NIST SP 800-30 also can be used to complete ISO 27005 standard in performing risk assessments [13].

Figure 5 illustrates the flow of procedures for implementing risk assessments in NIST SP 800-30 [14].

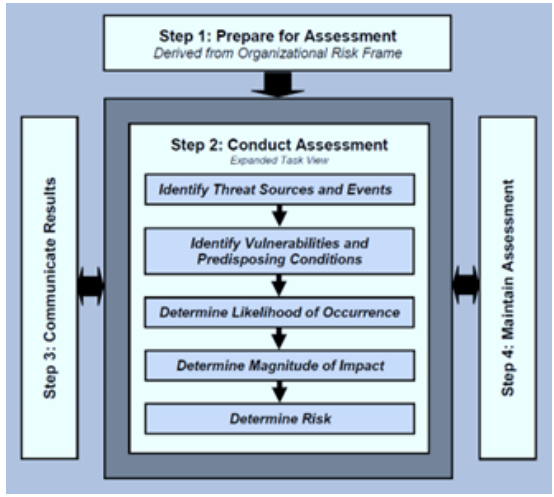


**Figure 5.** Risk Assessment Process in NIST SP 800-30

There are several processes in carrying out risk assessment:

a. Prepare for Assessment, at this stage identifies the context of the risk assessment process,
b. Conduct Assessment, at this stage a list of information security risks is obtained which can be prioritized based on the level of risk and this will be used to determine decisions regarding the response to be taken.
c. Communicate Results, at this stage the directors of the agency or organization receive the results of the risk assessment of the agency or organization as material for decision making
d. Maintain Assessment, at this stage the risk assessment process is to update the organizational risks that support continuous monitoring of decisions taken in risk management.

ISO/IEC 27002:2022 is the latest standard issued by the International Organization for Standardization (ISO) and the International Electronical Commission (IEC) and replaces ISO/IEC 27002:2013, where this standard is a reference that contains a set of controls for information security along with guidelines in apply these controls. ISO/IEC 27002:2022 was created based on ISO/IEC 27001 and is used to implement information security controls for agencies or organizations based on an internationally recognized framework and is useful as a reference for specialized agencies or

organizations in managing information security. In the ISO/IEC 27002:2022 document it consists of 3 main structures [15]:

a. Clauses containing existing controls within the organization, controls for the human resources category, physical security controls, as well as security controls for the technology used.
b. Themes and attributes where control is categorized into 4, namely human resources, physical, technological, or if categorized as agency or organizational risk.
c. A control layout consists of a control title, attribute table, controls, objectives, guides, and other information.

Based on the literature study process related to risk management frameworks which has been explained in detail in the previous sub-chapter, a comparison of the risk management frameworks is carried out:

a. In the ISO/IEC 27005:2022 framework, which is a framework with the topic of information security risk management, it is more suitable when used to assess risks that exist in the context of information security. This framework uses 6 processes to produce reports on risk management information security.
b. In the ISO 31000:2018 framework, which is a framework on the topic of risk management in general and can be applied to all sectors without exception, this a. framework was not specifically created to assess risks in the context of information security.
c. In the NIST SP 800-30 Revision 1 framework, the framework with the topic of information security risk management is more suitable when used to assess risks that exist in the context of information security. This framework uses 4 processes to produce reports on risk management, information security, and other information.

Table I below is a comparison table of information management frameworks.

**Table 1.** Comparison of Risk Management Frameworks

| Criteria | ISO/IEC 27005:2022 | ISO 31000:2018 | NIST SP 800-30 Revision 1 |
|---|---|---|---|
| Publisher | ISO/IEC | ISO | NIST |
| Publish Year | 2022 | 2018 | 2012 |
| Scope | Processes related to information security | Can be implemented in all existing risk types and sectors | Processes related to information security |
| Risk Management Process | 6 stages | 6 stages | 4 stages |
| Company scale | Large/ massive scale companies | Large/ massive scale companies | Large/ massive scale companies |
| Organizational Level Targets | Management and Operations | Management and Operations | Management and Operations |

In this research, the ISO/IEC 27005:2022 information security risk management framework was chosen as the basis for the development that will be carried out by the author. ISO/IEC 27005:2022 was chosen because it has more detailed steps in the risk assessment process. ISO/IEC 27005:2022 is also based on ISO 27001 which is a standard that contains reference requirements that must be provided by agencies or organizations related to information security management systems. With this connection, in this research the author uses ISO/IEC 27002:2022 as the standard. used to control existing risks where ISO/IEC 27002:2022 is based on ISO/IEC 27001.

Table II presents related research to the theme raised, namely the preparation of an information security risk management framework.

**Table 2.** Related Research

| Name | Research Title | Description |
|---|---|---|
| Ricko Dwi Pambudi (2023) | Design and Analysis of Security Risk Management for the Supervision Management Information System (SIMWAS) at XYZ Agency | Using ISO/IEC 27005:2018 and NIST SP 800-30 as a method for conducting risk assessments and using ISO/IEC 27002:2022 as a reference for controlling existing risks. |
| Mohamad Lutfi Ismail (2022) | Information Security Risk Assessment Using ISO/IEC 27005 Case Study: PT XYZ Personnel Information System | Using ISO/IEC 27005:2018 as a method for conducting risk assessments and using ISO/IEC 27002:2022 as a reference for controlling existing risks. |
| Amalia Fitri Kurnia Dewi (2022) | Design of an Information Security Risk Management Framework Based on Risk Profiling Studies in the Health Sector (Case Study of Health Service Facilities in Indonesia) | Combining ISO/IEC 27005:2018, NIST SP 800-39, NIST SP 800-30, ISSP Risk Assessment Framework, and Facilitated Risk Analysis and Assessment Process (FRAAP) to design an information security risk management framework in the health sector |

## 3. Research Methodology

Several stages were used to produce conclusions, the stages carried out were formulating the problem that occurred, conducting a literature study, preparing the methods, and instruments used in the research. This study used qualitative research methods. Qualitative research methods are research procedures that produce descriptive data in the form of written or spoken words from individuals and observed behavior [16]. The research stages can be seen in Figure 6.

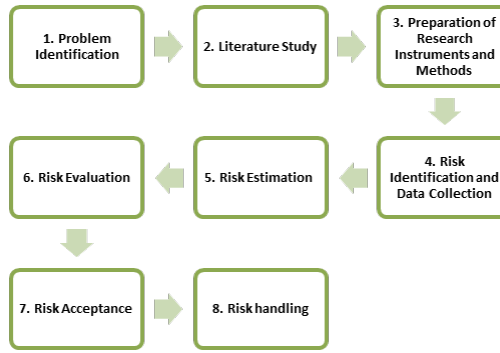


**Figure 6.** Research Methodology

In the first stage, problem identification is observing the as is condition and incident report in audit internal XYZ department. The output of this stage are lists of business process, problems, research questions, scope, and purpose of this research. Next, the researcher conducted a literature study according to the research problem. Information was collected by searching for theories, concepts and definitions by reading scientific papers from IEEE Xplore. From this stage, researchers get a theoretical framework a risk assessment process was carried out using the ISO/IEC information security risk management framework 27005:2022.

The third stage is preparation of research instruments and methods. In this stage researchers decide the research flow, data collection methods, data collection instruments, and methods used to carry out data analysis. Qualitative methods were used to conduct data analysis. The data sources used were interview transcripts and documents obtained. The data collection method used in this study is by conducting interviews with two stakeholders who directly interact with AMS and the information contained in the system and also conducting literature studies on documents obtained and reports with supporting topics. The information that we want to obtain from interviews with sources is the risk appetite of the internal audit department, incident reports on AMS, and possible threats and vulnerabilities. Table III shows a list of stakeholder sources and data to be obtained from the results of the interviews.

**Table 3.** List of Stakeholder and data obtained

| Stakeholders | Obtained Data |
|---|---|
| Risk Officer in Audit Internal Department | XYZ internal audit department risk appetite, incident reports that occurred at AMS |
| IT Audit Manager | The objectives of XYZ internal audit department, XYZ internal audit department business processes, AMS key and supporting assets and possible threats and vulnerabilities. |

The research instrument used was a list of interview questions created based on the context of information security risk management in AMS at XYZ internal audit agency. There are 10 questions for Risk Officer in Audit Internal Department and 9 questions for IT Audit Manager.

The data processing method used in this research is to carry out thematic analysis. In this research, the coding process in thematic analysis was carried out to give marks or labels to data related to this research which was collected from the interview process [17]. The data processing tools used are Microsoft Word and Microsoft Excel. Table IV below explains the labeling information used in this research.

**Table 4.** Information Labeling

| Related Information | Code |
|---|---|
| Main assets in AMS | MA |
| Supporting assets in AMS | SA |
| Vulnerability | V |
| Threat | T |

The fourth stage is doing risk identification and data collection. This research collect data with interviews. The resource persons are staff at the XYZ internal audit agency who serve as Risk Officer and Audit IT Manager. The output are transcripts of interview results, documents containing objectives and controls, assets, risk acceptance criteria, threats and vulnerabilities.

The five stages, researchers use data on threats, vulnerabilities, and possible occurrences in AMS. The data is then processed, and risk estimates are carried out using consequence criteria and likelihood criteria which are adjusted to the needs of the internal audit department. Next stages, evaluation of existing risks is carried out and adjusted to the risk acceptance criteria described through interviews with sources with a background as a risk officer in the internal audit department. After that the next stage is risk acceptance. At the risk acceptance stage, adjustments are made to existing risks and grouped according to risk acceptance criteria.

The last stage is risk handling. The risk handling stage is carried out using information security control criteria. The control recommendations that will be suggested in this research will be based on an information security control framework that is relevant to the information security risk management framework used in this research.

## 4. Analysis and Test Result

### *4.1 Context Establishment*

Based on the results of interviews with stakeholders, it is known that there needs to be data classification to assess how sensitive the data contained in the system used at XYZ company. In this study, information classification categories are added to the consequence criteria, this is based on the differences in data types in the system, where systems that have data with limited and confidential classifications will have higher consequences if the data falls into the hands of irresponsible parties. The information

classification category in this consequence criterion can be applied to all risks in the system that arise when the risk assessment process is carried out.

This categorization of consequence levels has been discussed with stakeholders so that it is aligned with the needs of XYZ company. The following is Figure 7 that contains the proposed scheme in the consequence criteria.

| Value | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Scale | Very Low | Low | Medium | High | Very High |
| Code | SR | R | S | T | ST |
| Data Classification on Information System | Data in the system is classified as open information and it cannot be processed into other information | Data in the system is classified as open information and it can be processed into other information | Data on the system is private (limited) | Data in the system is limited and confidential and if it falls into the hands of irresponsible parties it could be detrimental to the relevant agency | Data in the system is limited and confidential and if it falls into the hands of irresponsible parties it could harm other agencies. |

**Figure 7.** Proposed Consequence Criteria

Based on IBM's report on data leaks, it cannot only be based on the frequency of occurrence but also needs to consider other things such as whether a vulnerability check has been carried out on the system or the use of firewall devices to provide protection and ensure that vulnerabilities in the system have been identified and closed. In this study, a vulnerability check category was added to the system for the likelihood criteria. The results of interviews with stakeholders confirmed that it was necessary to conduct vulnerability checks on the systems owned by XYZ company. This was because XYZ company had various business lines so that it had various systems to accommodate different business processes.

The system vulnerability check category in this likelihood criteria can only be applied to risks with a vulnerability category in the system. If other risks arise besides system vulnerabilities, the frequency of occurrence criteria can be used. The following are Figure 8 the likelihood criteria that can be applied related to system risks.

| Value | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Scale | Very Low | Low | Medium | High | Very High |
| Code | SR | R | S | T | ST |
| Frequency | 1 x in more than 36 months | 1 x in 24 to 36 months | 1 x in 13 to 24 months | minimum 1x in 7 to 12 months | minimum 1x in 1 to 6 months |
| Vulnerability Assessment on System | Has been done in less than 6 months | Has been done in less than 1 year | Has been done in less than 2 year | Has been done in less than 3 year | Vulnerability testing has never been performed or has been performed in more than 3 years |

**Figure 8.** Proposed Likelihood Criteria

This research is using risk evaluation criteria using ISO/IEC 27005:2022 that consists of a risk matrix generated by multiplying both consequence and likelihood. The risk acceptance criteria in the internal audit department are to reduce the likelihood of risk occurring or the impact of risk, by mitigating high and very high risks and accepting and maintaining risk levels for medium, low and very low risks.

### *4.2 Risk Identification*

Based on the results of interviews conducted with the IT audit manager and risk officer of the internal audit department, it was discovered that:

a. There are 16 main assets (MA) in the form of business processes and data and 14 supporting assets (SA) in the form of hardware, software, and human resources.
b. There are 18 potential threats (T) that could have a negative impact on the assets owned by the XYZ internal audit department.
c. There are 19 potential vulnerabilities (V) that can be exploited and have a negative impact on assets owned by the XYZ internal audit department.

Based on data related to assets, threats, and vulnerabilities in the XYZ internal audit department, a risk compilation was carried out and 24 potential risks were found, of which 24 risks contained 6 risks related to vulnerabilities in the following system (R8, R9, R10, R15, R16, R17) the list of risks in the XYZ internal audit department are presented in Table V.

Table V shows that there are 4 asset categories consist of hardware, software, people, and business process and data, where in the hardware category there are 5 risks, in the software category there are 6 risks, in the people category there are 10 risks, and in the business process and data category there are 3 risks. The risk data obtained is then confirmed with the stakeholders to ensure the accuracy of the risks obtained by mapping the results between the main assets and supporting assets owned by XYZ internal audit department with possible threats and vulnerabilities contained in the system and XYZ internal audit department.

**Table 5.** Risk Identification

| Asset Category | Threat | Vulnerability | Risk Code |
|---|---|---|---|
| Hardware | T7 | V16 | R1 |
| | T11 | V13 | R2 |
| | T2 | V1 | R3 |
| | T13 | V2 | R4 |
| | T1 | V3, V6 | R5 |
| Software | T3 | V6 | R6 |
| | T14 | V13 | R7 |
| | T15 | V3, V4, V11, V6, V5, V18 | R8 |
| | T9 | V3, V4 | R9 |
| | T10 | V3, V4 | R10 |
| | T18 | V3, V4, V19 | R11 |

| Asset Category | Threat | Vulnerability | Risk Code |
|---|---|---|---|
| People | T4 | V10, V9 | R12 |
| | T5 | V10, V9 | R13 |
| | T6 | V10, V9 | R14 |
| | T8 | V10, V9, V14, V17, V4 | R15 |
| | T9 | V7, V15, V14, V17, V4 | R16 |
| | T10 | V7, V15, V14, V17, V4, V12 | R17 |
| | T16 | V7, V15, V14, V17, V12 | R18 |
| | T17 | V8 | R19 |
| | T18 | V10, V19 | R20 |
| | T12 | V7 | R21 |
| Business Process and Data | T15 | V3, V6 | R22 |
| | T10 | V7, V12 | R23 |
| | T16 | V7, V12 | R24 |

### *4.3 Risk Estimation and Evaluation*

Table VI shows that based on the calculation of the consequences and likelihood of the risk and then mapped into a risk matrix so that the risk level is known at very low, low, medium, high or very high levels. There is 1 risk with a very high level, 3 risks with a high level, 8 risks with a medium level, 11 risks with a low level, and 1 risk with a very low level. For 6 risks (R8, R9, R10, R15, R16, R17) related to the possibility of vulnerability in the system, all are low-level risks.

**Table 6.** Risk Level

| Risk Code | Consequence | Likelihood | Risk Level |
|---|---|---|---|
| R1 | 5 | 1 | 5 (Low) |
| R2 | 3 | 1 | 3 (Low) |
| R3 | 5 | 1 | 5 (Low) |
| R4 | 5 | 3 | 15 (High) |
| R5 | 2 | 1 | 2 (Very Low) |
| R6 | 5 | 1 | 5 (Low) |
| R7 | 5 | 1 | 5 (Low) |
| R8 | 5 | 2 | 10 (Medium) |
| R9 | 5 | 2 | 10 (Medium) |

| Risk Code | Consequence | Likelihood | Risk Level |
|---|---|---|---|
| R10 | 5 | 2 | 10 (Medium) |
| R11 | 5 | 1 | 5 (Low) |
| R12 | 5 | 1 | 5 (Low) |
| R13 | 5 | 2 | 10 (Medium) |
| R14 | 5 | 5 | 25 (Very High) |
| R15 | 5 | 2 | 10 (Medium) |
| R16 | 5 | 2 | 10 (Medium) |
| R17 | 5 | 2 | 10 (Medium) |
| R18 | 5 | 2 | 10 (Medium) |
| R19 | 3 | 4 | 12 (High) |
| R20 | 5 | 1 | 5 (Low) |
| R21 | 3 | 2 | 6 (Low) |
| R22 | 4 | 4 | 16 (High) |
| R23 | 5 | 1 | 5 (Low) |
| R24 | 5 | 1 | 5 (Low) |

### *4.4 Risk Acceptance and Handling*

Based on risk acceptance criteria, there are 4 risks that need to be mitigate (R4, R14, R19, R22). Table VII shows control from ISO/IEC 27002:2022 which matches the risks in high to very high category in XYZ internal audit department, this table also states that the PIC is responsible for carrying out controls in accordance with ISO 27002:2022.

| Risk Code | Risk Level | PIC | Controls Using ISO/IEC 27002:2022 |
|---|---|---|---|
| R4 | 15 (High) | Institution and Internal Audit Department | **6.3 Information Security Awareness, Education and Training** There is a need to provide training to employees regarding awareness of system security, and regular socialization of system security |

| | | | |
|---|---|---|---|
| | | | policies that are relevant to the main tasks and functions of employees. |
| R14 | 25 (Very High) | Institution and Internal Audit Department | **6.3 Information Security Awareness, Education and Training** There is a need to provide training to employees regarding awareness of system security, and regular socialization of system security policies that are relevant to the main tasks and functions of employees. |
| R19 | 12 (High) | Internal Audit Department | **5.2 Information Security Roles and Responsibilities** Information security roles and responsibilities should be defined and allocated according to the needs of the organization. |
| | | | **5.26 Response to Information Security Incidents** |

| | | | |
|---|---|---|---|
| R22 | 16<br>(High) | Institution and Internal Audit Department | Information security incidents that occur must be responded to and documented to ensure that the incident response is effective and efficient.<br>**6.8 Information Security Event Reporting**<br>The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner. |

## 5. Conclusion

Based on the results of the risk examination, it is known that there are 24 risks in the XYZ internal audit department. There is 1 risk with a very high level, 3 risks with a high level, 8 risks with a medium level, 11 risks with a low level, and 1 risk with a very low level. With the proposed likelihood categorization, it is known that there are 6 risks associated with the system and it has a low risk level because a vulnerability check has been carried out by the provider in July 2023. Risk appetite in XYZ internal audit department, there are 4 risks whose potential occurrence or impact will be reduced by carrying out mitigation and there are 20 risks whose risk levels will be accepted and maintained.

The results of the risk assessment using proposed likelihood and consequences criteria can represent in more detail the level of risk that may not be detected by the user or fail to be detected by the security system in the event of a zero-day cyber attack. In its application to the internal audit department of XYZ, it is known that data has been categorized, although it is not that detail, but if the proposed consequence criteria are applied to companies that do not have data categorization, it can be used to help find out how vital the data is and how much impact it will have on the company if there is data theft or damage.

For the next research, an analysis can be carried out regarding the costs that must be incurred to handle the risks that exist in the AMS used by XYZ's internal audit department. It is necessary to validate the results of interviews conducted in this research by Subject Matter Experts (SME) from external parties to reduce the level of subjectivity in this research.

## References


[1] Internal Audit Foundation. *Global Summary - 2024 Risk In Focus Survey Result*. 2023.

[2] *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi*. Republik Indonesia, 2022.

[3] Yulandi. *Pengembangan Disain Mitigasi Risiko Pada Otoritas Sertifikat Digital Pengadaan Barang/Jasa Secara Elektronik (OSD PSE) Berbasis COBIT 5 For Risk dan NIST SP 800-30 Revisi 1: Studi Kasus Balai Sertifikasi Elektronik*. 2019.

[4] National Institute of Standards and Technology (NIST). *NIST SP 800-30 Guide for Conducting Risk Assessments*. Tech. rep. Gaithersburg, MD: National Institute of Standards and Technology, 2012. DOI: 10.6028/NIST.SP.800-30r1.

[5] N. M. T. Nugraheni. *Analisis Penerapan Risk Based Audit dan Penyusunan Program Pemeriksaan Pada Kementerian Desa, Pembangunan Daerah Tertinggal dan Transmigrasi*. 2020.

[6] Sudarmono. *Perancangan Risk Based Internal Audit Plan Pada Divisi Internal Audit (Studi Kasus PT. XY)*. 2021.

[7] International Organization for Standardization (ISO) and International Electronical Commision (IEC). *ISO/IEC 31000:2018 Risk management - Guidelines*. 2018.

[8] I. Baehaki. *Desain Kerangka Kerja Manajemen Risiko Keamanan Informasi Berdasarkan Integrasi ISO/IEC 27005:2018, NIST SP 800-39, Octave Allegro dan COBIT 2019: Studi Penerapan Awal di Pusat Pendidikan dan Pelatihan Badan XYZ*. 2020.

[9] M. L. Ismail. *Penilaian Risiko Keamanan Informasi Menggunakan ISO/IEC 27005 Studi Kasus: Sistem Informasi Kepegawaian XYZ*. 2022.

[10] F. A. Shaikh and M. Siponen. "Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity". In: *Computers Security* 124 (2023), p. 102974. DOI: https://doi.org/10.1016/j.cose.2022.102974.

[11] International Organization for Standardization (ISO) and International Electronical Commision (IEC). *ISO/IEC 27005:2022 Information Security, Cybersecurity and Privacy Protection — Guidance on Managing Information Security Risks*. 2018.

[12] M. Al Fikri et al. "Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency". In: *Procedia Computer Science*. Elsevier B.V., 2019, pp. 1206–1215. DOI: 10.1016/j.procs.2019.11.234.

[13] F. A. Putra, A. R. Pradana, and H. Setiawan. "Design of Information Security Risk Management Using ISO/IEC 27005 and NIST SP 800-30 Revision 1: A Case Study at Communication Data Applications of XYZ Institute". In: *International Conference on Information Technology Systems and Innovation (ICITSI)*. 2017.

[14] National Institute of Standards and Technology (NIST). *Guide for Conducting Risk Assessments*. Tech. rep. Gaithersburg, MD: National Institute of Standards and Technology, 2012. DOI: 10.6028/NIST.SP.800-30r1.

[15] International Organization for Standardization (ISO) and International Electronical Commision (IEC). *ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Controls*. 2022.

[16] M. Fitrah and Luthfiyah. *Metode Penelitian, Penelitian Kualitatif, Tindakan Kelas dan Studi Kasus*. CV Jejak Publisher, 2017.

[17] J. Recker. *Scientific Research in Information Systems Second Edition*. [Online]. Available: http://www.springer.com/series/10440. 2021.