1. Cover Jurnal

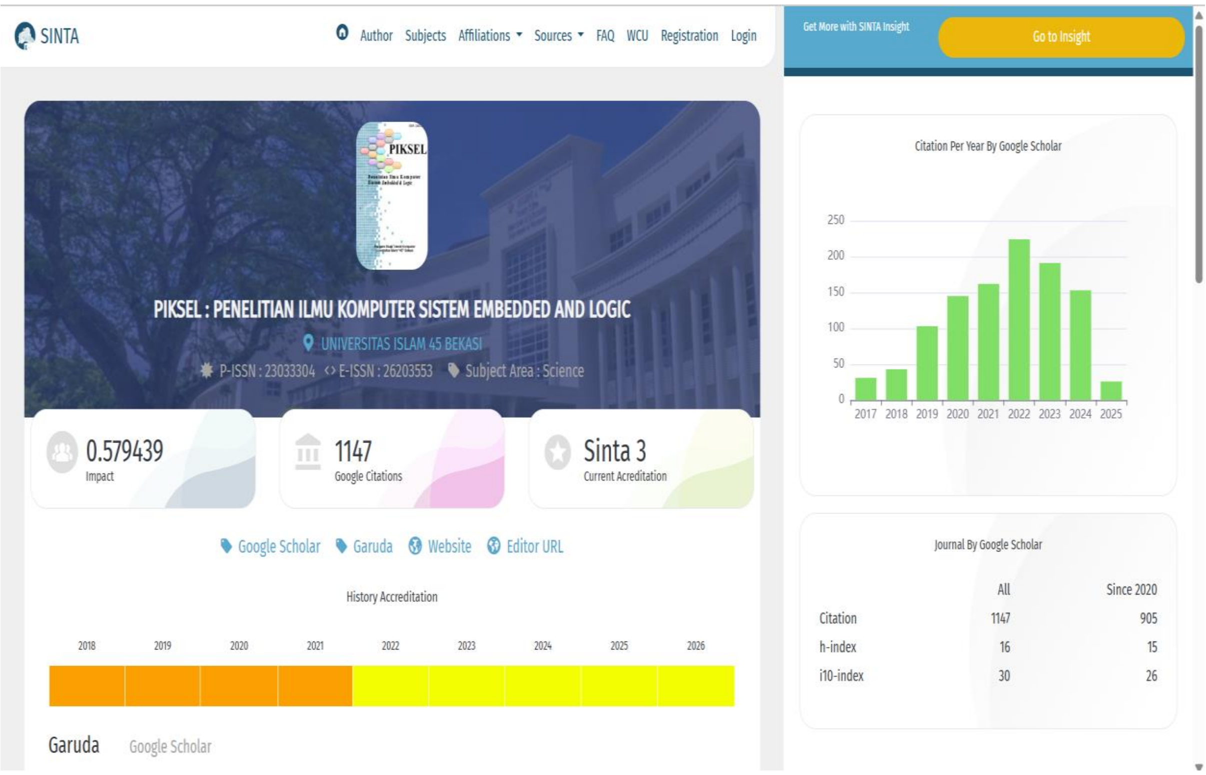
ISSN: 2303-3304

PIKSEL

Penelitian Ilmu Komputer
Sistem *Embedded & Logic*

Program Studi Teknik Komputer
Universitas Islam "45" Bekasi

2. Akreditasi SINTA 3



PIKSEL : PENELITIAN ILMU KOMPUTER SISTEM EMBEDDED AND LOGIC

UNIVERSITAS ISLAM 45 BEKASI

P-ISSN : 23033304 E-ISSN : 26203553 Subject Area : Science

0.579439 Impact

1147 Google Citations

Sinta 3 Current Acreditation

Google Scholar Garuda Website Editor URL

History Accreditation

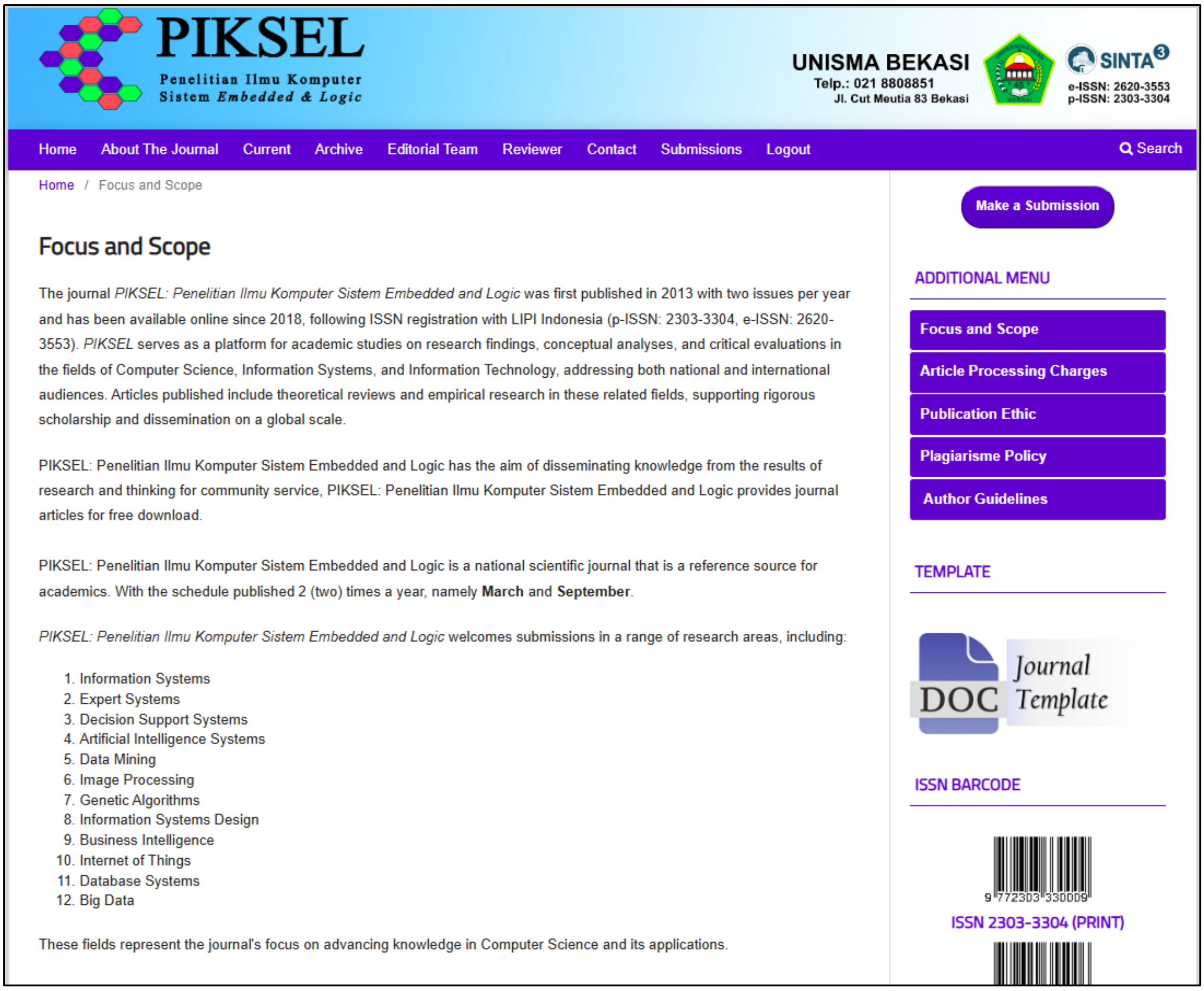
Garuda Google Scholar

Citation Per Year By Google Scholar

Journal By Google Scholar

	All	Since 2020
Citation	1147	905
h-index	16	15
i10-index	30	26

3. Focus and Scope



Focus and Scope

The journal *PIKSEL: Penelitian Ilmu Komputer Sistem Embedded and Logic* was first published in 2013 with two issues per year and has been available online since 2018, following ISSN registration with LIPI Indonesia (p-ISSN: 2303-3304, e-ISSN: 2620-3553). *PIKSEL* serves as a platform for academic studies on research findings, conceptual analyses, and critical evaluations in the fields of Computer Science, Information Systems, and Information Technology, addressing both national and international audiences. Articles published include theoretical reviews and empirical research in these related fields, supporting rigorous scholarship and dissemination on a global scale.

PIKSEL: Penelitian Ilmu Komputer Sistem Embedded and Logic has the aim of disseminating knowledge from the results of research and thinking for community service, PIKSEL: Penelitian Ilmu Komputer Sistem Embedded and Logic provides journal articles for free download.

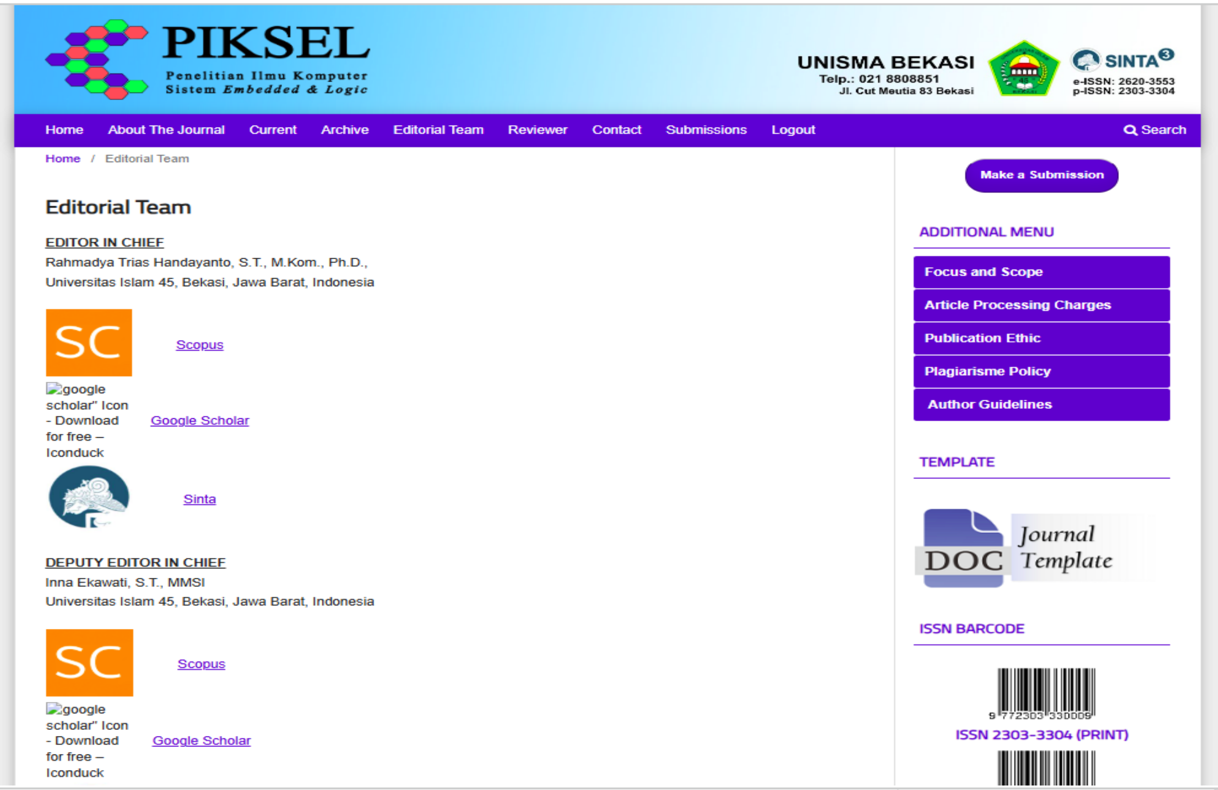
PIKSEL: Penelitian Ilmu Komputer Sistem Embedded and Logic is a national scientific journal that is a reference source for academics. With the schedule published 2 (two) times a year, namely **March** and **September**.

PIKSEL: Penelitian Ilmu Komputer Sistem Embedded and Logic welcomes submissions in a range of research areas, including:

1. Information Systems
2. Expert Systems
3. Decision Support Systems
4. Artificial Intelligence Systems
5. Data Mining
6. Image Processing
7. Genetic Algorithms
8. Information Systems Design
9. Business Intelligence
10. Internet of Things
11. Database Systems
12. Big Data

These fields represent the journal's focus on advancing knowledge in Computer Science and its applications.

4. Editorial Board



Editorial Team

EDITOR IN CHIEF

Rahmadya Trias Handayanto, S.T., M.Kom., Ph.D.,
Universitas Islam 45, Bekasi, Jawa Barat, Indonesia

SC Scopus

google scholar" Icon - Download for free – Iconduck Google Scholar

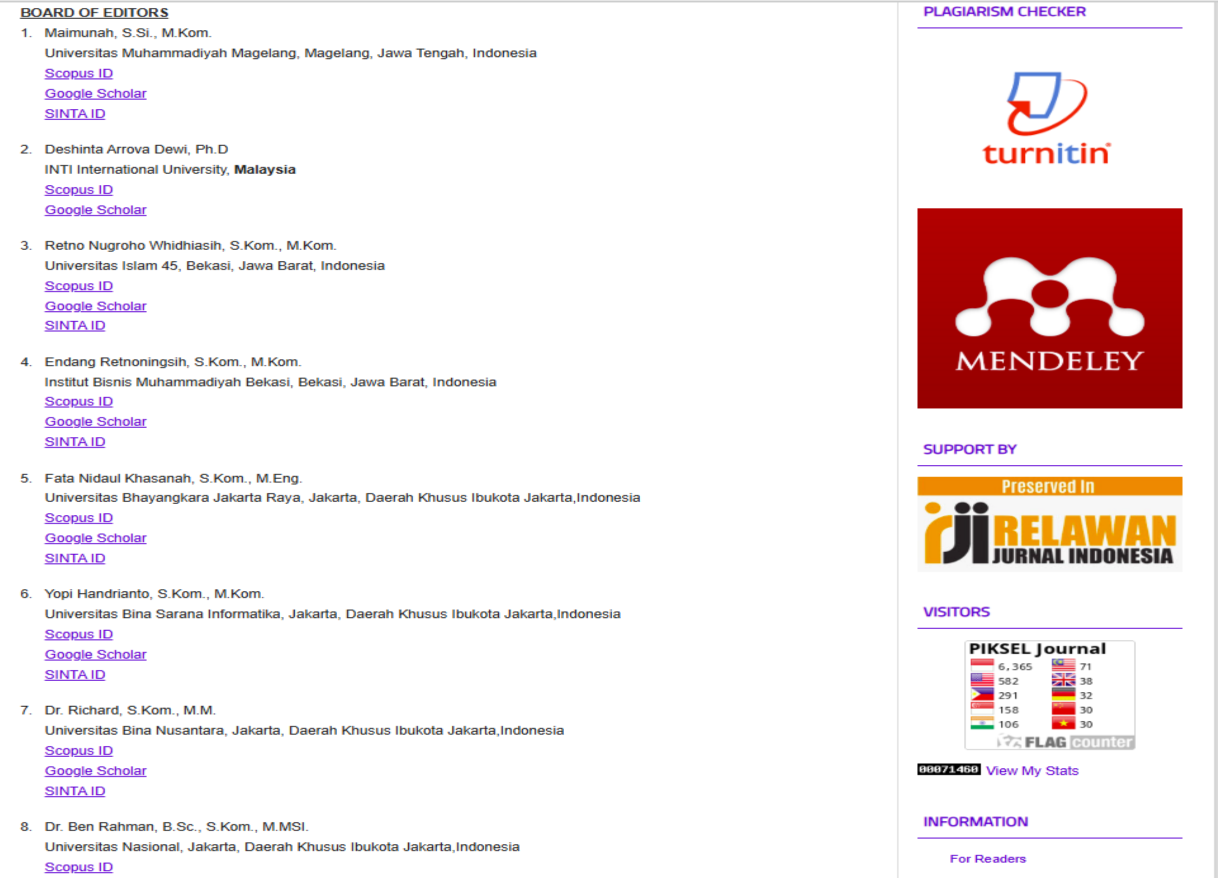
Sinta

DEPUTY EDITOR IN CHIEF

Inna Ekawati, S.T., MMSI
Universitas Islam 45, Bekasi, Jawa Barat, Indonesia

SC Scopus

google scholar" Icon - Download for free – Iconduck Google Scholar



BOARD OF EDITORS

1. Maimunah, S.Si., M.Kom.
   Universitas Muhammadiyah Magelang, Magelang, Jawa Tengah, Indonesia
   Scopus ID
   Google Scholar
   SINTA ID

2. Deshinta Arrova Dewi, Ph.D
   INTI International University, **Malaysia**
   Scopus ID
   Google Scholar

3. Retno Nugroho Whidhiasih, S.Kom., M.Kom.
   Universitas Islam 45, Bekasi, Jawa Barat, Indonesia
   Scopus ID
   Google Scholar
   SINTA ID

4. Endang Retnoningsih, S.Kom., M.Kom.
   Institut Bisnis Muhammadiyah Bekasi, Bekasi, Jawa Barat, Indonesia
   Scopus ID
   Google Scholar
   SINTA ID

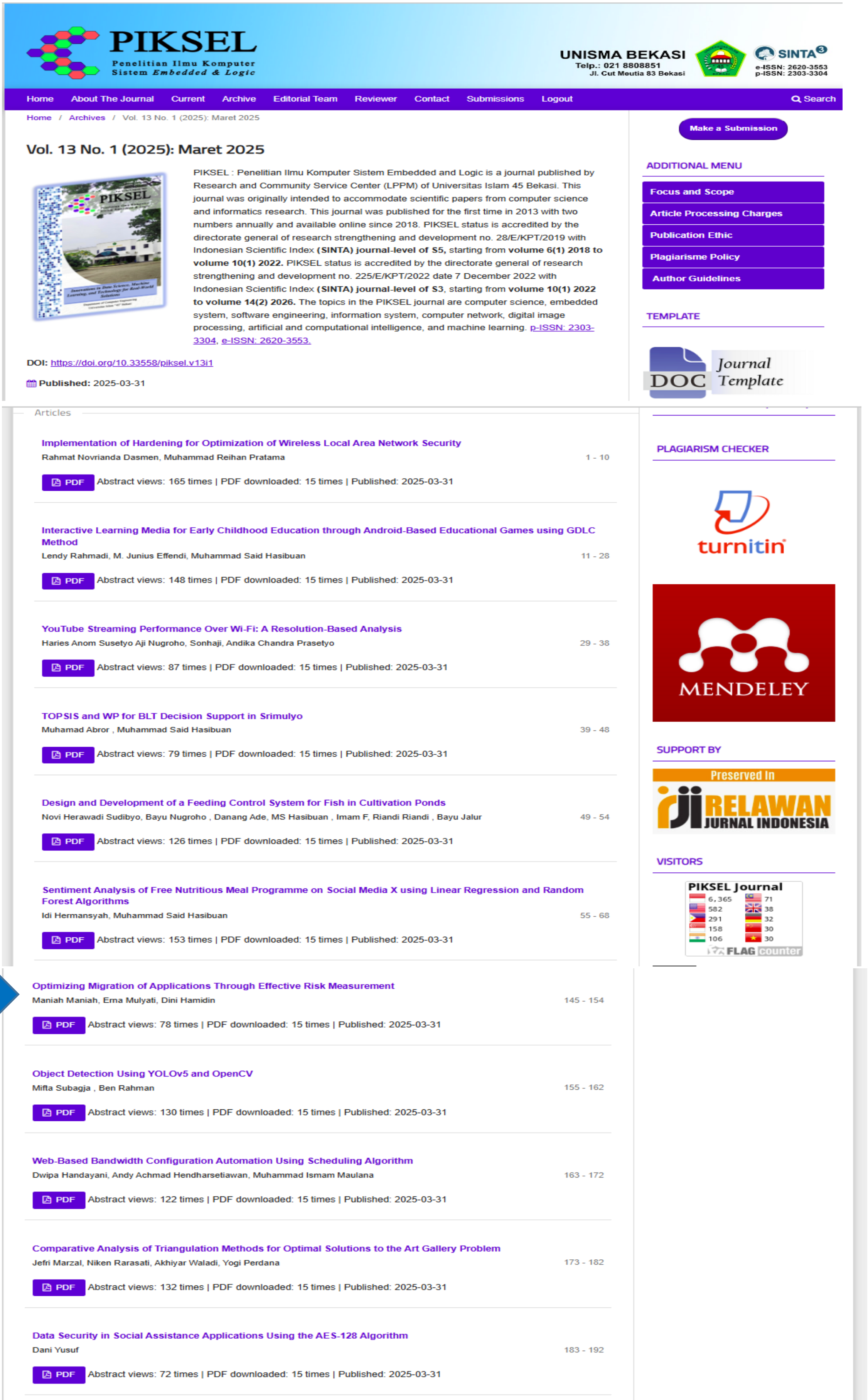
5. Fata Nidaul Khasanah, S.Kom., M.Eng.
   Universitas Bhayangkara Jakarta Raya, Jakarta, Daerah Khusus Ibukota Jakarta,Indonesia
   Scopus ID
   Google Scholar
   SINTA ID

6. Yopi Handrianto, S.Kom., M.Kom.
   Universitas Bina Sarana Informatika, Jakarta, Daerah Khusus Ibukota Jakarta,Indonesia
   Scopus ID
   Google Scholar
   SINTA ID

7. Dr. Richard, S.Kom., M.M.
   Universitas Bina Nusantara, Jakarta, Daerah Khusus Ibukota Jakarta,Indonesia
   Scopus ID
   Google Scholar
   SINTA ID

8. Dr. Ben Rahman, B.Sc., S.Kom., M.MSI.
   Universitas Nasional, Jakarta, Daerah Khusus Ibukota Jakarta,Indonesia
   Scopus ID

5. **Daftar Isi**



PIKSEL
Penelitian Ilmu Komputer
Sistem Embedded & Logic

UNISMA BEKASI
Telp.: 021 8808851
Jl. Cut Meutia 83 Bekasi

SINTA 3
e-ISSN: 2620-3553
p-ISSN: 2303-3304

Home / Archives / Vol. 13 No. 1 (2025): Maret 2025

Vol. 13 No. 1 (2025): Maret 2025

PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic is a journal published by Research and Community Service Center (LPPM) of Universitas Islam 45 Bekasi. This journal was originally intended to accommodate scientific papers from computer science and informatics research. This journal was published for the first time in 2013 with two numbers annually and available online since 2018. PIKSEL status is accredited by the directorate general of research strengthening and development no. 28/E/KPT/2019 with Indonesian Scientific Index **(SINTA) journal-level of S5,** starting from **volume 6(1) 2018 to volume 10(1) 2022.** PIKSEL status is accredited by the directorate general of research strengthening and development no. 225/E/KPT/2022 date 7 December 2022 with Indonesian Scientific Index **(SINTA) journal-level of S3,** starting from **volume 10(1) 2022 to volume 14(2) 2026.** The topics in the PIKSEL journal are computer science, embedded system, software engineering, information system, computer network, digital image processing, artificial and computational intelligence, and machine learning. p-ISSN: 2303-3304, e-ISSN: 2620-3553.

DOI: https://doi.org/10.33558/piksel.v13i1

Published: 2025-03-31

Articles

ADDITIONAL MENU

TEMPLATE

PLAGIARISM CHECKER

SUPPORT BY

VISITORS

PIKSEL Journal

🇮🇩	6,365	🇲🇾	71
🇺🇸	582	🇬🇧	38
🇵🇭	291	🇩🇪	32
🇸🇬	158	🇨🇳	30
🇮🇳	106	🇻🇳	30

PIKSEL
Penelitian Ilmu Komputer
Sistem Embedded and Logic

Penelitian Ilmu Komputer, Sistem Embedded and Logic
p-ISSN: 2303-3304, e-ISSN: 2620-3553
Vol. 13 (1): 145– 154 (March 2025)
The DOI 10.33558/piksel.v13i1.10800

Optimizing Migration of Applications Through Effective Risk Measurement

Maniah [1,*], Erna Mulyati [1], Dini Hamidin [2]

* Corespondence Author: e-mail: maniah@ulbi.ac.id

[1] Logistic Management Magister Program, Universitas Logistik dan Bisnis Internasional, Jl. Sariasih No.54, Sarijadi, Kec. Sukasari, Kota Bandung, Jawa Barat; 40151, Indonesia; e-mail: maniah@ulbi.ac.id ernamulyati@ulbi.ac.id
[2] Informatics Engineering, Universitas Logistik dan Bisnis Internasional Jl. Sariasih No.54, Sarijadi, Kec. Sukasari, Kota Bandung, Jawa Barat; 40151, Indonesia; e-mail: dinihamidin@ulbi.ac.id

Submitted : **14/02/2025**
Revised : **01/03/2025**
Accepted : **10/03/2025**
Published : **31/03/2025**

Abstract

Cloud Computing is a service that provides network storage space and computer resources using an internet connection as an access medium. The process of migrating to cloud computing goes through several stages sequentially and continuously, but sometimes the process of migrating to cloud computing faces obstacles or even failure, this is of course a risk for cloud service users. For this reason, before migrating to the cloud, it is necessary to prepare well, because if not, it will cause losses which will have a risk impact on the company. An effort to minimize risks for cloud service users is to carry out a risk assessment. The aim of this research is to create a model for risk assessment of logistics business applications in cloud migration. The risk value measurement model developed adopts the risk management model from the ISACA Risk IT Framework, the risk management process part of the ISO 31000 standard and adopts the phases of the OCTAVE method. Based on the method of measuring risk values from the results of this research, companies will know how much risk is likely to arise due to the use of cloud data centers, so that risk mitigation can be carried out immediately. This will have an impact on increasing the security of cloud services, and this is the main thing in increasing public confidence in using cloud services.

***Keywords**: Adoption, Cloud Migration, Risk Assessment, Security*

Introduction

A cutting-edge technology, cloud computing can offer data transaction capabilities for activities involving information sharing and cooperation with trading partners in the manufacturing, finance, distribution, sales, and customer support sectors. Businesses move to cloud computing for a variety of reasons, such as the fact that cloud providers offer options for server settings, software upgrades, and hardware setup, among other things, allowing businesses using cloud services to concentrate more on creating more inventive and superior products (Khan & Ullah, 2016). Optimizing migration strategies by focusing on resource allocation and risks associated with migration delays, addressing technical challenges inherent in the application migration process (Lin et al., 2023).

Cloud migration can mean the process of deploying part or all of digital assets, services, IT resources, or applications to the cloud, but when migrating to the cloud is likely to cause disruption to the company's business (Ahmad et al., 2018). Information security is one of the biggest risk components during cloud migration (Maniah, Soewito, Lumban Gaol, et al., 2022), so that a tailored risk assessment is required for the migration process, which is a mitigation strategy to identify risks (Fargnoli & Murgianu, 2023). Cloud computing service providers (CSPs) have provided facilities and services such as saving costs, maintaining information security and service stability, so that companies that use cloud services, do not pay special attention to how to handle risks and prepare good risk mitigation when the company decided to migrate to cloud computing (Islam et al., 2017a). The choice of risk before migration is an important thing for cloud service users to consider (Ahmad et al., 2018), this is because there are many cloud services offered with various qualities (Yang et al., 2022).

This research was conducted by referring to several previous studies, including research which aims to analyze and control risks for migrating to the cloud, where the risk value (*R*) is obtained from the number of risks based on the risk factors of each asset (r_i) divided by the number of risk factors. influential (*n*), where ri value: the risk value of each asset based on the probability of the risk factor $P(r_i)$ times the risk impact (*I*). The risk components used are assets, risk factors and risk impacts (Islam et al., 2017a). The next research aims to measure the risk value for information security in Cloud Computing, where the risk value for information security in the cloud *(R*) is obtained from multiplying the possibility of a threat (p_t) with the possibility of using a vulnerability (p_v), and the value of damage due to the threat (*d*) divided with the indicator control value on the cloud service (k_c). The risk components used are threat, vulnerability, damage value and control value (Kozlov & Noga, 2018).

Furthermore, there is research aimed at analyzing risks in the Healthcare Information System (HIS), with the research stages starting from Assets Identification and Evaluation, Threat Identification, Vulnerability Identification, and Risk Assessment: Likelihood Determination, Impact Analysis. The risk components used are assets, threats, vulnerabilities, likelihood, and impact (Abrar et al., 2018). Apart from that, there is further research which aims to analyze and predict the performance of cloud service providers (CSP) regarding services for cloud service customers (CSC) for effective service levels. The risk components used include availability, reliability, performance, security and financial risk (Maeser, 2020). An assessment model for project risk management, with a scientific and statistical approach, focused on modern project risks, highlighting the relevance of advanced statistical techniques for application migration assessment (Zhao, 2024).

The results of the study (Islam et al., 2017a; Kozlov & Noga, 2018) the risk value in cloud migration is obtained at the beginning when the company will decide to migrate to the cloud. Then, what is the risk value for applications that will be migrated to the cloud? This study will develop a risk value measurement model for logistics applications that will be migrated to cloud computing. This risk value measurement model is divided into several stages, namely identifying risks, determining risk assessment indicators, calculating asset weight values, and finally the risk value is obtained by taking into account asset threats and vulnerabilities. This risk value measurement model is useful for companies in mitigating risks.

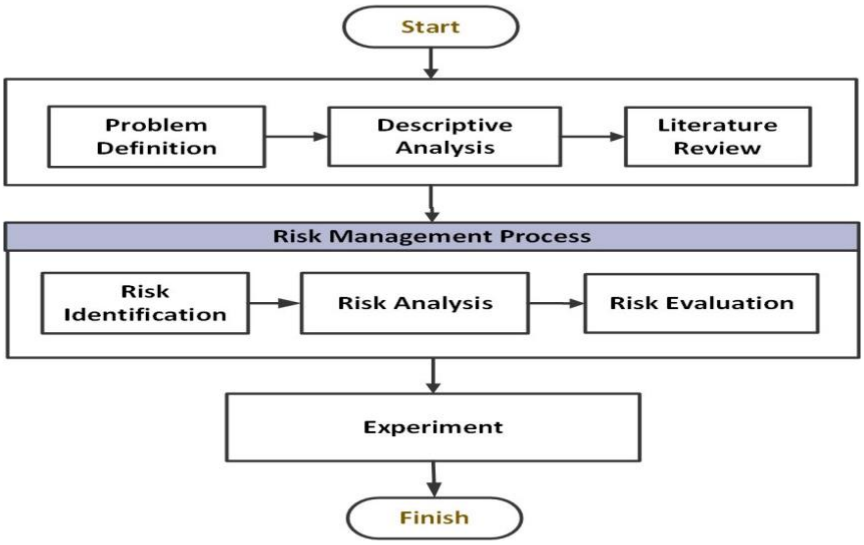
2. Research Method

The research method approach used in this research is a mixture of a qualitative approach and a semi-quantitative approach. Qualitative/descriptive approach, namely a research approach that uses investigative strategies such as narrative, phenomenology, ethnography, grounded theory studies, or case studies (Malek et al., 2019). In this research, the sampling method uses non-probability sampling with selected sampling techniques (purposive sampling), based on the criteria or characteristics of respondents that have been determined by the researcher. The criteria or characteristics used to determine the units that will be the research sample are as follows: 1. Included in the logistics services business. 2. As a user of cloud computing services.

Data collection methods to obtain data in this research, it was done in several ways, namely:

1. Provide questionnaires and interviews to related parties in the logistics services industry to obtain the data needed by researchers. The targets for collecting data through questionnaires are:
    a. Head of Information Communication and Technology (ICT).
    b. Information Communication and Technology (ICT) staff.
2. Through Focus Group Discussion (FGD) activities to obtain more detailed information about the implementation of cloud computing in the logistics business.
    The results of this FGD activity obtained input to determine:
    a. The magnitude of the possible risks from each threat to cloud migration;
    b. Level of vulnerability in cloud migration;
    c. Determine the risk aspects that have an impact on the company and the weight of each risk aspect;
    d. Determine environmental aspects and the weight of each environmental aspect when migrating and after migrating to cloud computing.

The researcher is fully involved in data collection, and the researcher also involves other people to help collect data, where these people are previously given sufficient explanation of the aims and objectives of this data collection. During the data collection process, the people involved are always under the supervision of researchers. In this research, the research implementation stages are structured based on research problems which are used as technical guidance to produce the model in this research. The complete research implementation stages are shown in Figure 1 below:



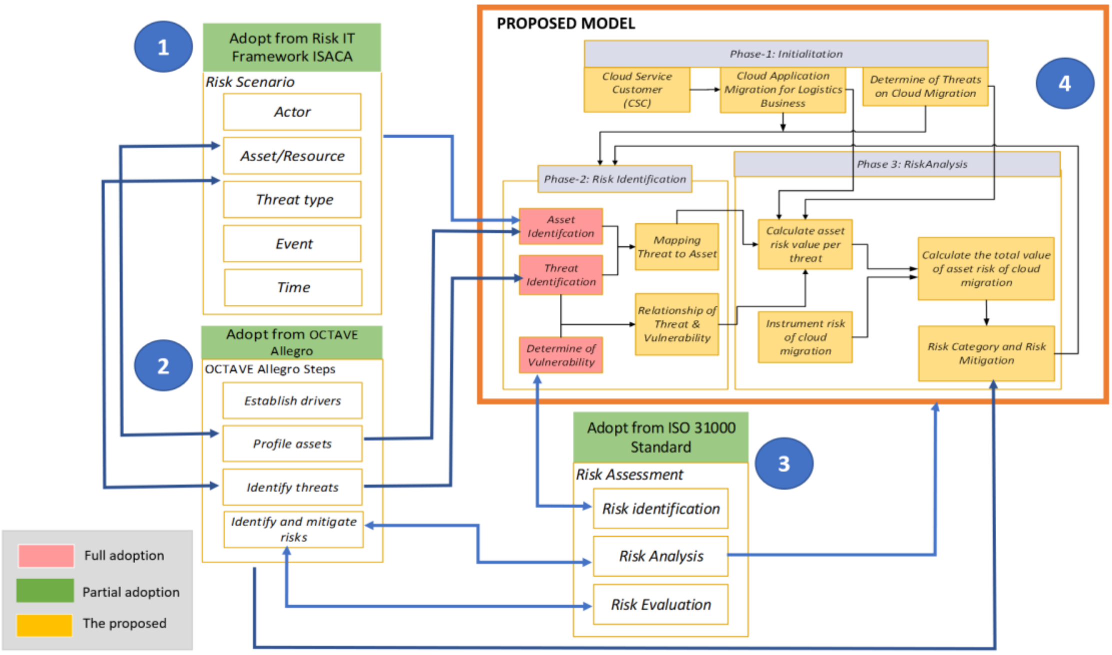
Source: Research Result (2024)

Figure 1. Research Implementation Stage

This research stage starts from defining the problem, then a literature review of previous research is carried out to find solutions to existing problems. Next is risk identification, risk analysis and risk evaluation. In determining the steps for this risk management process, this research adopted the ISACA Risk IT Framework, ISO 31000 International Standard, and the OCTAVE Allegro method. The data collection techniques used in this research were Literature Review, Questionnaire, Interview, and Focus Group Discussion (FGD), and adopted the risk measurement formula from (Islam et al., 2017b; Kozlov & Noga, 2018).

3. Results and Analysis

The proposed model aims to calculate the risk in applications that will be migrated to cloud computing and is created systematically which can provide facilities for cloud service users in calculating the possible risk value for applications that will be migrated to cloud computing. The model developed by this researcher adopts the risk evaluation stages of the Risk IT Framework, adopts risk scenarios from the ISO 31000 standard and adopts the phases of the OCTAVE method. The scenario of step by step development of the proposed model begins with extracting from the three frameworks (Risk IT Framework ISACA, ISO 31000 standard, and OCTAVE Allegro method) as shown in Figure 2.


1
Adopt from Risk IT Framework ISACA
Risk Scenario
Actor
Asset/Resource
Threat type
Event
Time
2
Adopt from OCTAVE Allegro
OCTAVE Allegro Steps
Establish drivers
Profile assets
Identify threats
Identify and mitigate risks
Full adoption
Partial adoption
The proposed
PROPOSED MODEL
Phase-1: Initialitation
Cloud Service Customer (CSC)
Cloud Application Migration for Logistics Business
Determine of Threats on Cloud Migration
4
Phase-2: Risk Identification
Asset Identifcation
Threat Identification
Determine of Vulnerability
Mapping Threat to Asset
Relationship of Threat & Vulnerability
Phase 3: RiskAnalysis
Calculate asset risk value per threat
Instrument risk of cloud migration
Calculate the total value of asset risk of cloud migration
Risk Category and Risk Mitigation
Adopt from ISO 31000 Standard
3
Risk Assessment
Risk identification
Risk Analysis
Risk Evaluation

Source: Research Result (2024)

Figure 2. Proposed Model

The phases in the risk value analysis measurement model for applications that will be migrated to cloud computing can be explained as follows:

Phase 1: The initialization process is divided into 3 (three) parts, namely:

1. Determine the cloud service user logistics company that will be the object. It is necessary to determine the company profile because it will affect the scope and characteristics of the company.
2. Determine the applications that will be migrated to cloud computing and whose risk values will be calculated. Different companies will allow different applications to be used.
3. Determine the threats that may arise in cloud migration. To find out the threats to cloud migration, you can search through literature reviews of previous research.

Phase 2: Identifying risks, in this phase the following steps are taken:

1. Identification of company assets in the form of application systems that support the company's business processes, both internal and external, that will be migrated to cloud computing.
2. Identification of threats that exist in cloud migration based on references or sources, in this study researchers took sources from Top Threats to Cloud Computing the Egregious 11 (Caralli et al., 2007).
3. Determine vulnerabilities that will provide potential threats to cloud migration.

3.1. Asset, Threats, and Vulnerability Identification

Asset identifiers are a way to define information for risk analysis in a cloud context. Based on the results of the analysis carried out by researchers, there are logistics applications that will be migrated to the cloud. The list of applications above is an example of a number logistics business applications aimed at internal and external company needs that are generic, meaning there is no limit whatsoever to the number of applications migrated to the cloud. The difference between internal and external company applications is based on the purpose and scope of the application, applications that aim to support the company's business processes externally have relatively greater complexity compared to internal applications, because external applications will have a relatively greater impact on business transactions in the company. So, this will have an impact on the risk value of the application, the greater the complexity of an application, the relatively greater risk value it will have as well. The applications identified are intended for applications that represent almost all applications used by logistics companies that will provide services to their customers, both national and international. So that sampling of these applications is quite representative based on their scope or complexity, and if used in other similar research can produce relatively similar results.

Next is the threat identification stage in cloud computing. Based on the results of previous research (Maniah, Soewito, Gaol, et al., 2022), there are 11 (eleven) types of threats to cloud migration taken from the results of the Cloud Security Alliance (CSA) survey, namely: T-1 (Data Breaches), T-2 (Misconfiguration and Inadequate Change Control), T-3 (Lack of Cloud Security Architecture and Strategy), T-4 (Insufficient Identity, Credential, Access and Key Management), T-5 (Account Hijacking), T-6 (Insider Threat), T-7 (Insecure Interfaces and APIs), T-8 (Weak Control Plane), T-9 (Meta structure and Appl structure Failures), T-10 (Limited Cloud Usage Visibility), T-11 (Abuse and Nefarious Use of Cloud Services) (Adam, 2022). Referring to research results from (Maniah, Soewito, Gaol, et al., 2022), each threat to cloud computing has a probability of occurrence value (%).

Each threat will have an impact on applications that are migrated to the cloud by giving a value between 1 to 100 with low-risk categories (0 to 30), medium-risk (30 to 60), and high-risk (61 to 60). /d 100). Next, the result assessment value is calculated using the formula:

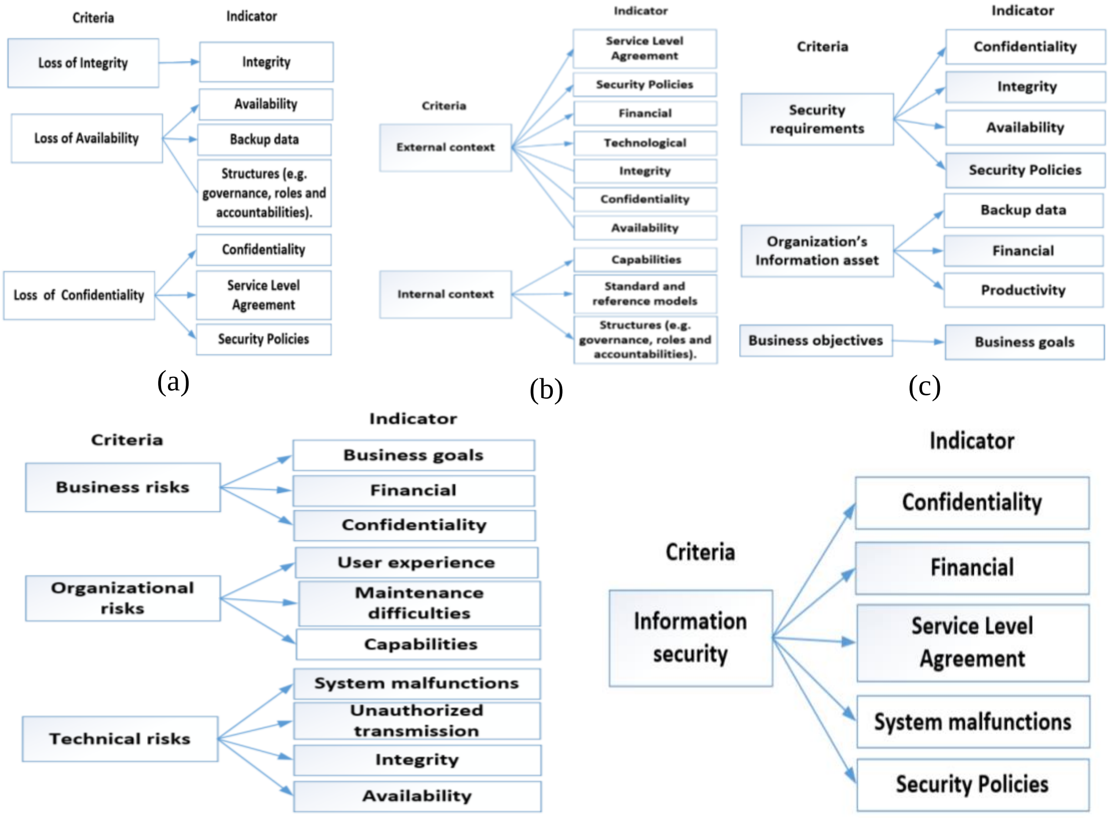
$$r_a = \sum_{1}^{n} p_o v_a \tag{1}$$

Where:
r_a = result assessment for each asset
p^o = probability of occurrence the possibility of a threat occurring.
v_o = asset value
1…n= the number of threats identified.

Next, we will look at the threats that have been defined above, what are the potential possibilities for these threats to emerge, which we call vulnerabilities. Based on references from previous research, with the level of vulnerability divided into 4 (four), namely: Low (0 to 3.9), Average (4 to 6.9) , High(7 to 9.9) and Critical is 10 (Kozlov & Noga, 2018). To determine the level of vulnerability for each vulnerability, it is determined based on the results of the agreement in the Focus Group Discussion which provides input for the level of vulnerability based on a range of values for the level of vulnerability.

3.2. Risk Assessment Indicators

The risk assessment indicators used in this research are adopted from several indicators contained in existing risk management models or frameworks (Giude, 2008; ITA, 2017; Musungwini & Mahlangu, 2016), and added with indicators from the results of previous studies (Islam et al., 2017a; Kozlov & Noga, 2018).

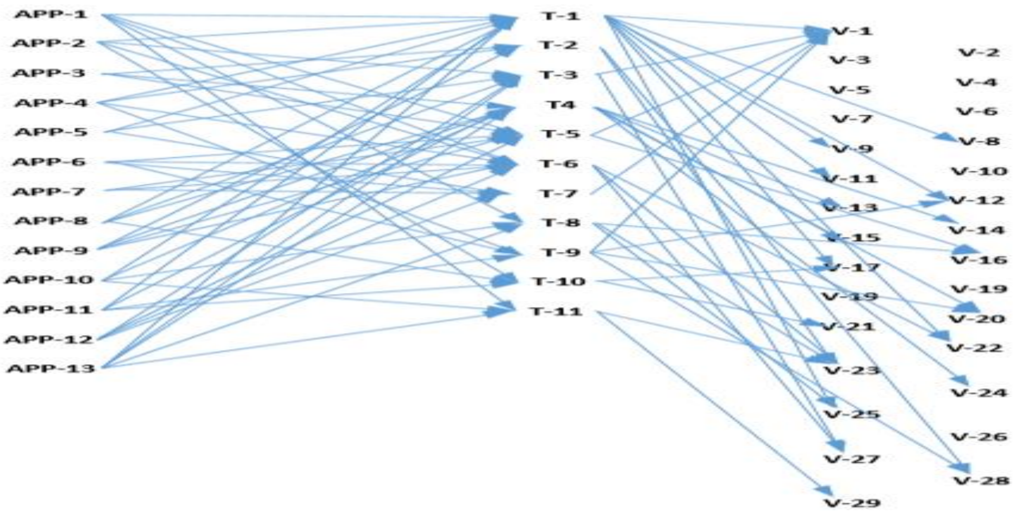


Source: (a) IT Risk Management Framework v.1(E.oman, 2017); (b) ISO/IEC Guide 73 (Giude, 2008); (c) OCTAVE Allegro v1.0 (Musungwini & Mahlangu, 2016); and Criteria and indicator of risk assessment (a) (Islam et al., 2017a), (b) (Kozlov & Noga, 2018)

Figure 3. Risk Assessment Indicators

3.3. Mapping Assets to Threats, and Threats to Vulnerabilities

Asset to threat mapping aims to find out how many threats are likely to arise against the security of applications that will be migrated to cloud computing. The number of threats to these applications also really depends on the empirical experience experienced by cloud service users and can be applied to logistics companies that will migrate their applications to cloud computing. This mapping was obtained from the results of the researcher's questionnaire which was submitted online to the ICT team who owns the logistics application. Every 1 (one) application can have several types of security threats in the cloud. To determine what types of threats to the logistics application, this really depends on the opinion of the manager and owner of the application, because they know in detail the characteristics of the application. Vulnerability is a potential possibility of a threat occurring. In this research, the relationship between threats and vulnerabilities is assumed to mean that 1 (one) threat can have several (N) vulnerabilities, so that the relationship between threats and vulnerabilities is 1-N (one to many).



Source: Research Result (2024)

Figure 4. Mapping Assets to Threats, and Threats to Vulnerabilities

Mapping threats (T) to assets (APP) aims to find out how many threats are likely to arise against the security of applications that will be migrated to cloud computing. The number of threats to these applications also really depends on the empirical experience experienced by cloud service users and can be applied to logistics companies that will migrate their applications to cloud computing. Meanwhile, for mapping between threats (T) and vulnerabilities (V), it is assumed that 1 (one) threat can have several (N) vulnerabilities, so that the relationship between threats and vulnerabilities is 1-N (one to many). The magnitude of the vulnerability value of each threat is by adding up the value of each potential vulnerability to that threat. Next, the average value is calculated which will be used as the final vulnerability value for a threat, and this value will be used to calculate the risk value for all applications that are migrated to the cloud.

Example, threats in T-1 have 8 (eight) potential vulnerabilities, namely V-1, V-8, V-9, V-11, V-12, V-17, V-22, V-25, so the total vulnerability values for the T-1 threat are as follows: Vulnerability value v = 7+3+3+5+4+3+8+5 = 38, and the vulnerability value at T-1 is =38/8 = 4.75 ~ 4.8. In the same way to calculate the vulnerability value for the 2nd threat (T-2) and so on.

3.4. Calculating Risk Value

Based on the result assessment value, vulnerability value, and the weight value for each indicator from the risk assessment, the risk value can then be calculated for each application (asset) that will be migrated to cloud computing.

$$R = \sum_{1}^{n} (R_a V) W_i \qquad (2)$$

Where:

R = total risk value

R_a = result assessment for each asset

V = vulnerability value for each asset

W = percentage of indicator weight

1…n= the number indicators identified

The complete risk calculation results per asset migrated to cloud computing can be shown in Table 1.

Table 1. Risk Analysis Value in Cloud Migration

ID_App	R_a	*V*	Indicators																	Risk Value (*R*)
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
Criteria Weigh			**8%**	**8%**	**8%**	**5%**	**5%**	**5%**	**6%**	**6%**	**5%**	**5%**	**5%**	**8%**	**5%**	**5%**	**6%**	**5%**	**5%**	
AP-1	78.5	6.8	79.0	79.0	79.0	78.8	78.8	78.8	78.9	78.9	26.5	78.8	78.8	79.0	78.8	78.8	78.9	78.8	78.8	**74.1**
AP-2	74.4	5.6	74.9	74.9	74.9	74.7	74.7	74.7	74.7	74.7	21.0	74.7	74.7	74.9	74.7	74.7	74.7	74.7	74.7	**69.9**
AP-3	39.2	6.5	39.7	39.7	39.7	39.5	39.5	39.5	39.6	39.6	12.7	39.5	39.5	39.7	39.5	39.5	39.6	39.5	39.5	**37.2**
AP-4	45.6	6.0	46.1	46.1	46.1	45.9	45.9	45.9	46.0	46.0	13.7	45.9	45.9	46.1	45.9	45.9	46.0	45.9	45.9	**43.0**
AP-5	47.5	6.3	48.0	48.0	48.0	47.8	47.8	47.8	47.8	47.8	14.8	47.8	47.8	48.0	47.8	47.8	47.8	47.8	47.8	**44.8**
AP-6	80.6	7.0	81.2	81.2	81.2	80.9	80.9	80.9	81.0	81.0	28.0	80.9	80.9	81.2	80.9	80.9	81.0	80.9	80.9	**76.2**
AP-7	82.3	7.3	82.8	82.8	82.8	82.6	82.6	82.6	82.7	82.7	29.9	82.6	82.6	82.8	82.6	82.6	82.7	82.6	82.6	**77.9**
AP-8	48.5	5.3	48.9	48.9	48.9	48.8	48.8	48.8	48.8	48.8	12.9	48.8	48.8	48.9	48.8	48.8	48.8	48.8	48.8	**45.6**
AP-9	62.2	6.7	62.7	62.7	62.7	62.5	62.5	62.5	62.6	62.6	20.8	62.5	62.5	62.7	62.5	62.5	62.6	62.5	62.5	**58.8**
AP-10	45.4	6.2	45.9	45.9	45.9	45.7	45.7	45.7	45.8	45.8	14.1	45.7	0.3	45.9	45.7	45.7	45.8	45.7	45.7	**38.8**
AP-11	40.3	5.1	40.7	40.7	40.7	40.5	40.5	40.5	40.6	40.6	10.2	40.5	40.5	40.7	40.5	40.5	40.6	40.5	40.5	**37.8**
AP-12	62.2	*7.2*	62.7	62.7	62.7	62.5	62.5	62.5	62.6	62.6	22.4	62.5	62.5	62.7	62.5	62.5	62.6	62.5	62.5	**58.9**
AP-13	47.2	*6.4*	47.7	47.7	47.7	47.5	47.5	47.5	47.5	47.5	15.0	47.5	47.5	47.7	47.5	47.5	47.5	47.5	47.5	**44.6**

Source: Research Result (2024)

We group risks into 3 (three) categories of low risk (0-30), medium risk (31-60), and high risk (61-100). Next, the risk level can be determined through a risk map. The purpose of a risk map is to determine the priority scale for handling risks, where each company determines the level of risk through a risk map which will vary from one company to another depending on the agreement of the company's management. The results of the risk analysis value in table 1 above will be used as a reference for determining a risk map to determine risk appetite based on the Risk IT Framework from ISACA as a risk mitigation approach as shown in Table 2.

Table 2. Risk Mitigation Approach

Risk Value	Risk Category	Risk Map
0 - 30	Low	*Opportunity*
31 - 60	Medium	*Acceptable or Unacceptable*
61 - 100	High	*Really Unacceptable*

Source: Research Result (2024)

Several strategies will be used to approach risk mitigation for the low, medium and high-risk categories as the company's efforts to handle risk. The strategies proposed for the risk categories are as follows:

- Opportunity: the risk value is in the low category; the company does not have to take action to overcome the risk.
- Acceptable: the risk value is in the medium category, the company can create a strategy to overcome possible threats or minimize the impact of threats, but the company does not need to take special measures.
- Unacceptable: risk value in the medium category, the company can still accept the risk but allows the company to take special action to handle the risk, for example transferring the risk to another party.
- Really Unacceptable: the risk value is in the high category, including a type of risk that the company cannot accept, and the company must analyze existing risks in more detail and collect additional information to monitor and re-evaluate decisions regarding assets that have high risk.

4. Conclusion

Information security risks are very closely related to data breaches, so the impact of risks that often arise is threats to privacy and data integrity. Using servers together (multitenant) is also a risk factor in cloud computing. There are several risk factors in cloud migration, including technological factors, environmental factors, and organizational factors. Choosing the right CSP is also an important thing to pay attention to before migrating to the cloud. To ensure security in cloud migration is a shared responsibility for related parties, for example government, private organizations, education and researchers. This research has produced a risk value measurement model for logistics business applications that will be migrated to the cloud by considering risk management indicators obtained through the adoption process from several previous studies as well as the possible threat of cloud computing to data security. With this proposed model, cloud service users will be given easier and more structured steps in carrying out risk assessments starting from measuring asset weights, mapping the relationship between assets and threats and then calculating the vulnerability value for each threat until finally being able to determine the level of risk for each threat. applications to be migrated to cloud computing.

Acknowledgements

This research was funded by the Directorate General of Higher Education, Research and Technology, Directorate General of Vocational Education, Ministry of Education, Culture, Research and Technology in the Research and Community Service Grant program. The author would like to express his sincere thanks for this research grant. The author also would like to thank the University of Logistics and International Business as the institutional institution where the author currently works, for the support provided to the author.

Author Contributions

Maniah proposed the topic and design model; Dini Hamidin designed the experiments; Erna Mulyati analysed the result.

Conflicts of Interest

The author declare no conflict of interest.

References

Abrar, H., Hussain, S. J., Chaudhry, J., Saleem, K., Orgun, M. A., Al-Muhtadi, J., & Valli, C. (2018). Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry. *IEEE Access*, *6*, 19140–19150. https://doi.org/10.1109/ACCESS.2018.2805919

Adam, E. (2022). Cloud Security Alliance Egregious 11. In *Альманах Современной Науки И Образования* (Vol. 10, Issue 77, pp. 1–6). Security Innovation. https://blog.securityinnovation.com/cloud-security-alliance-egregious-11

Ahmad, N., Naveed, Q. N., & Hoda, N. (2018). Strategy and procedures for Migration to the Cloud Computing. *2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, 1–5.

Caralli, R. A., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process. In *Software Engineering Institute* (Issue May). http://www.sei.cmu.edu/publications/pubweb.html

E.oman. (2017). *IT Risk Management Framework*. https://www.moheri.gov.om/userupload/Policy/IT Risk Management Framework.pdf

Fargnoli, M., & Murgianu, L. (2023). A Resilience Engineering Approach for the Risk

Assessment of IT Services. *Applied Sciences (Switzerland)*, *13*(20). https://doi.org/10.3390/app132011132

Giude. (2008). *Risk management — Vocabulary ISO/IEC CD 2 Guide 73,* (Issue 30, pp. 1–12).

Islam, S., Fenz, S., Weippl, E., & Mouratidis, H. (2017a). A Risk Management Framework for Cloud Migration Decision Support. *Journal of Risk and Financial Management*, *10*(2), 1–24. https://doi.org/10.3390/jrfm10020010

Islam, S., Fenz, S., Weippl, E., & Mouratidis, H. (2017b). A Risk Management Framework for Cloud Migration Decision Support. *Risk and Financial Management*, *10*(10). https://doi.org/10.3390/jrfm10020010

ITA. (2017). IT Risk Management Framework - Governance & Standards Division. In *IT Risk Management Framework* (1.0, p. 23).

Khan, S. U., & Ullah, N. (2016). Challenges in the adoption of hybrid cloud: an exploratory study using systematic literature review. *The Journal of Engineering*, *2016*(5), 107–118. https://doi.org/10.1049/joe.2016.0089

Kozlov, A. D., & Noga, N. L. (2018). Risk Management for Information Security of Corporate Information Systems Using Cloud Technology. *2018 Eleventh International Conference "Management of Large-Scale System Development" (MLSD)*, 1–5. https://doi.org/10.1109/MLSD.2018.8551947

Lin, C., Sun, H., Wang, S., An, C., Qi, H., & Luo, X. (2023). Container Migration Strategy Based on Multi-objective Optimization for Edge-Cloud Coordination enabled Smart Grids. *Journal of Computers*, *34*(6), 047–062. https://doi.org/10.53106/199115992023123406004

Maeser, R. (2020). Analyzing CSP Trustworthiness and Predicting Cloud Service Performance. *EEE Open Journal of the Computer Society*, *1*, 1–12. https://doi.org/10.1109/OJCS.2020.2994095

Malek, M., Oghabian, Z., Tabibian, E., Rahmani, M., Yazdi, S. N. M., Oghabian, M. A., & Parviz, S. (2019). Comparison of qualitative (time intensity curve analysis), semi-quantitative, and quantitative multi-phase 3T dce-mri parameters as predictors of malignancy in adnexal. *Asian Pacific Journal of Cancer Prevention*, *20*(6), 1603–1611. https://doi.org/10.31557/APJCP.2019.20.6.1603

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

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

Musungwini, S., & Mahlangu, G. (2016). Framework for Threat Modelling for a Power Utility : Case of Zimbabwe Power Utility Company. *Internastional Journal of Computer Science and Business Informatics*, *16*(1), 8–23. https://www.semanticscholar.org/paper/Framework-for-threat-modelling-for-a-power-utility%3A-Musungwini-Mahlangu/52f98d207a6f4b02aff2e49e5daa51b7f8f9334b

Yang, M., Gao, T., Xie, W., Jia, L., & Zhang, T. (2022). The Assessment of Cloud Service Trustworthiness State Based on D-S Theory and Markov Chain. *IEEE Access*, *10*(June), 68618–68632. https://doi.org/10.1109/ACCESS.2022.3185684

Zhao, B. (2024). Construction of an Assessment Model for Project Risk Management Effectiveness Based on Statistics. *Highlights in Business, Economics and Management*, *42*, 70–75. https://drpress.org/ojs/index.php/HBEM/article/view/27212/26755