

From Design to Evaluation: A Novel Mitigation Model for Public Cloud Adoption

Nur Chalik Azhar ^{1,*}, Muhammad Zarlis ², Yulyani Arifin ¹ and Benfano Soewito ³

¹ Computer Science Department, BINUS Graduate Program - Doctor of Computer Science, Bina Nusantara University, Jakarta (11480), Jakarta, Indonesia

² Information Systems Management Department, BINUS Graduate Program - Master of Information Systems Management, Bina Nusantara University, Jakarta (11480), Indonesia

³ Computer Science Department, BINUS Graduate Program - Master of Computer Science, Bina Nusantara University, Jakarta, Indonesia 11480

* Correspondence: nur.azhar@binus.ac.id;

Received: August 4, 2026; Received in revised form: October 25, 2026; Accepted: October 26, 2026; Available online: October 26, 2026

Abstract: Cloud computing technology can provide several benefits to organizations. However, several threats and risks can significantly impact the information technology infrastructure in public clouds, potentially affecting organizational processes. A structured approach is needed to effectively identify, assess, and mitigate emerging threats and risks. However, widely adopted frameworks do not yet fit the conditions and characteristics of public cloud. Therefore, the purpose of this study is to develop a model that helps in identifying, assessing, and mitigating risks in public cloud adoption in organizations. In developing this model, the design science research methodology framework was adopted, as it is commonly used in research related to computer science and information systems. The results show that the model has three main phases in the model components: initiation (three sub-components), assessment (four sub-components), and mitigation (three sub-components). Risk factors and mitigation strategies have been adapted to the public cloud environment, which can assist in implementing the risk mitigation model. The proposed risk mitigation model is appropriate and suitable for use in public cloud environment adoption, following rigorous in-depth interviews. The academic findings can contribute to the development of risk management models, which include the identification of threat types, controls, risk factors, and mitigation strategies that have been adapted and mapped within the public cloud context. Practical benefits can help mitigate risks and potential impacts in public cloud environments.

Keywords: Mitigation Model; Public Cloud; DSRM; Risk Factors; Mitigation Strategies

1. Introduction

Public cloud is a solution for organizations that want to gain several benefits from adopting it. According to research from [1], there are several benefits of adopting public cloud for organizations, including, among others, easy scalability of IT infrastructure, increased efficiency in the use of team resources, and easy organization of IT resources according to needs. In addition to providing benefits in public cloud adoption, several threats can disrupt assets in the public cloud environment, such as applications and other application supporting components (databases, virtual machines, etc) [2]. For example, from the information security aspect, the threat of database damage to applications caused by hacking through insecure API security holes [3].

In addition, threats from the privacy aspect, such as internal IT staff who intentionally steal or damage application databases in the public cloud environment. The risks that can arise based on the

type of threat can impact operations and affect the reputation of the organization [4]. A risk management approach is needed to identify and analyze threats and risks that will or are currently occurring, and to mitigate the risks of using public cloud within the organization [5]. However, each component of the existing framework is still general, and an artifact in the form of a research model that is appropriate to the conditions and characteristics of the public cloud, so this research is important to help IT managers in reducing the value and impact of risks that will or are currently occurring [6].

Previous studies aimed to design and implement risk assessment models, as well as evaluate risk values in the use of cloud [7]. Information security [7, 8, 9, 10, 11], privacy [10], trust [10, 12], and environment [13] are the most commonly explored aspects in the development of risk assessment model components. Commonly explored service models are only one of Infrastructure as a Service (IaaS) [8], Platform as a Service (PaaS) [11], and Software as a Service (SaaS) [10]. In addition, they are implemented in the context of logistics companies [11], smart building [12], and organizations in general [10]. Based on previous studies, many proposed research models only explore one of the service models among IaaS [8], PaaS [11], and SaaS [10], and aspects of the most common risk assessment components are explored is aspect of information security. The risk analysis approaches adopted are mostly quantitative [13], and both quantitative and qualitative [12].

The development of model components from previous research only reached the risk identification and assessment phases [11], and there are still few models that discuss the identification, assessment, and risk mitigation stages in the public cloud environment, especially in information security and privacy. In addition, there is still little discussion regarding the evaluation of the proposed model, except for studies that have discussed model validation to determine the suitability of network components as well as trust assessment of IoT and IT infrastructure in smart building environments [12]. The source of threat types and vulnerabilities still relies on Common Vulnerabilities and Exposures (CVE) from NIST, so it is not yet suitable for the property context, especially in smart buildings.

Therefore, based on previous research, this study formulates several research questions, including the following:

- RQ 1: How to develop a risk mitigation model suitable for public cloud environments?
- RQ 2: How to evaluate the risk mitigation model developed for public cloud environments?

This research is crucial as Fortinet reports that 96% of organizations will be concerned about cloud security by 2024 [14]. This means that stakeholders in organizations do not want to experience losses in assets/applications that have been migrated to the cloud, as well as risks that can impact operations in the cloud environment. For example, access control threats in public clouds, where IT staff misconfigure Identity and Access Management (IAM), allowing unauthorized users to access and view data in applications [4]. As a result, it is difficult to track the cause of errors in applications that have been migrated to the cloud and can potentially lead to application data leaks [8].

A potential risk when a data breach occurs is the loss of an organization's reputation due to a lack of credibility and professionalism in securing data within the organization [14]. Organizational data is an asset that must be secured in a strict and structured manner. Organizations adopting public cloud must be prepared to face future information security and privacy issues.

Therefore, this study proposes a risk mitigation model in the context of the public cloud to identify, assess, and mitigate risks in applications that have and have not yet migrated to the cloud.

A rigorous and structured process can help organizations mitigate potential risks when migrating applications to the cloud. Organizations can be facilitated in the threat and risk identification process because the research outputs are not only related to the risk mitigation model but also produce appropriate threat and risk identification outputs in the public cloud context. Furthermore, this study proposes a prototype to demonstrate the model's suitability for implementation.

The first specific contribution of this research model is the proposal of several components to support the implementation of the mitigation phase. These include a "determine risk treatment strategy" component, which helps identify the assets for which risk treatment is required; a "determine risk treatment plan" component, which assists the IT department head in formulating risk mitigation plans tailored to the context of this research; and a "risk mitigation monitoring" component, which is used to oversee the implementation of the risk treatment measures planned in the preceding component.

The second contribution involves identifying 9 types of threats, 16 types of controls (divided into 8 for information security and 8 for privacy), 8 risk factors, and 11 types of risk mitigation strategies for the adoption of public cloud services within a university environment. These identified elements have been adapted and mapped to the context of this study and reviewed by experts in the fields of information security, cloud computing, and risk management to enhance the research's credibility.

The third theoretical contribution in proposing an appropriate risk mitigation model in the context of public cloud, as the research of Maniah's [13] and Abed Saif Ahmed Alghawli & Tamara Radivilova's [11] did not discuss the risk mitigation stage. Furthermore, this research can provide a practical prototype representation suitable for implementation models, because the types of threats, risk factors, and mitigation strategies can be used in the prototype. The novelty proposed in this research lies not only in its methodology but also in its technological results, which many organizations can use in implementing public cloud.

In assisting the development of proposed risk mitigation models, a structured framework is needed to maintain compliance and rigor in every stage of the research [11]. The design science research methodology (DSRM) framework is the right choice [15], because it is common and proven to be used in assisting the development of artifacts in the form of models, especially in research related to computer science and information systems. In addition, it is easy to implement and is legitimately well accepted [5].

The first section of this research covers the background, state of the art, research gaps, research questions, the adopted methodology framework, and urgency. The second section relates to the concept of the public and the adopted framework, as well as gaps in detail in previous research models. The third section relates to the research design, data sources, data collection, and analysis techniques. The fourth section presents the results with reference to the research questions and is presented according to the sequence of the DSRM steps. The fifth section interprets the research results in relation to the questions and explains their relationship to related research. The sixth section presents the conclusions, including a summary of the results and discussion, theoretical and practical implications, a brief comparison with related research, the study's limitations, and suggestions for further research.

2. Literature Review

2.1. Public Cloud

Public cloud is a computing technology where IT infrastructure can be configured using only an internet network connection [16]. Public cloud supports IT infrastructure virtualization because, in general, users can configure memory, storage, network connectivity, security, and other IT infrastructure components within the public cloud scope [17]. Public cloud technology is already commonly used in various sectors, such as education, finance, government, retail, banking, health, oil, and gas. Examples of the use of public cloud in general include the retail sector, where it aims to optimize storage of large daily inventory-related data. In the health sector, its use aims to store daily scanned medical documents. In the banking sector, it can help provide sites for digital advertising and store customer data within the public cloud scope [18].

The use of public cloud can provide several general benefits in organizations. According to [19], there are several benefits of using public cloud in organizations, including easily increasing the scalability of IT resources, increasing the efficiency of human resource utilization, easily adapting IT resource needs to types of businesses, reducing hardware dependence, more data backup options compared to physical servers, having the capability to utilize IT resources from all public cloud service providers, and having visibility into what IT resources are used throughout the public cloud environment.

Types of cloud services that can be owned and operated by cloud service providers and can be rented to the public or organizations via the internet. Organizations wishing to rent from cloud service providers do not need to own hardware, because all IaaS, PaaS, and SaaS services can be accessed virtually. The characteristics of public clouds include the ability to share resources, high scalability, and maintenance by the cloud service provider. Examples of public cloud implementations include Google Cloud Platform (GCP), Microsoft Azure, Alibaba Cloud, Amazon Web Services (AWS), and others [18, 19].

2.2. OCTAVE Allegro

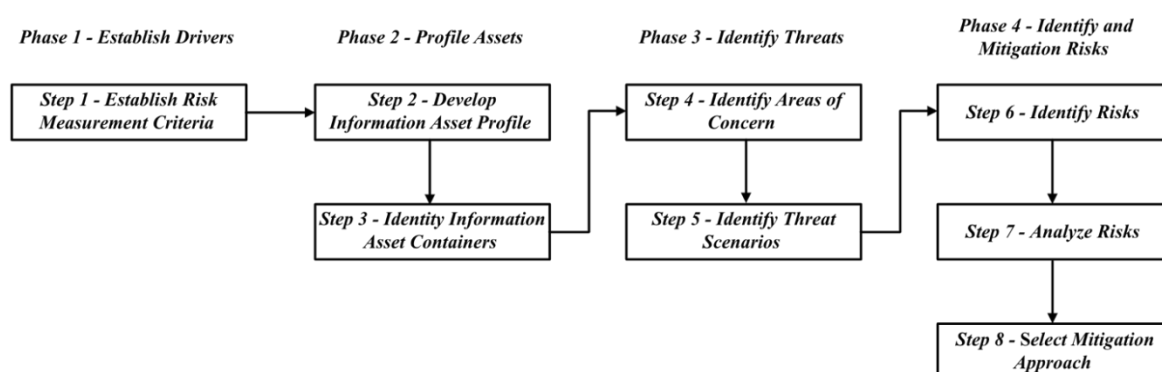


Figure 1. OCTAVE Allegro Steps [20].

OCTAVE (Operational Critical Threat, Asset, and Vulnerability Evaluation) Allegro is a commonly adopted framework for conducting risk assessment and risk mitigation processes within organizational assets [20]. In the context of organizational assets, how can organizations identify, analyze, and evaluate the types of vulnerabilities, threats, and risks that can disrupt and damage organizational assets [21]. Another explanation from [22], that the principles of OCTAVE Allegro can

improve alignment between organizational goals and strategic security plans for organizational assets.

The OCTAVE Allegro framework can help stakeholders reduce bias during risk assessment and risk mitigation processes, as it specifically focuses on security risks within the organization's assets. This can positively impact organizations by making processes more efficient and effective [23]. In addition, the framework has been commonly used in conducting risk assessments and risk mitigation related to public cloud security in organizations [22]. In general, OCTAVE Allegro can provide benefits in organizations [21], including the following: 1) making it easier for stakeholders to develop risk evaluation criteria, 2) making it easier to identify types of threats and vulnerabilities to assets in the organization, and 3) making it easier to identify and evaluate risks that occur within the organization.

Component adjustments in the design must take into account all aspects of the research. This aims to limit the scope of the research model design and generate clear and measurable contributions. The OCTAVE Allegro framework is a suitable choice to assist in the development of this research model, as it is characteristically related to information security, such as confidentiality, integrity, and availability [21]. The framework has also provided examples of instruments for identifying, assessing, and mitigating risks in public cloud environments [20]. It is relevant to smaller organizations by emphasizing information system principles such as people, processes, and technology [24].

2.3. ISO 31000 Framework

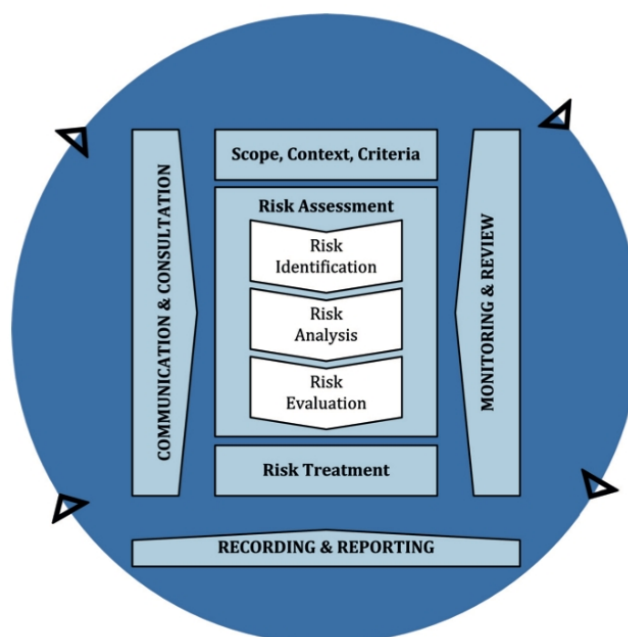


Figure 2. ISO 31000 Framework [25, 26].

OCTAVE Allegro has a perspective related to information security [22]. In the context of research, information security in the adoption of public cloud. However, other aspects are needed to support the development of research models. ISO 31000 has a more general perspective compared to the OCTAVE Allegro framework [27], so it is necessary to combine frameworks in developing research models because the types of risks are not only related to information security, but have different aspects. For example, related to environment [13], and organization aspects [28].

In carrying out business processes and achieving organizational goals, several threats and risks may occur within the organization [27]. Risk management is the most common approach to addressing several threats and risks that exist in an organization. The International Organization for Standardization (ISO) 31000 provides a structured and standardized approach to risk management and is widely used in several other sectors [29]. In addition, it is commonly used in risk management within the cloud computing environment, where, in the context of research, it can be used in risk management related to the public cloud environment [30].

2.4. Related Works

Based on identified research within the scope of risk management and cloud computing, the proposed models are still fragmented and lack comprehensive coverage. Some studies propose more specific models for risk analysis and evaluation, namely, a threat-specific approach with information security requirements and using the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) method [7], and a game theory-based approach to improve information security in organizations [9]. Other studies explore automation and integration of application development in organizations with the Risk-Driven Fault Injection (RDFI) method to test information security resilience in cloud environments [8], as well as an approach capable of automating quantitative risk value calculations with the Factor Analysis of Information Risk (FAIR) framework [11].

A proposed risk analysis model can be applied to cloud-based mobile applications, where there are risk analysis stages to determine the risk values of behavioral patterns and all access rights in each application [10]. In the context of risk analysis, there is a proposed model that is able to analyze risks in web-based logistics applications migrated to the cloud in conditions before, during, and after. However, it does not specifically mention what type of deployment model (public, private, or hybrid) the risk is analyzed for [13]. The latest development is the proposal of a model that is able to analyze risks related to the level of trust and health of the platform (network, memory, and CPU) in applications migrated to the cloud, especially applications connected to IoT devices and has been implemented in smart villages [12].

Adopting cloud computing technology can provide several benefits to organizations, particularly in the public cloud. Common issues include threats and risks within Platform as a Service (PaaS) [11], and Infrastructure as a Service (IaaS) environments [8], particularly in information security [7, 8, 9, 10, 11]. These types of threats and risks can arise before and after the adoption of cloud computing in an organization. Information security is a major concern for stakeholders and is most commonly explored in previous studies, particularly in supporting organizational operations. In general, many organizations have adopted frameworks to mitigate risks in the context of cloud computing. However, the available frameworks for conducting risk assessments are still general and not yet appropriate to the conditions in public cloud.

The general objective is that there are still many studies that propose risk analysis models that can identify types of threats and vulnerabilities [13] and can carry out risk assessments in the scope of Infrastructure as a Service (IaaS) [8] and Platform as a Service (PaaS) [11]. The components proposed in previous studies tend to be related to information security. The most common frameworks adopted in the development of research models, such as the National Institute of Standards and Technology (NIST), are useful in supporting the development of model components

with the Common Vulnerability Scoring System (CVSS) approach [7, 8, 12], and the National Vulnerability Database (NVD) [7, 8, 11].

The CVSS function aims to support the identification of threat and vulnerability types in the form of a matrix [8]. The NVD function aims to serve as a reference for threat and vulnerability types in the context of information security [7], especially related to confidentiality, integrity, and availability (CIA) [22], as well as software and hardware. When implementing the identification stage of assets, threats, and vulnerabilities in the operational scope of cloud, other researchers can refer to the NVD reference source from the NIST framework, so that the identification stage of threats and vulnerabilities to assets owned by the organization becomes faster, because it has been provided with easily accessible information [7].

ISO 31000 is the second most commonly adopted framework for developing model components in other studies, as it relates to risk management in general [6]. Unlike the OCTAVE Allegro and ISO/IEC 13335-1:2004 frameworks, which only focus on information security aspects [21]. Compared with ISO/IEC 13335-1:2004, OCTAVE Allegro is the third-most commonly adapted framework in other studies. Although many studies have adopted and combined several standardized frameworks, such as OCTAVE Allegro [13], NIST [7], and other ISO series [6], few have further explored the risk mitigation model for a public cloud environment. In addition, few studies have explored validating the proposed research model, so its suitability for use in a public cloud remains unknown.

3. Methodology

3.1. Research Design

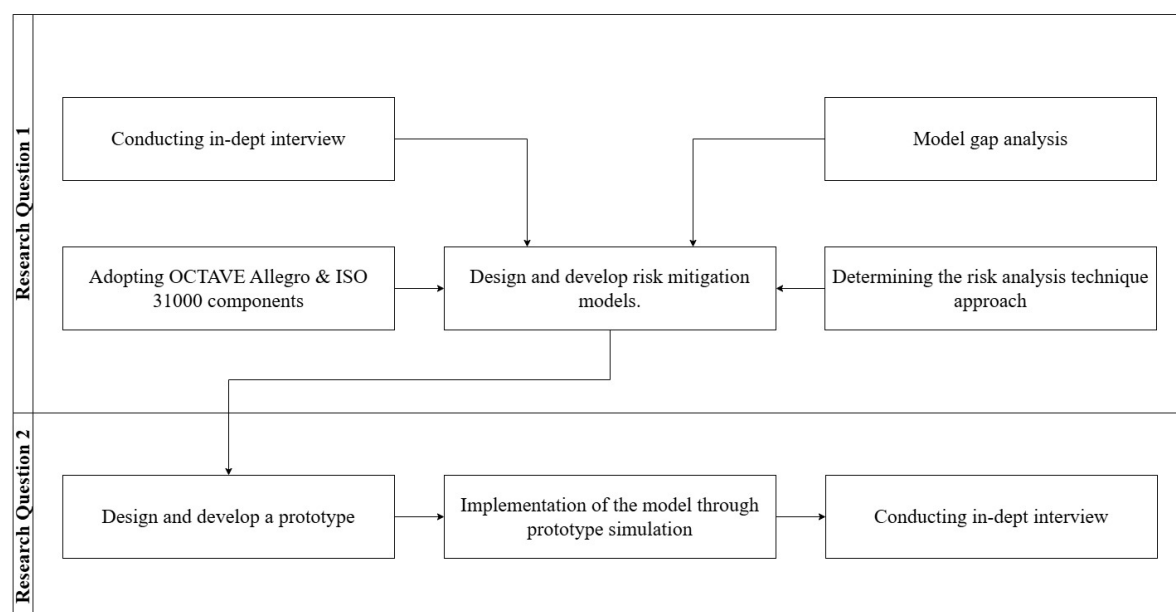


Figure 3. Research Design.

This study adopted a qualitative approach because it can provide in-depth insight into participants perspectives to address the risks of using public cloud in universities in Indonesia. Procedurally, it is more open and flexible, and it can adapt participant criteria to the research context [31]. There are 4,614 higher education institutions in Indonesia, which include private universities, state universities, government-affiliated civil service institutions, and specialized public service universities [32]. Each university has a distinct IT infrastructure, so it is necessary to consider the characteristics of the subjects to ensure the information obtained aligns with the research criteria.

Figure 3 below presents a research design that explains the stages in a structured manner for answering each research question.

3.1.1. Conducting In-Depth Interview

Conducting the in-depth interview stage at the beginning of the research is important to understand the problems that occurred before and after the adoption of the public cloud, as well as to understand these problems from the perspectives of people, processes, and technology in the university environment. The results of the in-depth interview stage at the beginning can be used as material for further rigorous analysis of the problems obtained from the primary source, namely the university, as well as secondary sources from related papers. Meanwhile, the in-depth interview stage at the end aims to determine the suitability and shortcomings of the risk mitigation model proposed in the research, where the model's shortcomings can be evaluated or improved so that the results can be implemented through the development of a prototype [33].

3.1.2. Model Gap Analysis

The results of in-depth interviews at the next stage can be analyzed more closely. Analysis of previous studies is necessary to determine the research position and identify gaps in the development of model components. The previous stage was to search for research published in the last 5 years and identify papers on risk management in public cloud. Next, analysis can be carried out by comparing each proposed model component and by examining the limitations of previous research models to identify opportunities for model renewal, considering the conditions and characteristics of universities in Indonesia [34].

3.1.3. Adoption OCTAVE Allegro & ISO 31000

The research model design process requires a standardized and commonly adopted framework within the scope of cloud and risk management. Based on related research, the NIST framework has been widely adapted for risk management in identifying threats and responding to cyberattacks in the cloud computing scope [7, 11]. However, the NIST framework has general stages and is not as comprehensive as the OCTAVE Allegro and ISO 31000 frameworks. The NIST framework has 4 stages [22], which consist of several stages, including; 1) the first stage functions to determine the risk management strategy, 2) the second stage functions to identify threats, vulnerabilities, potential impacts, and the frequency of risks that occur, 3) the third stage functions to determine the risk handling plan and implementation, and 4) the fourth stage functions to supervise the implementation of the risk.

According to research [22], OCTAVE Allegro has differences such as; 1) the first phase has 1 stage that functions to determine risk criteria, 2) the second phase has 2 stages, where the third stage functions to identify assets and the third stage for asset identification from internal and external aspects, 3) the third phase has 2 stages, where the fourth stage is for identifying the asset area to be identified and the fifth stage is for risk evaluation based on the level of risk frequency and risk impact, 4) the fourth phase has 3 stages, where the sixth stage is for risk identification, the seventh stage is for risk analysis, and the eighth stage is for making a mitigation plan.

The difference between the ISO 31000, NIST, and OCTAVE Allegro frameworks is that ISO 31000 has components that NIST and OCTAVE Allegro do not have, namely monitoring & review, which functions to ensure that risk handling is in accordance with the plan, as well as identifying risks on

an ongoing basis based on the assets owned by the organization, because in principle ISO 31000 is dynamic. The Communication & consultation component involves internal and external stakeholders in communicating risk criteria based on the level of risk occurrence (likelihood) and risk impact (impact) in the adoption of public cloud within the university, which must be adjusted through the in-depth interview stage with the Head of the University's IT Department, so that the results can be used as a reference for further research in the context of the same research in the future [25].

Therefore, it is necessary to adjust the components by considering the university's characteristics and conditions when adopting services (IaaS, PaaS, & SaaS) and deployment models (public cloud), because each university is different and not all components are adapted in this study. The most commonly adopted deployment model by universities is the public cloud, where cloud computing services tend to involve lecturers, staff, and students. The process of designing the research model must be adjusted to the characteristics and conditions of the university, so that it can achieve the suitability of the proposed research model in reducing the risks in the public cloud environment [35].

3.1.4. Determine The Risk Analysis Technique

Risk assessment techniques can refer to previous research or commonly used frameworks. When adopting techniques, one must consider the university's conditions, as universities are nonprofit institutions [36], meaning that many organizations within the university environment lack strong risk management capabilities, especially in the context of cloud computing use. Easy-to-use techniques are needed in implementing risk assessments, so this study adopted semi-quantitative techniques from [37] and [10].

$$R = L * I \quad (1)$$

Where the risk value is obtained from the likelihood level (L) multiplied by the risk impact (I) [37]. The head of a university's IT department can determine the likelihood level based on the likelihood criteria proposed in this study. The process of determining the likelihood level must take into account the specific conditions and characteristics of the university regarding its adoption of public cloud services, particularly concerning the frequency of risk occurrences. The basis for establishing these likelihood levels draws upon previous research that addressed risk assessment implementation for learning systems within higher education. The proposed likelihood criteria consist of five levels: very low, low, medium, high, and very high [37]. However, adjustments are necessary to reflect the university's unique circumstances and characteristics regarding public cloud adoption; therefore, the frequency thresholds proposed in this study should be reviewed, confirmed, and refined in consultation with the head of the IT department.

The basis for determining the risk impact level is adapted from the impact criteria proposed in a study by Putra, A. P., & Soewito, B. [38]. That study suggests impact criteria covering the individual, organizational operations, assets, and national levels. However, the present study excludes the national-level criteria; this decision is based on in-depth interviews with the head of the university's IT department, which indicated that risks with a national-scale impact have never occurred in the context of public cloud adoption within a university that holds an "A" or "Excellent" accreditation.

Consequently, this study incorporates risk impact criteria covering individuals, organizational operations, and assets that have been adapted into application-specific components to better align with the context of applications being migrated to the cloud. The basis for determining the levels or scales of risk impact is derived from previous research; however, further confirmation and refinement

were necessary to ensure their suitability for the risk impact criteria defined in this study. The risk impact levels proposed herein include: very low, low, medium, high, and very high [39].

Furthermore, a method is required to determine risk level classifications in order to ascertain inherent and residual risk values, which can then be mapped to the risk level classifications proposed in this study. The approach for determining these risk level classifications adopts the ISO 27005 standard, which encompasses four categories: low, medium, high, and extreme. Inherent and residual risk values are identified following the risk analysis and mitigation phases; these values are then displayed within a risk matrix—featured in the research prototype's dashboard—where specific colors are used to convey distinct meanings. In the context of this study, the color-coding within the proposed dashboard matrix has been adapted from previous research [37] and aligned with the color-based classifications defined in the ISO 27005 standard [40].

In that standard, the color used for the "low" risk level classification is yellow, whereas this study has adopted green for the "low" risk level classification. For the "moderate/medium" risk level classification, the standard uses amber, and this study has adopted the same color for the "medium" risk level classification. For the "high" risk level classification, the standard uses orange, and this study has likewise adopted this color for the "high" risk level classification. Furthermore, this study has adopted the color red to clearly designate the "extreme" risk level classification [40].

The results of the model's design and development can be implemented through a web-based prototype simulation. A prototype is a commonly used approach in model validation, aimed at determining the suitability of components for the university's cloud computing environment [41]. In addition, it can determine the [13] effectiveness in reducing the risk values of cloud use and the potential operational impacts in the university environment [37]. The prototype was developed using the CodeIgniter PHP framework. The working method is structured, easy to maintain, and can be developed to meet future needs [42].

3.1.5. Design & Develop Risk Mitigation Model

Based on the risk value analysis technique determined and referenced in related research [37], the calculation process can produce risk values based on the assets owned. In this context, assets in the form of supporting applications such as databases, virtual machines, networking, and others are considered, and the risk value can be low, medium, high, or extreme under conditions before and after the adoption of public cloud in the university environment [40].

The developed model components are sourced from previous studies. In general, many studies have developed model components from the NIST framework [7, 8, 9, 12], ICASA [13], ISO 31000 [13], OCTAVE Allegro [13], and ISO/IEC 13335-1:2004 [9]. The development of model components must be based on the conditions and characteristics of universities' cloud use, so not all components are adopted from these frameworks.

In developing the model components, the OCTAVE Allegro framework was adopted, because many organizations are very concerned about information security, due to the many types of threats that appear in the cloud environment [22]. In addition to OCTAVE Allegro, ISO 31000 is an option because it provides general principles and guidelines for organizations seeking to identify, assess, and mitigate risks associated with the use of public cloud in universities [32].

The proposed research model is divided into three main phases. The first phase of initiation aims to identify the list of assets, types of threats, and controls in the adoption of public cloud within the university. The second phase of assessment aims to conduct a risk assessment using risk analysis

techniques determined in the research [37]. The third phase of mitigation aims to carry out the risk mitigation process by determining and planning mitigation strategies, as well as implementing and monitoring the mitigation plan implemented in the adoption of public cloud within the university. The proposed mitigation phase is an update of the research [13], and continues the previous research [12].

3.1.6 Design & Develop Prototype

Before designing and developing a prototype, the first step is to determine the system functionality to model user interaction with the application being developed. Use case diagrams are one of the tools and are included in the unified modeling language (UML) [43]. There are several functions of use case diagrams as follows [43]: 1) mapping what users can do and how the system responds, 2) determining which actors/users can use the system, and 3) being a reference for application developers in creating detailed application features. The difference in user roles between the Head of IT and the Administrator is only in managing user accounts.

3.1.7. Implementation Model with Prototype Simulation

Simulation scenarios are carried out by entering data into the modules available in the prototype and must reflect real conditions and characteristics within the university [43]. The purpose of the simulation is to determine the suitability of the proposed model components through prototype simulation [44]. The simulation scenario can be carried out by migrating several application support assets, such as application project files, virtual machines, databases, and others, to the cloud environment, which corresponds to the main phases of initiation, implementation, and mitigation.

In the context of research, it only goes as far as testing the functionality of the prototype's use [45]. Through the stages of identifying assets based on threats, analyzing risks using the specified method, and risk evaluation, which aims to determine which assets have the highest total risk based on conditions before and after the adoption of the public cloud within the university. In addition, users must go through the stages of risk mitigation scenarios, such as selecting which assets should be mitigated, preparing mitigation plans based on recommendations from the literature [46], implementing risk mitigation, and monitoring and reviewing follow-up mitigation measures.

3.2. Data Sources

The data sources in this study are divided into two parts: primary data and secondary data. Primary data were obtained through in-depth interviews with five practitioners in risk management, information security, and/or cloud computing. The group of practitioners includes one individual who holds a doctorate in computer science and possesses 35 years of experience in risk management and cybersecurity. Three individuals hold master's degrees in information technology and have over 15 years of experience in cloud computing and cybersecurity. One individual holds a bachelor's degree in informatics engineering and has 9 years of experience in risk management.

Furthermore, there are 6 heads of IT departments at universities that have adopted public cloud computing with institutional accreditation rated "Excellent " or "A". The selected universities are in the Province of Jakarta (3 universities), Central Java Province (2 universities), and East Java (1 university). The criteria were selected using a purposive sampling method because this method intentionally selects samples that meet the criteria, characteristics, or considerations specifically discussed in this study [47].

Secondary data were obtained from research sources, including journal papers and proceedings indexed by Scopus, with a credible reputation. One of the theoretical contributions of this research is to develop types of threats, risk factors, and mitigation strategies appropriate to the context of public cloud adoption in the university environment [46], which have been adjusted through in-depth interviews with practitioners and heads of university IT departments. In addition, the aim was to compare the results of the information obtained regarding public cloud adoption problems with the results of in-depth interviews with heads of university IT departments and reference sources referring to journals and proceedings.

3.3. Data Collection

This section contains two in-depth interviews: the first to identify initial issues and the second to evaluate the model during the demonstration phase. The purpose of the in-depth interviews with practitioners was to determine the alignment of the risk mitigation model with the principles and stages of the adopted framework. Meanwhile, the purpose of the in-depth interviews with six university IT department heads was to identify issues before and after public cloud adoption from the perspective of people, processes, and technology. The in-depth interviews to identify these issues were conducted online and lasted one hour with six university IT department heads.

The information gathered through initial interviews with 5 practitioners and 6 university IT department heads can be integrated into the development of a risk mitigation model—specifically one tailored to the unique characteristics of universities adopting public clouds, while aligning with the principles of the ISO 31000 standard. For instance, components concerning the identification of threats and controls, risk factors, and mitigation strategies can be linked to the "integrated" principle; this is because the threats and risks arising within a university's cloud infrastructure differ from those in other sectors, necessitating more rigorous adjustments when implementing controls and mitigation strategies to reduce the impact of potential threats and risks [48].

The in-depth interviews for the model evaluation were conducted online and lasted one hour and consisted of two sessions. The first session lasted 30 minutes and explained all model components, including their definitions, objectives, and characteristics. The second session included a 30-minute prototype simulation to assess the alignment of the proposed model components with the prototype modules.

Feedback from five practitioners and six university IT department heads regarding the evaluation of the model and prototype can also be linked to the principles and characteristics of public cloud adoption within a university setting. For instance, interview findings can assist in determining the sequence of phases for developing a risk mitigation model that aligns with the "structured and comprehensive" principle of the ISO 31000 standard. Furthermore, these insights can support the implementation of the "continual improvement" principle, ensuring that the outcomes of risk identification, assessment, and mitigation serve as lessons learned for future risk management implementation processes [48].

3.4. Analysis Techniques

The management method can be conducted using a thematic analysis approach, in which the results of in-depth interviews can be grouped based on contexts appropriate to IT infrastructure problems in on-premises and public cloud environments [49]. Data and information are analyzed by identifying frequently occurring sentences and compiled into a list of problems that are conditions

before and after the adoption of public cloud at the university level. The problems explored relate to the types of threats that arise, the controls used by the university IT department, and the risks that have an operational impact within the scope of cloud computing infrastructure.

Raw data and information recorded in a notes application and written on paper can facilitate in-depth and concise analysis, ensuring that the results are contextualized. The evaluation phase yields input and suggestions on the proposed mitigation model components and prototypes, enabling further refinement based on the university's conditions and characteristics for adopting the public cloud. This allows for iteration from the evaluation phase to the design and development phase, or to the goal-and-solution determination phase [33]. The plan for the entire evaluation methodology must be precisely defined to ensure the reliability of the research outcomes. Therefore, it must be executed through structured and rigorous stages. Table 1 below outlines the aspects, methods, and scope of this research.

Table 1. Evaluation Plans.

No.	Aspects	Methods	Scopes
1	Proposal for the identification and mapping of threat types, controls, risks, and mitigation strategies	In-depth interview, thematic analysis, member checking, & expert scoring	Limited to identifying types of threats and controls within the realm of information security and privacy
2	Proposed risk mitigation model	In-depth interview	Not all stages/phases from OCTAVE Allegro and ISO 31000 are adapted, as they must be aligned with the characteristics and principles of public cloud adoption within a university environment
3	Prototype	Simulation	The simulation was conducted for only one e-learning application migrated to the cloud at each university; specifically, this study presents a single scenario at University XYZ and does not implement a risk mitigation monitoring component using actual data, as doing so would require additional costs and concrete supporting evidence

4. Results

4.1. Problem Identification & Motivation

Based on the results of in-depth interviews with 6 heads of IT departments at each university, a summary of on-premises IT infrastructure problems across the people, process, and technology dimensions is presented in Table 2 below.

Table 2. University IT Infrastructure Issues in The On-Premise Environment.

Aspect	Identified Problems	Current Impacts
People	Lack of oversight in software updates, due to limited administrator time availability	Administrators cannot access virtual machines and applications
Process	There is no standardized guide from the IT department regarding how to maintain IT infrastructure	Still dependent on one person, so that knowledge is not spread, and it takes quite a long time to solve the problem

Aspect	Identified Problems	Current Impacts
Process	There are still a few who adopt information security and privacy standards for IT infrastructure in the on-premises environment	The controls implemented by the IT department are not up to standard, making it difficult to resolve problems when new threats arise.
Technology	High hardware maintenance costs	Difficulties in increasing the scalability of IT infrastructure
Technology	Server physical memory is vulnerable to damage	Virtual machine and applications cannot be accessed
Technology	Unable to handle a large number of requests from users	Application access speed becomes slow, and availability is disrupted

Cloud computing technology can help organizations and other industries meet their IT infrastructure needs by providing services tailored to their specific requirements and conditions [50]. However, based on the results of in-depth interviews with several heads of IT departments at universities, a summary of problems and impacts in the public cloud within the university is presented, including those shown in Table 3 below.

Table 3. Public Cloud Issues in The University Environment.

Aspect	Identified Problems	Current Impacts
People	Lack of attention to privacy	Employees who have resigned still have access to the control
People	Too long adaptation	Lack of knowledge regarding the types of threats that arise
Process	There are no standards in the university context for assessing and mitigating risks	Difficulty in mitigating if risks occur
Process	Not having cost planning in cloud adoption	High monthly billing costs
Process	High security support costs	The university IT department is improving security independently without following standards
Technology	Prone to configuration errors	Virtual machine in the cloud is having problems
Technology	The many types of threats in the public cloud environment	Application availability is disrupted

Several internal, external, and both applications (internal and external) are being migrated to the cloud computing environment such as, e-learning (internal), web portal (internal & external), academic (internal), registration admission (external), e-library (internal & external), and research & community services (internal). Several types of threats can arise in the cloud computing environment [46]. However, they have not been adapted to the conditions and characteristics of universities adopting public cloud services, including IaaS, PaaS, and SaaS, and have not been classified in terms of information security and user privacy.

Table 4 presents various types of threats, ordered according to their probability of occurrence. Before establishing this order, the initial step involved identifying potential threats based on previous research [46]. While that research identified 20 types of threats, only 9 were adapted for this study. This selection was made to align with the specific conditions and characteristics of universities adopting public cloud services, specifically those accredited as "A" or "Excellent" by the Indonesian government.

The adjustment process was carried out through in-depth interviews to identify the types of threats and the frequency of their occurrence within the university environment. Feedback provided

by the head of the IT department helped ensure the validity of the findings. It allowed for the categorization of the nine identified threat types into two domains: information security and privacy [35]. The second stage involved ranking these mapped threats categorized by information security and privacy aspects based on their frequency of occurrence. The total frequency was normalized to 100% to illustrate the relative proportion of each of the nine identified and mapped threat types.

Furthermore, the in-depth interview phase also ensures reliability through an expert scoring technique, in which practitioners are asked to evaluate the alignment between the identified and mapped threats and the established categories of information security and privacy. The Content Validity Index (CVI) method was adopted for this purpose, as it facilitates the assessment of content validity based on the mapping results [51].

During the interview process, each practitioner was presented with the identified threats and asked to rate them on a scale of 1 to 4 (1 = not relevant, 2 = somewhat relevant, 3 = quite relevant, and 4 = highly relevant). Subsequently, the Item-level Content Validity Index (I-CVI) was calculated for each specific type of threat. The I-CVI is determined by the number of practitioners (5 participants) who provided a score of 1, 2, 3, or 4 [51]. If all practitioners assign a score of 3 or 4, the I-CVI value is 1.00, indicating that all experts are in agreement regarding a particular type of threat. As shown in Table 4 below, the I-CVI values for all identified threats are 1.00, which indicates that the identification results are credible.

Table 4. Threat Type Identification Results Based on In-Depth Interviews [46].

ID	Categories	Threat Types	Probability of Threat Occurrence	References	Expert Scoring (Participant 1-5)	I-CVI
KN1	Information security	Website defacement	24%	[30, 35, 52, 53, 54, 55, 56, 57] [16, 28, 52, 53, 58, 59, 60, 61, 62, 63]	4, 4, 3, 4, 3	1.00
KN2	Information security	Denial of service (DoS) attacks	20%	[3, 30, 54, 56, 57, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75]	3, 3, 4, 3, 4	1.00
KN3	Information security	Access control issues	15%	[16, 28, 30, 35, 55, 56, 67, 70, 71, 76, 77, 78, 79]	4, 4, 4, 3, 3	1.00
KN4	Information security	Malware	12%	[16, 28, 35, 52, 53, 54, 59, 61, 62, 71, 80, 81] [30, 55, 56, 57, 67, 70, 71, 74]	3, 3, 3, 4, 4	1.00
KN5	Information security	Interface and API issues	10%	[16, 17, 28, 35, 50, 57, 68, 69, 75, 82, 83, 84, 85, 86]	4, 3, 3, 3, 4	1.00
KN6	Information security	Service hijacking	7%	[3, 35, 54, 55, 56, 57, 59, 63, 67, 70, 71, 76, 87, 88]	4, 4, 3, 4, 4	1.00
KN7	Privacy	Data leakage	6%	[3, 30, 52, 53, 56, 57, 58, 83]	3, 4, 4, 4, 3	1.00
KN8	Information security	Abuse and nefarious	4%	[30, 52, 54, 55, 56, 70, 71, 79, 89]	3, 3, 3, 4, 4	1.00

ID	Categories	Threat Types	Probability of Threat Occurrence	References	Expert Scoring (Participant 1-5)	I-CVI
KN9	Privacy	Data loss	2%	[3, 27, 30, 35, 52, 56, 58, 59, 67, 70, 71, 76, 77, 81, 88]	3, 3, 4, 3, 4	1.00

Based on Table 5, risk factors have been identified from previous research [46]. 8 risk factors can arise in the university public cloud environment, and the identification results have been adjusted and mapped to the types of threats in this study. Risk factors not included in the study are financial factors and errors in selecting cloud services. These results have been confirmed through an in-depth interview process with 6 Heads of IT Departments at universities in Province of Jakarta (3 universities), Central Java Province (2 universities), and East Java (1 university).

Table 5 below employs the same methodology used for the previous identification of threat types. However, it incorporates an additional question posed to all practitioners regarding the alignment between the identified threat types and the risk categories within this study. The expert scoring results for each risk category yielded an average score of 3 to 4, resulting in an I-CVI (Item-level Content Validity Index) value of 1.00 for all risk categories [51]. This indicates that the identification and mapping results are reliable and can therefore be adopted by university IT department heads for the implementation of a risk mitigation model via the proposed prototype.

Table 5. List of Risk Factors in The University Public Cloud [46].

ID	Risk Types	Threats ID	References	Expert Scoring (Participant 1-5)	I-CVI
KR1	Information security	KN1, KN2, KN3, KN4, KN5, KN6, KN8	[3, 16, 28, 30, 52, 53, 54, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75]	3, 4, 3, 4, 4	1.00
KR2	Locked access control	KN3	[17, 28, 35, 50, 53, 57, 62, 69, 71, 73, 85, 90, 91]	3, 4, 3, 4, 3	1.00
KR3	Compliance with various regulations and laws	KN7	[3, 35, 54, 55, 56, 57, 59, 63, 67, 70, 71, 76, 87, 88]	3, 4, 4, 3, 3	1.00
KR4	Configuration errors	KN5	[3, 27, 30, 35, 52, 56, 58, 59, 67, 70, 71, 76, 77, 81, 88]	4, 4, 3, 3, 3	1.00
KR5	Privacy	KN7, KN9	[16, 28, 30, 35, 55, 56, 67, 70, 71, 76, 77, 78, 79]	3, 3, 4, 3, 3	1.00
KR6	Virtual machine usage	KN3, KN5, KN6,	[16, 30, 35, 52, 54, 56, 57, 67, 70, 79]	4, 3, 4, 3, 3	1.00
KR7	Malicious insiders	KN5	[28, 30, 35, 52, 56, 59, 62, 79, 80, 81]	4, 3, 3, 4, 4	1.00
KR8	Loss of reputation	KN1, KN2, KN3, KN4, KN5, KN6, KN7, KN8, KN9	[30, 55, 56, 57, 67, 70, 74, 78, 92]	3, 3, 4, 4, 4	1.00

4.2. Define Objective & Solution

Based on problems identified from in-depth interviews and previous research, the output of the first research question is a proposed risk mitigation model aimed at reducing risk for universities that want to or have already adopted cloud computing. In addition, it can help university IT departments reduce potential risks by leveraging the proposed model's three main phases: initiation, assessment, and mitigation. The proposed mitigation phase was not identified in previous studies, as shown in Table 6.

Table 6. Comparison of Components from Previous Models.

Title	Initiation Phases	Assessment Phases	Mitigation Phases
Design and implementation of a threat-specific security risk assessment tool	Nodes & edges	Risk reports	-
CloudStrike: chaos engineering for security and resiliency in cloud infrastructure	Chaos controller, chaos manager, fault engine, fault injector, & chaos monitor	Chaos analyzer	-
Design of basic process of information security risk assessment in cloud computing environment	Risk data statistics & model building	Risk calculation	-
On the characterization and risk assessment of AI-powered mobile cloud applications	Characterize the system, identify threat conditions, classify threat conditions, assess the impact of threats, & determine the likelihood of threats	Compute gross risks, identify security controls, & calculate net risk	-
Risk assessment for logistics applications in cloud migration	Identify assets, threats, and vulnerabilities, asset and threat mapping, & determine risk environment	Establish risk measurement, calculate asset weight, & calculate total risk	-
Resilient cloud cluster with DevSecOps security model, automates a data analysis, vulnerability search and risk calculation	Identification of assets and threats	Assessing the frequency of threats, calculate of losses, & calculate risk	-
Holistic Cyber Risk Assessment in the Cloud		Domain network assessment (cloud native, network, service assessment & vulnerability assessment), trust assessment (platform, IoT monitor, edge monitor, cloud monitor), annotation layer, and risk assessment layer	-
Continuum: A Multi-Layer, Multi-Domain Approach	-		-

Title	Initiation Phases	Assessment Phases	Mitigation Phases
From Design to Evaluation: A Novel Mitigation Model for Public Cloud Adoption	Asset identification, threat types identification, & control types identification	Threats & controls mapping, risks identification, determine risk tolerance, & risk analysis in cloud computing adoption	Determine risk treatment strategy, determine risk treatment plan, & risk mitigation monitoring

In addition to the proposed new components related to the mitigation phase, there are other scientific contributions to the types of controls from the information security and privacy aspects. Table 7 below presents a reference list of control types in the context of information security and privacy, with reference to the ISO/IEC 27017 [93], and ISO/IEC 27701 framework [94], and has been adapted to the conditions and characteristics of universities in adopting public clouds. The types of controls that have been identified have been adapted and mapped based on the types of threats shown in this study.

ISO/IEC 27017 is an extension of ISO/IEC 27002, which focuses on providing detailed guidance in determining, implementing, and controlling practices in securing information security-related assets. ISO/IEC 27002 consists of 93 controls grouped by organization (37 controls), people (8 controls), physical (14 controls), and technology (34 controls) [93]. However, of the 93 types of controls, some are still general and require adjustments based on the conditions and characteristics of the university. Justification is needed from practitioners and heads of the university's IT department so that the 93 types of controls can be readjusted through the in-depth interview stage, with the aim of finding out what types of controls are commonly used/applied when a threat occurs in the public cloud environment.

ISO/IEC 27701 It is an extension of the ISO/IEC 27001 framework. ISO/IEC 27701 can help organizations comply with the personal data protection Law No. 27 of 2022 [95]. The characteristics of ISO/IEC 27701 have 2 types of control, namely data controller (PII controller) and data processor (PII processor) [94]. In the context of this research, the data controller is the university IT department. In contrast, the data processor is the cloud service provider, such as Google Cloud Platform (GCP), Amazon Web Services (AWS), and Alibaba Cloud, where the cloud service provider has been identified based on the results of an in-depth interview with the head of the university IT department.

However, the focus of this study is only to identify the types of controls from the data controller's side, because the main objective of this study is to propose a risk mitigation model, one of the benefits of which is to help the university's IT department identify the types of threats and controls based on applications that will be/have been migrated to the cloud. In addition, this study does not focus on identifying the types of controls from the data processor's side (cloud service provider).

Table 7 below employs the same methodology and scale used for identifying threat and risk types; however, it presents a question posed to all practitioners regarding the appropriateness of the identified and mapped controls in relation to the identified threats, as well as to aspects of information security and privacy. Expert scoring for the identified controls yielded values of 3 or 4. Furthermore, the I-CVI (Item-level Content Validity Index) values for each control type were found to be 1.00, indicating that the identification and mapping of these controls are reliable [51]. These identified controls can be adopted by university IT department heads to implement appropriate measures for the use of public clouds—particularly for applications that have already been migrated.

Table 7. List of Control Types in Information Security and Privacy Aspects [46].

ID	Control Types	Aspects	Threat Types ID	Reference	Expert Scoring (Participant 1-5)	I-CVI
KK1	Information Access Restriction	Information security	KN3	[93]	3, 4, 3, 4, 3	1.00
KK2	Access to Networks and Network Services	Information security	KN2, KN6, KN8	[93]	3, 4, 3, 3, 4	1.00
KK3	Administrator and operator logs	Information security	KN3	[93]	4, 3, 3, 4, 3	1.00
KK4	Backup and Restoration Control	Information security	KN9	[93]	4, 3, 3, 4, 4	1.00
KK5	Event Logging	Information security	KN3	[93]	4, 3, 4, 4, 4	1.00
KK6	Information Security Incident Management	Information security	KN1, KN2, KN3, KN4, KN5, KN6, KN8	[93]	3, 4, 4, 4, 4	1.00
KK7	Policies for information security	Information security	KN1, KN2, KN3, KN4, KN5, KN6, KN8	[93]	4, 4, 3, 4, 3	1.00
KK8	Inventory of Assets	Information security	KN1, KN5, KN9	[93]	4, 3, 4, 3, 4	1.00
KK9	Retention	Privacy	KN3, KN7	[94]	3, 4, 3, 3, 4	1.00
KK10	Limit Collection	Privacy	KN3, KN7, KN9	[94]	4, 4, 4, 3, 3	1.00
KK11	Limit Processing	Privacy	KN3, KN7	[94]	4, 3, 4, 3, 4	1.00
KK12	Disposal	Privacy	KN7, KN9	[94]	3, 4, 3, 4, 4	1.00
KK13	Accuracy and Quality	Privacy	KN3, KN7	[94]	4, 4, 3, 4, 3	1.00
KK14	PII De-identification and Deletion at the End of Processing	Privacy	KN3	[94]	4, 4, 3, 4, 4	1.00
KK15	PII Transmission Controls	Privacy	KN3, KN5	[94]	3, 4, 4, 4, 3	1.00
KK16	PII Minimization Objectives	Privacy	KN7	[94]	4, 4, 3, 3, 3	1.00

The research contribution not only identifies the types of threats, controls, and risk factors, but also generates mitigation strategies that can be used to implement the proposed model through prototype implementation. The mitigation strategies refer to previous research with 13 types of risks [46], but only 11 types of strategies were adapted in this study. This means that there are two types of mitigation strategies that are not used, such as honeypots and validation of cloud service provider certificates before public cloud adoption.

Furthermore, the validation phase for the identified mitigation strategies employs the same method: expert scoring. Five practitioners were asked to evaluate the alignment between the identified mitigation strategies and the corresponding risk types. The expert scoring results show that, on average, participants assigned a score of 3 or 4, and the I-CVI value reached 1.00, indicating that the identified mitigation strategies are reliable [51]. These identified mitigation strategies

contribute to providing recommendations for the head of the university IT department regarding the implementation of a risk mitigation model via a prototype. Table 8 below presents the types of risk mitigation strategies adapted to the context of public cloud adoption within a university environment.

Table 8. List of Risk Mitigation Strategies in Public Cloud Adoption [46].

ID	Mitigation Strategies	Risks ID	References	Expert Scoring (Participant 1-5)	I-CVI
M1	Consistent network monitoring	KR1, KR7	[3, 39, 58, 65, 68, 70, 71, 89, 91]	3, 4, 4, 3, 3	1.00
M2	Intrusion prevention	KR1, KR4, KR7	[53, 59, 65, 67, 70, 71, 82, 96]	4, 4, 3, 4, 3	1.00
M3	Consistently monitored identity and access management	KR1, KR5, KR7	[53, 59, 67, 70, 71, 80, 81, 89] [65, 71, 80]	4, 3, 4, 3, 4	1.00
M4	Encryption and authentication	KR1, KR2, KR5, KR6, KR7	[53, 67, 73, 78, 81, 83, 87]	4, 3, 4, 4, 4	1.00
M5	Distributed Denial of Service (DDoS) detection	KR1, KR4	[59, 64, 67, 68, 69, 71, 96, 97] [71, 81, 90]	3, 3, 4, 4, 4	1.00
M6	Enhancing security based on confidentiality, integrity, and availability	KR1, KR2, KR4, KR5, KR6, KR7, KR8	[3, 53, 67, 70, 74, 81, 87, 90, 91, 97]	4, 4, 3, 3, 4	1.00
M7	Monitoring the availability of supporting software and applications in the cloud computing environment	KR1, KR2	[65, 70, 80, 81, 89]	4, 4, 3, 4, 4	1.00
M8	Backing up data and ensuring that backed-up data can be restored properly	KR1, KR5	[71, 73, 81, 89]	3, 4, 4, 3, 4	1.00
M9	Designing virtual machine allocation policies	KR6	[67, 81, 90]	4, 3, 4, 4, 4	1.00
M10	Organizations should conduct training sessions on security and privacy prevention, as well as awareness for each individual	KR1, KR3, KR5	[67, 70, 81]	4, 3, 4, 3, 3	1.00
M11	Scanning for threats in the cloud environment	KR1, KR6	[68, 70, 91]	4, 3, 3, 4, 4	1.00

4.3. Design & Development

Based on the model development process in this study, a mapping of stages/phases has been created, adapted by considering three key aspects. First, the adapted stages/phases have been organized into components of the risk model, ensuring that the proposed components can be implemented as distinct modules within a prototype. Second, the model development has been tailored to the specific characteristics of universities adopting public clouds, as well as the principles inherent in the frameworks; consequently, not all stages from OCTAVE Allegro or phases from ISO 31000 have been incorporated. Third, the development process involved analyzing the limitations of the existing framework stages/phases, allowing for the weaknesses in OCTAVE Allegro to be addressed through the inclusion of elements from ISO 31000. The resulting mapping is presented in Table 9 below.

Table 9. Mapping of Adapted Components.

No.	Proposed Components	Steps Adapted in OCTAVE Allegro	Phases Adapted in ISO 31000	Alignment of Principles in ISO 31000 (Point a-h)
1	Identification of asset list	Develop information asset profile	There is no explicit equivalent	b) Structured and comprehensive, d) Inclusive, & g) Human and cultural factors
2	Identification of threat types	Identify threat scenarios	There is no explicit equivalent	b) Structured and comprehensive, f) Best available information, c) Customized, & d) Inclusive
3	Identification of control types	Identify threat scenarios	There is no explicit equivalent	b) Structured and comprehensive, c) Customized, d) Inclusive, & f) Best available information
4	Threat mapping and asset control	Identify threat scenarios	There is no explicit equivalent	b) Structured and comprehensive, d) Inclusive, & g) Human and cultural factors
5	Identification of risk	Identify risks	Risk identification	b) Structured and comprehensive, & d) Inclusive
6	Determine risk target	Identify risks	Risk identification	b) Structured and comprehensive, & d) Inclusive
7	Risk analysis in public cloud adoption	Analyze risks	Risk analysis	a) Integrated, b) Structured and comprehensive, c) Customized, d) Inclusive, e) Dynamic, & f) Best available information
8	Determine risk treatment strategy	Select mitigation approach	Risk treatment	a) Integrated, b) Structured and comprehensive, Inclusive, e) Dynamic, & g) Human and cultural factors
9	Determine risk treatment plan	Select mitigation approach	Risk treatment	a) Integrated, b) Structured and comprehensive, c) Customized, d) Inclusive, e) Dynamic, & f) Best available information
10	Risk mitigation monitoring	There is no explicit equivalent	Monitoring & review	a) Integrated, b) Structured and comprehensive, d) Inclusive, e) Dynamic, h) Continual improvement

Before implementing the mitigation model in a prototype, it is necessary to determine the levels of risk, such as low, moderate, high, and critical [40]. In addition, determine the criteria for the likelihood of threat and risk impact, which can be related to the risk assessment aspects in this study, such as the aspects of information security and privacy in the adoption of cloud computing in the university environment. The likelihood criteria in this study are based on the frequency of occurrence of various threat types in the public cloud, from an information security and privacy perspective. Table 10 shows the likelihood criteria based on the frequency of risk occurrences [37], with several levels: very low (very unlikely), low (unlikely), medium (possible), high (likely), and very high (frequent).

The process of establishing likelihood criteria in this study consists of two stages. The first stage involves defining a likelihood scale, adapted from relevant research that addresses risk assessment within the context of cloud-based learning systems in higher education. The second stage entails determining the frequency of risk occurrence, which is verified through in-depth interviews with the heads of IT departments at six universities. Subsequently, a synthesis is performed by comparing the frequency of risk occurrences across these universities in the context of public cloud adoption. A one-semester timeframe was selected because it facilitates the alignment of evaluation processes within the universities' internal institutional frameworks [37].

Table 10. Likelihood Criteria.

Value	Scale	Description
1	Very low	Frequency in 1 semester 1 times
2	Low	Frequency in 1 semester 2 times
3	Medium	Frequency in 1 semester 3 times
4	High	Frequency in 1 semester 4 times
5	Very high	Frequency in 1 semester more than 5 times

In addition to the likelihood criteria, Table 11 presents the risk-impact criteria from a security and privacy perspective in the cloud computing domain, adopted and modified from the research. In determining the risk impact criteria, they must be adjusted to the conditions and characteristics of public cloud adoption across several universities, and they have also been confirmed with the IT department head through in-depth interviews. In Tables 11, there are 5 scales: very low, low, moderate, high, and very high [38].

The method for determining impact criteria in this study is quite similar to the approach used for establishing likelihood criteria; however, the distinction arises during the in-depth interview process, specifically when posing questions to the heads of university IT departments regarding the types of impact (encompassing operational aspects, application components, and individuals) and the scale of the risks associated with the adoption of public cloud services.

Table 11. Impact Criteria.

Value	Scale	Description
1	Very low	The impact of risks to information security and privacy in organizational operations, application components, and/or individuals is very low
2	Low	The impact of risks to information security and privacy in organizational operations, application components, and/or individuals is low
3	Medium	The impact of risks to information security and privacy in organizational operations, application components, and/or individuals is medium
4	High	The impact of risks to information security and privacy in organizational operations, application components, and/or individuals is high
5	Very high	The impact of risks to information security and privacy in organizational operations, application components, and/or individuals is very high

The risk mitigation model consists of three main phases, as illustrated in Figure 4: initiation, assessment, and mitigation. All components have been tailored to the specific conditions and characteristics of universities adopting public cloud services. The initiation phase comprises several components: asset identification, identification of threat types, and identification of control types. The assessment phase includes components such as threat mapping and asset control, risk identification, determination of risk targets, and risk analysis within the context of public cloud adoption. The mitigation phase, which receives the most focus, as it represents the primary proposal and core

contribution of this research, encompasses components such as determining risk treatment strategies, establishing risk treatment plans, and monitoring risk mitigation efforts.

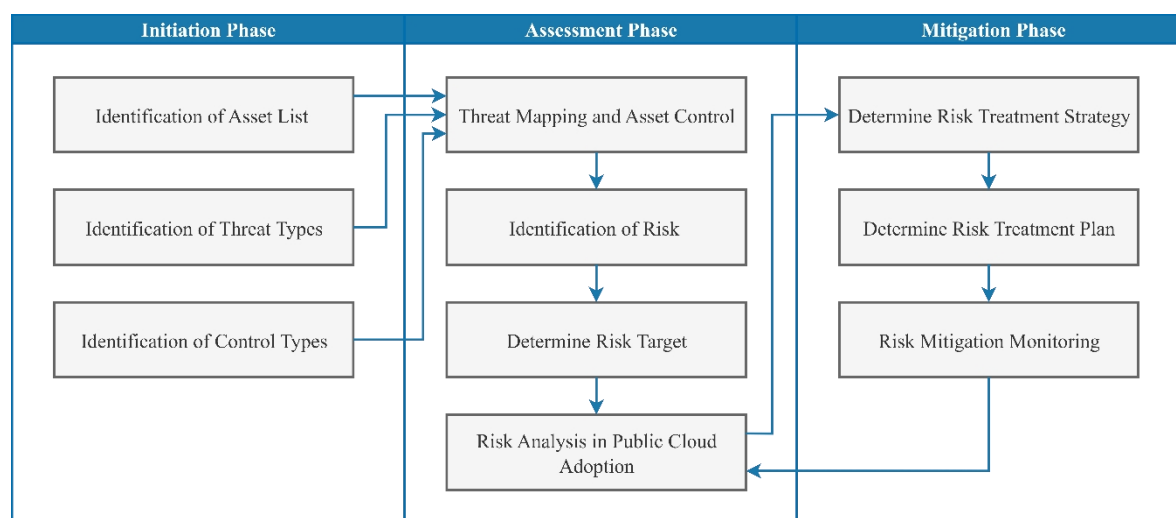


Figure 4. Risk Mitigation Model for Public Cloud Adoption in Universities.

Assets owned by the university must be identified before migrating to a cloud environment; not all assets are migrated because this impacts IT resources and costs, which the IT department must consider. In addition, the risks and potential impacts that may arise are not yet known, so further analysis and consideration are needed for migration to a cloud environment [2]. The threat types identification component aims to identify threats in the public cloud environment, particularly in IaaS, PaaS, and SaaS services, so that threat types can be mapped to appropriate controls for the university environment [13]. In identifying the types of threats, they are divided into 2 aspects, namely information security and privacy, where examples of types of information security threats [77, 98], are interface and API issues, platform misconfiguration, malicious insiders, denial of service, system vulnerabilities, and others.

Meanwhile, examples of privacy threats identified in research [99], include leakage-resistant data, complete data deletion, personally identifiable information (PII), sensitive data, location, and others. In this study, the types of controls can refer to the ISO/IEC 27017-2015 framework, as it has been adapted to information security aspects within the scope of cloud services, especially IaaS, PaaS, and SaaS [93]. The assessment phase includes several components: threats and controls mapping, risks identification, risk target determination, and risk analysis in cloud computing adoption. The development of the threats and controls mapping component draws on previous research [13]. The objective of this component is to map which assets are at risk in the public cloud based on each university's conditions and the types of controls currently implemented.

The mitigation phase is a key component that differs from the proposed model in previous research [73]. This phase consists of several components, including determine risk treatment strategy, determine risk treatment plan, and monitoring risk mitigation. The determining risk treatment strategy component aims to determine the choice of mitigation strategies such as avoidance, acceptance, transfer, and mitigation [38]. There is an iteration that connects the risk mitigation monitoring component to the risk analysis in cloud computing adoption, by updating the inherent risk values after implementing mitigation actions in accordance with the previous plan [6].



Figure 5. Use Case Diagram for the Risk Mitigation Prototype.

After developing the model, the next step is to design a use case diagram to identify the modules needed to implement all model components. Figure 5 shows a use case diagram consisting of two actors: the head of IT department and the administrator.

4.4. Demonstration

The developed model must be ensured to be in accordance with the conditions and characteristics of the university in adopting public cloud. Validation through prototype simulation is required with the aim of determining the suitability of the model components [41]. Before conducting the simulation, things that must be considered are determining the scenario by moving several university assets to the cloud scope that are in accordance with the initiation, implementation, and mitigation phases.

One application must be determined to be moved to the cloud scope because, based on the results of in-depth interviews with 6 heads of university IT departments, one application consists of several supporting components such as databases, application files, and others [2]. So, a very careful configuration process is required so as not to cause gaps or threats that may arise in the future. In this study, one application used as a reference for the simulation is e-learning because many are accessed simultaneously at the same time by students and lecturers in supporting the learning and teaching process [37]. However, this study focuses on a single case higher education institution XYZ in Jakarta, to illustrate the implementation of the phases within the risk mitigation model via a prototype, specifically covering the modules for determining risk treatment strategies, establishing risk treatment plans, and monitoring risk mitigation.

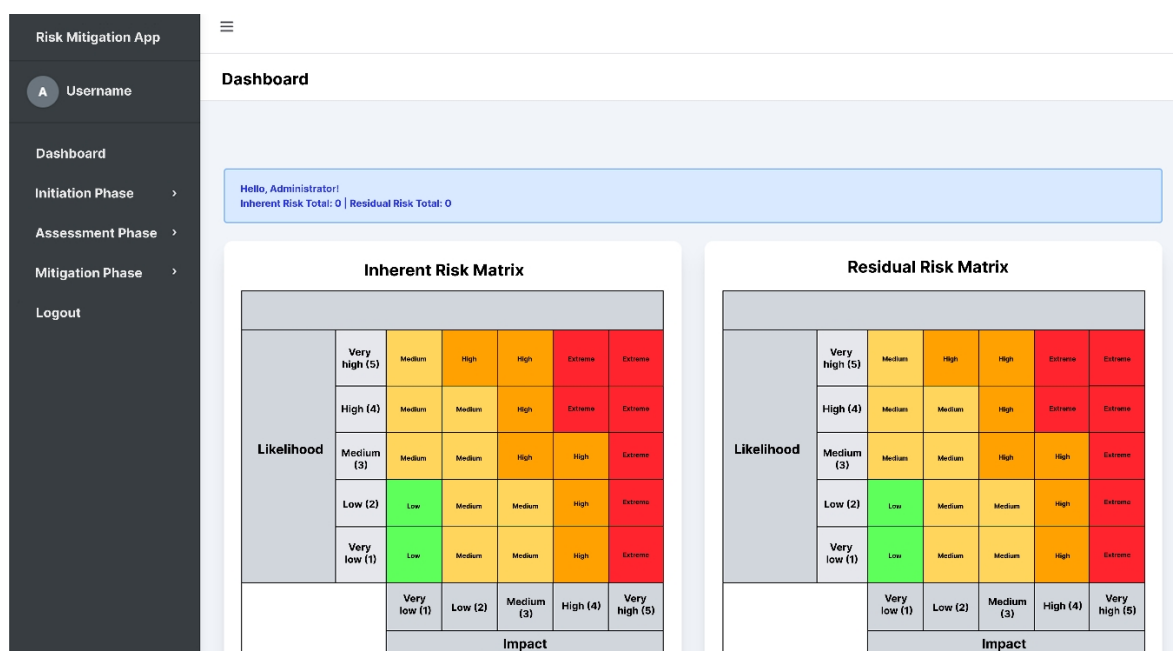


Figure 6. Develop Prototype for Implementation Risk Mitigation Model.

The proposed prototype design is shown in Figure 6. There are several main menus, such as the dashboard, initiation phase, assessment phase, and mitigation phase. In the dashboard, there are 2 risk matrices: the inherent risk and residual risk matrices.

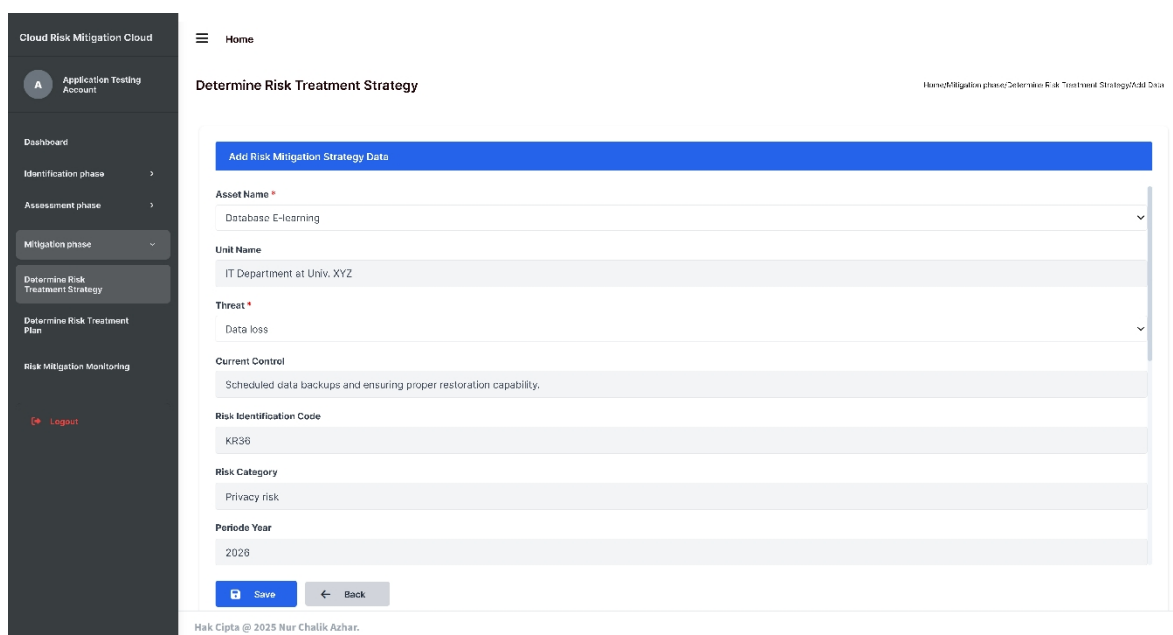


Figure 7. Data Entry Process in the Determine Risk Treatment Strategy Module.

Figure 7 above illustrates the input process for the "determine risk treatment strategy" module within the mitigation phase. In the first step, the university's IT department head must select the assets to be addressed; data entered during previous stages will appear based on the assets that have undergone risk analysis in the context of this research. These include components related to the e-learning application, such as databases, compute engines, and other elements [2]. The second step represents the most critical input phase within the "determine risk treatment strategy" module, as the IT department head must select a specific strategy, such as accept, avoid, transfer, or mitigate, to proceed to the "determine risk treatment plan" stage [48].

The screenshot displays the 'Determine Risk Treatment Plan' module within the 'Cloud Risk Mitigation Cloud' application. The sidebar on the left contains navigation links: 'Dashboard', 'Identification phase', 'Assessment phase', 'Mitigation phase', 'Determine Risk Treatment Strategy', 'Determine Risk Treatment Plan' (highlighted), and 'Risk Mitigation Monitoring'. The main content area is titled 'Determine Risk Treatment Plan' and includes a 'Add Risk Mitigation Plan Data' button. Below this is a 'Risk Mitigation Plan Details' section with the instruction 'Create a detailed implementation plan to address the identified risk'. The form contains the following fields: 'Risk Mitigation Strategy' (a dropdown menu), 'Person in Charge' (a text field with an example: 'IT Security Team, DevOps Team, Network Security Team'), 'Mitigation Start Date' (a date picker), and 'Mitigation End Date' (a date picker). At the bottom of the form are 'Save' and 'Back' buttons. The footer of the page reads 'Copyright © 2025 Nur Chalik Azhar'.

Figure 8. Data Entry Process in the Determine Risk Treatment Plan Module.

Figure 8 above illustrates the module for inputting data related to determining a risk treatment plan. The first step is similar to the input process in the previous stage: one must select a specific asset for which a mitigation plan is to be defined. In the second step, the university's IT department head must determine a risk mitigation strategy, which can be tailored to the university's specific conditions and characteristics regarding the adoption of a public cloud. In this context, the mitigation strategies have been customized based on identification results and validated through in-depth interviews with five practitioners and six university IT department heads. Consequently, these 11 types of strategies are available for selection within the "risk mitigation strategy" field.

Figure 9 below illustrates the data entry process for risk mitigation monitoring. The initial steps are largely similar to those previously described; however, the input procedure within this module requires the university's IT department head to provide data reflecting actual conditions. This includes the realization date, costs (optional), notes for the person responsible for implementing the risk response, evidence of implementation, and the execution status (not yet started, in progress, or completed).

Cloud Risk Mitigation Cloud

Home

Risk Mitigation Monitoring

Home/Mitigation phase/Risk Mitigation Monitoring/Add Data

Add Risk Mitigation Plan Data

Mitigation Implementation & Monitoring
Fill in the results of risk mitigation monitoring implementation below.

Mitigation Realization Date *
dd/mm/yyyy
Select a date according to the risk mitigation target timeframe.

Mitigation Cost (If Any)
Rp. 0
Optional, enter the nominal mitigation cost that has been incurred, if any.

Notes (Optional)
Add notes or additional information related to the mitigation implementation...

Mitigation Evidence (Upload File) *
Choose File No file chosen
Supported file formats: PDF, DOCX, XLSX, JPG, PNG, ZIP, etc.

Implementation Status *
Select status

Saves **Back**

Copyright © 2025 Nur Chalik Azhar.

Figure 9. Data Entry Process in the Risk Mitigation Monitoring Module.

Once the risk mitigation monitoring phase is complete, the next step is to update the residual risk data within the risk analysis module, as illustrated in Figure 10 below. The head of the university's IT department can perform these updates by selecting values for the "residual risk likelihood" and "residual risk impact level" fields. These fields contain criteria for likelihood and impact that can be adjusted following the implementation of previously planned mitigation measures. The process of updating risk values in the risk analysis module requires the involvement of various stakeholders within the university's IT department, such as the department head, section heads, and IT staff, to ensure that the updated values accurately reflect the actual situation. This approach aligns with the "inclusive" principle set out in the ISO 31000 standard [48].

Cloud Risk Mitigation Cloud

Home

Update Risk Analysis Data

Home/Assessment phase/Update Risk Analysis Data

Ubah Data Analisis Risiko

Residual Risk
Remaining risk after implementing mitigation actions

Residual Risk Likelihood Level *
1 - Very Low

Residual Risk Impact Level *
2 - Low

Residual Risk Value *
2
Automatic calculation result: Likelihood Level x Impact Level

Saves **Back**

Copyright © 2025 Nur Chalik Azhar.

Figure 10. Updating Residual Risk Values within The Risk Analysis Module.

Figure 11 below is an example of infrastructure in a public cloud service using Google Cloud Platform (GCP), which contains several assets or components of the e-learning application. The

database serves as a storage medium that holds all structured data. Redis (Remote Dictionary Server) is a very fast in-memory data structure storage. Redis is a bridge between traditional databases (such as MySQL) and applications tasked with handling data that needs to be accessed quickly. Google Cloud Filestore is a Network Attached Storage (NAS) service fully managed by Google Cloud. Unoconv (Universal Office Converter) in Moodle is a document converter feature that allows Moodle to automatically convert various file formats (such as .docx, .odt, or .rtf) to PDF format. IaaS services that function to create and run virtual machines on Google's infrastructure are grouped.

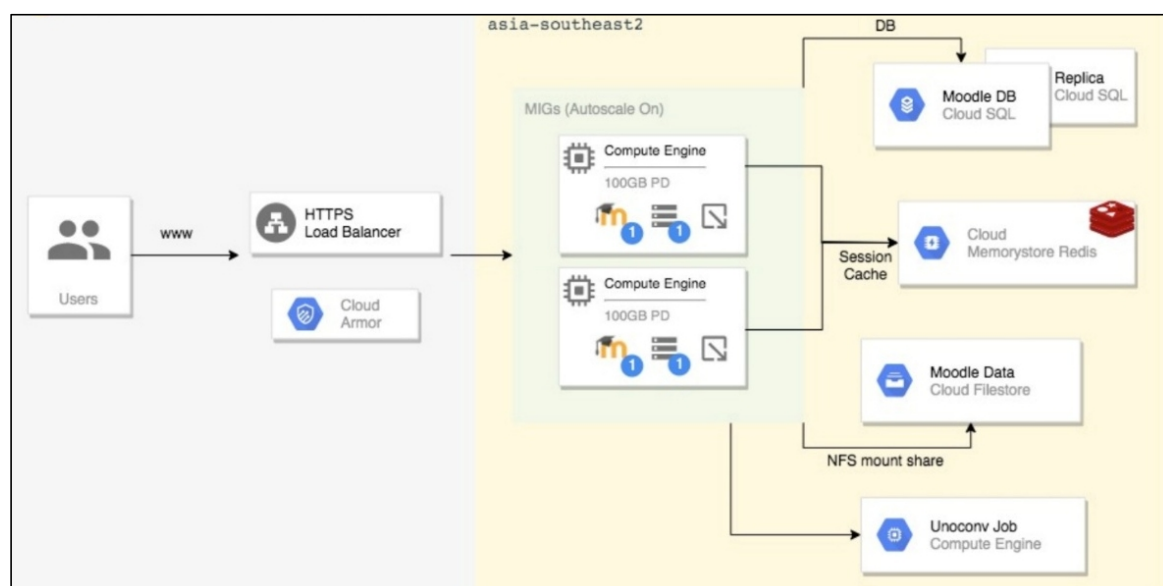


Figure 11. Cloud E-learning Application Infrastructure at XYZ University. Source: In-Depth Interview Results.

The demonstration was conducted online for 1 hour. Each IT practitioner and department head at the university completes the instruments provided within the prototype, including demonstration scenarios, which can be customized by inputting asset data that reflects the specific conditions of each university, particularly regarding the migration of e-learning applications to the cloud. In this session, the interviewer asked participants open-ended questions about the proposed risk mitigation model, as shown in Table 12. In the next session, participants were allowed to provide answers and suggestions outside the list of questions asked in the previous third session.

Table 12. List of Questions.

No	Questions	Objectives
1	What is your response to the proposed main stages of initiation, assessment, and mitigation?	To find out the opinions of participants regarding the initiation, assessment, and mitigation phases that have been proposed in the risk mitigation model
2	What is your response to the proposed components of the initiation phase?	To find out the opinions of participants regarding the proposed components in the initiation phase
3	What is your response regarding the components in the proposed assessment phase?	To find out the opinions of participants regarding the proposed components in the assessment phase
4	What is your response regarding the components in the proposed mitigation phase?	To find out the opinions of participants regarding the proposed components in the mitigation phase

4.5. Evaluation

Based on the questions in Table 12 above, several summaries of practitioners' and IT heads' responses at the university are provided. Based on the proposed risk mitigation model, these improvements result from the suggestions given in Table 13.

Table 13. Response from Participants. Source: In-Depth Interview Results.

No	Response from Practitioner	Response from Head of IT
Question 1	The proposed main phases are in accordance with risk management principles	The proposed main phases are in accordance with risk management principles
Question 2	The types of threats and controls in the identification threats and controls components are in accordance with standards and Personally Identifiable Information (PII), so that the Head of the IT Department can refer to the proposed component references	The list of threat types and controls can be related to privacy and refer to previous research or existing frameworks
Question 3	First, the risk assessment can be linked to specific areas, such as information security and privacy, organizational integrity, and reputation. Second, the risk score calculation formula should be based on previous research or a widely accepted framework	The risk-targeting component focuses on risk assessment before cloud migration, while risk analysis is conducted after migration
Question 4	First, not all assets subject to mitigation are determined based on the highest risk value. Second, a new component related to mitigation monitoring is added to determine its status (not yet implemented, in progress, or completed)	First, components for mitigation implementation can be added and referenced within existing frameworks. Second, mitigation plans can address privacy issues. Third, mitigation should only be applied to the highest-value assets

4.6. Communication

The purpose of the previous evaluation phase was to determine the suitability of the model components for public cloud adoption in the conditions and characteristics of universities in Province of Jakarta (3 universities), Central Java Province (2 universities), and East Java (1 university). Therefore, suggestions regarding the components' conditions and characteristics must be refined and communicated through follow-up interviews with practitioners and heads of university IT departments.

To ensure that the components align with the university's conditions and characteristics, a re-identification phase is conducted to identify the types of threats and controls in the cloud environment. After that, follow-up interviews are conducted to confirm that the identified threat types align with the university's conditions and the characteristics of public cloud usage. Furthermore, the same steps are followed: follow-up interviews with practitioners to ensure appropriate controls for information security and privacy in the public cloud environment.

5. Discussion

5.1. Design and Develop Risk Mitigation Model

The first research question is "How to develop a suitable risk mitigation model for public cloud environments?", which results in a risk mitigation model for public cloud adoption in a university

environment with the aim of mitigating potential risks after application migration. Although this framework has structured stages [100], each research stage must be carried out rigorously and thoroughly to produce a credible and reliable contribution.

The first stage in the DSRM framework is problem identification and motivation, which is based on the results of in-depth interviews showing that administrators are still not very concerned with monitoring software updates due to limited time for supervision. The problem in the process aspect is that there are no general standards adopted regarding infrastructure maintenance and improving security and privacy, so that when IT infrastructure problems occur, the controls applied are not standard. The university's IT department is only reactive; there is no clear plan for maintenance related to software updates and improving information security and privacy. One common problem in the technology aspect is the lack of capability in handling many users accessing academic applications simultaneously, which can be a strong motivation for universities in adopting public cloud.

A common problem that occurs after applications are migrated to the cloud is the lack of attention to privacy for access control. This problem is similar to the problem in on-premises IT infrastructure, where there is a lack of awareness among administrators. As a result, the university IT department has not optimally implemented the Personal Data Protection Law No 27 of 2022 [95], which indirectly has the potential for losses in cloud infrastructure, especially applications that have been migrated. The most common problem that is most noticed in the process aspect is the lack of standards in risk identification, assessment, and mitigation, where risks that are not managed properly can have a large impact. The university IT department is only reactive when risks occur.

This potentially violates the regulations of the Personal Data Protection Law No 27 of 2022 [95], if problems arise related to user data privacy. Incident response is slow [101], and there is no risk mitigation plan that is appropriate to the conditions of public cloud adoption. Problems in the technological aspect are more likely related to information security, such as the threat of SSH misconfiguration and cross-site scripting (XSS) security vulnerabilities in web applications. It can be concluded that the problems in the conditions before and after the adoption of public cloud are almost similar, especially the one that is of great concern is the absence of standards for risk management, so the first research question arises with the motivation to be able to provide scientific contributions to develop a useful model to mitigate risks in accordance with the standards and conditions in the university's public cloud environment.

The objective of this research is to develop a risk mitigation model to reduce the potential impact of risks in public cloud adoption in a university environment. There is no related research which explores the mitigation phase. However, there is a study that has contributed a structured risk assessment model to identify types of threats, vulnerabilities, and risks, and can map between threats and vulnerabilities based on previously identified assets (applications) [13]. However, this study has not explored the mapping results comprehensively, including mapping types of threats and controls, risk factors and mitigation strategies that are appropriate to the public cloud context. In addition, only a few studies have proposed prototypes for trials or simulations with the aim of determining the suitability of the proposed model components. For example, there are proposed prototypes on a mobile platform with the Android OS [10] and web-based [13].

Based on the risk mitigation model proposed in this study, the overall risk management stages have been indirectly implemented, but not all components are adopted in this study. Therefore, the

components in the identification, assessment, and mitigation phases have unique characteristics in the model because the list of threat types and controls can be implemented in the threat identification and control components and can be used when mapping threat types and controls based on identified assets or applications. Meanwhile, the contribution of the risk factor list can be implemented in the risk identification component, and the list of mitigation strategies can also be implemented in the risk management plan component. During the prototype simulation, the head of the IT department can select and adapt them to the conditions of each university.

Based on the adaptation of the stages/phases from OCTAVE Allegro and ISO 31000, as mapped in this study, the starting point for the risk mitigation model is the "identification of asset list" component. The OCTAVE Allegro framework is oriented toward information assets, specifically within the context of information security. However, the ISO 31000 standard does not provide a mechanism for asset identification, focusing instead on establishing context based on internal and external scopes, which is why this study incorporates the "develop information asset profiles" stage from the OCTAVE Allegro framework [20].

The ISO 31000 standard does not provide an explicit mechanism for identifying various types of threats in a general sense. Consequently, the risk mitigation model proposed here consists of several components: the identification of threat types, the identification of control types, and threat mapping and asset control. These components are structured to facilitate the input and output processes for users of the proposed prototype. The approach taken in this study is supported by the work of Maniah [13], who also categorized components related to threat identification; furthermore, this study incorporates the "identify threat scenarios" stage from the OCTAVE Allegro framework.

The components within the risk mitigation model, specifically "identification of risks" and "determine risk target", are derived by adapting the "identify risks" stage from OCTAVE Allegro and the "risk identification" phase from ISO 31000. In principle, the "identification of risks" component serves to establish a list of risks associated with assets that are intended for migration, or have already been migrated—to a cloud environment. Meanwhile, the "determine risk target" component is used to define the desired risk levels, as specified by the head of the IT department, prior to the migration of assets to the cloud. The functions of these components are consistent with the frameworks provided by OCTAVE Allegro [20] and ISO 31000 [48].

The risk analysis component aligns with the "analyze risk" stage in OCTAVE and the "risk analysis" phase in ISO 31000. Therefore, this study does not place significant emphasis on tailoring the risk analysis component for public cloud adoption, as the general utility of such a component is largely similar to that found in related research by Maniah [13] and Abed Saif Ahmed Alghawli & Tamara Radivilova [11].

The components within the risk mitigation model, which have been divided into several sections, pertain not only to the identification phases but also encompass the determination of risk treatment strategies and the formulation of risk treatment plans. This structure is intended to facilitate user interaction during the input and output processes of the prototype. The risk mitigation monitoring component proposed in this study is adapted solely from the ISO 31000 standard; as there is no equivalent component within the OCTAVE Allegro framework, this represents a limitation of the model.

In general, the principles adapted from the ISO 31000 standard, specifically regarding the "integrated" aspect, encompass components such as risk analysis in public cloud adoption,

determination of risk treatment strategies, development of risk treatment plans, and monitoring of risk mitigation. These components are critical in deciding whether assets that have undergone risk analysis can proceed to the subsequent stages of defining strategies, planning, and implementing risk mitigation measures. The entire risk mitigation model can be executed in a structured manner, following a sequence that begins with the primary phase of identification and concludes with mitigation.

The development of components within the risk mitigation model aligns with the "customized" principle of the ISO 31000 standard. Specifically, components such as the identification of threat types, identification of control types, risk analysis for public cloud adoption, and the determination of risk treatment plans have been tailored to the characteristics of a university adopting a public cloud, particularly one that has attained an "A" or "Excellent" accreditation from the Indonesian government. Furthermore, the identified threat types, controls, risk factors, and mitigation strategies have been adapted to the context of this study, drawing upon previous research [46].

The outcome of these adjustments, which involved university IT practitioners and department heads, aligns with the principles of inclusivity and consideration for human and cultural factors, ensuring that the identified elements are appropriate for the context of this research. Furthermore, as the information obtained from the university is considered reliable, the validation processes, specifically the in-depth interviews, were conducted in a structured and rigorous manner. The available data and information proved useful for developing the components of the risk mitigation model. Consequently, the principle of using the "best available information" was implicitly applied in the development of the model [48].

The dynamic principle within the ISO 31000 standard has been applied to components such as risk analysis in public cloud adoption, the determination of risk treatment strategies and plans, and the monitoring of risk mitigation, reflecting the fact that the nature of threats and risks is inherently dynamic over time. This necessitates adjustments in setting target risk values, as well as the continuous updating of analyses and mitigation strategies to enhance the resilience of cloud infrastructure within a university setting [8]. Furthermore, to ensure organizational sustainability in the implementation of risk management, components aligned with the principle of continual improvement have been proposed [48].

There are similarities in the names or functions of the components proposed in this study with previous studies for the identification phase, such as asset identification [9, 13] and threats [9, 10, 13], but this study does not discuss the vulnerability identification component with the aim of reducing the stages in the identification phase, because universities are not-for-profit institutions. Only a few universities have human resources who can manage risk management according to general standards [102]. In addition, the vulnerability identification component is not the most important concern, because in the context of public cloud services, infrastructure or hardware is managed directly by the cloud service provider [16, 17].

However, this research remains important to do because threats to information security and privacy continue to emerge, and the potential impact of risks in the public cloud scope may occur in the future. Therefore, the proposed model is not general, but has uniqueness and characteristics that are appropriate to the environment of universities accredited "Excellent" or "A" by the Indonesian government.

The components of the assessment phase in this study have similar functions to previous research [13], especially in the threat and control mapping components based on assets and risk identification and analysis. The threat and control mapping component functions to map threats and types of controls based on assets or applications migrated to the cloud. The results of this mapping can help in risk identification, where the function of the risk identification component is to identify risks based on asset types, threats, risk categories, scenarios/causes of risk occurrence, impact areas (operational, financial, technology, etc.), and potential impacts. This component does not include risk analysis based on the level of likelihood and risk impact, because this component only identifies which applications are to be moved to the cloud environment [48]. In addition, the results of the risk factor identification in Table 5 can be applied to the risk identification components of this study.

The risk target determination component is adopted from the identify risk component in OCTAVE Allegro and risk identification in ISO 31000. Although they have different component names, they have the same function, namely aiming to determine risk targets against expected risk values [20]. In this context, determining the expected risk value is based on the risks that may occur in the adoption of public cloud within the university. The Head of the University IT Department can determine risk targets by considering the level of possibility (likelihood) and risk impact (impact) [48]. The results of these components are used as a reference for the next stage, namely the "Risk Analysis in Public Cloud Adoption" component.

The difference between the "Determine Risk Target " and "Risk Analysis in Public Cloud Adoption" components lies in their functions. The "Determine Risk Target" component is limited to determining the expected risk target value before an application is migrated to the cloud and does not represent actual risk values. Meanwhile, the "Risk Analysis in Public Cloud Adoption" component can perform inherent and residual risk analysis.

The proposed risk analysis component differs from related research [13], where the proposed risk analysis component analyzes risks before, during, and after cloud adoption. In this study, risk target determination is used to determine the risk value before adoption, and risk analysis is used to determine the risk value after adoption. This difference stems from in-depth interviews with six IT managers, who concluded that the risk analysis stage is unnecessary due to the excessive number of processes and the similar functional meanings of the stages before and during cloud adoption. In addition, related research is limited to only assessing the risks after adopting cloud computing [7, 8, 9, 10, 11, 12].

The scientific contribution that differentiates the related research lies in the proposed mitigation phase components. The risk management strategy component only determines the type of risk management strategy, such as accept, avoid, transfer, and mitigate. Not all assets whose risk has been analyzed must be mitigated; only those with low-risk values are not proceeded to the mitigation stage. The condition for choosing an avoid strategy is when risk values are high and to serve as a reminder in the future of uncontrolled risk values. In general, implementation methods that can be applied in choosing an avoid strategy include designing and implementing policies, conducting training, and developing applications with the aim of reducing risk values [48].

The condition for choosing a transfer strategy is when the risk values are high and cannot be handled by the organization itself, which in this context is the university's IT department. In general, the implementation method in the transfer strategy is to collaborate with other organizations or companies to help manage risks according to the conditions and objectives of the organization. The

condition for choosing a mitigation strategy is when the risk values are high, uncontrolled, and need to be addressed immediately. In general, the conditions in question include natural disasters, cyber-attacks on assets, and unforeseen asset errors/failures. The method in the mitigation strategy is to implement other backup plans when risks occur, taking into account impacts such as operational, financial, reputational, and others [48].

The adapted components are still the same as the Select Mitigation Approach in OCTAVE Allegro and Risk Treatment in ISO 31000, but have different functions from the "Determination of Risk Treatment Strategy" component. The head of the university IT department can determine risk handling plans, such as target completion times and those responsible for the mitigation process. The risk handling plan can be adopted from the list of mitigation strategies shown in Table 8 above. Meanwhile, the risk mitigation monitoring component functions to monitor the mitigation implementation process, where the head of the university IT department can fill in evidence of actions or handling, and ensure that risk handling can be completed within the time specified in the previous risk handling component [48].

5.2. Evaluation Risk Mitigation Model

The second research question was "How to evaluate the risk mitigation model developed for public cloud environments?" The evaluation results showed differences in the answers between the five practitioners and the six heads of university IT departments, indicating that many of the suggestions related to the risk mitigation model proposed in this study were general. The suggestions provided by the heads of IT were still general, while those provided by the practitioners were more detailed. The majority of answers to the first question for each phase of the risk mitigation model were in accordance with the principles and stages in the OCTAVE Allegro and ISO 31000 frameworks.

In general, the answer to the second question for the results of threat identification and control must be linked to the privacy aspect, especially related to Law Number 27 of 2022 concerning Personal Data Protection in Indonesia. Prior to the evaluation, the list of types of threats and controls was limited to the information security aspect. In Indonesia, issues related to privacy are of great concern, especially the occurrence of user data leaks in the public due to information security factors, as well as data trading to unauthorized parties, which has resulted in many Indonesians complaining about being frequently contacted by unknown people [48].

The results of the identification related to the list of types of threats and controls in the information security and privacy aspects are up-to-date, because they refer to the standards of Law Number 27 of 2022 concerning Personal Data Protection in Indonesia. Although the privacy aspect has been explored in related research to identify types of threats [10], it does not specifically refer to regional standards or international standards that are commonly adopted to improve user privacy, so the reliability of the identification results has not been met and does not comply with standards. For example, the California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), General Data Protection Regulation (GDPR), ISO/IEC 27001, or 27701.

The practitioner's third question was that aspects of the risk assessment phase are not limited to information security and privacy, but also include a list of other risk factors. Based on Table 4 above, this study lists nine risk factors that can be adopted in implementing the risk analysis component. Furthermore, the risk targeting component can be implemented before applications are migrated to the cloud, which aligns with the IT head's recommendations. The results of the fourth question revealed that there was similarity between practitioners and university IT department heads

regarding only high-risk applications to be mitigated. This recommendation aligns with the mitigation stages, which define assets that can be mitigated for medium, high, or extreme risk, while those with low risk are acceptable [48].

A potential threat that arises during the evaluation phase, specifically during the in-depth interviews with the experts, is the risk of bias in the feedback provided. This is particularly relevant when verifying and refining the components of the risk mitigation model, as well as identifying threats, controls, risks, and proposed mitigation strategies. To address this, the present study employs an expert scoring approach, which serves to mitigate potential bias and ensure the reliability of the contributions made through this research.

The evaluation plan proposed in this study does not cover how to assess the effectiveness of the suggested mitigation strategies within the "risk mitigation monitoring" component. This is because each university possesses distinct characteristics, principles, and IT environments; consequently, the scope of this research is limited to verifying and ensuring that the proposed components of the risk mitigation model align with the principles and steps/phases outlined in OCTAVE Allegro and ISO 31000.

6. Conclusions

Based on the research questions, the results can provide detailed information regarding the development of a risk mitigation model for public cloud adoption within universities in Province of Jakarta, Central Java, and East Java. In addition, it provides detailed information on the evaluation results of model artifacts through prototype simulations with several practitioners and heads of university IT departments. The results, after improvements based on suggestions from the model evaluation stage, showed that the model components were consistent with the conditions and characteristics of universities in the context of public clouds and could help reduce risk values and potential impacts on university assets.

Practical contributions of this research are that it can provide references to heads of IT departments of universities in Indonesia regarding ways to adopt public cloud with a risk management approach that has been adjusted within the scope of universities that have been accredited A or Excellent by the Ministry of Higher Education, Science, and Technology, Indonesia, and is useful for other universities that intend to or have adopted public cloud to use this risk mitigation model. In addition, it can provide advice to the head of the university's IT department on continuing to improve information security, including confidentiality, integrity, and availability (CIA). It can enhance user privacy, as regulated by the Personal Data Protection (PDP) Law number 27 of 2022. It can help plan appropriate future mitigation measures for each university.

Academic contributions of this research include providing updates on the proposed risk mitigation model for public cloud adoption within universities, tailored to cloud providers such as AWS, GCP, Microsoft Azure, and Alibaba Cloud. The proposed new model consists of three main phases: initiation, assessment, and mitigation. The mitigation phase, however, has seen limited research exploring the risk assessment and mitigation components of information security and user privacy. This research can contribute to the implementation of methodological references using the DSRM approach to develop risk mitigation and evaluation models through a prototype. Each stage is clearly explained, allowing academics to follow each step. This research can provide information

on the representation of modules in the risk mitigation prototype, which can be implemented and adjusted at each university, as it explains which data are input into the prototype instrument.

The methodological limitations of this research are the limited number of participants for in-depth interviews, which limits the generalizability of the results to a broader scope across universities in countries other than Indonesia, as they have different conditions and characteristics in adopting cloud computing. There is no established model component for measuring the maturity or readiness of university IT infrastructure to adopt public cloud systems that aligns with standard frameworks, such as COBIT, ITIL, TOGAF, ISO/IEC 27001, and the NIST Cybersecurity Framework. Consequently, aspects of assessing the feasibility of public cloud adoption remain misaligned with standardized IT governance principles in the university environment.

Therefore, the evaluation was conducted only at a few universities accredited with an A or Excellent rating and that have adopted cloud computing, so that it can be generalized to universities in the Province of Jakarta, Central Java, and East Java. Another limitation related to the methodology is that there has been no evaluation stage with a statistical approach related to the risk mitigation model and the proposed prototype, as noted in the limitations of this study.

Furthermore, a limitation in the evaluation phase is that the risk mitigation model and the mitigation strategies identified to reduce risk values effectively have not been explored in depth. In this study, the evaluation plan involved university IT department heads applying the framework using actual data, covering the process from the "identification of asset list" phase through to the "determination of a risk treatment plan," and testing the alignment of the proposed risk mitigation model's components with the steps and phases of OCTAVE Allegro and ISO 31000. Consequently, future research could empirically test the identified mitigation strategies (based on the proposed model and prototype) to determine their effectiveness in reducing risk values. This is because the implementation of such strategies may entail costs and requires concrete, supporting evidence, particularly for the "risk mitigation monitoring" component of the proposed model.

It is hoped that future researchers can further explore the development of a risk mitigation model that includes maturity measurement components before adopting cloud computing in the public and private cloud spheres by paying attention to evaluations such as the number of participants who are more spread out in universities other than Java Island. For example, universities in the islands of Sumatra, Kalimantan, and others. In addition, conducting model evaluations with statistical methods or approaches to the developed models.

Future research in this study is to explore risk mitigation models and add participants from several universities outside Java, including universities in Southeast Asian countries, so that the developed model can be more widely represented. Second, it can explore the components to measure the level of IT governance maturity in several universities in Java, Sumatra, Kalimantan, and others, so that before adopting the public cloud, the level of IT governance maturity in universities in Indonesia can be known. Third, it could evaluate the prototype using a statistical approach to assess application acceptance, using Partial Least Squares Structural Equation Modeling (PLS-SEM) within the Technology Acceptance Model (TAM) framework. This framework emphasizes perceived ease of use and usefulness variables and can predict a user's intention to use a technology.

Contributions: N.C.A. contributed to the conceptualization of the research, determining the methodology, developing the risk mitigation model, collecting data through interviews, validating the risk mitigation model, and writing the paper. M.Z. was responsible for ensuring the methodology

and proposed risk mitigation model were in accordance with the principles of OCTAVE Allegro and ISO 31000, as well as ensuring the writing of the paper was in accordance with the structure of qualitative research writing. Y.A. contributed to the conceptualization of the research, determining the methodology, developing the risk mitigation model, and writing the paper. B.S. was responsible for the literature review, developing the components of the risk mitigation model to suit the conditions and characteristics of the university in adopting public cloud, validating the interview results, and ensuring the writing of the paper was in accordance with the general structure of research writing.

Acknowledgments: Not applicable.

Funding: This research received no external funding

Conflicts of Interest: The authors declare no conflict of interest.

References

- [1] Yin, X., Zhang, X., Pei, L., Hu, R., Ye, K., & Cai, K. (2025). Optimization and benefit evaluation model of a cloud computing-based platform for power enterprises. *Scientific Reports*, 15(1), 26366. <https://doi.org/10.1038/s41598-025-10314-5>
- [2] Al-Turkistani, H. F., & AlFaadhel, A. (2021). Cyber Resiliency in the Context of Cloud Computing Through Cyber Risk Assessment. 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA), 73–78. <https://doi.org/10.1109/CAIDA51941.2021.9425195>
- [3] Gao, H., Li, L., Lin, H., Wan, J., Deng, D., & Li, J. (2021). DECH: A Novel Attack Pattern of Cloud Environment and Its Countermeasures. 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), 117–122. <https://doi.org/10.1109/CSP51677.2021.9357594>
- [4] Maniah, Soewito, B., Lumban Gaol, F., & Abdurachman, E. (2022). A systematic literature Review: Risk analysis in cloud migration. *Journal of King Saud University - Computer and Information Sciences*, 34(6), 3111–3120. <https://doi.org/10.1016/j.jksuci.2021.01.008>
- [5] Baskerville, R., Baiyere, A., Gergor, S., Hevner, A., & Rossi, M. (2018). Design Science Research Contributions: Finding a Balance between Artifact and Theory. *Journal of the Association for Information Systems*, 19(5), 358–376. <https://doi.org/10.17705/1jais.00495>
- [6] Berrada, H., Boutahar, J., & El Houssaini, S. E. G. (2023). Roadmap and Information System to Implement Information Technology Risk Management. *International Journal of Safety and Security Engineering*, 13(6), 987–1000. <https://doi.org/10.18280/ijssse.130602>
- [7] Nhlabatsi, A., Hussein, A., Fetais, N., & Khan, K. M. (2020). Design and Implementation of a Threat-Specific Security Risk Assessment Tool. 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT), 511–518. <https://doi.org/10.1109/ICIoT48696.2020.9089459>
- [8] Torkura, K. A., Sukmana, M. I. H., Cheng, F., & Meinel, C. (2020). CloudStrike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure. *IEEE Access*, 8, 123044–123060. <https://doi.org/10.1109/ACCESS.2020.3007338>
- [9] Huang, M. (2021). Design of basic process of information security risk assessment in cloud computing environment. 2021 IEEE International Conference on Consumer Electronics and Computer Engineering (ICCECE), 494–499. <https://doi.org/10.1109/ICCECE51280.2021.9342156>
- [10] Elahi, H., Wang, G., Xu, Y., Castiglione, A., Yan, Q., & Shehzad, M. N. (2021). On the Characterization and Risk Assessment of AI-Powered Mobile Cloud Applications. *Computer Standards & Interfaces*, 78(October 2020), 103538. <https://doi.org/10.1016/j.csi.2021.103538>
- [11] Alghawli, A. S. A., & Radivilova, T. (2024). Resilient cloud cluster with DevSecOps security model, automates a data analysis, vulnerability search and risk calculation. *Alexandria Engineering Journal*, 107(April), 136–149. <https://doi.org/10.1016/j.aej.2024.07.036>
- [12] Gatti, G., Valero, J. M. J., Manuel Gil Pérez, & Basile, C. (2025). Holistic Cyber Risk Assessment in the Cloud Continuum: A Multi-Layer, Multi-Domain Approach. *IEEE Access*, 13(October). <https://doi.org/10.1109/ACCESS.2025.3622915>

- [13] Maniah, Soewito, B., Gaol, F. L., & Abdurachman, E. (2022). Risk Assessment for Logistics Applications in Cloud Migration. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, 16(3), 325. <https://doi.org/10.22146/ijccs.74567>.
- [14] Fortinet. (2024). Cloud Security Report 2024. <https://global.fortinet.com/lp-en-2024-cloud-report>
- [15] Figueiredo, J., & García-Peñalvo, F. J. (2024). Design science research applied to difficulties of teaching and learning initial programming. *Universal Access in the Information Society*, 23(3), 1151–1161. <https://doi.org/10.1007/s10209-022-00941-4>
- [16] Nhlabatsi, A., Hussein, A., Fernandez, R., Fetais, N., Hong, J., Kim, D., & Khan, K. M. (2019). ThreatRiskEvaluator: A Tool for Assessing Threat-Specific Security Risks in the Cloud. 2019 International Conference on Cyber Security for Emerging Technologies (CSET), 1–6. <https://doi.org/10.1109/CSET.2019.8904894>
- [17] Surya, P., Pachauri, P., Pachauri, A., Chaturvedi, P., Yadav, S. A., & Singh, D. (2021). Virtualization Risks and associated Issues in Cloud Environment. 2021 International Conference on Technological Advancements and Innovations (ICTAI), (November), 521–525. <https://doi.org/10.1109/ICTAI53825.2021.9673424>
- [18] Will Forrest, Mark Gu, James Kaplan, Michael Liebow, Raghav Sharma, Kate Smaje, & Steve Van Kuiken. (2021). Cloud’s trillion-dollar prize is up for grabs. McKinsey Digital, (February)
- [19] Linthicum, D., States, U., Thomas, C., States, U., Kearns-manolatos, D., States, U., & Parveen, I. (2023). Cloud benefits could be maximized across business functions with C-suite collaboration. Deloitte Digital. <https://www2.deloitte.com/us/en/insights/technology-management/maximizing-cloud-benefits.html>
- [20] Caralli, R. a. C., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process. Young, (May), 1–113
- [21] Irsheid, A., Murad, A., AlNajdawi, M., & Qusef, A. (2022). Information security risk management models for cloud hosted systems: A comparative study. *Procedia Computer Science*, 204, 205–217. <https://doi.org/10.1016/j.procs.2022.08.025>
- [22] Ali, T., Al-Khalidi, M., & Al-Zaidi, R. (2024). Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review. *Journal of Computer Information Systems*, 66(1), 1–28. <https://doi.org/10.1080/08874417.2024.2329985>
- [23] Akinrolabu, O., New, S., & Martin, A. (2019). CSCCRA: A novel quantitative risk assessment model for saas cloud service providers. *Computers*, 8(3), 1–17. <https://doi.org/10.3390/computers8030066>
- [24] Shabdin, N. I., and Yaacob, S, and Ibrahim, Roslina, Developing a Comprehensive Digitalization Gap Analysis Components: Bridging Gaps in People, Process, and Technology for Public Sector Transformation. <https://dx.doi.org/10.2139/ssrn.5065161>
- [25] Institute of Risk Management. (2018). A Risk Practitioners Guide to ISO 31000 : 2018 (Second Edi). Institute of Risk Management
- [26] Sousa, V., Almeida, N. M. De, & Dias, L. A. (2012). Risk Management Framework for the Construction Industry According to the ISO 31000 : 2009 Standard. *Journal of Risk Analysis and Crisis Response*, 2(4), 261–274. <https://jracr.com/index.php/jracr/article/view/48/49>
- [27] Annunziata, G., Sheykina, A., Palomba, F., De Lucia, A., Catolino, G., & Ferrucci, F. (2024). Security Risk Assessment on Cloud: A Systematic Mapping Study. *Proceedings of the 28th International Conference on Evaluation and Assessment in Software Engineering*, 604–613. <https://doi.org/10.1145/3661167.3661287>
- [28] Wulf, F., Strahringer, S., & Westner, M. (2019). Information Security Risks, Benefits, and Mitigation Measures in Cloud Sourcing. 2019 IEEE 21st Conference on Business Informatics (CBI), 1, 258–267. <https://doi.org/10.1109/CBI.2019.00036>
- [29] Mulgund, P., Pahwa, P., & Chaudhari, G. (2019). Strengthening IT Governance and Controls Using COBIT. *International Journal of Risk and Contingency Management*, 8(4), 66–90. <https://doi.org/10.4018/ijrcm.2019100104>
- [30] Maniah, Abdurachman, E., Gaol, F. L., & Soewito, B. (2019). Survey on Threats and Risks in the Cloud Computing Environment. *Procedia Computer Science*, 161, 1325–1332. <https://doi.org/10.1016/j.procs.2019.11.248>
- [31] Faizi, A., Padyab, A., & Naess, A. (2022). From rationale to lessons learned in the cloud information security risk assessment: a study of organizations in Sweden. *Information & Computer Security*, 30(2), 190–205. <https://doi.org/10.1108/ICS-03-2021-0034>

- [32] Welch, A., & Aziz, E. A. (2023). Higher Education in Indonesia. In L. P. Symaco & M. Hayden (Eds.), *International Handbook on Education in Southeast Asia* (1st ed., Vol. 1, pp. 1–1488). Springer Nature Singapore. https://doi.org/10.1007/978-981-16-8136-3_41-2
- [33] José Osvaldo De Sordi. (2021). *Design Science Research Methodology*. In *Design Science Research Methodology: Theory Development from Artifacts* (1st ed.). Palgrave Macmillan Cham. <https://doi.org/10.1007/978-3-030-82156-2>
- [34] Luo, Z., Lu, W., He, J., & Wang, Y. (2022). Combination of research questions and methods: A new measurement of scientific novelty. *Journal of Informetrics*, 16(2), 101282. <https://doi.org/10.1016/j.joi.2022.101282>
- [35] Flores, D. A., & Morochó, G. (2020). Cloud-GMR: A Qualitative Framework for Governance and Risk Management of Cloud-hosted Public Services. 2020 XLVI Latin American Computing Conference (CLEI), 294–303. <https://doi.org/10.1109/CLEI52000.2020.00041>
- [36] Elmagrhi, M. H., & Ntim, C. G. (2023). Non-financial reporting in non-profit organisations: the case of risk and governance disclosures in UK higher education institutions. *Accounting Forum*, 47(2), 223–248. <https://doi.org/10.1080/01559982.2022.2148854>
- [37] Maniah, Soewito, B., Gaol, F. L., & Abdurachman, E. (2019). Risk Assessment on Cloud Computing for The Learning System in The Education Environment. 2019 IEEE International Conference on Engineering, Technology and Education (TALE), 1–6. <https://doi.org/10.1109/TALE48000.2019.9225941>
- [38] Putra, A. P., & Soewito, B. (2023). Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. *International Journal of Advanced Computer Science and Applications*, 14(4), 625–633. <https://doi.org/10.14569/IJACSA.2023.0140468>
- [39] Yihui, Z. (2024). Design of cloud data storage security and financial risk control management early warning system based on sensor networks. *Measurement: Sensors*, 32(February), 101064. <https://doi.org/10.1016/j.measen.2024.101064>
- [40] Carlson, C., Hutton, A., & Gilliam, A. (2010). *Technical Guide FAIR – ISO / IEC 27005 Cookbook*.
- [41] Wieringa, R. J. (2014). *Design Science Methodology for Information Systems and Software Engineering*. In *Design Science Methodology: For Information Systems and Software Engineering* (1st ed.). Springer Berlin Heidelberg. <https://doi.org/10.1007/978-3-662-43839-8>
- [42] Abutaleb, H., Tamimi, A., & Alrawashdeh, T. (2021). Empirical Study of Most Popular PHP Framework. 2021 International Conference on Information Technology (ICIT), 608–611. <https://doi.org/10.1109/ICIT52682.2021.9491679>
- [43] Seidl, M., Scholz, M., Huemer, C., & Kappel, G. (2015). *UML @ Classroom - An Introduction to Object-Oriented Modeling* (1st ed.). Springer Cham. <https://doi.org/10.1007/978-3-319-12742-2>
- [44] Venable, J., Pries-Heje, J., & Baskerville, R. (2012). A Comprehensive Framework for Evaluation in Design Science Research. In *Proceedings of the 7th International Conference on Design Science Research in Information Systems* (pp. 423–438). https://doi.org/10.1007/978-3-642-29863-9_31
- [45] Beniwal, R., Jain, M., & Gupta, Y. (2021). Opinion Mining to Aid User Acceptance Testing for Open Beta Versions. In *Advances in Intelligent Systems and Computing* (Vol. 1164, pp. 291–301). https://doi.org/10.1007/978-981-15-4992-2_28
- [46] Azhar, N. C., Zarlis, M., Arifin, Y., & Soewito, B. (2024). Threats, Risks, and Mitigations in Cloud Computing Environment. 2024 Ninth International Conference on Informatics and Computing (ICIC), 1–6. <https://doi.org/10.1109/ICIC64337.2024.10956511>
- [47] Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). Purposive sampling: complex or simple? Research case examples. *Journal of Research in Nursing*, 25(8), 652–661. <https://doi.org/10.1177/1744987120927206>
- [48] ISO Central Secretariat, *ISO 31000:2018*, Second Edi. Vernier, Geneva: International Organization for Standardization, 2018
- [49] Aspers, P., & Corte, U. (2019). What is Qualitative in Qualitative Research. *Qualitative Sociology*, 42(2), 139–160. <https://doi.org/10.1007/s11133-019-9413-7>
- [50] Huawei Technologies Co., L. (2023). *Network Basics in Cloud Computing*. In *Cloud Computing Technology* (pp. 145–195). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-3026-3_4
- [51] Polit, D. F., and Beck, C. T. (2006). The content validity index: Are you sure you know what's being reported? critique and recommendations, *Research in Nursing & Health*, 29(5), pp. 489–497. <https://doi.org/10.1002/nur.20147>

- [52] Akinrolabu, O., Nurse, J. R. C., Martin, A., & New, S. (2019). Cyber risk assessment in cloud provider environments: Current models and future needs. *Computers & Security*, 87, 101600. <https://doi.org/10.1016/j.cose.2019.101600>
- [53] Bhajantri, L. B., & Mujawar, T. (2019). A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures. 2019 Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 376–380. <https://doi.org/10.1109/I-SMAC47947.2019.9032545>
- [54] Waguia, J. D. K., & Menshchikov, A. (2021). Threats and Security Issues in Cloud Storage and Content Delivery Networks: Analysis. 2021 28th Conference of Open Innovations Association (FRUCT), 194–199. <https://doi.org/10.23919/FRUCT50888.2021.9347609>
- [55] Weil, T. R. (2020). Standards for Cloud Risk Assessments - What's Missing? 2020 IEEE Cloud Summit, 11–17. <https://doi.org/10.1109/IEEECloudSummit48914.2020.00008>
- [56] Gamal, M., Helal, I. M. A., Mazen, S. A., & Elhennawy, S. (2022). IS Risks Governance for Cloud Computing Service. In *COVID-19 Challenges to University Information Technology Governance* (pp. 287–307). Springer International Publishing. https://doi.org/10.1007/978-3-031-13351-0_14
- [57] Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manufacturing*, 44(2019), 655–662. <https://doi.org/10.1016/j.promfg.2020.02.243>
- [58] Lambropoulos, G., Mitropoulos, S., & Douligeris, C. (2021). A Review on Cloud Computing services, concerns, and security risk awareness in the context of Digital Transformation. 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), (October), 1–6. <https://doi.org/10.1109/SEEDA-CECNSM53056.2021.9566267>
- [59] El Kafhali, S., El Mir, I., & Hanini, M. (2021). Security Threats, Defense Mechanisms, Challenges, and Future Directions in Cloud Computing. *Archives of Computational Methods in Engineering*, 29(1), 223–246. <https://doi.org/10.1007/s11831-021-09573-y>
- [60] Balani, Z., & Varol, H. (2020). Cloud Computing Security Challenges and Threats. 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 1–4. <https://doi.org/10.1109/ISDFS49300.2020.9116266>
- [61] Moiz, S., Majid, A., Basit, A., Ebrahim, M., Abro, A. A., & Naeem, M. (2024). Security and Threat Detection through Cloud-Based Wazuh Deployment. 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), (January), 1–5. <https://doi.org/10.1109/KHI-HTC60760.2024.10482206>
- [62] Bedi, A., Pandey, N., & Khatri, S. K. (2019). Analysis of Detection and Prevention of Malware in Cloud Computing Environment. 2019 Amity International Conference on Artificial Intelligence (AICAI), 918–921. <https://doi.org/10.1109/AICAI.2019.8701418>
- [63] Negi, P. S., Garg, A., & Lal, R. (2020). Intrusion Detection and Prevention using Honeypot Network for Cloud Security. 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 129–132. <https://doi.org/10.1109/Confluence47617.2020.9057961>
- [64] Potluri, S., Mangla, M., Satpathy, S., & Mohanty, S. N. (2020). Detection and Prevention Mechanisms for DDoS Attack in Cloud Computing Environment. 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 1–6. <https://doi.org/10.1109/ICCCNT49239.2020.9225396>
- [65] Odeh, A., Aboshgifa, A., & Belhaj, N. (2023). Mitigating DDoS Attacks in Cloud Computing Environments: Challenges and Strategies. 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET), 1–4. <https://doi.org/10.1109/ICECET58911.2023.10389269>
- [66] Akbarian, F., Tärneberg, W., Fitzgerald, E., & Kihl, M. (2023). Attack Resilient Cloud-Based Control Systems for Industry 4.0. *IEEE Access*, 11, 27865–27882. <https://doi.org/10.1109/ACCESS.2023.3259063>
- [67] Gahane, S., & Verma, P. (2023). The Research Study on Identification of Threats and Security Techniques in Cloud Environment. 2023 1st DMIHER International Conference on Artificial Intelligence in Education and Industry 4.0 (IDICAIEI), (February), 1–6. <https://doi.org/10.1109/IDICAIEI58380.2023.10407003>
- [68] Pavloski, M. (2019). Detecting and Mitigating Storm Attacks in Mobile Access to the Cloud. 2019 IEEE International Conference on Fog Computing (ICFC), 53–58. <https://doi.org/10.1109/ICFC.2019.00016>
- [69] Dong, S., Abbas, K., & Jain, R. (2019). A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments. *IEEE Access*, 7(c), 80813–80828. <https://doi.org/10.1109/ACCESS.2019.2922196>

- [70] Pandi (Jain), G. S., Shah, S., & Wandra, K. H. (2020). Exploration of Vulnerabilities, Threats and Forensic Issues and its impact on the Distributed Environment of Cloud and its mitigation. *Procedia Computer Science*, 167(2019), 163–173. <https://doi.org/10.1016/j.procs.2020.03.194>
- [71] Kumar, R., & Goyal, R. (2019). On cloud security requirements, threats, vulnerabilities and countermeasures: A survey. *Computer Science Review*, 33, 1–48. <https://doi.org/10.1016/j.cosrev.2019.05.002>
- [72] Mehedi Hasan, M. G. M., & Rahman, M. A. (2020). A signaling game approach to mitigate co-resident attacks in an IaaS cloud environment. *Journal of Information Security and Applications*, 50, 102397. <https://doi.org/10.1016/j.jisa.2019.102397>
- [73] Ali, O., Shrestha, A., Chatfield, A., & Murray, P. (2020). Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, 37(1), 101419. <https://doi.org/10.1016/j.giq.2019.101419>
- [74] Ohilla, S., & Mathew, R. (2020). Comparison of Cloud Computing Security Threats and Their Counter Measures. *Academia.Edu*, 224–231. https://doi.org/10.1007/978-3-030-43192-1_25
- [75] Muntés-Mulero, V., Ripolles, O., Gupta, S., Dominiak, J., Willeke, E., Matthews, P., & Somosköi, B. (2019). Agile risk management for multi-cloud software development. *IET Software*, 13(3), 172–181. <https://doi.org/10.1049/iet-sen.2018.5295>
- [76] Alouffi, B., Hasnain, M., Alharbi, A., Alosaimi, W., Alyami, H., & Ayaz, M. (2021). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access*, 9, 57792–57807. <https://doi.org/10.1109/ACCESS.2021.3073203>
- [77] Nagarajan, G., & Sampath Kumar, K. (2021). Security Threats and Challenges in Public Cloud Storage. 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 7, 97–100. <https://doi.org/10.1109/ICACITE51222.2021.9404641>
- [78] Syed, A., Purushotham, K., & Shidaganti, G. (2020). Cloud Storage Security Risks, Practices and Measures: A Review. 2020 IEEE International Conference for Innovation in Technology (INOCON), 1–4. <https://doi.org/10.1109/INOCON50539.2020.9298281>
- [79] Patel, A., Shah, N., Ramoliya, D., & Nayak, A. (2020). A detailed review of Cloud Security: Issues, Threats Attacks. *Proceedings of the 4th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2020*, 758–764. <https://doi.org/10.1109/ICECA49313.2020.9297572>
- [80] Garg, T., Shalu, Saini, N., & Singh, M. (2023). Comparative Study of Security Threats in Cloud Computing. 2023 5th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), (June), 1405–1410. <https://doi.org/10.1109/ICAC3N60023.2023.10541394>
- [81] Mandal, S., & Khan, D. A. (2020). A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic. 2020 International Conference on Smart Electronics and Communication (ICOSEC), (Icosec), 837–842. <https://doi.org/10.1109/ICOSEC49089.2020.9215374>
- [82] Chadwick, D. W., Fan, W., Costantino, G., de Lemos, R., Di Cerbo, F., Herwono, I., Manea, M., Mori, P., Sajjad, A., & Wang, X.-S. (2020). A cloud-edge based data security architecture for sharing and analysing cyber threat information. *Future Generation Computer Systems*, 102, 710–722. <https://doi.org/10.1016/j.future.2019.06.026>
- [83] Hussein, O. (2019). Identification of Threats and Vulnerabilities in Public Cloud-Based Apache Hadoop Distributed File System. 2019 15th International Computer Engineering Conference (ICENCO), 44–49. <https://doi.org/10.1109/ICENCO48310.2019.9027300>
- [84] Mahrin, M. N., Subbarao, A., Chuprat, S., & Abu Bakar, N. A. (2023). Cloud-based big data framework towards strengthening disaster risk reduction: systematic mapping. *Journal of Science and Technology Policy Management*, 14(6), 1–21. <https://doi.org/10.1108/JSTPM-03-2022-0049>
- [85] A Framework for Cloud Security Risk Management based on the Business Objectives of Organizations. *International Journal of Advanced Computer Science and Applications*, 10(12), 186–194. <https://doi.org/10.14569/IJACSA.2019.0101226>
- [86] Carrera-Rivera, A., Ochoa, W., Larrinaga, F., & Lasa, G. (2022). How-to conduct a systematic literature review: A quick guide for computer science research. *MethodsX*, 9, 101895. <https://doi.org/10.1016/j.mex.2022.101895>
- [87] Jia, Y., Xing, L., Mao, Y., Zhao, D., Wang, X., Zhao, S., & Zhang, Y. (2020). Burglars' IoT Paradise: Understanding and Mitigating Security Risks of General Messaging Protocols on IoT Clouds. 2020 IEEE Symposium on Security and Privacy (SP), 2020-May, 465–481. <https://doi.org/10.1109/SP40000.2020.00051>

- [88] Gupta, H., & Kumar, D. (2019). Security Threats in Cloud Computing. 2019 International Conference on Intelligent Computing and Control Systems (ICCS), (Iciccs), 1158–1162. <https://doi.org/10.1109/ICCS45141.2019.9065542>
- [89] Sasubilli, M. K., & R, V. (2021). Cloud Computing Security Challenges, Threats and Vulnerabilities. 2021 6th International Conference on Inventive Computation Technologies (ICICT), 476–480. <https://doi.org/10.1109/ICICT50816.2021.9358709>
- [90] Wang, X., Wang, L., Miao, F., & Yang, J. (2019). SVMDF: A Secure Virtual Machine Deployment Framework to Mitigate Co-Resident Threat in Cloud. 2019 IEEE Symposium on Computers and Communications (ISCC), 2019-June, 1–7. <https://doi.org/10.1109/ISCC47284.2019.8969721>
- [91] Pauley, E., Sheatsley, R., Hoak, B., Burke, Q., Beugin, Y., & McDaniel, P. (2022). Measuring and Mitigating the Risk of IP Reuse on Public Clouds. 2022 IEEE Symposium on Security and Privacy (SP), 2022-May(1), 558–575. <https://doi.org/10.1109/SP46214.2022.9833784>
- [92] Sandi, M. R. (2024). Soal Kebocoran Data, Universitas Indonesia Buka Suara - PAGE ALL : Okezone Edukasi. Okezone.Com. <https://edukasi.okezone.com/read/2024/07/19/65/3036603/soal-kebocoran-data-universitas-indonesia-buka-suara?page=all>
- [93] ISO Standard. (2015). ISO/IEC 27017-2015. In ISO Central Secretariat (Vol. 2015). <https://www.iso.org/standard/43757.html>
- [94] ISO Standard. (2019). ISO/IEC 27701-2019. <https://www.iso.org/standard/71670.html>
- [95] Undang-Undang Nomor 27 Tahun 2022, Pub. L. Nomor 27 Tahun 2022, Kementrian Sekretariat Negara Republik Indonesia, Deputy Bidang Perundang-undangan dan Administrasi Hukum 1 (2022). <https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022>
- [96] Eddermoug, N., Mansour, A., Azmi, M., Sadik, M., Sabir, E., & Bahassi, H. (2023). A Literature Review on Attacks Prevention and Profiling in Cloud Computing. *Procedia Computer Science*, 220(January), 970–977. <https://doi.org/10.1016/j.procs.2023.03.134>
- [97] Ahmad, S., Mehruz, S., & Beg, J. (2022). Assessment on potential security threats and introducing novel data security model in cloud environment. *Materials Today: Proceedings*, 62(September), 4909–4915. <https://doi.org/10.1016/j.matpr.2022.03.536>
- [98] Kharma, M., & Taweel, A. (2023). Threat Modeling in Cloud Computing - A Literature Review. In *Communications in Computer and Information Science: 1768 CCIS* (pp. 279–291). https://doi.org/10.1007/978-981-99-0272-9_19.
- [99] Yang, P., Xiong, N., & Ren, J. (2020). Data Security and Privacy Protection for Cloud Storage: A Survey. *IEEE Access*, 8, 131723–131740. <https://doi.org/10.1109/ACCESS.2020.3009876>
- [100] J. R. Venable, J. Pries-heje, R. L. Baskerville, J. R. Venable, and J. Pries-heje, “Choosing a Design Science Research Methodology,” 2017, [Online]. Available: <https://aisel.aisnet.org/acis2017/112>
- [101] Angraini, Megawati, & Haris, L. (2018). Risk Assessment on Information Asset an academic Application Using ISO 27001. 2018 6th International Conference on Cyber and IT Service Management (CITSM), (Citsm), 1–4. <https://doi.org/10.1109/CITSM.2018.8674294>
- [102] Göttlichová, M. (2020). Higher Education and Innovation in the Non-profit Sector. In *Springer Proceedings in Business and Economics* (pp. 331–340). https://doi.org/10.1007/978-3-030-36126-6_36
- [103] He, D., Yang, M., Jiang, R., Li, T., & Wang, J. (2025). Comprehensive assessment of privacy security of financial services in cloud environment. *Scientific Reports*, 15(1), 34266. <https://doi.org/10.1038/s41598-025-16457-9>



Copyright © 2026 by the authors. This is an open access article distributed under the CC BY-NC 4.0 license (<http://creativecommons.org/licenses/by-nc/4.0/>).