LAPORAN AKHIR TAHUN

SKEMA PENELITIAN: PENELITIAN DOSEN PEMULA

Hasil Pendanaan dari Direktorat Riset dan Pengabdian kepada Masyarakat, Kemenristek DIKTI

Model Penilaian Risiko Aplikasi Bisnis Logistik pada Cloud Migration

Tahun ke 1 dari rencana 1 tahun

TIM:

Dr. Maniah, S.Kom., M.T. (Ketua) NIDN: 0427076701

Dr. Erna Mulyati, S.T., MT. (Anggota) NIDN: 0427107501

Dini Hamidin, S.Si., MBA., M.T. (Anggota) NIDN: 0402127502

UNIVERSITAS LOGISTIK DAN BISNIS INTERNASIONAL

DESEMBER, 2023

Direktorat Riset dan Pengabdian Masyarakat Direktorat Jenderal Riset dan Pengembangan
Kementerian Riset, Teknologi, dan Pendidikan Tinggi
Gedung BPPT II Lantai 19, Jl. MH. Thamrin No. 8 Jakarta Pusat
https://simlitabmas.ristekdikti.go.id/

LAPORAN AKHIR PENELITIAN

ID Proposal: 01dbbf74-ace5-466f-ad3b-23169a50960d
laporan akhir Penelitian: tahun ke-1 dari 1 tahun

1. IDENTITAS PENELITIAN

A. JUDUL PENELITIAN

Model Penilaian Risiko Aplikasi Bisnis Logistik pada Cloud Migration

B. BIDANG, TEMA, TOPIK, DAN RUMPUN BIDANG ILMU

Bidang Fokus RIRN / Bidang Unggulan Perguruan Tinggi	Tema	Topik (jika ada)	Rumpun Bidang Ilmu
Teknologi Informasi dan Komunikasi	-		Sistem Informasi

C. KATEGORI, SKEMA, SBK, TARGET TKT DAN LAMA PENELITIAN

Kategori (Kompetitif Nasional/ Desentralisasi/ Penugasan)	Skema Penelitian	Strata (Dasar/ Terapan/ Pengembangan)	SBK (Dasar, Terapan, Pengembangan)	Target Akhir TKT	Lama Penelitian (Tahun)
Penelitian Kompetitif Nasional			SBK Riset Pembinaan/ Kapasitas	3	1

2. IDENTITAS PENGUSUL

Nama (Peran)	Perguruan Tinggi/ Institusi	Program Studi/ Bagian	Bidang Tugas	ID Sinta	H-Index
ERNA MULYATI - Anggota Pengusul	Universitas Logistik dan Bisnis Internasional	Logistik Bisnis	Menyusun rancangan penelitian dan memberikan saran mengenai teori-teori Logistik yang digunakan dalam penelitian.	6175475	1
MANIAH - Ketua	Universitas Logistik dan	Manajemen Informatika	Menyusun roadmap penelitian, menyusun metode penelitian agar	6097708	3

Pengusul	Bisnis Internasional		dapat menjawab permasalahan penelitian, dan melaksanakan penelitian sesuai dengan rancangan penelitian yang sudah disusun.		
DINI HAMIDIN - Anggota Pengusul	Universitas Logistik dan Bisnis Internasional	Manajemen Transportasi	Menyusun Rancangan Biaya Penelitian yang disesuaikan dengan tahapan penelitian yang dilakukan	5978964	0

3. MITRA KERJASAMA PENELITIAN (JIKA ADA)

Pelaksanaan penelitian dapat melibatkan mitra kerjasama, yaitu mitra kerjasama dalam melaksanakan penelitian, mitra sebagai calon pengguna hasil penelitian, atau mitra investor

Mitra	Nama Mitra

4. LUARAN DAN TARGET CAPAIAN

Luaran Wajib

Tahun Luaran	Jenis Luaran	*Status target capaian (accepted, published, terdaftar atau granted, atau status lainnya)*	*Keterangan (url dan nama jurnal, penerbit, url paten, keterangan sejenis lainnya)*
1	Feasibility Study		
1	Artikel di jurnal internasional	Submited	

Luaran Tambahan

Tahun Luaran	Jenis Luaran	*Status target capaian (accepted, published, terdaftar atau granted, atau status lainnya)*	*Keterangan (url dan nama jurnal, penerbit, url paten, keterangan sejenis lainnya)*

5. ANGGARAN

Rencana anggaran biaya penelitian mengacu pada PMK yang berlaku dengan besaran minimum dan maksimum sebagaimana diatur pada buku Panduan Penelitian dan Pengabdian kepada Masyarakat

Total RAB 1 Tahun Rp. 0

Tahun 1 Total Rp. 0

Jenis Pembelanjaan	Komponen	Item	Satuan	Vol.	Biaya Satuan	Total

Tahun 2 Total Rp. 0

Jenis Pembelanjaan	Komponen	Item	Satuan	Vol.	Biaya Satuan	Total

Tahun 3 Total Rp. 0

Jenis Pembelanjaan	Komponen	Item	Satuan	Vol.	Biaya Satuan	Total

6. KEMAJUAN PENELITIAN

A. RINGKASAN

Era revolusi industri 4.0 merupakan era yang ditandai dengan transisi teknologi informasi dan komunikasi yang mampu menciptakan investasi berbasis teknologi baru. Internet of things (IoT), Big Data, dan Cloud Computing, merupakan fondasi yang mendasari revolusi industri 4.0 ini. Cloud Computing adalah sebuah layanan yang menyediakan ruang penyimpanan jaringan dan sumber daya komputer dengan menggunakan koneksi internet sebagai media akses. Proses migrasi ke cloud computing ini melalui beberapa tahap secara berurutan dan saling berkesinambungan, namun terkadang proses migrasi ke cloud computing menghadapi kendala atau bahkan kegagalan, hal ini tentunya menjadi risiko bagi pengguna layanan cloud. Untuk itu sebelum melakukan migrasi ke cloud perlu untuk mempersiapkannya dengan baik, karena jika tidak maka akan menimbulkan kerugian yang berdampak risiko bagi perusahaan. Upaya untuk memperkecil risiko bagi pengguna layanan cloud adalah dengan melakukan penilaian risiko. Tujuan penelitian ini adalah membuat model untuk penilaian risiko terhadap aplikasi bisnis logistik pada cloud migration. Model pengukuran nilai risiko yang dikembangkan ini mengadopsi dari model risk management dari ISACA Risk IT Framework, risk management process part of the ISO 31000 standard, dan mengadopsi dari the phases of the OCTAVE method. Metode penelitian yang digunakan adalah Risk Assessment Method berbasis ISO 31000, metode ini digunakan untuk melakukan penilaian risiko berdasarkan bobot ancaman terhadap asset, kriteria dampak risiko, dan likelihood pada cloud migration. Luaran penelitian ini adalah 1(satu) artikel ilmiah dimuat di jurnal internasional dengan status submit. Berdasarkan pengukuran Tingkat Kesiapterapan Teknologi (TKT) saat ini, penelitian ini berada pada TKT-1 yang merupakan ranah baru dalam perangkat lunak yang sedang didalami oleh komunitas riset dasar sebesar 80%, dan mencakup juga pengembangan dari penggunaan tingkat dasar, sifat dasar dari arsitektur perangkat lunak, formulasi matematika, dan algoritma umum sebesar 80%, sehingga untuk luaran yang dihasilkan, penelitian ini menargetkan capaian Tingkat Kesiapterapan Teknologi (TKT-3). Berdasarkan cara pengukuran nilai risiko dari hasil penelitian ini, maka perusahaan akan mengetahui berapa besar risiko yang kemungkinan muncul akibat penggunaan pusat data cloud, sehingga dapat segera dilakukan mitigasi risikonya. Hal ini akan berdampak terhadap peningkatan security layanan cloud, dan ini menjadi hal yang utama dalam meningkatkan kepercayaan masyarakat dalam penggunaan layanan cloud.

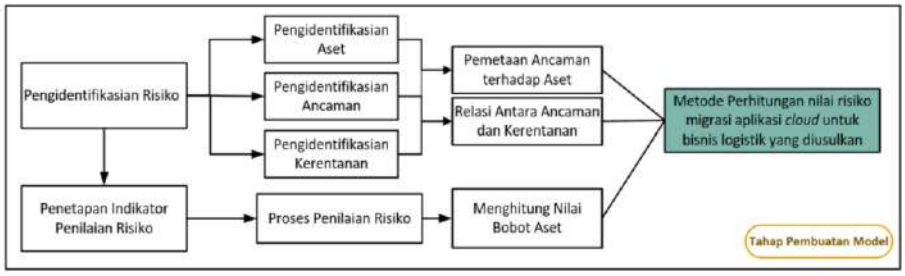
B. KATA KUNCI

Model; penilaian risiko; cloud migration; adopsi; security

Pengisian poin C sampai dengan poin H mengikuti template berikut dan tidak dibatasi jumlah kata atau halaman namun disarankan seringkas mungkin. Dilarang menghapus/memodifikasi template ataupun menghapus penjelasan di setiap poin.

C. **HASIL PELAKSANAAN PENELITIAN:** Tuliskan secara ringkas hasil pelaksanaan penelitian yang telah dicapai sesuai tahun pelaksanaan penelitian. Penyajian meliputi data, hasil analisis, dan capaian luaran (wajib dan atau tambahan). Seluruh hasil atau capaian yang dilaporkan harus berkaitan dengan tahapan pelaksanaan penelitian sebagaimana direncanakan pada proposal. Penyajian data dapat berupa gambar, tabel, grafik, dan sejenisnya, serta analisis didukung dengan sumber pustaka primer yang relevan dan terkini.

Hasil pelaksanaan penelitian yang sudah dilaksanakan dapat dijelaskan sesuai Gambar 1 berikut ini:



Gambar 1. Tahap Penelitian

A. TAHAP-TAHAP PERHITUNGAN NILAI RISIKO

1. Pengidentifikasian Risiko

Bagian ini akan menjelaskan terntang pengidentifikasian risiko, dimana sub bagian yang terkait disini adalah pengidentifikasian aset, pengidentifikasian ancaman, dan pengidentifikasian kerentanan yang akan menjadi komponen dasar pengukuran risiko dalam penelitian ini.

a. Pengidentifikasian Aset

Pengidentifikasi aset adalah cara untuk menentukan informasi yang akan dianalisis risikonya dalam konteks *cloud*. Berdasarkan hasil analisis yang dilakukan oleh peneliti, terdapat aplikasi-aplikasi logistik yang akan di migrasi ke *cloud*, seperti ditunjukkan pada Tabel 1 berikut ini:

Tabel 1 Aplikasi logistik yang di migrasi ke *cloud*

ID-App	Nama Aplikasi	Lingkup /Kompleksitas	Tujuan Aplikasi
AP-1	*Human Resource Information System*	Internal / Cukup Kompleks	Aplikasi HRIS digunakan untuk mencatat data pegawai, penggajian, pengaturan dan pencatatan *achievement* dan *punishment* pegawai, pencatatan mutasi, pencatatan dan pengajuan *travel form*, Pencatatan *personal value* serta Permir/presensi. Aplikasinya berbasis web dan android, sehingga memudahkan pegawai untuk menggunakannya.
AP-2	*Fuel Cost Control System*	Internal / Cukup Kompleks	FCCS adalah aplikasi untuk pengendalian penggunaan bahan bakar minyak kendaraan bermotor. Bertujuan untuk mengendalikan tingkat efisiensi *reimbursment* biaya bahan bakar.
AP-3	*Warehouse application*	Internal / Sederhana	Aplikasi untuk mencatat barang masuk dan keluar sebuah gudang, membuat laporan stok/persedian barang Gudang.
AP-4	*Manifest_application-1*	Internal / Cukup Kompleks	Untuk mencatat manifest beserta jumlah dan berat kantong yang dibawa oleh kendaraan, serta mencatat jam keberangkatan dan kedatangan kendaraan.

ID-App	Nama Aplikasi	Lingkup /Kompleksitas	Tujuan Aplikasi
AP-5	*Manifest_application-2*	Internal / Cukup Kompleks	Untuk mencatat manifest perjalanan kendaraan beserta barang yang dibawa, serta mentatat jam kedatangan dan keberangkatan kendaraan pada lokasi yang telah ditentukan.
AP-6	*Vendor Management System Application*	Eksternal / Sangat Kompleks	Aplikasi untuk mencatat dan melakukan verifikasi kelayakan vendor (kapasitas siap layan, tingkat keahlian, aset yang dimiliki dan tarif) serta untuk melakukan e-Procurement.
AP-7	*Sales Management Application*	Eksternal / Sangat Kompleks	Aplikasi untuk mencatat daftar calon pelanggan, mencatat kegiatan/activitas petugas sales dan mencatat jenis layanan yang dibutuhkan pelanggan.
AP-8	*Financial Applications*	Internal / Cukup Kompleks	Aplikasi manajemen bisnis dan keuangan. Untuk pencatatan biaya, pendapatan, piutang dan mencetak ledger (laporan keuangan perusahaan).
AP-9	*Delivery application*	Eksternal / Sangat Kompleks	Aplikasi transaksional layanan Cargo Ritel untuk membuat resi kiriman, mannifest kiriman dan update informasi kedatangan barang pada lokasi yang ditentukan.
AP-10	*Production Dashboard Collection*	Internal / Sederhana	Dashboard untuk menampilkan data produksi semua unit bisnis.
AP-11	*Knowledge Management System*	Internal / Sederhana	Perpustakaan Digital Perusahaan, mencatat dan mendokumentasikan semua dokumen yang berkaitan dengan kedinasan
AP-12	*Transactional application at the airport*	Eksternal / Sangat Kompleks	Aplikasi transactional kegiatan operasional di Lini1 Bandara Soetta, untuk mencatat barang yang masuk gudang dan menentukan tarif/biaya simpan barang saat pengambilan
AP-13	*Simple Inventory*	Internal / Cukup Kompleks	Aplikasi untuk mencatat barang masuk dan keluar sebuah gudang, membuat laporan stok/persedian barang gudang

Daftar aplikasi pada Tabel 1 di atas adalah contoh sejumlah aplikasi bisnis logistik yang ditujukan untuk kebutuhan internal dan eksternal perusahaan yang bersifat jenerik, artinya tidak membatasi berapapun jumlah aplikasi yang dimigrasikan ke *cloud*. Perbedaan aplikasi internal dan eksternal perusahaan didasarkan kepada tujuan dan lingkup aplikasi tersebut, aplikasi yang bertujuan untuk mendukung bisnis proses perusahaan secara eksternal relatif memiliki kompleksitas yang lebih besar dibandingkan dengan aplikasi internal, sebab aplikasi eksternal akan memiliki dampak yang relatif lebih besar terhadap transaksional bisnis pada perusahaan. Sehingga hal ini akan berdampak terhadap nilai risiko aplikasi tersebut, semakin besar kompleksitas suatu aplikasi maka akan memiliki nilai risiko yang relatif lebih besar juga. Aplikasi-aplikasi yang diidentifikasikan ini ditujukan bagi aplikasi-aplikasi yang mewakili hampir seluruh aplikasi yang digunakan oleh perusahaan logistik yang akan memberikan layanan kepada pelanggannya baik nasional ataupun internasional. Sehingga pengambilan *sample* aplikasi-aplikasi ini cukup representatif berdasarkan lingkup atau kompleksitasnya, dan jika digunakan dalam penelitian lain yang sejenis dapat menghasilkan hasil yang relatif sama.

b. Pengidentifikasian Ancaman

Selain pengidentifikasian aset, berikutnya adalah tahap pengidentifikasian ancaman (*threats identification*) pada *cloud computing*. Pengidenifikasian *threat* ini menggunakan referensi dari *Top Threats to Cloud Computing The Egregious* 11 [1], hasil survei *Cloud Security Alliance* (CSA) Tahun 2020 terhadap ancaman pada keamanan *cloud* yang diurut berdasarkan rankingnya. Dari hasil survei

ini terdapat daftar ancaman, risiko dan kerentanan yang menonjol dilingkungan *cloud computing* ditunjukkan pada Tabel 2 berikut ini:

Tabel 2 Jenis Ancaman pada *Cloud Computing* [1]

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

Threats type pada Table 4.6 didapat dari hasil survei pada 241 pakar industri sebagai responden tentang masalah keamanan di *cloud*, dan hasilnya terdapat 11 (sebelas) ancaman yang menonjol pada masalah keamanan *cloud computing.* Kolom *ranking* dihitung berdasarkan poin yang diberikan oleh responden dengan memberikan rentang poin 1 sampai 10 untuk setiap jenis ancaman, dimana poin "1" adalah "sangat tidak signifikan" dan "10" adalah "sangat signifikan". Selanjutnya poin dari setiap jenis ancaman di rata-ratakan untuk diberi peringkat menurut nilai rata-ratanya [1]. Sedangkan kolom *Probability of Occurrence* adalah besarnya prosentase kemungkinan terjadinya risiko setiap jenis ancaman pada keamanan *cloud*. Nilai *Probability of Occurrence* untuk setiap ancaman didapat berdasarkan hasil dari kegiatan *Focus Group Discussion* (FGD) yang merupakan salah satu cara peneliti mendapatkan referensi penelitian. Besarnya persentase kemungkinan risiko yang diberikan pada setiap ancaman diatas juga merupakan keputusan dari pihak pengguna layanan *cloud*. Berdasarkan Tabel 4.6 diatas, pengguna layanan *cloud* merasakan masih kurangnya strategi keamanan dan disusul oleh masih terjadi pembajakan akun di *cloud.*

c. Pengidentifikasian Kerentanan

Berikutnya kita akan melihat dari ancaman yang sudah didefenisikan di atas, apa saja yang menjadi potensi kemungkinan ancaman tersebut muncul, yang kita sebut sebagai kerentanan. Untuk itu perlu untuk mengidentifikasi kerentanan yang kemungkinan akan menjadi potensi terjadinya ancaman seperti ditunjukkan pada Tabel 3 berikut ini:

Tabel 3 Daftar Kerentanan pada Cloud Computing [2]

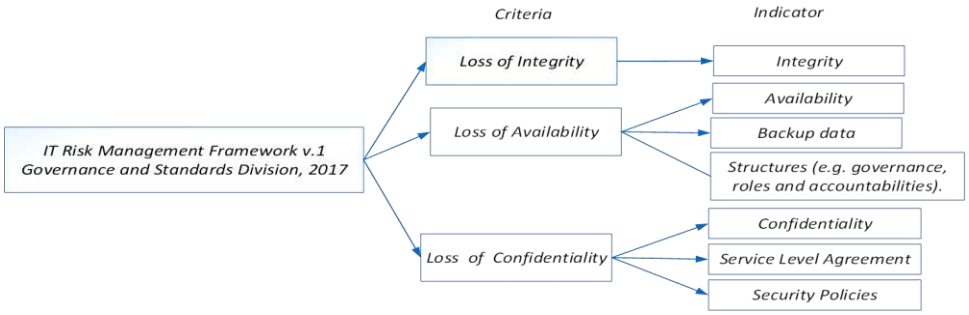
Vulnerability_ ID	***Vulnerability_name***	***Level of Vulnerabilities***
V01	*Insecure Interfaces and APIs*	7
V02	*Unlimited Allocation of Resources*	4
V03	*Data Related Vulnerabilities*	7
V04	*Virtual Machines Vulnerabilities*	7
V05	*Virtual Machine Images Vulnerabilities*	7
V06	*Hypervisor Vulnerabilities*	5
V07	*Vulnerabilities in Virtual Networks*	7
V08	*AAA Vulnerabilities*	3
V09	*Inappropriate encryption of data in rest and in transit.*	3
V10	*Impossibility of processing of encrypted data while in transit.*	4
V11	*Possibility that internal network probing will occur (cloud).*	5
V12	*Application vulnerabilities or poor patch management.*	4
V13	*Service Level Agreement thrashing in multi-vendor*	4

Vulnerability_ ID	*Vulnerability_name*	*Level of Vulnerabilities*
	environment	
V14	*Service Level Agreement clauses containing exclusive business risk.*	7
V15	*Audit not available to customers.*	4
V16	*Session Riding and Hijacking*	8
V17	*Reliability and Availability of Service*	3
V18	*Insure Cryptography*	5
V19	*Data Protection and Portability*	5
V20	*Virtual Machine Escape*	8
V21	*CSP lock-in*	4
V22	*Internet Dependency*	8
V23	*Malicious Insider Threats*	7
V24	*Unclear Roles and Responsibilities*	7
V25	*Poor Provider Selection*	5
V26	*System or Operating system Vulnerabilities*	5
V27	*Lack of Security Awareness*	7
V28	*Mal-configuration*	5
V29	*Malicious Users*	8

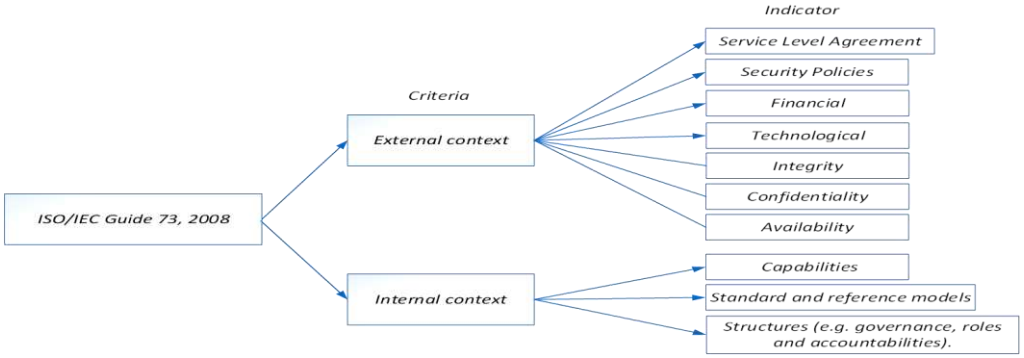
Daftar kerentanan dan tingkat kerentanan pada Tabel 4.7 di atas didapat berdasarkan referensi dari penelitian sebelumnya, dengan tingkat kerentanan dibagi menjadi 4(empat), yaitu: *Low*(0 s/d 3,9), *Average*(4 s/d 6,9), *High*(7 s/d 9,9) dan *Critical* adalah 10 [2]. Untuk menentukan tingkat kerentanan pada masing-masing kerentanan ditetapkan berdasarkan hasil kesepakatan pada FGD yang memberikan masukkan untuk tingkat kerentanannya berdasarkan rentang nilai pada tingkat kerentanan, seperti ditunjukkan pada kolom *level of vulnerabilities.*

2. Penetapan Indikator Penilaian Risiko

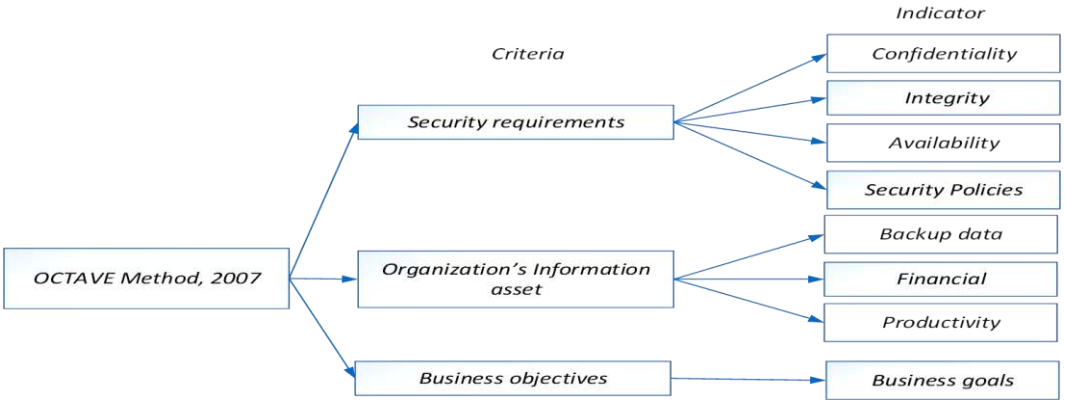
Indikator penilaian risiko yang digunakan dalam penelitian ini mengadopsi dari beberapa indikator yang terdapat pada model atau *framework* manajemen risiko yang sudah ada saat ini [3]–[5], serta ditambah dengan indikator dari hasil penelitian-penelitian sebelumnya [2], [6]. Secara detil indikator yang digunakan dapat digambarkan sebagai berikut:



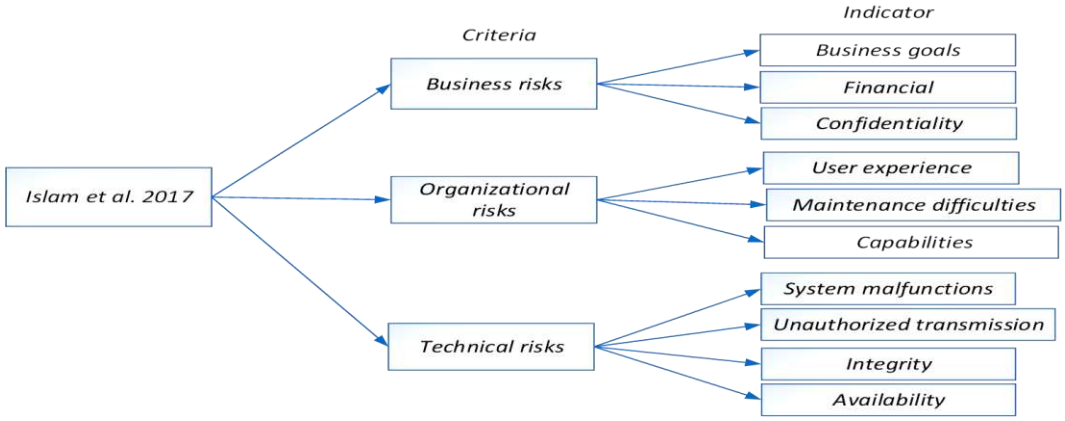
Gambar 1 Indikator Penilaian Risiko *by IT Risk Management* [3]



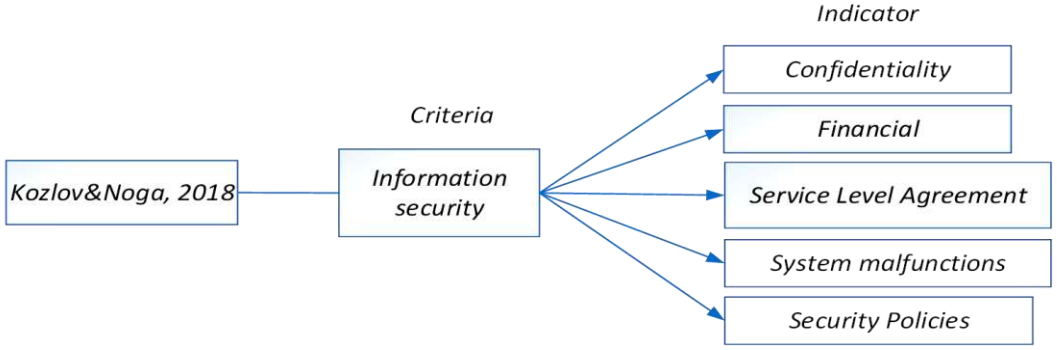
Gambar 2 Indikator Penilaian Risiko *by ISO/IEC Guide 73* [4]



Gambar 3 Indikator Penilaian Risiko *by OCTAVE Method* [5]



Gambar 4 Indikator Penilaian Risiko *by Categorize Risk* [6]



Gambar 5 Indikator Penilaian Risiko *by Information Security* [2]

Berdasarkan Gambar 2,3,4, dan 5 di atas terdapat 17(tujuh belas) indikator yang dapat diadopsi dalam dalam penelitian ini, sehingga membuat penelitian ini melebihi lengkap dari penelitian-penelitian sebelumnya dan ini merupakan novelty penelitian ini. Secara detil penjelasan dari masing-masing indikator dijelaskan sebagai berikut:

Tabel 4 Indikator Penilaian Risiko

No.	Indikator	Keterangan
1	*Integrity*	Tingkat/*level* informasi yang dapat digunakan tanpa adanya perubahan informasi.
2	*Availability*	Kesiapan informasi yang dapat diakses kapan saja (24 jam) oleh pengguna

3	*Confidentiality*	Menjamin kerahasiaan informasi melalui keamanan informasi dari penggunaan informasi yang tidak sah sehingga dapat menjaga kepercayaan pelanggan
4	*Service Level Agreement*	Tingkat kesesuaian dengan kebijakan per undang-undangan
5	*Security Policies*	Terdapat kebijakan-kebijakan terkait dengan keamananan informasi dan data perusahaan
6	*Financial*	Terjadinya peningkatan biaya operasional akibat migrasi ke *cloud*
7	*Technological*	Besarnya perubahan teknologi yang digunakan akibat migrasi ke *cloud*
8	*Capabilities*	Tingkat kemampuan karyawan akibat migrasi ke *cloud*
9	*Standard and reference models*	Standar dan model referensi yang diadopsi oleh organisasi
10	*Structures (e.g. governance, roles and accountabilities).*	Besarnya perubahan tata kelola oragnisasi akibat migrasi ke *cloud*
11	*Backup data*	Proses *backup* data dilakukan secara berkelanjutan
12	*Productivity*	Terjadi peningkatan produktivitas kerja karyawan akibat migrasi ke *cloud*
13	*Business goals*	Terjadi peningkatan bisnis perusahaan akibat migrasi ke *cloud*
14	*User experience*	Pengalaman pelanggan yang tidak memadai dengan teknologi *cloud*
15	*Maintenance difficulties*	Tingkat kesulitan pemeliharaan saat bermigrasi dan beroperasi di *cloud*
16	*System malfunctions*	Sistem tidak berjalan sesuai fungsinya
17	*Unauthorized transmission*	Tingkat kesalahan dalam pengiriman data

3. Pemetaan Ancaman terhadap Aset

Pemetaan ancaman terhadap aset bertujuan untuk mengetahui seberapa banyak jumlah ancaman yang kemungkinan akan muncul terhadap keamanan aplikasi-aplikasi yang akan dimigrasikan ke *cloud computing*. Berdasarkan Tabel 1 dan Tabel 2 selanjutnya akan digambarkan pemetaan (*maping*) antara aplikasi-aplikasi yang akan dimigrasi ke *cloud computing* terhadap ancaman risiko yang ada. Adapun jumlah ancaman terhadap aplikasi-aplikasi ini juga sangat tergantung kepada pengalaman secara empiris yang dialami oleh pengguna layanan *cloud* dan dapat diterapkan pada perusahaan logistik yang akan migrasikan aplikasi-aplikasinya ke *cloud computing* . Pemetaan (*maping*) ini didapat dari hasil kuesioner secara *online* yang disampaikan kepada tim ICT Poslog dan hasilnya dapat ditunjukkan pada Tabel 5 berikut ini:

Tabel 5 Pemetaan Aplikasi vs Ancaman

ID-App	***ID_Threat***										
	TH-1	***TH-2***	***TH-3***	***TH-4***	***TH-5***	***TH-6***	***TH-7***	***TH-8***	***TH-9***	***TH-10***	***TH-11***
AP-1	√	-	-	-	√	√	-	√	-	-	√
AP-2	√	-	√	-	-	√	-	-	-	√	-
AP-3	-	√		√	√	-	-	-	-	-	-
AP-4	√	√	-	-	-	√	-	-	√	-	-
AP-5	√	-	√	-	-	-	√	-	-	-	-
AP-6	-	-	-	-	√	√	√	-	√	-	-
AP-7	-	-	-	-	√	√	√	-	-		-
AP-8	√	-	√	√	-	-	-	-	-	√	-
AP-9	-	√	-	√	√	√	-	-	-	-	-
AP-10	√	-	-	√	-	-	-	√	-	-	√
AP-11	√	-	-	√	-	-	-	-	√	√	-
AP-12	-	-	√	-	√	√	√	-	-	-	-
AP-13	√	-	√	√	-	-	-	√	-	-	√

ID_Threat (TH-1 s/d TH-11) pada Tabel 5 menunjukkan jenis ancaman yang kemungkinan muncul pada *cloud* dan *ID_App (AP-1 s/d AP-13)* adalah kode aplikasi logistik yang akan di migrasikan

ke *cloud*. Tanda "√" menunjukkan bahwa adanya kemungkinan munculnya ancaman pada aplikasi tertentu, sedangkan tanda "-" menunjukkan tidak adanya kemungkinan ancaman pada aplikasi tersebut. Berdasarkan Tabel 5 di atas, terlihat kemungkinan munculnya ancaman pada aplikasi-aplikasi yang dimigrasi ke *cloud* sangat bervariasi, hal ini dikarenakan sangat bergantung dari kesimpulan pihak pengguna layanan *cloud*, antara satu pengguna dengan pengguna lainnya kemungkinan akan berbeda. Untuk melihat lebih detil hasil pemetaan antara ancaman dan aset ditunjukkan pada Tabel 6 berikut ini:

Tabel 6 Ancaman pada masing-masing Aplikasi

ID-App	***Application_NAme***	***ID_Threat***	***Threats Type***
AP-1	*Human Resource Information System*	*TH-1*	*Data Breaches*
		TH-5	*Account Hijacking*
		TH-6	*Insider Threat*
		TH-8	*Weak Control Plane*
		TH-11	*Abuse and Nefarious Use of Cloud Services*
AP-2	*Fuel Cost Control System*	*TH-1*	*Data Breaches*
		TH-3	*Lack of Cloud Security Architecture and Strategy*
		TH-6	*Insider Threat*
		TH-10	*Limited Cloud Usage Visibility*
AP-3	*Warehouse application*	*TH-2*	*Misconfiguration and Inadequate Change Control*
		TH-4	*Insufficient Identity, Credential, Access and Key Management*
		TH-5	*Account Hijacking*
AP-4	*Manifest_application-1*	*TH-1*	*Data Breaches*
		TH-2	*Misconfiguration and Inadequate Change Control*
		TH-6	*Insider Threat*
		TH-9	*Meta structure and Applistructure Failures*
AP-5	*Manifest_application-2*	*TH-1*	*Data Breaches*
		TH-3	*Lack of Cloud Security Architecture and Strategy*
		TH-7	*Insecure Interfaces and APIs*
AP-6	*Vendor Management System Application*	*TH-5*	*Account Hijacking*
		TH-6	*Insider Threat*
		TH-7	*Insecure Interfaces and APIs*
		TH-9	*Meta structure and Applistructure Failures*
AP-7	*Sales Management Application*	*TH-5*	*Account Hijacking*
		TH-6	*Insider Threat*
		TH-7	*Insecure Interfaces and APIs*
AP-8	*Financial Applications*	*TH-1*	*Data Breaches*
		TH-3	*Lack of Cloud Security Architecture and Strategy*
		TH-4	*Insufficient Identity, Credential, Access and Key Management*
		TH-10	*Limited Cloud Usage Visibility*
AP-9	*Delivery application*	*TH-2*	*Misconfiguration and Inadequate Change Control*

ID-App	*Application_NAme*	*ID_Threat*	*Threats Type*
		TH-4	*Insufficient Identity, Credential, Access and Key Management*
		TH-5	*Account Hijacking*
		TH-6	*Insider Threat*
AP-10	*Production Dashboard Collection*	*TH-1*	*Data Breaches*
		TH-4	*Insufficient Identity, Credential, Access and Key Management*
		TH-8	*Weak Control Plane*
		TH-11	*Abuse and Nefarious Use of Cloud Services*
AP-11	*Knowledge Management System*	*TH-1*	*Data Breaches*
		TH-4	*Insufficient Identity, Credential, Access and Key Management*
		TH-9	*Meta structure and Applistructure Failures*
		TH-10	*Limited Cloud Usage Visibility*
AP-12	*Transactional application at the airport*	*TH-3*	*Lack of Cloud Security Architecture and Strategy*
		TH-5	*Account Hijacking*
		TH-6	*Insider Threat*
		TH-7	*Insecure Interfaces and APIs*
AP-13	*Simple Inventory*	*TH-1*	*Data Breaches*
		TH-3	*Lack of Cloud Security Architecture and Strategy*
		TH-4	*Insufficient Identity, Credential, Access and Key Management*
		TH-8	*Weak Control Plane*
		TH-11	*Abuse and Nefarious Use of Cloud Services*

Pemetaan (*maping*) ini didapat dari hasil kuesioner peneliti yang disampaikan secara *online* kepada tim ICT pemilik aplikasi logistik. Informasi yang dapat kita ketahui dari Tabel 6 di atas adalah bahwa 1(satu) aplikasi dapat memiliki beberapa jenis ancaman keamanan di *cloud*. Untuk menentukan jenis ancaman apa saja terhadap aplikasi logistik tersebut, ini sangat tergantung pada pendapat dari pengelola dan pemilik aplikasi tersebut, karena mereka yang mengetahui secara detil karakteristik aplikasi.

4. Pemetaan Ancaman terhadap Kerentanan

Kerentanan merupakan suatu potensi yang kemungkinan muncul terjadinya suatu ancaman. Berdasarkan Tabel 2 dan Tabel 3 kita akan membentuk relasi atau hubungan antara kerentanan terhadap ancaman risiko. Pada penelitian ini relasi antara ancaman dan kerentanan diasumsikan bahwa 1(satu) ancaman dapat mempunyai beberapa (N) kerentanan, sehingga relasi ancaman dan kerentanan adalah 1-N (satu ke banyak). Hubungan atau relasi antara ancaman dan kerentanan dapat ditunjukkan pada Tabel 7 berikut ini:

Tabel 7 Relasi Antara Ancaman dan Kerentanan

ID_Threat	Vulnerabilities_ID	Vulnerability_value
TH-1	*V01, V08, V09, V11, V12, V17, V22, V25*	4,8
TH-2	*V23, V28*	6,0

ID_Threat	Vulnerabilities_ID	Vulnerability_value
TH-3	*V01, V27*	7,0
TH-4	*V13, V14, V15, V20, V24*	6,0
TH-5	*V01, V16*	7,5
TH-6	*V22, V23, V27*	7,3
TH-7	*V01*	7,0
TH-8	*V16, V23, V25*	6,7
TH-9	*V01, V12, V20, V28*	6,0
TH-10	*V17, V21*	3,5
TH-11	*V23, V29*	7,5

Berdasarkan Tabel 7 sangat bervariasi jumlah kerentanan yang berpotensi terhadap ancaman yang ada. Setelah diketahui relasi antara ancaman dan kerentanan (*TH* terhadap *V*), selanjutnya dapat dihitung nilai kerentanan dari masing-masing ancaman dengan menjumlahkan nilai tiap-tiap kerentanan yang berpotensi pada ancaman tersebut. Selanjutnya dihitung nilai rata-ratanya yang akan dijadikan sebagai nilai akhir kerentanan sebuah ancaman, dan nilai ini akan digunakan untuk menghitung nilai risiko terhadap semua aplikasi yang dimigrasikan ke *cloud*.

Contoh, pada Tabel 4.11 di atas, ancaman pada *TH-1* memiliki potensi kerentanan sebanyak 8(delapan), yaitu *V01, V08, V09, V11, V12, V17, V22, V25* (kerentanan ke-1, ke-8, ke-9, ke-11, ke-12, ke-17, ke-22, dank e-25), sehingga berdasarkan Tabel 4.7 nilai total kerentanan untuk ancaman *TH-1* adalah sebagai berikut:

Nilai kerentanan v = 7+3+3+5+4+3+8+5 = 38;

Nilai kerentanan pada *TH-1* adalah $= \frac{38}{8}$ = 4,75 ~ **4,8.**

Dengan cara yang sama untuk menghitung nilai kerentanan pada ancaman yang ke-2 (*TH-2*) dan seterusnya.

5. Perhitungan Nilai Bobot Aset

Setiap ancaman akan berdampak pada aplikasi yang dimigrasikan ke cloud dengan memberikan nilai antara 1 hingga 100 dengan kategori risiko rendah (0 - 30), risiko sedang (31 - 60), dan risiko tinggi (61 - 100). Selanjutnya nilai penilaian hasil dihitung dengan menggunakan rumus:

$$r_a = \sum_{1}^{n} p_o v_a \qquad (1)$$

dimana:

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

Table 8. Result assessment per asset

No.	*ID_App*	***Threats***											***Result Assessment***
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	
Probability of Occurrence		**5%**	**9%**	**17%**	**5%**	**16%**	**14%**	**11%**	**5%**	**2%**	**7%**	**9%**	
1	*AP-1*	80	70	75	75	80	90	80	65	70	80	80	**78.45**
2	*AP-2*	75	80	80	85	70	60	70	80	70	75	85	**74.4**
3	*AP-3*	65	50	35	35	20	45	30	40	30	55	50	**39.2**
4	*AP-4*	70	70	60	25	60	45	35	65	50	50	35	**45.6**

No.	*ID_App*	*Threats*											*Result Assessment*
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	
Probability of Occurrence		**5%**	**9%**	**17%**	**5%**	**16%**	**14%**	**11%**	**5%**	**2%**	**7%**	**9%**	
5	*AP-5*	70	60	45	40	45	35	50	55	45	45	50	**47.45**
6	*AP-6*	80	85	80	85	80	75	75	80	80	90	85	**80.6**
7	*AP-7*	80	90	95	80	80	70	75	70	80	85	90	**82.25**
8	*AP-8*	75	60	20	40	80	50	35	30	80	45	45	**48.5**
9	*AP-9*	70	60	65	60	70	75	45	65	70	55	45	**62.15**
10	*AP-10*	55	45	25	55	70	50	20	40	70	60	40	**45.4**
11	*AP-11*	50	50	35	45	45	35	25	40	50	45	45	**40.25**
12	*AP-12*	60	70	55	55	65	65	60	70	60	65	60	**62.15**
13	*AP-13*	30	50	45	35	65	35	50	40	65	45	50	**47.15**

Remarks: This value is filled in based on the assumption that a threat will occur in the application

6. Perhitungan Nilai Risiko terhadap Aplikasi pada Cloud Migration
Berdasarkan nilai result assessment pada tabel 8, nilai kerentanan pada tabel 7, dan nilai bobot masing-masing indikator dari penilaian risiko, selanjutnya dapat dihitung nilai risiko untuk setiap aplikasi (aset) yang akan dimigrasikan ke cloud computing dengan formula (2).

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

dimana:
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

Secara lengkap hasil perhitungan risiko per asset yang dimigrasikan ke cloud computing dapat ditunjukkan pada tabel 8:

Table 5. 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 (1-100)			**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**

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 (1-100)			8%	8%	8%	5%	5%	5%	6%	6%	5%	5%	5%	8%	5%	5%	6%	5%	5%	
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**

Remarks:

High-risk Medium-risk

7. Kategori Risiko dan Mitigasi Risiko

Nilai risiko yang didapat dari hasil eksprimen dapat dikategorikan menjadi 3(tiga) kategori, yaitu: *Low* (< 30), *Medium* (30 - 60), dan *High* (> 60), selanjutnya dapat diditentukan level risikonya melalui *risk map.* Tujuan dari *risk map* adalah untuk menentukan skala prioritas penanganan risiko, dimana masing-masing perusahaan dalam menentukan level risiko melalui *risk map* akan berbeda-beda satu perusahaan dengan perusahaan yang lainnya bergantung kepada kesepakatan manajemen Perusahaan [7]. Dari hasil penilaian risiko pada Tabel 5 di atas akan digunakan sebagai acuan untuk menentukan peta risiko (*risk map*) untuk menentukan *risk appetite* berdasarkan *Risk IT Framework* dari ISACA sebagai pendekatan mitigasi risiko seperti ditunjukkan pada Tabel 6 berikut ini:

Table 5. Risk mitigation approach

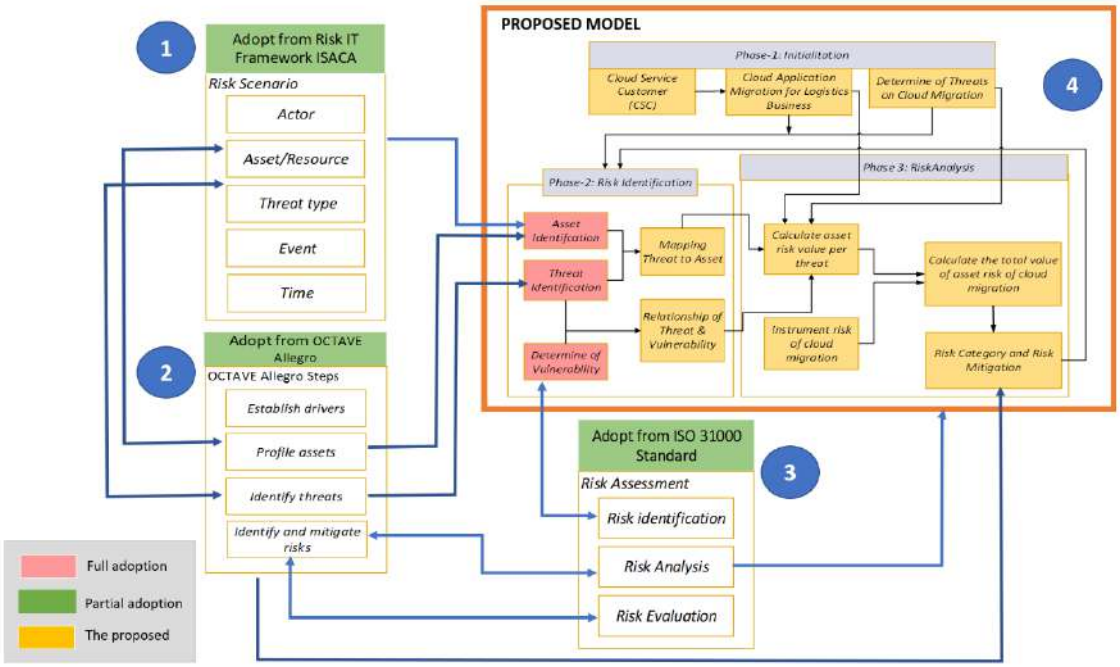
Risk Value	Risk Category	Risk Map
0 - 30	Low	*Opportunity*
31 - 60	Medium	*Acceptable or Unacceptable*
61 - 100	High	*Really Unacceptable*

Pendekatan mitigasi risiko ada 4(empat), yaitu:

- *Opportunity*: nilai risiko pada kategori *low*, perusahaan tidak harus mengambil suatu tindakan untuk mengatasi risiko.
- *Acceptable*: nilai risiko pada kategori *medium*, perusahaan dapat membuat strategi untuk mengatasi kemungkinan ancaman atau meminimalisir dampak dari ancaman, namun perusahaan tidak perlu melakukan penanganan khusus.
- *Unacceptable:* nilai risiko pada kategori *medium*, perusahaan masih dapat menerima resiko tetapi memungkinkan perusahaan untuk membuat sebuah tindakan khusus untuk menangani risiko, misal mengalihkan risiko ke pihak lain.
- *Really Unacceptable*: nilai risiko pada kategori *high*, termasuk dalam jenis risiko yang tidak dapat diterima perusahaan, dan perusahaan harus melakukan analisis terhadap risiko yang ada secara lebih detil dan mengumpulkan informasi-informasi tambahan untuk memantau dan mengevaluasi kembali keputusan terhadap aset yang memiliki risiko tinggi.

B. PENGEMBANGAN MODEL PERHITUNGAN NILAI RISIKO

Model yang diusulkan bertujuan untuk menghitung risiko pada aplikasi yang akan dimigrasi ke cloud computing dan dibuat secara sistematis yang dapat memberikan kemudahan bagi pengguna layanan cloud dalam menghitung kemungkinan nilai risiko pada aplikasi yang akan dimigrasi ke cloud computing. Model yang dikembangkan peneliti ini mengadopsi tahapan evaluasi risiko dari Risk IT Framework, mengadopsi skenario risiko dari standar ISO 31000 dan mengadopsi tahapan metode OCTAVE. Skenario pengembangan langkah demi langkah model yang diusulkan dimulai dengan mengekstraksi dari tiga kerangka kerja (Risk IT Framework ISACA, standar ISO 31000, dan metode OCTAVE Allegro) seperti yang ditunjukkan pada Gambar 6.



Gambar 6 Pengembangan Model Pengukuran Nilai Risiko (Peneliti)

Tahapan yang dilakukan untuk mengembangkan model ini dapat dijelaskan sebagai berikut:

1. Mengadopsi dari ISACA Risk IT Framework

   Pada bagian ini peneliti mengadopsi skenario risiko yang terdapat dalam tahap evaluasi risiko, antara lain siapa yang bertanggung jawab atas risiko perusahaan, jenis ancaman apa yang mungkin timbul dan merugikan, kejadian atau kejadian dan proses yang tidak sesuai, aset atau sumber daya yang terkena dampak. kejadian buruk, serta waktu terjadinya kejadian buruk tersebut.

2. Mengadopsi proses manajemen risiko dari standar ISO 31000

   Pada bagian ini peneliti mengadopsi tahapan penilaian risiko, yang meliputi: tahap identifikasi risiko, tahap analisis risiko, dan tahap evaluasi risiko.

3. Mengadopsi dari fase-fase pada metode OCTAVE

   Peneliti melakukan langkah-langkah yang terdapat pada tahapan metode OCTAVE antara lain: tahap penentuan tingkat kriteria risiko, penentuan profil aset dan identifikasi ancaman, identifikasi risiko, analisis risiko, dan pelaksanaan mitigasi risiko.

4. Pengembangan model yang diusulkan

   Berdasarkan 3 (tiga) adopsi framework yang telah dijelaskan di atas, selanjutnya akan diuraikan secara rinci bagian-bagian yang membentuk model pengukuran analisis risiko yang lebih praktis yang dapat digunakan perusahaan dalam menghitung nilai risiko pada aplikasi yang akan dimigrasikan ke cloud computing.

   Tahapan model pengukuran analisis nilai risiko pada aplikasi yang akan dimigrasikan ke cloud computing dapat dijelaskan sebagai berikut:

Tahap 1: Proses inisialisasi dibagi menjadi 3 (tiga) bagian, yaitu:

1. Menentukan perusahaan logistik pengguna layanan cloud yang akan menjadi objek. Penentuan profil perusahaan perlu dilakukan karena akan mempengaruhi ruang lingkup dan karakteristik perusahaan.
2. Menentukan aplikasi yang akan dimigrasikan ke cloud computing dan akan dihitung nilai risikonya. Perusahaan yang berbeda akan mengizinkan penggunaan aplikasi yang berbeda.
3. Menentukan ancaman yang mungkin timbul dalam migrasi cloud. Untuk mengetahui ancaman terhadap migrasi cloud, Anda dapat mencari melalui tinjauan literatur penelitian sebelumnya.

Fase 2: Mengidentifikasi risiko, pada fase ini dilakukan langkah-langkah sebagai berikut:

1. Identifikasi aset perusahaan berupa sistem aplikasi yang mendukung proses bisnis perusahaan baik internal maupun eksternal yang akan dimigrasikan ke cloud computing.
2. Identifikasi ancaman yang ada pada migrasi cloud berdasarkan referensi atau sumber, pada penelitian ini peneliti mengambil sumber dari Top Threats to Cloud Computing the Egregious 11 [1]
3. Menentukan kerentanan yang akan memberikan potensi ancaman terhadap migrasi cloud.

D. **STATUS LUARAN**: Tuliskan jenis, identitas dan status ketercapaian setiap luaran wajib dan luaran tambahan (jika ada) yang dijanjikan. Jenis luaran dapat berupa publikasi, perolehan kekayaan intelektual, hasil pengujian atau luaran lainnya yang telah dijanjikan pada proposal. Uraian status luaran harus didukung dengan bukti kemajuan ketercapaian luaran sesuai dengan luaran yang dijanjikan. Lengkapi isian jenis luaran yang dijanjikan serta mengunggah bukti dokumen ketercapaian luaran wajib dan luaran tambahan melalui BIMA.

Luaran penelitian:

1. Luaran wajib
   Luaran wajib berupa publikasi jurnal, status **submit** ke International Journal of Computer Information Systems and Industrial Management Applications, Terindeks Scopus (Q3) SJR 2022 (0,25).

   Bukti dokumen paper:
   https://drive.google.com/file/d/1daNNt9I_zZCRpD1wYzZRyORFQcHku-w2/view?usp=sharing

   Bukti submit ke jurnal:
   https://drive.google.com/file/d/1_qUXMGz_k3vTXZZznvsgxyfSsIF0ZdVh/view?usp=sharing

   Bukti upload file:
   https://drive.google.com/file/d/1uN3hupilLPwd9oafabj3L0kQCJJAKmpG/view?usp=sharing

2. Luaran tambahan
   Dokumen feasibility study merupakan luaran tambahan dalam penelitian ini. tujuan feasibility study ini adalah untuk menggali informasi sedalam-dalamnya guna meyakinkan bahwa penelitian ini layak untuk dilakukan.
   Bukti dokumen feasibility study:
   https://drive.google.com/file/d/1BRFVHxESp2olboAdj9ZbPqmlEREJVMp1/view?usp=sharing

E. **PERAN MITRA:** Tuliskan realisasi kerjasama dan kontribusi Mitra baik *in-kind* maupun *in-cash* (untuk Penelitian Terapan, Penelitian Pengembangan, PTUPT, PPUPT serta KRUPT). Bukti pendukung realisasi kerjasama dan realisasi kontribusi mitra dilaporkan sesuai dengan kondisi yang sebenarnya. Bukti dokumen realisasi kerjasama dengan Mitra diunggah melalui BIMA.

-

F. **KENDALA PELAKSANAAN PENELITIAN**: Tuliskan kesulitan atau hambatan yang dihadapi selama melakukan penelitian dan mencapai luaran yang dijanjikan, termasuk penjelasan jika pelaksanaan

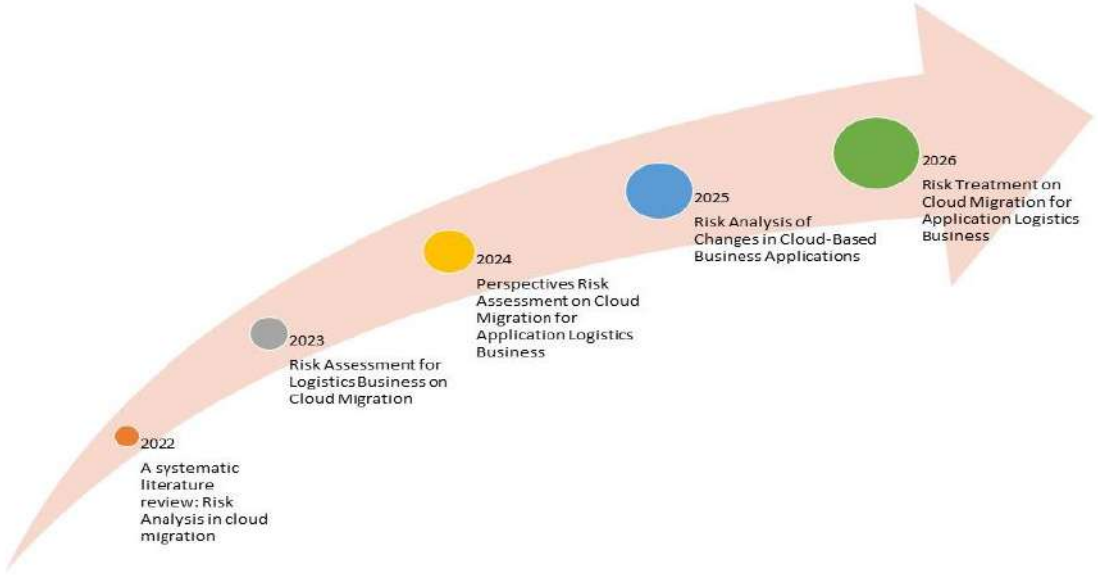
penelitian dan luaran penelitian tidak sesuai dengan yang direncanakan atau dijanjikan.

Kendala Pelaksanaan Penelitian:

Secara keseluruhan mulai dari pelaksanaan feasibility study sampai dengan penyusunan progres laporan penelitian, peneliti tidak menemukan kendala yang signifikan. Namun ketika akan melakukan submit jurnal dan memilih jurnal tertentu kami terbentur masalah pembiayaan, karena biaya penelitian tidak cukup untuk pembayaran biaya jurnal.

G. **RENCANA TAHAPAN SELANJUTNYA:** Tuliskan dan uraikan rencana penelitian di tahun berikutnya berdasarkan indikator luaran yang telah dicapai, rencana realisasi luaran wajib yang dijanjikan dan tambahan (jika ada) di tahun berikutnya serta *roadmap* penelitian keseluruhan. Pada bagian ini diperbolehkan untuk melengkapi penjelasan dari setiap tahapan dalam metoda yang akan direncanakan termasuk jadwal berkaitan dengan strategi untuk mencapai luaran seperti yang telah dijanjikan dalam proposal. Jika diperlukan, penjelasan dapat juga dilengkapi dengan gambar, tabel, diagram, serta pustaka yang relevan. Jika laporan kemajuan merupakan laporan pelaksanaan tahun terakhir, pada bagian ini dapat dituliskan rencana penyelesaian target yang belum tercapai.

Roadmap penelitian mulai tahun 2022 sampai 2026 dapat dilihat pada Gambar 7 dibawah ini:



Gambar 7 Roadmap Penelitian

Berdasarkan roadmap penelitian tahun 2022 – 2026, maka rencana penelitian tahun 2024 akan fokus terhadap perspectives Risk Assesment yang dapat diterapkan di bisnis logistik yaitu melakukan penilaian resiko terhadap kegiatan logistik pergerakan barang dari lokasi asal ke tujuan untuk memenuhi keinginan konsumen, meliputi bisnis Courier & Service, Express/ Distribution, Value Added Warehouse & Distribution, Freight Forwarding, Distributor, Ritel: Terminal Peti Kemas, Ocean Carrier (Shipping) Air Carrier (Air Cargo): Land Carrier. Penelitian ini fokus pada bisnis logistik karena kedepannya perkembangan bisnis logistik ini sangat dinamis karena diperngaruhi oleh evolusi teknologi, perkembangan perdagangan online yang pesat yang merubah semua bisnis melakukan transformasi digitalisasi, perubahan dalam tren konsumen, peningkatan perdagangan global, kebutuhan akan efisiensi operasional, dan tantangan lingkungan. Hal ini berdampak pada industry logisti yang akan migrasikan aplikasi nya ke cloud yang sesuai dengan Peraturan Pemerintah (PP) No. 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Pasal 17 serta UU RI No. 11 Tahun 2008 Tentang Informasi Transaksi Elektronik, Pasal 9. Bagi penyelenggara Sistem Elektronik untuk pelayanan publik wajib memiliki rencana keberlangsungan kegiatan untuk menanggulangi gangguan atau bencana sesuai dengan risiko dari dampak yang ditimbulkannya.

H. DAFTAR PUSTAKA: Penyusunan Daftar Pustaka berdasarkan sistem nomor sesuai dengan urutan pengutipan. Hanya pustaka yang disitasi pada laporan kemajuan yang dicantumkan dalam Daftar Pustaka.

[1] J. M. C. Brook, V. Chin, S. Lumpe, and A. Ulskey, "Top Threats to Cloud Computing Security: The Egregious Eleven," Asia Pacific, 2020.

[2] 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.

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

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

[5] 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: http://www.sei.cmu.edu/publications/pubweb.html

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

[7] T. J. Betcher, "Cloud Computing: Key IT-Related Risks and Mitigation Strategies for Consideration by IT Security Practitioners," Eugene, Oregon, Amerika Serikat, 2010. [Online]. Available: http://hdl.handle.net/1794/10207

Ringkasan eksekutif maksimum 500 kata: memberikan gambaran umum tentang isi yang terkandung dalam dokumen studi kelayakan. Bagian ini merupakan ringkasan poin penting dari detail yang terkandung dalam keseluruhan dokumen studi kelayakan dan deskripsi singkat tentang produk dan/atau jasa yang dianggap sudah melalui tahapan kajian sebelumnya.

Ringkasan:
Cloud computing sudah banyak diimplementasikan di dunia bisnis tidak terkecuali di bidang logistik. Terkait dengan penilaian risiko pada *cloud computing*, saat ini banyak Perusahaan logistik yang belum pernah mengukur nilai risiko terhadap aplikasi-aplikasi yang akan dimigrasikan ke *cloud*. Model Risk Analysis Measurement Model in Migration Applications yang dikembangkan memberikan 17 indikator untuk menilai risiko 13 aplikasi generik yang digunakan di industri logistik dengan melihat dari berbagai persepektif, yaitu Asset Identification, Threat Identificaion dan Determine of Vulnerability

Pasar Produk/Layanan maksimum 500 kata: menjelaskan pasar yang ada untuk produk dan/atau jasa yang sedang dikembangkan. Peneliti sebaiknya memaparkan keunggulan-keunggulan kompetitif dan komparatif produk/jasa yang sedang dikembangkan, dengan membandingkannya dengan calon pesaing, mampu menawarkan nilai yang lebih besar kepada calon konsumen dari pada yang ditawarkan pesaing, serta keunikan-keunikan tertentu dari produk/hasil penelitiannya yang sulit ditiru produsen lain, perkiraan pasar yang bisa direbut.

Pasar Produk/Layanan:

1. Bidang Logistik

Di bidang logistik penelitian ini memberikan rekomendasi ketika perusahaan memutuskan untuk migrasi ke *cloud*, dimana masalah keamanan data menjadi hal penting, ini dapat terlihat ketika perusahaan pengguna layanan *cloud* akan melakukan migrasi dari *on premise* ke *cloud*. Dampak Covid-19 menuntut perusahaan logistik untuk bertransformasi digital dalam segala aktivitasnya, tentu ini akan berpengaruh pada peningkatan penggunaan pusat data perusahaan. Dalam kondisi seperti ini, maka penggunaan pusat data *cloud* sangat tepat untuk diterapkan oleh perusahaan. Berdasarkan cara pengukuran nilai risiko hasil penelitian ini, maka perusahaan akan mengetahui berapa besar risiko yang kemungkinan muncul akibat penggunaan pusat data *cloud*. Sebelum perusahaan memutuskan untuk migrasi ke pusat data *cloud*, maka aplikasi-aplikasi pendukung bisnis logistik yang akan dimigrasikan ke *cloud* terlebih dahulu diukur nilai risikonya. Hal ini memungkinkan perusahaan sektor logistik dapat mengurangi kemungkinan munculnya risiko pada aplikasi-aplikasi yang dimigrasikan ke platform cloud, sehingga dapat lebih meningkatkan layanannya kepada pelanggan.

2. Bidang Teroritis/Keilmuan

Pada beberapa model/*framework* manajemen risiko TI yang ada saat ini seperti *Risk IT Framework*, Standar ISO 31000, dan metode OCTAVE atau model-model risiko TI dari penelirian-penelitian sebelumnya (Islam et al. 2017; Kozlov and Noga 2018) belum dijelaskan secara kuantitatif bagaimana menghitung nilai risiko sebelum migrasi, saat melaksanakan migrasi, dan setelah migrasi ke *cloud* dengan mempertimbangkan indikator pada kriteria dampak risiko yang akan berdampak pada perusahaan, seperti yang dilakukan dalam penelitian ini. Perbedaannya terlihat dari indikator pengukuran nilai risiko yang digunakan. Pada penelitian yang diusulkan

menggunakan 17(tujuh belas) indikator yang diadopsi dari 5(lima) sumber, yaitu: *IT Risk Management Framework v.1 Governance and Standards Division, Risk management — Vocabulary SO/IEC Guide 73, OCTAVE Method*, dan dari penelitian-penelitian sebelumnya (Islam et al. 2017) dan (Kozlov and Noga 2018).

Tabel 1. Perbandingan Framework/Model Manajemen Risiko TI

Indicator / Model/Framework IT Risk Management	Integrity	Availability	Service Level Agreement	Technological	Capabilities	Standard and reference models	Confidentiality	Structures (e.g. governance, roles and accountabilities)	Security Policies	Backup data	Productivity	Business goals	Financial	User experience	Maintenance difficulties	System malfunctions	Unauthorized transmission
IT Risk Management Framework v.1 Governance and Standards Division, 2017	√	√	√				√	√		√							
ISO/IEC Guide 73, 2008	√	√	√	√	√	√	√	√	√				√				
OCTAVE Method, 2007	√	√					√		√	√	√	√	√				
Kozlov&Noga, 2018			√				√		√				√			√	
Islam et al. 2017	√	√			√		√					√	√	√	√	√	√
Penelitian yang Diusulkan	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√

Setelah dikembangkan model pengukuran nilai risiko *application migration* pada *cloud migration* untuk bisnis logistik, terlihat bahwa perusahaan mengetahui nilai risiko migrasi ke *cloud* untuk masing-masing aplikasi yang dimigrasikan. Hal ini dapat dijadikan sebagai bahan penunjang dalam pengambilan keputusan serta dapat menjadi rekomendasi untuk perencanaan dan persiapan *risk mitigation* yang merupakan bagian dari tahap dalam *risk management*.

3. Bidang Cloud Computing

Ketika perusahaan memutuskan untuk migrasi dari *on premise* ke *cloud*, maka masalah keamanan data menjadi hal penting. Dengan mengimplementasikan model hasil penelitian yang diusulkan ini penanganan masalah keamanan pada *cloud* dapat diminimalisir dengan mengurangi risiko ancaman dalam konteks *cloud* terhadap aplikasi logistik yang akan dimigrasikan ke *cloud.* Hal ini dikarenakan model yang diusulkan dapat memberikan perhitungan nilai risiko setiap aplikasi berdasarkan pada *Probability of Occurrence* setiap jenis ancaman yang kemungkinan terjadi terhadap aplikasi yang dimigrasikan ke cloud, selanjutnya berdasarkan nilai risiko pada masing-masing aplikasi tersebut di kategorikan pada level risiko (*low*, *medium*, atau *high*). Dengan adanya penanganan terhadap ancaman yang cepat, maka dapat meningkatkan *security* layanan *cloud*, dan ini menjadi hal yang utama dalam meningkatkan kepercayaan masyarakat dalam penggunaan layanan *cloud*. Selain itu memungkinkan bagi CSP untuk merubah atau memodifikasi dari topologi atau sistem *cloud* yang ada saat ini melalui proses audit sistem kemanan *cloud*.

Pertimbangan Teknologi/Sosial maks 500 kata: menjelaskan pertimbangan apa saja yang dibuat oleh peneliti terkait dengan aspek teknologi, lingkungan, sosial, dan hukum. Peneliti perlu menjelaskan bahwa teknologi atau solusi teknis yang diusulkan implementatif dan kompetitif, serta apakah saat ini mereka menguasai teknologi dan keahlian teknis yang diperlukan tersebut. Peneliti perlu memaparkan sumber dari teknologi yang dipakai, apakah dari internal atau eksternal, serta HKI dari teknologi-teknologi tersebut. Perlu dijelaskan apakah perlu mengembangkan teknologi baru, atau cukup meggunakan teknologi yang ada, serta kemungkinan untuk membeli teknologi yang sudah ada.

Pertimbangan Teknologi/Sosial:

Aspek Teknologi

Produk aplikasi bisnis logistik yang ditujukan untuk kebutuhan internal dan eksternal perusahaan saat ini yang banyak dimigrasi ke layanan cloud, diantaranya berkaitan dengan aplikasi bisnis logistik diantaranya adalah Human Resource Information System (HRIS), Fuel Cost Control System (FCCS), Warehouse application, Manifest_application-1, Manifest_application-2, Vendor Management System Application, Sales Management Application, Financial Applications, Delivery application, Production Dashboard Collection, Knowledge Management System, Transactional application at the airport dan Simple Inventory. Model Risk Analysis Measurement Model in Migration Applications merupakan model yang dapat secara menyeluruh menilai risiko migrasi aplikasi-aplikasi tersebut. Sehingga model ini merupakan pengembangan yang lebih lengkap dari model risk Teknologi Informasi yang sudah ada.

Aspek Lingkungan

Aspek Lingkungan yang berdampak pada Perusahaan sebagai indikator yang ada dalam model Risk Analysis Measurement Model in Migration Applications berkaitan dengan 17 indikator yang terdiri dari 1) integrity; 2) Availability; 3) Confidentiality; 4) Security policies; 5) Standard and Reference Models; 6) Backup Data; 7) System Malfunctions, 8) Unauthorized Transmission; 9) Service Level Agreement; 10) Financial; 11) Technological; 12) Business Goals; 13) Capabilities; 14) Structures (e.g. governance, roles, and accountabilities); 15) Productivity; 16) User Experience; dan 17) Maintenance Difficulties. Indikator-indikator tersebut melengkapi framework ISACA, model Octave allegro dan standar ISO 31000 yang sudah ada sebelumnya. Sehingga dengan model Risk Analysis Measurement Model in Migration Applications yang dikembangkan, perhitungan risiko lebih relative akurat dengan mengambil dari berbagai persepektif, yaitu Asset Identification, Threat Identificaion dan Determine of Vulnerability

Aspek Sosial

Sistem logistic mengintegrasikan antara sistem pelayanan kepabeanan dengan pelayanan perdagangan (*trade system*) dan pelayanan kepelabuhan (*port system*) yang
digunakan untuk pengurusan ekspor dan impor. Selain itu sudah dilakukan penguatan sistem logistik domestik yang diimplementasikan pada tahun 2015 dengan terbangunnya sistem otomasi dan informasi logistik nasional yang terintegrasi secara elektronik (INALOG) di tahun 2020 sudah terkoneksi dengan jaringan logistik regional ASEAN (Peraturan Presiden Republik Indonesia No. 26 Tahun 2012). Sehingga model dapat menjadi alternatif solusi dalam melakukan penilaian risiko migrasi aplikasi-aplikasi yang digunakan perusahaan logistik ke teknologi cloud.

Aspek Hukum

Sistem logistik domestik harus menerapkan persyaratan yang dijelaskan dalam UU RI No. 11 Tahun 2008 Tentang Informasi Transaksi Elektronik, Pasal 9. Bagi penyelenggara Sistem Elektronik untuk pelayanan publik wajib memiliki rencana keberlangsungan kegiatan untuk menanggulangi gangguan atau bencana sesuai dengan risiko dari dampak yang ditimbulkannya, serta wajib menempatkan pusat data dan pusat pemulihan bencana di wilayah Indonesia untuk kepentingan penegakan hukum, perlindungan, dan penegakan kedaulatan negara terhadap data warga negaranya, ini dijelaskan dalam Peraturan Pemerintah (PP) No. 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Pasal 17. Banyaknya industri logistik yang menerapkan *Cloud Computing* untuk mendukung proses logistik. Oleh karena itu, model ini sangat mendukung dan relevan dengan Peraturan Pemerintah tersebut.

Bukti keterlibatan Mitra
Penelitian Dosen Pemula THUN 2023
“Model Penilaian Risiko Aplikasi Bisnis Logistik pada Cloud Migration”

No	Tanggal	Kegiatan	Catatan
1	12 Juni 2023	Rapat Bersama mitra dalam merumuskan tujuan penelitian dan keterlibatan mitra. Di kantor Poslog Bandung, Jl. Sukabumi Bandung Peserta rapat: Ibu Aisah (Poslog), Bapak Rivo (Poslog), Ibu Maniah (ULBI), Ibu Erna (ULBI), Ibu Dini Hamidin (ULBI) Pembahasan tentang Mapping antara ancaman terhadap aplikasi bisnis logistik yang akan dimigrasikan ke cloud computing. 	Offline
2	27 Juli 20223	Tema rapat: Identifikasi aplikasi bisnis logistik yang akan dimigrasikan ke cloud computing. Peserta rapat: Bapak Wasli (Poslog), Bapak Rivo (Poslog), Ibu Manaih (ULBI), Ibu Erna (ULBI, Ibu Dini Hamidin (ULBI) 	Offline

Bandung, 10 Oktober 2023
Ketua Peneliti,

Dr. Maniah,S.Kom.,M.T

International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 12 (2020) pp. XXX-XXX

Received: XX April 202X; Accepted: XX May, 202X; Published: 2X May, 202X

Risk Analysis Measurement Model in Migration Applications

Maniah[1], Erna Mulyati [2] and Dini Hamidin[3]

[1] Informatics Management, Universitas Logistik dan Bisnis International
Bandung 40151, Indonesia
maniah@ulbi.ac.id

[2] Management Logistics, Universitas Logistik dan Bisnis International
Bandung 40151, Indonesia
ernamulyati@ulbi.ac.id

[3] Transportation Management, Universitas Logistik dan Bisnis International
Bandung 40151, Indonesia
dinihamidin@ulbi.ac.id

***Abstract*: The era of industrial revolution 4.0 is an era marked by the transition of information and communication technology which can create new technology-based investments. Internet of things (IoT), Big Data, and Cloud Computing, are the foundations underlying this industrial revolution 4.0. 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: Model, risk assessment, cloud migration, adoption, security.

I. Introduction

Currently, many logistics companies are implementing cloud computing. Cloud Computing is an innovative technology that can provide data transaction facilities for manufacturing, finance, distribution, sales, customer service activities that can share information and collaborate with trading partners [1]. The reasons why companies migrate to cloud computing include: (1) because cloud computing services have scalability, which means that they can meet the needs of information technology resources according to the company's needs; (2) because the cloud provider has provided settings for both hardware configuration and software updates or server settings and others, so that companies as users of cloud services are more focused on developing better innovative products; (3) because cloud providers have data centers that provide fast and efficient computing services, so this will have an effect on high performance in the cloud compared to data centers owned by companies [2]. Cloud migration can mean the process of deploying part or all of digital assets, services, IT resources, or applications to the cloud [3], but when migrating to the cloud is likely to cause disruption to the company's business [4]. This is as illustrated when there is a cloud outage which can cripple a company's business as a result [5]. 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 [6]. The choice of risk before migration is an important thing for cloud service users to consider [4]. Several previous studies have proposed a risk assessment model to support users in making migration decisions to the cloud [6], and to assess risks to information system security in the cloud context [7]. Based on the results of research [6], [7] 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 research 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 stages, namely identifying risks, determining risk assessment indicators, then calculating the asset weight value so that the risk value is obtained by taking into account the threats and vulnerabilities of the asset. This risk value measurement model will be able to provide preparation for companies in carrying out risk mitigation. In this research, samples were taken from several logistics companies with varying business coverage ranging from small, medium and large scale, but the results of this research can be used by all logistics companies throughout the world.

II. Related Work

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 [6]. 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 [7]. 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 [8]. 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 [9].

III. Risk Analysis Model

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 1.

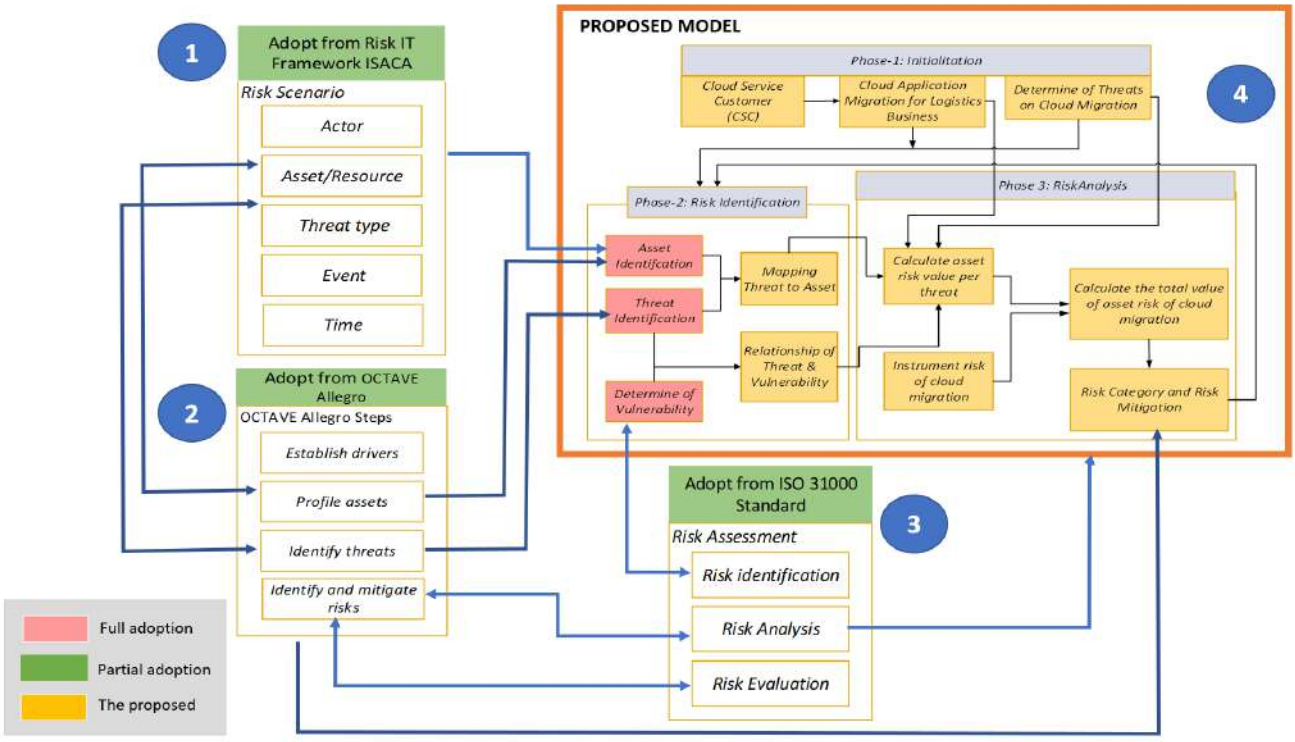


Figure 1. Proposed Model (Researcher)

The stages taken to develop this model can be explained as follows:

1. Adopting the ISACA Risk IT Framework

In this section the researcher adopts the risk scenario contained in the risk evaluation stage, including who is responsible for the company's risks, what types of threats are likely to arise and be detrimental, inappropriate

events or events and processes, assets or resources that are affected of adverse events, as well as the time when the adverse event occurred.

2. Adopting the risk management process part of the ISO 31000 standard

   In this section the researcher adopts the stages of risk assessment, which include: the risk identification stage, the risk analysis stage, and the risk evaluation stage.

3. Adopting the phases of the OCTAVE method

   In part, the researcher adopted the steps contained in the phases of the OCTAVE method, including: the stage of determining the level of risk criteria, determining the asset profile and identifying threats, identifying risks, analyzing risks, and carrying out risk mitigation.

4. Developing the proposed model

   Based on the 3 (three) adoptions of the framework described above, we will then describe in detail the parts that form a more practical risk analysis measurement model that companies can use in calculating the risk value for applications that will be migrated to cloud computing.

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 [10].
3. Determine vulnerabilities that will provide potential threats to cloud migration.

A. 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, as shown in Table 1.

Table 1. List of applications migrated to the cloud.

ID-App	Scope	Application Name
APP-1	Internal	Human Resource Information System
APP-2	Internal	Fuel Cost Control System
APP-3	Internal	Warehouse application
APP-4	Internal	Manifest application 1
APP-5	Internal	Manifest application 2
APP-6	External	Vendor Management System Application
APP-7	External	Sales Management Application
APP-8	Internal	Financial Applications
APP-9	External	Delivery application
APP-10	Internal	Production Dashboard Collection
APP-11	Internal	Knowledge Management System
APP-12	External	Transactional application at the airport
APP-13	Internal	Simple Inventory

The list of applications in Table 1 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 [11], 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) [12].

Referring to research results from [11], 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:

$$r_a = \sum_{1}^{n} p_o v_a \qquad (1)$$

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

Table 2. Result assessment per asset

No.	*ID_App*	***Threats***											
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	***Result Assessment***
Probability of Occurrence		**5%**	**9%**	**17%**	**5%**	**16%**	**14%**	**11%**	**5%**	**2%**	**7%**	**9%**	
1	*AP-1*	80	70	75	75	80	90	80	65	70	80	80	**78.45**
2	*AP-2*	75	80	80	85	70	60	70	80	70	75	85	**74.4**
3	*AP-3*	65	50	35	35	20	45	30	40	30	55	50	**39.2**
4	*AP-4*	70	70	60	25	60	45	35	65	50	50	35	**45.6**
5	*AP-5*	70	60	45	40	45	35	50	55	45	45	50	**47.45**
6	*AP-6*	80	85	80	85	80	75	75	80	80	90	85	**80.6**
7	*AP-7*	80	90	95	80	80	70	75	70	80	85	90	**82.25**
8	*AP-8*	75	60	20	40	80	50	35	30	80	45	45	**48.5**
9	*AP-9*	70	60	65	60	70	75	45	65	70	55	45	**62.15**
10	*AP-10*	55	45	25	55	70	50	20	40	70	60	40	**45.4**
11	*AP-11*	50	50	35	45	45	35	25	40	50	45	45	**40.25**
12	*AP-12*	60	70	55	55	65	65	60	70	60	65	60	**62.15**
13	*AP-13*	30	50	45	35	65	35	50	40	65	45	50	**47.15**

Remarks: This value is filled in based on the assumption that a threat will occur in the application

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. For this reason, it is necessary to identify vulnerabilities that are likely to become potential threats as shown in Table 3.

Table 3. List of vulnerabilities in cloud computing [7]

Vul_ID	Vulnerability_name	Level
V-1	Insecure Interfaces and APIs	7
V-2	Unlimited Allocation of Resources	4
V-3	Data Related Vulnerabilities	7
V-4	Virtual Machines Vulnerabilities	7
V-5	Virtual Machine Images Vul.	7
V-6	Hypervisor Vulnerabilities	5
V-7	Vulnerabilities in Virtual Networks	7
V-8	AAA Vulnerabilities	3
V-9	Inappropriate encryption of data in rest and in transit.	3
V-10	Impossibility of processing of encrypted data while in transit.	4
V-11	Possibility that internal network probing will occur (cloud).	5
V-12	Application vulnerabilities or poor patch management.	4
V-13	Service Level Agreement thrashing in multi-vendor environment	4
V-14	Service Level Agreement clauses containing exclusive business risk.	7
V-15	Audit not available to customers.	4
V-16	Session Riding and Hijacking	8
V-17	Reliability and Availability of Service	3
V-18	Insure Cryptography	5
V-19	Data Protection and Portability	5
V-20	Virtual Machine Escape	8
V-21	CSP lock-in	4
V-22	Internet Dependency	8
V-23	Malicious Insider Threats	7
V-24	Unclear Roles and Responsibilities	7
V-25	Poor Provider Selection	5
V-26	System or Operating system Vulnerabilities	5
V-27	Lack of Security Awareness	7
V-28	Mal-configuration	5
V-29	Malicious Users	8

The list of vulnerabilities and levels of vulnerability in Table 2 above was obtained 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 [7]. 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, as shown in the level of vulnerabilities column.

B. Risk Assessment Indicators

The risk assessment indicators used in this research are adopted from several indicators contained in existing risk management models or frameworks [13]–[15], and added with indicators from the results of previous studies [6], [7].

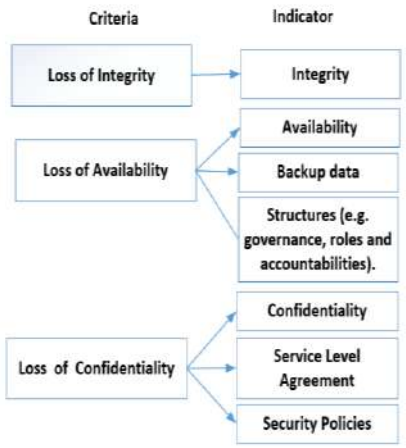


Figure 2. IT Risk Management Framework v.1[16]

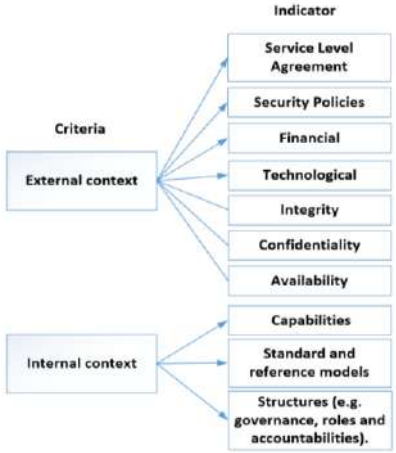


Figure 3. ISO/IEC Guide 73 [14]

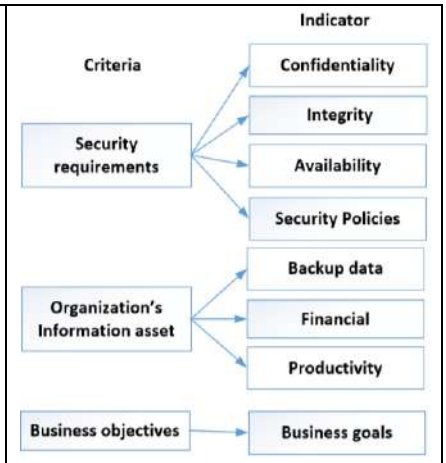


Figure 4. OCTAVE Allegro v1.0 [15]

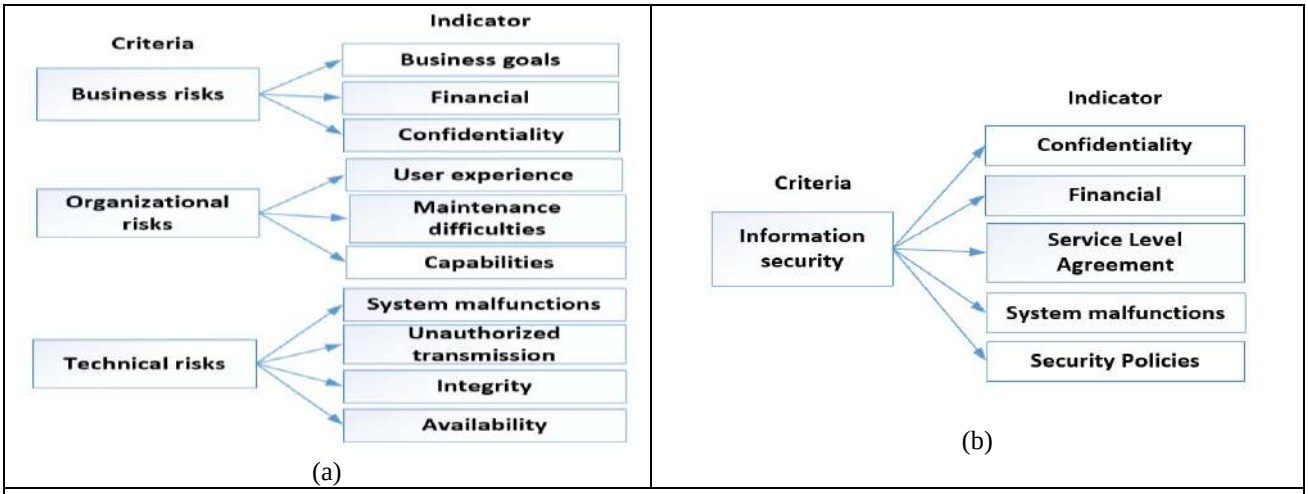


Figure 5. Criteria and indicator of risk assessment (a) [6], (b) [7]

C. 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).

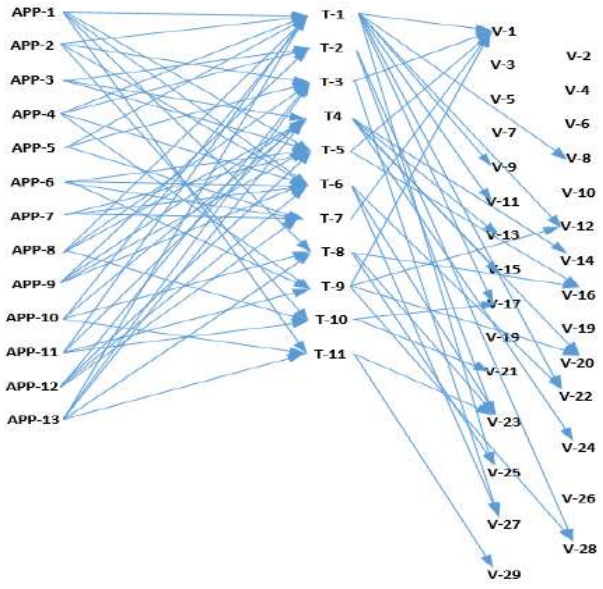


Figure 6. Mapping Assets to Threats, and Threats to Vulnerabilities

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, based on Figure 6 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. The vulnerability value of each threat can be shown in detail in table 4.

Table 4. Vulnerability value

ID Threat	Vulnerability value
T-1	4,8
T-2	6,0
T-3	7,0
T-4	6,0
T-5	7,5
T-6	7,3
T-7	7,0
T-8	6,7
T-9	6,0
T-10	3,5
T-11	7,5

D. Calculating Risk Value

Based on the result assessment value in table 2, vulnerability value in table 4, 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.

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

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

Secara lengkap hasil perhitungan risiko per asset yang dimigrasikan ke cloud computing dapat ditunjukkan pada tabel 5.

Table 5. Risk analysis value in cloud migration

ID_App	R_a	V	Indicators																	
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	Risk Value (R)
Criteria Weigh (1-100)			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**

Remarks:

High-risk Medium-risk

E. Risk Category and Risk Mitigation

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 [17]. The results of the risk analysis value in table 5 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 5.

Table 5. Risk mitigation approach

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

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.

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.

Acknowledgment

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 2023 Research and Community Service Grant program. The author would like to express his deepest gratitude for the grant this research. The author also would like to thank the University of Logistics and International Business as the institutional institution the author is currently working at, for the support provided to the author.

References

[1] E. Doherty, M. Carcary, and G. Conway, “Risk Management Considerations in Cloud Computing Adoption,” 2012.

[2] S. U. Khan and N. Ullah, “Challenges in the adoption of hybrid cloud: an exploratory study using systematic literature review,” *J. Eng.*, vol. 2016, no. 5, pp. 107–118, 2016, doi: 10.1049/joe.2016.0089.

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

[4] 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.

[5] 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.

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

[7] 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.

[8] H. Abrar *et al.*, “Risk Analysis of Cloud Sourcing in Healthcare and Public Health Industry,” *IEEE Access*, vol. 6, pp. 19140–19150, 2018, doi: 10.1109/ACCESS.2018.2805919.

[9] R. Maeser, “Analyzing CSP Trustworthiness and Predicting Cloud Service Performance,” *EEE Open J. Comput. Soc.*, vol. 1, pp. 1–12, 2020, doi: 10.1109/OJCS.2020.2994095.

[10] 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: http://www.sei.cmu.edu/publications/pubweb.html

[11] Maniah, B. Soewito, F. L. Gaol, and E. Abdurachman, "Risk Assessment for Logistics Applications in Cloud Migration," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 16, no. 3, p. 325, 2022, doi: 10.22146/ijccs.74567.

[12] E. Adam, "Cloud Security Alliance Egregious 11," *Альманах Современной Науки И Образования*, vol. 10, no. 77. Security Innovation, Canada, pp. 1–6, 2022. [Online]. Available: https://blog.securityinnovation.com/cloud-security-alliance-egregious-11

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

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

[15] S. Musungwini and G. Mahlangu, "Framework for Threat Modelling for a Power Utility : Case of Zimbabwe Power Utility Company," *Internastional J. Comput. Sci. Bus. Informatics*, vol. 16, no. 1, pp. 8–23, 2016, [Online]. Available: https://www.semanticscholar.org/paper/Framework-for-threat-modelling-for-a-power-utility%3A-Musungwini-Mahlangu/52f98d207a6f4b02aff2e49e5daa51b7f8f9334b

[16] E.oman, "IT Risk Management Framework," 2017. [Online]. Available: https://www.moheri.gov.om/userupload/Policy/IT Risk Management Framework.pdf

[17] T. J. Betcher, "Cloud Computing: Key IT-Related Risks and Mitigation Strategies for Consideration by IT Security Practitioners," Eugene, Oregon, Amerika Serikat, 2010. [Online]. Available: http://hdl.handle.net/1794/10207

Author Biographies

Maniah contributed to the creation of the background and developed the risk analysis model based on a review of the state-of-the-art of previous research. Apart from that, Maniah also initiated the manuscript of this journal.

Erna Mulyati Supports the preparation of risk analysis models in determining logistics applications and possible threats to logistics applications.

Dini Hamidin Contribute to the feasibility study section on risk analysis for logistics applications that will be migrated to cloud computing.

International Journal of Computer Information Systems and Industrial Management Applications

Submission

Thank you for your submission. Your submission ID number is 981. Please write this number down and include it in any communications with us.

Below is the information submitted. We have also emailed a copy to the submission contact. If you notice any problems or do *not* receive the email within 24 hours, please contact us.

Submission ID: 981

Title: Risk Analysis Measurement Model in Migration Applications

Author 1:
First Name: Maniah
Last Name: maniah
Organization: Universitas Logistik dan Bisnis International
Country: Indonesia
Email: maniah@ulbi.ac.id

Author 2:
First Name: Erna
Last Name: Mulyati
Organization: Universitas Logistik dan Bisnis International
Country: Indonesia
Email: ernamulyati@ulbi.ac.id

Author 3:
First Name: Dini
Last Name: Hamidin
Organization: Universitas Logistik dan Bisnis International
Country: Indonesia
Email: dinihamidin@ulbi.ac.id

Contact Author: Author 1

Alternate Contact: maniah@poltekpos.ac.id

Topic(s): default

Keywords: Model, risk assessment, cloud migration, adoption, security.

Abstract: The era of industrial revolution 4.0 is an era marked by the transition of information and communication technology which can create new technology-based investments. Internet of things (IoT), Big Data, and Cloud Computing, are the foundations underlying this industrial revolution 4.0. 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.

Comments:

Hibah Dosen Pemula

Model Penilaian Risiko Aplikasi Bisnis Logistik pada Cloud Migration

- Ketua Peneliti: Dr. Maniah, S.Kom., MT.
- Anggota : Dini Hamidin, S.Si., MBA., MT.
- Dr. Erna Mulyati, ST., MT.

Universitas Logistik dan Bisnis Internasional
Bandung 2023

Latar Belakang

Banyak keuntungan yang didapat perusahaan ketika migrasi ke *cloud*, namun tidak sedikit juga kelemahan yang didapat, bahkan kemungkinan akan menimbulkan gangguan atau risiko pada bisnis perusahaan (Ahmad et al. 2018)

Pengukuran risiko sebelum migrasi ketika perusahaan akan memutuskan untuk migrasi ke *cloud* (Islam et al. 2017; Kozlov and Noga 2018)

Tujuan Penelitian

Tujuan penelitian ini adalah membuat model untuk penilaian risiko terhadap aplikasi bisnis logistik pada cloud migration.

Model/Framework IT Risk Management \ Indicator	Integrity	Availability	Service Level Agreement	Technological	Capabilities	Standard and reference models	Confidentiality	Structures (e.g. governance, roles and accountabilities)	Security Policies	Backup data	Productivity	Business goals	Financial	User experience	Maintenance difficulties	System malfunctions	Unauthorized transmission
IT Risk Management Framework v.1 Governance and Standards Division, 2017	√	√	√				√	√		√							
ISO/IEC Guide 73, 2008	√	√	√	√	√	√	√	√	√				√				
OCTAVE Method, 2007	√	√					√		√	√	√	√	√				
Kozlov&Noga, 2018			√				√		√				√			√	
Islam et al. 2017	√	√			√		√					√	√	√	√	√	√
Penelitian yang Diusulkan	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√

Kebaruan Penelitian

Terdapat 17 indikator dalam Model Pengukuran Nilai Risiko yang dikembangkan

Metodologi Penelitian

Pendekatan Metode Penelitian

Pendekatan metode penelitian yang digunakan dalam penelitian ini adalah campuran antara pendekatan kualitatif dan pendekatan semi kuantitatif

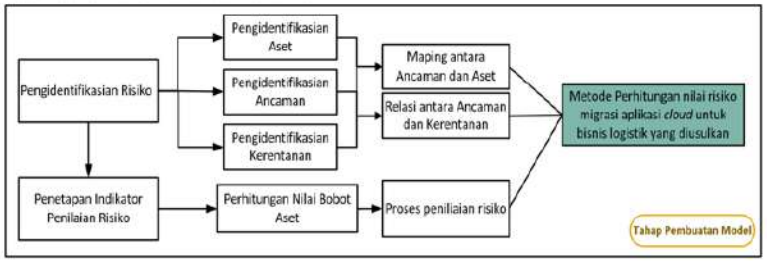
Sample Penelitian

1. Termasuk dalam bisnis jasa logistik.
2. Sebagai pengguna layanan cloud computing.

Metode Pengumpulan data

1. Angket atau kuesioner dan interview
2. Focus Group Discussion (FGD).

Tahap Pelaksanaan Penelitian



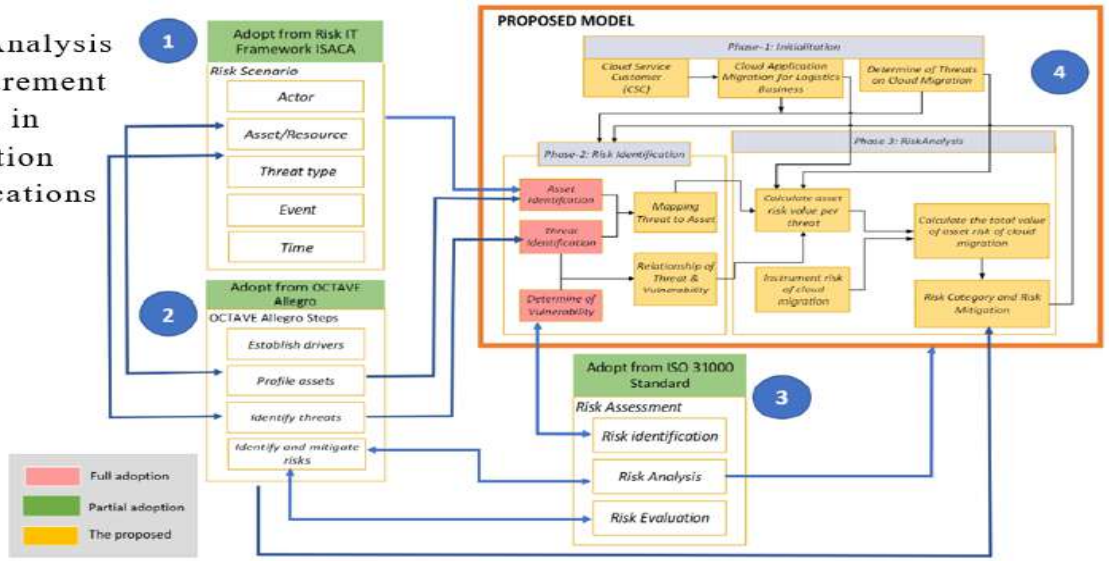
Hasil Penelitian (1)

- Risk Analysis Value in cloud Migration

ID_App	R_s	V	Indicators																Risk Value (R)
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	
Criteria Weigh (1-100)			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

Remarks:
High-risk Medium-risk

- Risk Analysis Measurement Model in Migration Applications



Hasil Penelitian (2)

Luaran Penelitian

Publikasi di Jurnal International **Journal of Computer Information Systems and Industrial Management Applications** terindeks Scopus Q3 di (**Submitted**)

International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 12 (2020) pp. XXX-XXX
© MIR Labs, www.mirlabs.net/ijcisim/index.html

Received: XX April 202X; Accepted: XX May, 202X; Published: 2X May, 202X

Risk Analysis Measurement Model in Migration Applications

Maniah[1], Erna Mulyati [2] and Dini Hamidin[3]

[1] Informatics Management, Universitas Logistik dan Bisnis International
Bandung 40151, Indonesia
maniah@ulbi.ac.id

[2] Management Logistics, Universitas Logistik dan Bisnis International
Bandung 40151, Indonesia
ernamulyati@ulbi.ac.id

[3] Transportation Management, Universitas Logistik dan Bisnis International
Bandung 40151, Indonesia
dinihamidin@ulbi.ac.id

Abstract: **The era of industrial revolution 4.0 is an era marked by the transition of information and communication technology which can create new technology-based investments. Internet of things (IoT), Big Data, and Cloud Computing, are the foundations underlying this industrial revolution 4.0. 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**

with trading partners [1]. The reasons why companies migrate to cloud computing include: (1) because cloud computing services have scalability, which means that they can meet the needs of information technology resources according to the company's needs; (2) because the cloud provider has provided settings for both hardware configuration and software updates or server settings and others, so that companies as users of cloud services are more focused on developing better innovative products; (3) because cloud providers have data centers that provide fast and efficient computing services, so this will have an effect on high performance in the cloud compared to data centers owned by companies [2]. Cloud migration can mean the process of deploying part or all of digital assets, services, IT resources, or applications to the cloud [3], but when migrating to the cloud is likely to cause disruption to the

Kesimpulan

Dengan model yang diusulkan ini pengguna layanan *cloud* akan diberikan langkah-langkah yang lebih mudah dan terstruktur dalam melakukan penilaian risiko mulai dari pengukuran bobot aset, memetakan hubungan antara aset dengan ancaman lalu menghitung nilai kerentanan pada masing-masing ancaman sampai akhirnya dapat mengetahui tingkat risiko pada aplikasi yang akan dimigrasikan ke *cloud*.

Saran dan Rekomendasi

Dikarenakan penilaian risiko dalam konteks *cloud* ini sangat penting, maka sangat diperlukan keseriusan serta fokus perusahaan pengguna layanan *cloud* dalam menangani risiko, misalnya menetapkan bidang khusus secara permanen yang menangani risiko pada *cloud migration*.

Foto kunjungan ke Poslog Indonesia

Foto FGD secara Offline

Foto FGD secara Online

TERIMA KASIH

SURAT PERNYATAAN TANGGUNG JAWAB BELANJA

Yang bertanda tangan di bawah ini :

Nama : Dr MANIAH S.Kom, M.T

Alamat : Komplek Griya Cihanjuang Blok A/10

berdasarkan Surat Keputusan Nomor 180/E5/PG.02.00.PL/2023 dan Perjanjian / Kontrak Nomor 002/SP2H/PTV/RT-MONO/LL4/2023 mendapatkan Anggaran Penelitian Model Penilaian Risiko Aplikasi Bisnis Logistik pada Cloud Migration Sebesar 10,948,000

Dengan ini menyatakan bahwa :

1. Biaya kegiatan Penelitian di bawah ini meliputi :

No	Uraian	Jumlah
01	**Bahan** Kertas untuk mendukung administrasi riset	48,000
02	**Pengumpulan Data** Biaya konsumsi untuk persiapan FGD Transport lokal HR Pembantu penelitian, HR Sekretariat/Administrasi penelitian, Konsumsi snak untuk FGD sebanyak 15 orang, 2x, Honor Narasumber FGD 1 orang 1 jam, 2 x	3,800,000
03	**Analisis Data(Termasuk Sewa Peralatan** HR Pembantu penelitian /perekayasa pertama (Analisis Data)	600,000
04	**Pelaporan, Luaran Wajib dan Luaran Tambahan** Biaya Submit ke Journal Q3	6,500,000
05	**Lain-lain** -	0
	Jumlah	10,948,000

2. Jumlah uang tersebut pada angka 1, benar-benar dikeluarkan untuk pelaksanaan kegiatan Penelitian dimaksud.

Demikian surat pernyataan ini dibuat dengan sebenarnya.

, 18-12-2023

Ketua,

(Dr MANIAH S.Kom, M.T)

NIP/NIK 3217026707670009

Lesty Copy Centre

Jl. Purwakarta No.154 Antapani Telp. : 0811 2266 663

Kepada Yth

ULBI

NOTA

PHOTO COPY * JILID SKRIPSI * JILID SPIRAL * LAMINASI * ATK * DLL

Banyak	Jenis Jasa	Harga Satuan	Jumlah
1	A4/F4/B5	40.000	40.000
	A3/B4		
	Perkecil/Perbesar		
	Laminating		
	Jilid Hard Cover		
	Jilid Soft Cover		
	Jilid Ring/Kawat/Plastik		
	Jilid Biasa		
	Jilid Langsung		
1x	Print		8000

PERHATIAN
Pesanan yang tidak diambil dalam tempo 2 bulan hilang atau tertukar kami tidak bertanggung jawab
TANPA BON INI KAMI TIDAK BISA MENYERAHKAN PESANAN ANDA

Total	48.000
U. Muka	
Sisa	—

Ket. Pesanan

Banyak Judul ..... Naskah/Book

1 _____

2 _____

3 _____

4 _____

Selesai Tgl .....

Yang Menerima Order

1/6-2023

Terima Kasih

COOKies

jl. cikutra baru v no. 3
bandung 40124
phone. 7274759
08122180675

souvenir for wedding,
party, gift, delivery
and more .....

No. : .....

Nama : Marah
Alamat : .....
.....
Telp. : .....
Hp : .....

ORDER	TANGGAL	JAM
TERIMA	9 Juni 2023	
SELESAI		
Diambil / Dikirim		

No.	ITEM	Jumlah	Harga Satuan	Jumlah (Rp.)
	dus	6		120.000
				2

- Pesanan > 300 minimal 1 minggu sebelumnya
- Uang muka minimal 50%, jika dibatalkan uang muka tidak kembali.
- Pesanan yang tidak diambil 3 hari dari waktu "selesai" dapat dialihkan.

Jumlah	120.000
Uang Muka	
Sisa	

Pemesan

( )

Hormat kami,

( )

TGL : 25/7-203 NO. 208766

CLEMMONS 3

PORSI	I T E M	PRICE	SUB TOTAL
1	P.C	F	21000
3	P.C	E	69500

TABLE NUMBER : 31

Total Rp. 79.500

KUITANSI

BUKTI PEMBAYARAN HONORARIUM

No Kuitansi: 1123003

Sudah Terima dari	Dr. Maniah
Banyaknya Uang	Tiga Ratus Ribu Rupiah
Untuk Pembayaran	Honorarium Pembantu penelitian

300.000

Jumlah Kotor	300.000
Pajak PPh 2.5%	7.500
Jumlah yang diterimakan	292.500

Bandung, 20 November 202

Yang Menerima,

Alif Rahmanudin

KUITANSI

BUKTI PEMBAYARAN HONORARIUM

No Kuitansi: 1123001

Sudah Terima dari	Dr. Maniah
Banyaknya Uang	Sembilan Ratus Ribu Rupiah
Untuk Pembayaran	Honorarium Sekretariat/Administrasi penelitian

900.000

Jumlah Kotor	900.000
Pajak PPh 2.5%	22.500
Jumlah yang diterimakan	877.500

Bandung, 20 November 202

Yang Menerima,

Hesti Sugesti, SPd. MM.

12 Juni 2023

Tuan
Toko

NOTA No.

BANYAKNYA	NAMA BARANG	HARGA	JUMLAH
15	paket ayam		300.000

Jumlah Rp. 300.000

Tanda Terima

Hormat kami,

27 Juli 2023

Tuan .....
Toko

Nota No. .....

Banyaknya	Nama Barang	Harga	Jumlah
15	Ayam Bakar		300 000

Yang terima.

JUMLAH Rp. 300 000

Hormat kami.

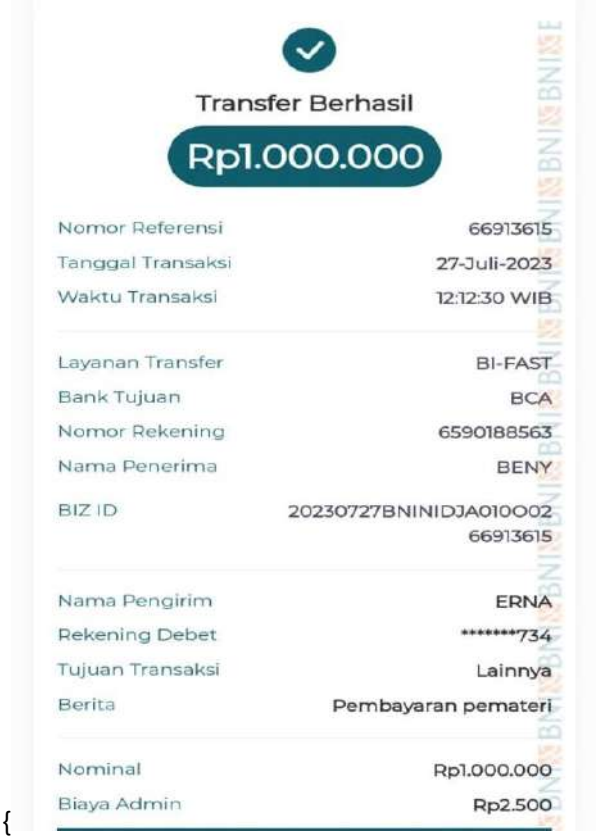
RM PAWON SUNDA
Jl.Surya Sumantri 111 Bandung
Tlp. 0821 2000 7560

Bukti honorarium narasumber FGD Penelitian Model Penilaian Risiko Aplikasi Bisnis Logistik pada Cloud Migration:

Pelaksanaan secara Online, pada tanggal 27 Juli 2023

Nara sumber: Bapak Beny

Besar honor: Rp. 1000.000,-



{

KUITANSI

BUKTI PEMBAYARAN HONORARIUM

No Kuitansi: 0623001

Sudah Terima dari	Dr. Maniah
Banyaknya Uang	Delapan Ratus Ribu Rupiah
Untuk Pembayaran	Honorarium Narasumber FGD Penelitian Model Penilaian Risiko Aplikasi Bisnis Logistik pada Cloud Migration

800.000

Jumlah Kotor	800.000
Pajak PPh 2,5%	20.000
Jumlah yang diterimakan	780.000

Bandung, 12 Juni 2023

Yang Menerima,

Lia Sukmayanti, ST.

KUITANSI

BUKTI PEMBAYARAN HONORARIUM

No Kuitansi: 1123004

Sudah Terima dari	Dr. Maniah
Banyaknya Uang	Enam Ratus Ribu Rupiah
Untuk Pembayaran	Honorarium Perekayasa Pertama

600.000

Jumlah Kotor	600.000
Pajak PPh 2.5%	15.000
Jumlah yang diterimakan	585.000

Bandung, 20 November 202

Yang Menerima,

Yogi Permadi Maksudi

NOAH OFFSET DIGITAL PRINTING

Jl. Pagarsih No. 51 0813 1217 1838
Email : noahpagarsih51@gmail.com

INVOICE

Pelangan : ULBI
Alamat : Sariasih 54
No. Tlp / Hp :

Tanggal: 20 Nop 2023

Qty	Produk	Harga	Jumlah
3	Cetak laporan penelitian	500.000	1.500.000

Terbilang :	**Total**	1.500.000
Satu juta lima ratus ribu rupiah	**DP**	-
	Sisa	1.500.000

LUNAS

NOAH OUTDOOR & INDOOR PRINTING

Hormat Kami,

No. _____

Telah terima dari Manian (ULBI)

Uang sejumlah Satu Juta Lima Ratus Ribu Rupiah

Untuk pembayaran Cetak Laporan Penelitian

Bandung, 20 November 2023

Rp. 1.500.000

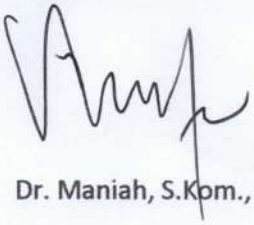
METERAI TEMPEL
10000
BD852AKX778086822

KUITANSI

SUDAH TERIMA DARI	:	ULBI
JUMLAH UANG	:	Rp5,000,000
TERBILANG	:	*Lima Juta Rupiah*
UNTUK PEMBAYARAN	:	Biaya Publish Jurnal Internasional

keterangan pembayaran	:	Biaya Publish Jurnal Internasional	Rp5,000,000
		Jumlah	**Rp5,000,000**

Bandung, 20 November 2023
Ketua Tim Peneliti,



Dr. Maniah, S.Kom., M.T.