



IJCCS (Indonesian Journal of Computing and Cybernetics Systems)

Accredited "B" by the Ministry of Research, Technology and Higher Education of the Republic of Indonesia
Publish jointly by The Department of Computer Science and Electronics, FMIPA UGM and IndoCEISS
ISSN 1978-1520 (print); ISSN 2460-7258 (online)



Home > Vol 16, No 3 (2022) > **Maniah**

Risk Assessment for Logistics Applications in Cloud Migration

 <https://doi.org/10.22146/ijccs.74567>

Maniah Maniah^(1*), Benfano Soewito⁽²⁾, Ford Lumban Gaol⁽³⁾, Edi Abdurachman⁽⁴⁾

- (1) Prodi D3 Manajemen Informatika, Politeknik Pos Indonesia, Bandung
(2) Computer Science Department, BINUS Graduate Program, Doctor of Computer Science, Bina Nusantara University, Jakarta
(3) Computer Science Department, BINUS Graduate Program, Doctor of Computer Science, Bina Nusantara University, Jakarta
(4) Computer Science Department, BINUS Graduate Program, Doctor of Computer Science, Bina Nusantara University, Jakarta
(*) Corresponding Author

Abstract

The increase in the number of cloud data centers is due to an increase in the number of companies migrating to cloud computing. There are many advantages that companies get when migrating to the cloud, but there are also many disadvantages. Multitenancy security and privacy are important challenges for cloud migration users. This study proposes a way to assess the risks that may arise in the cloud migration process for logistics business applications. The research method used is semi-quantitative with a 3-phase approach, namely before migration, during migration, and after migration by considering the criteria for risk aspects and environmental aspects that will have an impact on the company, so that companies can make risk mitigation plans. The results of this study identified 11 (eleven) threats in the cloud that occupy the top ranking and identify as many as 17 (seventeen) indicators obtained from the identification of indicators in the previous model or framework used to assess risks in logistics business applications that will be implemented. migrated to the cloud. Based on the experimental results in this study, the application risk value during migration and after migration has a higher value than before migration, and the risk value during migration are higher than the risk value after migration.

Keywords

Cloud Computing; Cloud Migration; Threats; Indicators; Risk Value

Full Text:

References

[1] C. Pahl, H. Xiong, and R. Walshe, "A comparison of on-premise to cloud migration approaches," *Comput. Sci.*, vol. 8135 LNCS, no. ESOC 2013, pp. 212–226, 2013, DOI: 10.1007/978-3-642-40651-5_18.

[2] D. Rountree and I. Castrillo, *The Basics of Cloud Computing Understanding the Fundamentals of Cloud Computing in Theory and Practice*, Syngress. Hai Jiang, 2013.

[3] R. J. Priyadarsini and L. Arokiam, "Failure Management In Cloud : An Overview," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 10, 2013.

[4] P. Gupta and C. Gupta, "Evaluating the Failures of Data Centers in Cloud Computing," *Int. J. Comput. Appl.*, vol. 108, no. 4, pp. 29–34, 2014, [Online]. Available: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.671.5978&rep=rep1&type=pdf>.

[5] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," *IEEE Internet Comput.*, vol. 16, no. 1, pp. 69–73, 2012.

[6] R. Patil, H. Dudeja, and C. Modi, "Designing in-VM-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing," *Int. J. Inf. Secure.*, vol. 19, pp. 147–162, 2019, DOI: 10.1007/s10207-019-00447-w.

[7] R. Felani, M. N. Al Azam, D. P. Adi, A. Widodo, and A. B. Gumelar, "Optimizing Virtual Resources Management Using Docker on Cloud Applications," *IJCCS (Indonesian J. Comput. Cybern. Syst.)*, vol. 14, no. 3, pp. 319–330, 2020, DOI: 10.22146/ijccs.57565.

[8] S. Islam, S. Fenz, E. Weippl, and H. Mouratidis, "A Risk Management Framework for Cloud Migration Decision Support," *J. Risk Finance. Manag.*, vol. 10, no. 2, pp. 1–24, 2017, DOI: 10.3390/jrfm10020010.

[9] A. D. Kozlov and N. L. Noga, "Risk Management for Information Security of Corporate Information Systems Using Cloud Technology," in *2018 Eleventh International Conference "Management of large-scale system development" (MLSD)*, 2018, pp. 1–5, DOI: <https://journal.ugm.ac.id/ijccs/article/view/74567>

Editorial Board
Focus & Scope
Ethics & Malpractice Statement
Author Guidelines
Peer Review Process
Reviewer Guidelines
Screening Plagiarism
Online Submission
Author Fee
Statement of Originality
Copyright Transfer Form
Peer Reviewers
The College's Commitment
Decree of Accreditation
New Membership IndoCEISS
Membership Update IndoCEISS
Visitor Statistics

CITATION ANALYSIS

-  **SCOPUS**
-  **Google Scholar**

NOTIFICATIONS

-  **View**
-  **Subscribe**

USER

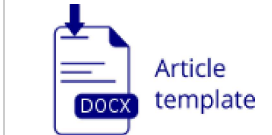
Username

Password

☐ Remember me

Login

DOWNLOAD



10.1109/MLSD.2018.8551947.

[10] O. Akinrolabu, S. New, and A. Martin, "Assessing the Security Risks of Multicloud SaaS Applications: A Real-World Case Study," *Proc. - 6th IEEE Int. Conf. Cyber Secure. Cloud Comput. CSCloud 2019 5th IEEE Int. Conf. Edge Comput. Scalable Cloud, EdgeCom 2019*, pp. 81–88, 2019, DOI: 10.1109/CSCloud/EdgeCom.2019.00-14.

[11] J. Zaki, S. M. R. Islam, N. S. Alghamdi, M. Abdullah-Al-Wadud, and K. S. Kwak, "Introducing Cloud-Assisted Micro-Service-Based Software Development Framework for Healthcare Systems," *IEEE Access*, vol. 10, pp. 33332–33348, 2022, DOI: 10.1109/ACCESS.2022.3161455.

[12] S. Sarmah, A. Li, and S. S. Sarmah, "Cloud Migration-Risks and Solutions," *Sci. Technol.*, vol. 2019, no. 1, pp. 7–11, 2019, DOI: 10.5923/j.scit.20190901.02.

[13] N. Ahmad, Q. N. Naveed, and N. Hoda, "Strategy and procedures for Migration to the Cloud Computing," *2018 IEEE 5th Int. Conf. Eng. Technol. Appl. Sci.*, pp. 1–5, 2018.

[14] Guide, "Risk management — Vocabulary ISO/IEC CD 2 Guide 73," no. 30. Geneva 20, pp. 1–12, 2008.

[15] ITA, "IT Risk Management Framework - Governance & Standards Division," in *IT Risk Management Framework*, 1.0., Oman, 2017, p. 23.

[16] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, "Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process," Qatar, 2007. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf.



[17] J. M. C. Brook, V. Chin, S. Lumpe, and A. Ulskey, "Top Threats to Cloud Computing Security: The Egregious Eleven," Asia Pacific, 2020. [Online]. Available: <https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/>.

[18] N. Amara, H. Zhiqui, and A. Ali, "Cloud Computing Security Threats and Attacks with their Mitigation Techniques," in *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2017, pp. 244–251, DOI: 10.1109/CyberC.2017.37.

[19] Y. A. Singgalen, H. D. Purnomo, and I. Sembiring, "Exploring MSMEs Cybersecurity Awareness and Risk Management : Information Security Awareness," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 15, no. 3, pp. 233–244, 2021, DOI: 10.22146/ijccs.67010.

DOI: <https://doi.org/10.22146/ijccs.74567>

Article Metrics

 Abstract views : 615 |  views : 690

Refbacks

- There are currently no refbacks.

 SHARE   

Copyright (c) 2022 IJCCS (Indonesian Journal of Computing and Cybernetics Systems)



This work is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).

Copyright of :
IJCCS (Indonesian Journal of Computing and Cybernetics Systems)
ISSN 1978-1520 (print); ISSN 2460-7258 (online)
is a scientific journal the results of Computing
and Cybernetics Systems
A publication of IndoCEISS.
Gedung S1 Ruang 416 FMIPA UGM, Sekip Utara, Yogyakarta 55281
Fax: +62274 555133
email: ijccs.mipa@ugm.ac.id | <http://jurnal.ugm.ac.id/ijccs>

[View My Stats1](#)
[View My Stats2](#)

TOOLS REFERENCE



JOURNAL CONTENT

Search

Search Scope

All

Search

Browse

- [By Issue](#)
- [By Author](#)
- [By Title](#)
- [Other Journals](#)

INFORMATION

- [For Readers](#)
- [For Authors](#)
- [For Librarians](#)

INDEXING



ABOUT THE AUTHORS

Maniah Maniah

 * Corresponding Author



<https://scholar.google.com/cit?hl=id&user=BABhVFcAAAAJ>

Prodi D3 Manajemen
Informatika, Politeknik Pos
Indonesia, Bandung
Indonesia

Benfano Soewito

Computer Science
Department, BINUS
Graduate Program, Doctor of
Computer Science, Bina
Nusantara University, Jakarta
Indonesia

Ford Lumban Gaol

Computer Science
Department, BINUS
Graduate Program, Doctor of
Computer Science, Bina
Nusantara University, Jakarta
Indonesia

Risk Assessment for Logistics Applications in Cloud Migration

Maniah^{*1}, Benfano Soewito², Ford Lumban Gaol³, Edi Abdurachman⁴

¹Prodi D3 Manajemen Informatika, Politeknik Pos Indonesia, Bandung, Indonesia

^{2,3,4}Computer Science Department, BINUS Graduate Program, Doctor of Computer Science,
Bina Nusantara University, Jakarta, Indonesia

e-mail: ^{*1}maniah@poltekpos.ac.id, ²bsoewito@binus.edu, ³fgaol@binus.edu,

⁴edia@binus.ac.id

Abstrak

Peningkatan jumlah pusat data cloud disebabkan karena peningkatan jumlah perusahaan yang migrasi ke cloud computing. Banyak keuntungan yang didapat perusahaan ketika migrasi ke cloud, namun tidak sedikit juga kelemahannya. Keamanan dan privasi multitenancy merupakan tantangan penting bagi pengguna cloud migration. Penelitian ini mengusulkan cara menilai risiko yang kemungkinan akan muncul dalam proses cloud migration terhadap aplikasi bisnis logistik. Metode penelitian yang digunakan adalah semi kuantitatif dengan pendekatan 3 fase, yaitu sebelum migrasi, saat migrasi dan setelah migrasi dengan mempertimbangkan kriteria aspek risiko dan aspek lingkungan yang akan berdampak pada perusahaan, sehingga perusahaan dapat membuat perencanaan mitigasi risikonya. Hasil penelitian ini mengidentifikasi 11(sebelas) ancaman pada cloud yang menduduki ranking teratas, serta mengidentifikasi sebanyak 17(tujuh belas) indikator yang didapat dari hasil pengidentifikasian terhadap indikator-indikator pada model atau framework sebelumnya yang digunakan untuk menilai risiko pada aplikasi bisnis logistik yang akan dimigrasikan ke cloud. Berdasarkan hasil eksperimen dalam penelitian ini, bahwa nilai risiko aplikasi saat migrasi dan setelah migrasi memiliki nilai yang lebih tinggi dibandingkan sebelum migrasi, dan nilai risiko saat migrasi lebih tinggi dibandingkan nilai risiko setelah migrasi.

Kata kunci—Cloud Computing, Cloud Migration, Ancaman, Indikator, Nilai Risiko

Abstract

The increase in the number of cloud data centers is due to an increase in the number of companies migrating to cloud computing. There are many advantages that companies get when migrating to the cloud, but there are also many disadvantages. Multitenancy security and privacy are important challenges for cloud migration users. This study proposes a way to assess the risks that may arise in the cloud migration process for logistics business applications. The research method used is semi-quantitative with a 3-phase approach, namely before migration, during migration, and after migration by considering the criteria for risk aspects and environmental aspects that will have an impact on the company, so that companies can make risk mitigation plans. The results of this study identified 11 (eleven) threats in the cloud that occupy the top ranking and identify as many as 17 (seventeen) indicators obtained from the identification of indicators in the previous model or framework used to assess risks in logistics business applications that will be implemented. migrated to the cloud. Based on the experimental results in this study, the application risk value during migration and after migration has a higher value than before migration, and the risk value during migration are higher than the risk value after migration.

Keywords—Cloud Computing, Cloud Migration, Threats, Indicators, Risk Value

1. INTRODUCTION

The company's increasing business growth requires a large area of data storage. If this is done independently (on-premise), then the company must prepare a data storage area and infrastructure to access the data independently. [1], Of course, it will pose many challenges or risks, including the server workload that will increase due to access to that set of data. Companies that have large data sets, intend to migrate to cloud computing, which means that companies will get collective server facilities, software, infrastructure, data storage, services, and information technology resources according to company needs. [2]–[4]. When the researcher conducted a Focus Group Discussion (FGD) with several cloud service customers, it reveals that with cloud computing technology the company got several advantages, including (1) growing customer satisfaction, so that public trust increased; (2) information can be obtained by customers more quickly, especially during the current pandemic, businesses must continue to run, and companies are very dependent on the cloud; (3) accelerate business products; (4) cost efficiency; (5) data security, such as firewall, recovery. The disadvantage of cloud migration is that users cannot directly control the system in processing their data and applications. It happens because data users and cloud servers are not in the same domain. Multitenancy security and privacy is an important challenge for cloud users, as multitenancy allows multiple users to run their applications simultaneously on the same infrastructure and opens the door to possible privacy leaks [5]. Virtual machines are one of the risks that arise due to attacks in the cloud environment such as viruses, worms, malware, and others [6], [7].

Several previous studies that proposed a risk assessment framework to support users in making migration decisions to the cloud were carried out by analyzing risks and the techniques used with a semi-quantitative approach [8]. The results of his research explain the steps in preparing for migration to the cloud, starting from initiating risks, identifying and categorizing risks, then analyzing and controlling risks. The final risk value calculation is calculated based on the average risk factor value estimated with the overall risk probability and impact and does not explain how to calculate the risk value during or after migration to the cloud [8]. Then further research by [9] to assess the security of information systems, the results of his research propose steps to be taken in assessing risks to information system security in the cloud context starting from (1) determining asset information; (2) defining threats; (3) determine existing vulnerabilities; (4) perform risk analysis and assessment; and (5) processing the existing risks. The calculation of risk value is calculated by considering 1 (one) coefficient indicator which states as the ratio of the control level, and in this study does not compare the residual risk or risk with a value that is close to the actual result, so that the risk value in this study there is only one formula for calculating risk, namely before migration (before migration). Further research [10] analyzed the risks of using Software as a Service (SaaS) applications to validate supply chain usage with the Cloud Supply Chain Cyber Risk Assessment (CSCCRA) model, the results of this model enable CSPs to understand, manage, and make well-informed decisions about their cloud risks Software as a Service (SaaS) application users. In addition, a cloud-based health service has also been developed to solve problems in integrated health services [11]. Many solutions are offered by CSP in the process of migrating to the cloud, but we still have to be smart in determining which solution is the most appropriate for us to use so that we will get the maximum cloud migration service that suits our company's needs [12]. Based on the results of these previous studies, there are no studies that measure the risk value of migrating applications to a special cloud to support the logistics company's business. Even though the development of the logistics business is currently growing rapidly, especially since the Covid-19 pandemic the need for logistics services such as transportation, warehousing, and sales is increasing. This makes logistics companies must be able to adapt quickly to maintain their company's business, such as carrying out digital transformation. When the company has made a digital transformation, it is very likely that the business processes or systems that are run by the company are already cloud-based.

Based on research results [8], [9] the measurement of the risk value in cloud migration does not explain how much the risk value during migration and after the migration is. Even though this is an important thing for decision makers to consider because during migration and after migration to the cloud it is likely to disrupt the company's business and is a risk. [13], as illustrated when there is a cloud outage by amazon, because data is stored centrally in the cloud, this can paralyze the business of companies that depend on that data [4]. For companies to know the risks that might arise in this cloud migration process, companies need to carry out risk calculations on applications that will be migrated to the cloud by considering the criteria for risk aspects and environmental aspects that will have an impact on the company. can know from the start whether the impact of cloud migration is dangerous or not. So this is an opportunity for researchers to contribute to developing previous studies by creating a risk value calculation model for applications that will be migrated to the cloud for the logistics business as measured by a 3 (three) phase approach, namely before migration, during migration, and after. migration.

2. METHODS

We divide the phase in risk assessment for logistics applications on cloud migration into 2 (two) phases, namely the initiation phase and the implementation phase, as shown in Figure 1.

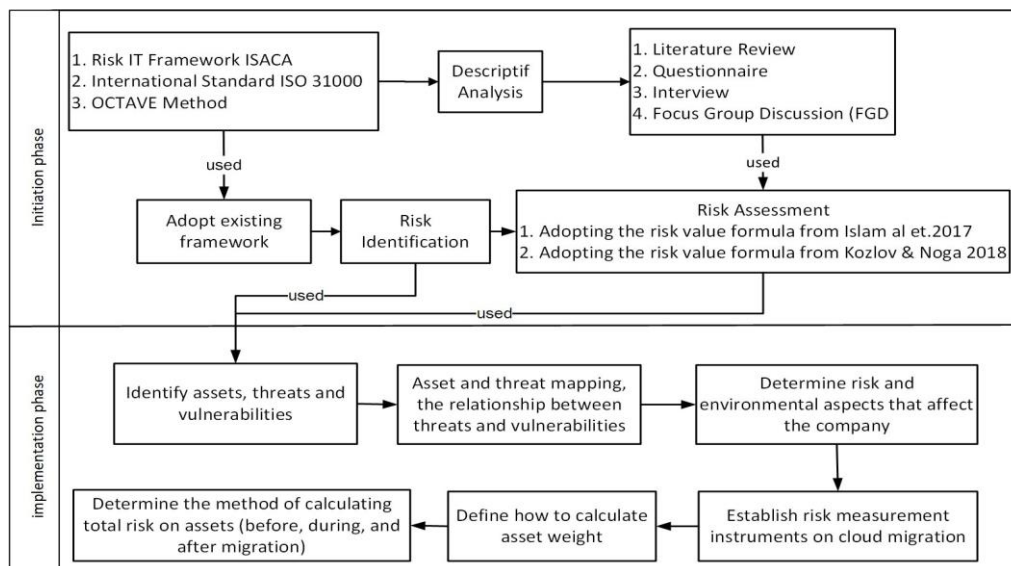


Figure 1 Research design

2.1 Initiation Phase

The steps in this research design are adopted from the risk assessment process of the ISO/IEC Guide 7 standard [14], risk scenario in the risk evaluation of the IT Risk Management Framework v.1 Governance and Standards Division [15], and risk assessment using the OCTAVE method [16]. The data collection techniques used in this study were Literature Review, Questionnaire, Interview, and Focus Group Discussion (FGD), as well as adopting a risk measurement formula from the results of previous studies [8], [9].

2.2 Implementation Phase

This section will explain risk identification, where the sub-sections related here are asset identification, threat identification, and vulnerability identification which will be the basic components of risk measurement in this research. The next stage, mapping of threats to assets aims to find out how many threats are likely to appear to the security of applications that will be

migrated to cloud computing. We also make relationships between vulnerabilities to threats and risks. In this study, the relationship between threats and vulnerabilities is assumed that 1 (one) threat can have several (N) vulnerabilities, so the relationship between threats and vulnerabilities is 1-N (one to many). The method of assessing total risk on assets is carried out using 3 (three) approaches, namely before, during, and after migration, where previously we determined risk and environmental aspects that affect the company, set risk measurement instruments on cloud migration, and determined how to calculate asset weights. The stages carried out in the risk assessment of logistics applications that will be migrated to the cloud are:

1. Identify Assets, Threats, and Vulnerabilities
2. Asset and Threat Mapping, the relationship between threats and vulnerabilities
3. Determine Risk and Environmental Aspects that Affect the Company
4. Establish Risk Measurement Instruments on Cloud Migration
5. Define How To Calculate Asset Weight
6. Determine the method of calculating total risk on assets

3. RESULTS AND DISCUSSION

In this study to calculate the risk value of logistics applications that will be migrated to the cloud, the first step is to calculate the asset weight value. In calculating the value of asset weights, it is necessary to have criteria that have an impact on each application and the weight of each of these criteria. The asset weight measurement criterion is a qualitative measure used to evaluate the impact of risk on applications to be migrated to the cloud [16]. This asset weight criterion refers to the risk measurement criteria of the OCTAVE method, but in this study, the asset weight criterion is intended specifically for applications that support business processes in the logistics business. Our next step is to calculate risk values before migration, during migration, and after migration to cloud computing.

3.1 Threat Identification

The identification of this threat uses a reference from Top Threats to Cloud Computing The Egregious 11 [17], the results of the Cloud Security Alliance (CSA) 2020 survey of threats to cloud security sorted by ranking. From the results of this survey, there is a list of threats, risks, and vulnerabilities that stand out in the cloud computing environment as shown in Table 1.

Table 1 Types of Threats in Cloud Computing [17]

ID_Threat	Threats Type	Probability of Occurrence
TH-1	Data Breaches	5%
TH-2	Misconfiguration and Inadequate Change Control	9%
TH-3	Lack of Cloud Security Architecture and Strategy	17%
TH-4	Insufficient Identity, Credential, Access, and Key Management	5%
TH-5	Account Hijacking	16%
TH-6	Insider Threat	14%
TH-7	Insecure Interfaces and APIs	11%
TH-8	Weak Control Plane	5%
TH-9	Metastructure and Applistructure Failures	2%
TH-10	Limited Cloud Usage Visibility	7%
TH-11	Abuse and Nefarious Use of Cloud Services	9%

Threats type in Table 1 is obtained from the results of a survey of 241 industry experts as respondents about security issues in the cloud, and the result is that there are 11 (eleven) threats that stand out in cloud computing security issues [17]. The Probability of Occurrence column is the percentage of the possible risk of each type of threat in cloud security. The Probability of Occurrence value for each threat is obtained based on the results of the Focus Group Discussion (FGD) activity which is one way for researchers to obtain research references. The percentage of possible risk given to each of the above threats is also the decision of the cloud service user.

3. 2 Risk Assessment Indicator

The risk assessment indicators used in this study are adopted from several indicators contained in the current risk management model or framework [14]–[16] and added with indicators from the results of previous studies [8], [9]. In detail, the indicators used can be shown in Table 2.

Table 2 Risk Assessment Indicators

No.	Indicators	Before migration	During migration	After migration
1	Integrity	15%	10%	8%
2	Availability	20%	15%	8%
3	Confidentiality	15%	10%	8%
4	Security Policies	10%	8%	5%
5	Service Level Agreement	5%	8%	5%
6	Standard and reference models	15%	6%	5%
7	Backup data	10%	8%	6%
8	System malfunctions	10%	6%	6%
9	Unauthorized transmission		5%	5%
10	Financial		8%	5%
11	Technological		8%	5%
12	Business goals		8%	8%
13	Capabilities			5%
14	Structures (e.g. governance, roles, and accountabilities).			5%
15	Productivity			6%
16	User experience			5%
17	Maintenance difficulties			5%

Indicators for assessing risk before migration consists of integrity (level of information that can be used without any change in information), Availability (Readiness of information that can be accessed anytime 24 hours by users), Confidentiality (Ensure confidentiality of information through information security from the use of unauthorized to maintain customer trust), Security Policies (There are policies related to the security of information and company data), Service Level Agreement (Level of compliance with policies per legislation), Standard and reference models (Standards and reference models are adopted by the organization), data backup (data backup process is carried out on an ongoing basis), and system malfunctions (the system does not function properly). The indicators used to assess risk during migration are a number of indicators before migration plus Unauthorized transmission indicators (Error rate in data transmission), Financial (There is an increase in operational costs due to migration to the cloud), Technological (The amount of change in technology used as a result of migration to the cloud), cloud), Business goals (There is an increase in the company's business due to migration to the cloud), while for risk assessment after migration we add indicators of Capabilities (level

of employee ability due to migration to the cloud), Structures e.g. governance, roles and accountabilities (The magnitude of changes in organizational governance due to migration to the cloud), Productivity (There is an increase in employee work productivity due to migration to the cloud), User experience (Sufficient customer experience with cloud technology), and Maintenance difficulties (level of maintenance difficulties when migrate and operate in the cloud).

3. 3 Risk Assessment (Before-During-After) Migration

First, we calculate the weight value of each logistics application that will be migrated to the cloud with the equation (1).

$$r_a = \sum (V_{appl} * w) \quad (1)$$

where: r_a = result assessment; v_{appl} = value of asset (application); w = criteria weight.

The formula on equation (1) will add up all existing asset weight values against each application that will be migrated to the cloud. Value of asset (v_{appl}) is the value that will be given by cloud service users by considering the asset weight criteria (low, medium, or high) based on the data entry rubric for asset weight, while w is the amount of asset weight value according to the predetermined asset weight criteria.

Risk assessment is carried out in 3 (three) phases, namely risk assessment before migration, risk value during migration, and risk after migration to the cloud. Figure 2 shows an example of a script to measure risk values before migration, during migration, and after migration to the cloud. Risk assessment before migration is calculated by considering possible threats to assets and their vulnerability values, risk assessment during migration is obtained from the accumulation of the average risk value before migration and risk value when migrating to the cloud by considering several risk aspect criteria, while risk value assessment after migration to the cloud, obtained from the average risk value before migration is accumulated with the risk value after migration to the cloud by considering several environmental aspects criteria.

Before Migration	During Migration	After Migration
<pre>def calculate_risk_before_migration(): for id_threat, sum in sorted(dict_temp_th_2.items()): dict_temp_th_sum[id_threat] = sum final_sum_th[k] = dict_temp_th_sum list_data_final = [] for key, value in data_id_app.items(): temp_dict = {} temp_dict[key] = { 'probabilities_threat': final_sum_th[key], 'weight': assets_weight_value[key], 'final_score': final_score[key] } list_data_final.append(temp_dict) final_data = { 'data': list_data_final } return final_data</pre>	<pre>def calculate_risk_during_migration (data_during_migration): data_unique_id_app = {} final_data = calculate_risk_before_migration () data_final = {} sum_data_risk = {} for datas in final_data['data']: for data in datas: data_final[data] = datas[data]['final_score'] for data in data_during_migration: if data[0] not in data_unique_id_app: sum_data = data_final[data[0]] + data[6] sum_data_risk[data[0]] = round((sum_data / 2, 2) final_data = {} for id_app in sum_data_risk: final_data[id_app] = { 'risk_value': sum_data_risk[id_app] } return final_data</pre>	<pre>def hitung_risiko_after_migration (data_after_migration): final_data = calculate_risk_before_migration() data_final = {} for datas in final_data['data']: for data in datas: data_final[data] = datas[data]['final_score'] score_data = {} for data in data_after_migration: if data[0] not in score_data: score_data[data[0]] = round((data_final[data[0]] + data[6]) / 2, 2) final = {} for id_app in score_data: final[id_app] = { 'risk_value': score_data[id_app] } return final</pre>

Figure 2 Before-During-After Migration Application Script

The measurement of the risk value before migrating to the cloud begins by reviewing the list of assets and the weight of each criterion on the asset to determine the value of the result assessment r_a , the value of the Probability of Occurrence p_o obtained from the magnitude of the possibility of a threat, and the value of vulnerability v on each asset that determined from the number of threats t to assets where each threat contains one or more vulnerabilities. First, the risk value of each asset r_i is calculated based on the value of the result assessment r_a and the value of the probability of occurrence p_o as much as the number of *threats-i*. Furthermore, if $I > n$, then the total risk value of each asset R_{1tot} is calculated by accumulating the risk value of r_i plus the value of v , as shown in equation (2).

$$R_1 = \sum (r_i)v \quad (2)$$

where: R_1 = total risk value; r_i = risk value; v = vulnerability.

The risk assessment during migration to cloud computing aims to calculate the possible magnitude of risk value when carrying out migration by considering indicators of risk aspects before migration as shown in Table 1. The risk value during R_{2tot} migration is the total risk value before R_{1tot} migration plus the calculated r_a result assessment value first based on the value of possible threats to the asset value p_o against the weight of the risk aspect criteria by considering the indicators that have been set. The formula for assessing the risk during migration is shown in equation (3).

$$R_{2tot} = (R_{1tot} + r_a)/2 \quad (3)$$

where: R_{2tot} = total risk value during migration to the cloud; R_{1tot} = total risk value before cloud migration; r_a = *result assessment* (asset weight value per application adjusted for risk aspect indicators).

The risk assessment after migration to the cloud is intended to determine the possible magnitude of the risk value that will arise after the migration process to cloud computing is completed. Where the risk value after R_{3tot} migration is the total risk value before R_{1tot} migration plus the result assessment value r_a which is calculated first based on the value of possible threats to the asset value p_o to the weight of the environmental aspect criteria indicators (after migration) as shown in Table 1. To get the value of risk after migration used the formula as shown in equation (4)

$$R_{3tot} = (R_{1tot} + r_a)/2 \quad (4)$$

where: R_{3tot} = total risk value after migration to the cloud; R_{1tot} = total risk value before migration to cloud; r_a = *result assessment* (asset weight values per application adjusted for environmental indicators).

3. 4 Risk Assessment Results

Equation (1) can be used to find the weight value of each asset. In this study, the assets used are logistics business applications that will be migrated to the cloud (in this case there are 13 applications, AP-1 to AP-13). To get the asset weight value in the 1st application (AP-1) the value given to each asset weight indicator for example 50, 50, 30, 40, 50, 40, 60, 30, then the sum of the results of the weight assessment is:

$$\text{result assessment } (r_a) = (50 \times 15\%) + (50 \times 20\%) + (30 \times 15\%) + (40 \times 10\%) + (50 \times 5\%) \\ + (40 \times 15\%) + (60 \times 10\%) + (30 \times 10\%) = \mathbf{43,50}$$

The same way is done to calculate the value of asset weights for the second application and so on (AP-2 to AP-13). The value of vulnerability in each asset can be determined by conducting a survey first to cloud service users, this is because the value of vulnerability to assets is very dependent on how we handle threats to our assets. Vulnerability value is how likely the threat can occur.

Based on the results of the calculation of asset weights, the value of vulnerability in each asset, and taking into account the weight value of each indicator on the risk aspect, the risk value is obtained before migration, during migration, and after migration, to the cloud, as shown in Table 3.

Table 3 Experimental Results

ID_App	Result Assessment	Vulnerability	Before Migration	During Migration	After Migration
AP-1	43,50	6,75	28,07	36,33	35,93
AP-2	47,75	5,65	26,18	37,19	36,19
AP-3	53,00	6,83	22,73	35,37	35,49
AP-4	57,75	6,02	23,35	39,32	39,20
AP-5	55,00	6,25	24,40	38,05	36,05
AP-6	60,00	6,96	32,76	46,83	45,60
AP-7	51,75	5,31	26,53	40,22	39,37
AP-8	49,25	7,28	24,02	30,22	33,84
AP-9	57,25	6,71	31,90	44,65	44,12
AP-10	46,00	6,23	17,27	31,73	30,48
AP-11	41,50	5,06	12,95	26,60	25,30
AP-12	56,50	7,21	39,98	49,11	47,99
AP-13	40,75	6,38	23,09	31,60	31,25

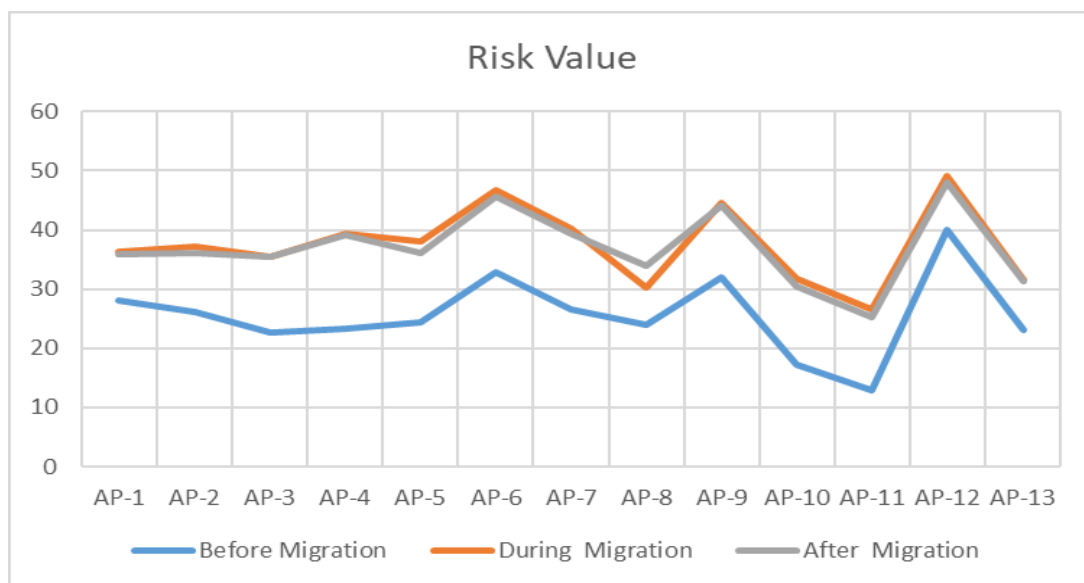


Figure 3 Trends of Risk Value

In calculating the risk value, the resulting value is not a fixed risk value, this depends on how the company strategizes against possible threats. In this study, the risk value generated as shown in Table 3 is not fixed, because the measurement of the risk value is influenced by the magnitude of the possibility of threats to each application that is migrated to the cloud, the magnitude of the possible impact from the risk aspect, and the magnitude of the possible impact from the environmental aspect that occurs. in conditions before migration, during migration, and after migration to the cloud.

Based on Figure 3, it can be seen that the risk value during migration and after migration to the cloud has a relatively higher value than the risk value before migration, while the average risk value during migration has a relatively higher value than after migration risk value. This shows that the possibility of threats and risks that occur during the migration process is higher. System services by companies that are migrating to the cloud to customers may be disrupted due to this migration process. For this reason, it is a particular concern for companies that use cloud services, that when the company has decided to migrate to the cloud, it is necessary to take risk mitigation actions first by the company by conducting a risk assessment of the assets to be migrated to the cloud [18]. So that the company can quickly find out what possible threats will threaten the assets to be migrated and how much risk the company must face. This risk mitigation step is one form of effort toward the company's business sustainability [19].

4. CONCLUSION

The research design used in this study was carried out in 2 (two) phases, namely the initiation phase and the implementation phase which became the method for measuring the risk value of logistics business applications in cloud migration.

Based on the experimental results, it proves that the risk value the during migration phase provides a relatively high-risk value compared to the risk value before and after migration in cloud migration.

ACKNOWLEDGEMENTS

I want to thank the Pos Indonesia Polytechnic institution for providing the opportunity and support to me, and also thank the lecturers of Doctor of Computer Science at Bina Nusantara University for their support so that this research can be completed properly.

REFERENCES

- [1] C. Pahl, H. Xiong, and R. Walshe, "A comparison of on-premise to cloud migration approaches," *Comput. Sci.*, vol. 8135 LNCS, no. ESOC 2013, pp. 212–226, 2013, DOI: 10.1007/978-3-642-40651-5_18.
- [2] D. Rountree and I. Castrillo, *The Basics of Cloud Computing Understanding the Fundamentals of Cloud Computing in Theory and Practice*, Syngress. Hai Jiang, 2013.
- [3] R. J. Priyadarsini and L. Arokiam, "Failure Management In Cloud : An Overview," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 2, no. 10, 2013.
- [4] P. Gupta and C. Gupta, "Evaluating the Failures of Data Centers in Cloud Computing," *Int. J. Comput. Appl.*, vol. 108, no. 4, pp. 29–34, 2014, [Online]. Available: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.671.5978&rep=rep1&type=pdf>.
- [5] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," *IEEE*

- Internet Comput.*, vol. 16, no. 1, pp. 69–73, 2012.
- [6] R. Patil, H. Dudeja, and C. Modi, “Designing in-VM-assisted lightweight agent-based malware detection framework for securing virtual machines in cloud computing,” *Int. J. Inf. Secure.*, vol. 19, pp. 147–162, 2019, DOI: 10.1007/s10207-019-00447-w.
 - [7] R. Felani, M. N. Al Azam, D. P. Adi, A. Widodo, and A. B. Gumelar, “Optimizing Virtual Resources Management Using Docker on Cloud Applications,” *IJCCS (Indonesian J. Comput. Cybern. Syst.)*, vol. 14, no. 3, pp. 319–330, 2020, DOI: 10.22146/ijccs.57565.
 - [8] S. Islam, S. Fenz, E. Weippl, and H. Mouratidis, “A Risk Management Framework for Cloud Migration Decision Support,” *J. Risk Finance. Manag.*, vol. 10, no. 2, pp. 1–24, 2017, DOI: 10.3390/jrfm10020010.
 - [9] A. D. Kozlov and N. L. Noga, “Risk Management for Information Security of Corporate Information Systems Using Cloud Technology,” in *2018 Eleventh International Conference “Management of large-scale system development” (MLSD)*, 2018, pp. 1–5, DOI: 10.1109/MLSD.2018.8551947.
 - [10] O. Akinrolabu, S. New, and A. Martin, “Assessing the Security Risks of Multicloud SaaS Applications: A Real-World Case Study,” *Proc. - 6th IEEE Int. Conf. Cyber Secure. Cloud Comput. CSCloud 2019 5th IEEE Int. Conf. Edge Comput. Scalable Cloud, EdgeCom 2019*, pp. 81–88, 2019, DOI: 10.1109/CSCloud/EdgeCom.2019.00-14.
 - [11] J. Zaki, S. M. R. Islam, N. S. Alghamdi, M. Abdullah-Al-Wadud, and K. S. Kwak, “Introducing Cloud-Assisted Micro-Service-Based Software Development Framework for Healthcare Systems,” *IEEE Access*, vol. 10, pp. 33332–33348, 2022, DOI: 10.1109/ACCESS.2022.3161455.
 - [12] S. Sarmah, A. Li, and S. S. Sarmah, “Cloud Migration-Risks and Solutions,” *Sci. Technol.*, vol. 2019, no. 1, pp. 7–11, 2019, DOI: 10.5923/j.scit.20190901.02.
 - [13] N. Ahmad, Q. N. Naveed, and N. Hoda, “Strategy and procedures for Migration to the Cloud Computing,” *2018 IEEE 5th Int. Conf. Eng. Technol. Appl. Sci.*, pp. 1–5, 2018.
 - [14] Guide, “Risk management — Vocabulary ISO/IEC CD 2 Guide 73,” no. 30. Geneva 20, pp. 1–12, 2008.
 - [15] ITA, “IT Risk Management Framework - Governance & Standards Division,” in *IT Risk Management Framework*, 1.0., Oman, 2017, p. 23.
 - [16] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process,” Qatar, 2007. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf.
 - [17] J. M. C. Brook, V. Chin, S. Lumpe, and A. Ulskey, “Top Threats to Cloud Computing Security: The Egregious Eleven,” Asia Pacific, 2020. [Online]. Available: <https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/>.
 - [18] N. Amara, H. Zhiqui, and A. Ali, “Cloud Computing Security Threats and Attacks with their Mitigation Techniques,” in *2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2017, pp. 244–251, DOI: 10.1109/CyberC.2017.37.
 - [19] Y. A. Singgalen, H. D. Purnomo, and I. Sembiring, “Exploring MSMEs Cybersecurity Awareness and Risk Management: Information Security Awareness,” *IJCCS (Indonesian J. Comput. Cybern. Syst.)*, vol. 15, no. 3, pp. 233–244, 2021, DOI: 10.22146/ijccs.67010.