

**ANALISIS MANAJEMEN RISIKO APLIKASI SRIKANDI
PADA KANTOR DISKOMINFO KOTA MANADO
MENGUNAKAN ISO 31000**

Harvie Cartens Samuel Suawa¹, Hanna Prillysca Chernovita²

^{1,2}Program Studi Sistem Informasi Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana

e-mail: ¹682017099@student.uksw.edu, ²hanna.chernovita@uksw.edu

ABSTRAK

Penelitian ini bertujuan untuk mengetahui hasil analisis manajemen resiko dengan menggunakan metode ISO 31000 pada aplikasi SRIKANDI dengan harapan dapat meminimalisir tingkat resiko pada penggunaan aplikasi SRIKANDI di Dinas Kominfo Pemerintah Kota Manado. Aplikasi SRIKANDI yaitu aplikasi yang digunakan untuk mempermudah kearsipan yang dapat mendukung pengelolaan arsip dan tata kelolah pemerintah berbasis elektronik. Beberapa tahapan yang sudah dilakukan antara lain tahap pengumpulan data, identifikasi resiko, analisis resiko, evaluasi resiko, dan perlakuan resiko. Berdasarkan hasil analisis yang dilakukan, hasil penelitian menunjukkan bahwa terdapat 23 kemungkinan resiko yang bisa saja terjadi dimana memiliki 13 kemungkinan resiko yang tinggi (High), 5 kemungkinan yang sedang (Medium), dan 5 kemungkinan resiko yang rendah (Low).

Abstract

This study aims to determine the results of risk management analysis using the ISO 31000 method in the SRIKANDI application in the hope of minimizing the level of risk in using the SRIKANDI application at the Manado City Government Communication and Information Office. The SRIKANDI application is an application used to facilitate archives that can support electronic-based archive management and government governance. Some of the stages that have been carried out include the stages of data collection, risk identification, risk analysis, risk evaluation, and risk treatment. Based on the results of the analysis conducted, the results showed that there are 23 possible risks that could occur which have 13 high-risk possibilities (High), 5 medium possibilities (Medium), and 5 low-risk possibilities (Low).

Kata kunci: Resiko, Manajemen Resiko, ISO 31000.

PENDAHULUAN

Pada era perkembangan teknologi informasi yang pesat semua aspek kehidupan tidak dapat dipisahkan dari teknologi, salah satunya Kantor Diskominfo Kota Manado yang saat ini menggunakan perkembangan teknologi informasi untuk mempermudah

dan membantu karyawan mencatat dan melaporkan lintas batas melalui sistem aplikasi yang komprehensif yang saat ini dikenal dengan aplikasi SRIKANDI.

Aplikasi SRIKANDI merupakan aplikasi umum pada bidang kearsipan baik itu pada Sistem Pemerintahan Berbasis Elektronik (SPBE), yang digunakan juga di Kantor Diskominfo Kota Manado untuk mempermudah perihal bagian kearsipan dalam pembuatan naskah dan prosedur pengiriman keluar, serta menerima dan menjadwalkan naskah yang diterima sehingga dapat mendisposisikannya. Selain itu memproses penandatanganan draft dan penomoran naskah sebelum proses pengiriman, memproses pengklasifikasian naskah yang diterima serta naskah yang keluar akan diarsipkan sesuai dengan ketentuan yang berlaku.

Namun demikian, setiap aplikasi memiliki potensi resiko yang merugikan seperti peretasan atau kejahatan dunia maya (Irawati dkk, 2021), sehingga perlu dilakukan analisis manajemen resiko aplikasi SRIKANDI secara berkala untuk meminimalisir dampak dan kesalahan yang mungkin akan terjadi di kemudian hari, baik itu secara internal maupun eksternal yang membuat setiap proses dalam aplikasi tersebut terhenti atau pun memiliki masalah seperti kurangnya kinerja dan tidak dapat berjalan secara maksimal.

Berdasarkan dari permasalahan tersebut, maka perlunya dilakukan penelitian dan dikaji resiko-resiko yang dapat muncul pada aplikasi SRIKANDI. Untuk dapat menghindari setiap kemungkinan terjadinya resiko maka dilakukanlah analisis manajemen resiko menggunakan ISO 31000 tujuannya adalah untuk mengetahui kemungkinan kelemahan dan kemungkinan resiko dalam aplikasi di masa mendatang, serta mengemukakan pendapat dan saran untuk menghindari resiko tersebut.

Penelitian Analisis Manajemen Resiko Menggunakan ISO 31000 pernah dilakukan oleh Miftakhatun (2020) pada *Website Ecofo* yang dikelola oleh KPH Benyumas Timur. Dari hasil analisis resiko yang telah dilakukan oleh Miftakhatun pada *Website Ecofo* Terdapat 24 kemungkinan resiko, dengan 3 resiko level tinggi (kegagalan sistem jaringan, jaringan terputus, *overload database*, *server down*), 10 resiko level *medium* (gempa bumi, kebakaran, listrik padam, penyalahgunaan akses, */user ID*, pegawai IT yang tidak mengikuti SOP secara keseluruhan, kerusakan *software*, kerusakan *hardware*, gagal dalam melakukan fungsi penyimpanan seperti *disk error*, *disk full*, *data corrupt*, *overheat* perangkat), dan 11 resiko level *low* (banjir, debu atau kotoran, *human error*, pencurian perangkat, data dan informasi tidak sesuai, *cybercrime*, kesalahan teknis, pengunduran diri, pegawai yang sakit atau cedera/meninggal, serangan virus, *malware*, *malicious program*).

Penelitian oleh Ramadhan dkk (2020) pada *Smart Canteen* SMA XYZ yang berfungsi untuk dapat membantu kinerja dan proses bisnis yang ada kantin tersebut. Dan dari hasil terdapat 19 resiko yang dapat terjadi. 1 resiko ekstrim, 2 resiko tinggi, 4 resiko sedang, dan 5 resiko rendah.

Penelitian oleh Rambli dan Sitikodna (2022), pada aplikasi *Rene Cashier* yang berfungsi untuk mempermudah karyawan dan staf pada Restoran Oemah Djari Salatiga dan terdapat 13 kemungkinan resiko (Kebakaran, banjir, gempa bumi, UI desain susah dipahami, kerusakan *hardware*, petir, *human error*, *hacking*, penyalahgunaan jabatan atau hak akses, pencurian data atau perangkat keras, *server down*, *data corrupt*, dan listrik

padam secara tiba-tiba.) yang dapat menjadi gangguan dalam kinerja kerja pada Restoran Oemah Djari Salatiga.

KAJIAN TEORI

Resiko

Resiko menurut Idroes (dalam Atmojo & Manuputty, 2020) merupakan suatu ancaman atau kemungkinan dari suatu tindakan yang bisa memicu dampak yang merugikan atau bertolak belakang dengan tujuan yang ingin dicapai.

Manajemen Resiko

Manajemen resiko dapat diartikan juga sebagai kegiatan praktis yang berhubungan dengan identifikasi, penilaian, pengontrolan dan meminimalisir resiko (Hidayat, 2013). Manajemen resiko sangat diperlukan dalam suatu perusahaan atau organisasi karena dibutuhkan sebagai standar atau pedoman yang bisa membantu dalam meminimalisir resiko yang mungkin terjadi (Munawwaroh, 2017; Rilyani dkk, 2015; Utamajaya dkk, 2021).

Analisis Manajemen Resiko ISO 31000

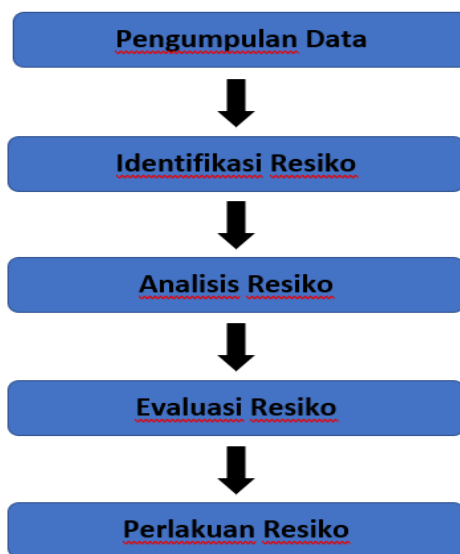
Salah satu penilaian yang dilakukan dalam analisis manajemen resiko yaitu berpedoman pada ISO 31000 yang diciptakan oleh *International Organization for Standardization*. Proses Manajemen Resiko ISO 31000:2009 Menurut Qintharah (2019) yakni yang pertama, pembuatan konteks. menetapkan tujuan, strategi, ruang lingkup, dan faktor lain yang berkaitan dengan proses pengelolaan resiko perusahaan. Proses kedua adalah menemukan resiko atau mengidentifikasi resiko. mengetahui di mana, kapan, mengapa, dan bagaimana sebuah kejadian dapat menghalangi, menurunkan, menunda, atau meningkatkan pencapaian tujuan. Proses ketiga yaitu menganalisis resiko di mana kontrol yang ada diidentifikasi dan dievaluasi. Ini menentukan akibat, kemungkinan, dan tingkat resiko yang mungkin terjadi. Proses keempat dalam manajemen resiko yaitu melakukan evaluasi resiko ini dilakukan dengan membandingkan perkiraan tingkat resiko dengan standar yang telah ditetapkan dan mempertimbangkan keuntungan dan risiko yang mungkin terjadi. Proses kelima yaitu melakukan pengendalian resiko di mana pengendalian resiko dilakukan dengan membuat dan menerapkan strategi dan rencana tindakan biaya efektif untuk meningkatkan potensi manfaat dan mengurangi biaya.

METODE PENELITIAN

Metode yang digunakan pada penelitian ini menggunakan penelitian kualitatif. Penelitian kualitatif merupakan penelitian yang bersifat deskriptif dan sering menggunakan analisis (Wahidmurni, 2017). Dalam penelitian kualitatif, proses dan makna lebih diutamakan (Ratnaningtyas dkk, 2023; Pusung dkk, 2021). Landasan teori dimanfaatkan sebagai pemandu agar fokus pada penelitian sesuai fakta yang ada di lapangan. Metode kualitatif bersifat dinamis yang mana artinya selalu terbuka untuk

adanya perubahan, penambahan, dan penggantian selama proses analisisnya. Metode kualitatif lebih menekankan pada pengamatan fenomena dan lebih meneliti pada substansi makna dari fenomena tersebut.

Metode penelitian kualitatif menjawab masalah penelitian dengan data berupa narasi yang diperoleh melalui pengamatan, pengalihan dokumen, dan wawancara (Priadana dan Sunarsi, 2021; Sandre dkk, 2021). Sangat penting untuk memahami konsep-konsep tersebut agar dapat menjelaskan dengan baik metode dan jenis penelitian, serta kehadiran dan lokasi peneliti, sumber data, metode pengumpulan data, analisis data, dan pengujian validitas hasil penelitian dalam proposal dan laporan. Adapun tahapan penelitian yang dilakukan pada penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. Metode Penelitian

1. **Pengumpulan Data**
Pada tahap ini untuk mengumpulkan data peneliti melakukan wawancara atau pun membagikan kuesioner, kepada pegawai Diskominfo yang telah menggunakan aplikasi SRIKANDI. Hasil dari wawancara dan kuesioner ini yang akan digunakan untuk menganalisis masalah serta resiko yang ada agar dapat meminimalisir dampak dan resiko yang bisa terjadi
2. **Identifikasi Resiko**
Setelah mengumpulkan data, peneliti melakukan identifikasi resiko yaitu mengidentifikasi kejadian maupun kondisi yang mungkin saja terjadi dan dapat menimbulkan suatu resiko ataupun dampak kerugian kedepannya sehingga dapat mengambil tindakan pencegahan untuk mengurangi tingkat resiko.
3. **Analisis Resiko**
Setelah melakukan identifikasi resiko, langkah selanjutnya adalah menganalisis resiko yang sudah ada dan mengidentifikasi dampak dari resiko yang sesuai, sehingga dapat

melakukan pengidentifikasian resiko yang mungkin terjadi serta cara penanganan yang sesuai.

4. Evaluasi Resiko

Pada tahap ini peneliti akan melakukan evaluasi resiko yang telah diidentifikasi untuk menentukan tingkatan dari setiap resiko yang sudah ada untuk menentukan langkah-langkah yang dapat diambil untuk meminimalkan dampak dan melakukan tindakan pencegahan pada resiko yang mungkin saja terjadi.

5. Perlakuan Resiko

Pada tahap ini peneliti melakukan perlakuan atau memberikan usulan pada tiap kemungkinan resiko dan dampak yang dapat terjadi dengan maksud meminimalisir dan mencegah tingkatan terjadinya kemungkinan resiko dan dampak yang tidak diinginkan.

Alat dan Bahan

Komponen yang diperlukan dalam memperoleh informasi resiko serta data dalam perancangan serta penerapan pada analisis manajemen resiko yang terdiri dari Perangkat Lunak (*Software*) dan Perangkat Keras (*Hardware*).

Hardware

1. *Processor*: Intel(R) Core(TM) i5-8250U CPU @ 1.60GHz 1.80 GHz

2. *Memory*: 12.0 GB RAM

Software

1. *Operating System Windows 10*

2. *Microsoft Word 2016*

3. *Microsoft Excel 2016*

4. *Google Chrome (Web Browser)*

HASIL PENELITIAN DAN PEMBAHASAN

Identifikasi Resiko

Pada tahap ini bertujuan untuk mendeskripsikan kemungkinan – kemungkinan resiko yang didapatkan dari hasil wawancara atau pun pada kuesioner yang sudah dibagikan kepada narasumber yang berkaitan untuk memperoleh informasi kemungkinan resiko yang bisa dapat terjadi. Kemungkinan resiko yang dapat terjadi dapat dilihat pada Tabel 1.

Tabel 1. Kemungkinan Resiko

No	Kemungkinan Resiko
1	Gempa bumi
2	Kebakaran
3	Banjir
4	Petir
5	Penyalahgunaan Hak Akses
6	<i>Human Error</i>
7	<i>Hacking</i>

No	Kemungkinan Resiko
8	Pencurian Data atau Perangkat Keras
9	UI Desain yang susah di pahami
10	<i>Trouble Web Server</i>
11	<i>Server Down</i>
12	Listrik padam secara tiba-tiba
13	Koneksi jaringan gangguan
14	Kerusakan <i>Hardware</i>
15	Kerusakan <i>Software</i>
16	<i>Data Corrupt</i>
17	Koneksi jaringan terputus
18	Koneksi jaringan tidak stabil
19	Data dan informasi yang tidak sesuai
20	Dokumentasi data tidak lengkap
21	Proses <i>maintenance</i> tidak terjadwal
22	Serangan Virus
23	<i>Backup Failure</i>
24	Kegagalan <i>Hardware</i>
25	Kegagalan <i>Software</i>

Dari tahap identifikasi resiko terdapat 23 kemungkinan resiko yang mungkin dapat terjadi, dan mengganggu dalam kinerja aplikasi SRIKANDI. Dampak resiko yang muncul diakibatkan karena beberapa faktor. dari 23 kemungkinan tersebut dibagi menjadi 3 faktor yaitu faktor alam, faktor manusia dan, faktor sistem atau infrastruktur. Tabel 2 merupakan uraian dari identifikasi dampak dan resiko.

Tabel 2. Identifikasi Kemungkinan Resiko dan Dampak Resiko

ID	Faktor	Kemungkinan	Dampak
R01	Faktor Alam	Gempa Bumi	Terjadi kerusakan infrastruktur aktivitas perusahaan terhambat
R02		Kebakaran	Terjadi kerusakan infrastruktur, perusahaan mengalami kerugian finansial, kegiatan perusahaan terhenti kegiatan perusahaan terhenti
R03		Banjir	Terjadi Kerusakan infrastruktur menghambat kegiatan perusahaan
R04		Petir	Terjadi Kerusakan infrastruktur dan mengalami kerugian finansial
R05	Manusia	Penyalahgunaan hak akses	Data dimanipulasi, kebocoran informasi dan data penting
R06		<i>Human Error</i>	Sistem operasi tidak berjalan secara optimal, menghambat proses perusahaan

ID	Faktor	Kemungkinan	Dampak
R07		<i>Hacking</i>	Terjadi pencurian data penting serta disalahgunakan/manipulasi data
R08		Pencurian Data/Perangkat Keras	Kehilangan data penting/ data dimanipulasi, mengalami kerugian finansial
R09	<i>System/ Infrastruktur</i>	UI Desain yang susah di pahami	Menghambat kinerja perusahaan dan pegawai
R10		<i>Trouble Web Server</i>	Kegagalan dalam melakukan hak akses aplikasi srikandi, menghambat kinerja perusahaan
R11		<i>Server Down</i>	Server aplikasi srikandi melambat dan gagal dalam melakukan hak akses aplikasi srikandi
R12		Listrik padam secara tiba-tiba	Aktivitas perusahaan terhambat ataupun terhenti dan pegawai tidak dapat mengakses aplikasi srikandi
R13		Koneksi jaringan gangguan	Menghambat proses penginputan dan pengiriman data dan menurunkan kinerja
R14		Kerusakan <i>Hardware</i>	Kerusakan Hardware dan tidak dapat digunakan
R15		Kerusakan <i>Software</i>	Kerusakan software tidak dapat berjalan
R16		<i>Data Corrupt</i>	Mengalami kerusakan data dan tidak dapat menerima data yang valid
R17		Koneksi jaringan terputus	Tidak dapat dalam melakukan pengiriman data dan kegagalan dalam melakukan hak akses ke aplikasi srikandi
R18		Koneksi jaringan tidak stabil	Memperlambat terselesainya pekerjaan
R19		Data dan informasi yang tidak sesuai	Data tidak valid, menghambat kinerja
R20		Dokumentasi data tidak lengkap	Data tidak valid, data dan informasi yang diperlukan tidak lengkap
R21		Proses <i>maintenance</i> tidak terjadwal	Tidak dapat mengakses aplikasi srikandi dan mengganggu kinerja perusahaan dan pegawai
R22		Serangan Virus	Mengalami kehilangan data dan proses kerja terganggu
R23		<i>Backup Failure</i>	Data yang di input atau di kirim tidak lengkap

Analisis Resiko

Pada tahap ini setelah melakukan identifikasi kemungkinan resiko dan dampak yang bisa terjadi. Dilanjutkan dengan tahap analisis resiko yang dimana identifikasi resiko yang sebelumnya, dianalisis. Analisis resiko dilakukan dengan cara memberikan nilai pada setiap resiko yang mungkin dapat terjadi berdasarkan kemungkinan dan dampak, pada tahap ini proses penilaian resiko menggunakan 2 tabel kriteria *Likelihood* seperti pada Tabel 3 dan *Impact* pada Tabel 4 yang dibagi menjadi 5 kriteria dengan menentukan berapa banyak kemungkinan resiko yang dapat terjadi di waktu - waktu tertentu. Kriteria yang pertama hampir tidak pernah terjadi (*Rare*), jarang terjadi (*Unlikely*), kadang terjadi (*Possible*), sering terjadi (*Likely*), pasti terjadi (*Certain*).

Tabel 3. Likelihood

Likelihood			
Nilai	Kriteria	Keterangan	Frekuensi Kejadian
1	<i>Rare</i>	Resiko tersebut hampir tidak pernah terjadi	> 2 Tahun
2	<i>Unlikely</i>	Resiko tersebut jarang terjadi	1-2 Tahun
3	<i>Possible</i>	Resiko tersebut kadang terjadi	7-12 Bulan
4	<i>Likely</i>	Resiko tersebut sering terjadi	4-6 Bulan
5	<i>Certain</i>	Resiko tersebut pasti terjadi	1-3 Bulan

Setelah menentukan nilai *likelihood* yang kemungkinan terjadi selanjutnya dengan menentukan nilai *impact* atau dampak kemungkinan yang bisa terjadi pada aplikasi srikandi. Ada 5 kriteria *impact* yang mungkin saja dapat terjadi yang pertama (*Insignificant*) tidak mengganggu aktivitas kantor, (*Minor*) aktifitas sedikit terhambat namun tidak mengganggu inti perusahaan, (*Moderate*) menghambat proses kinerja sehingga jalannya aktivitas terhambat, (*Major*) menghambat hampir seluruh aktivitas kantor, (*Catastrophic*) aktifitas terhenti karena mengalami gangguan total.

Tabel 4. Impact

Impact		
Nilai	Kriteria	Keterangan
1	<i>Insignificant</i>	Tidak mengganggu aktivitas kantor
2	<i>Minor</i>	Aktivitas kantor sedikit terhambat namun aktivitas inti perusahaan tidak mengganggu
3	<i>Moderate</i>	Menyebabkan gangguan pada proses kinerja sehingga jalannya aktivitas perusahaan terhambat
4	<i>Major</i>	Menghambat hampir seluruh aktivitas kantor
5	<i>Catastrophic</i>	Aktivitas kantor berhenti karena proses kinerja mengalami gangguan total

Setelah melakukan penilaian dengan menentukan nilai pada *likelihood* dan *impact* dengan mengidentifikasi kemungkinan resiko serta dampak resiko apa saja yang dapat

terjadi pada aplikasi SRIKANDI dengan menentukan nilai dan kriteria yang sesuai pada *likelihood* dan *impact*. Selanjutnya dengan mengkategorikan dan menentukan nilai dari setiap kemungkinan resiko dan dampak dengan kriteria yang sesuai.

Evaluasi Resiko

Tahap evaluasi resiko merupakan tahap terakhir yang mengidentifikasi dan menganalisis setiap kemungkinan – kemungkinan resiko yang sudah diidentifikasi sebelumnya. Hasil dari setiap kemungkinan resiko yang sudah diidentifikasi sebelumnya kemudian dimasukkan ke dalam matrix evaluasi resiko yang dapat dilihat pada tabel 5, pada matrix evaluasi resiko ini dibagi menjadi 3 kategori tingkatan resiko yaitu tingkatan kategori resiko rendah (*Low*), tingkatan kategori sedang (*Medium*), dan tingkatan kategori resiko yang tinggi (*High*).

Tabel 5. Matrix Evaluasi Resiko

<i>Likelihood</i>	Certain	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Possible	3	Low	Medium	Medium	Medium	High
	Unlikely	2	Low	Low	Medium	Medium	Medium
	Rare	1	Low	Low	Low	Medium	Medium
<i>Impact</i>			1	2	3	4	5
			Insignificant	Minor	Moderate	Major	Catastrophic

Dari setiap kemungkinan resiko yang sudah diidentifikasikan dan dikategorikan nilai dan kriterianya berdasarkan *likelihood* dan *impact*, selanjutnya dengan menyesuaikan tingkatan kemungkinan resiko dengan nilai dan level resiko yang sesuai dengan tingkatan resiko pada Tabel 6 mengenai matrix evaluasi resiko yaitu pada level *low*, *medium*, ataupun *high*.

Tabel 6. Penyesuaian Tingkatan Resiko

ID	Kemungkinan Resiko	Likelihood	Impact	Level Resiko
R05	Penyalahgunaan Hak Akses	4	4	High
R06	<i>Human Error</i>	5	3	High
R07	<i>Hacking</i>	4	5	High
R08	Pencurian Data/Perangkat Keras	3	5	High
R10	<i>Trouble Web Server</i>	5	5	High
R11	<i>Server Down</i>	5	5	High
R12	Listrik padam secara tiba-tiba	5	5	High
R13	Koneksi jaringan gangguan	5	5	High
R17	Koneksi jaringan terputus	5	4	High
R18	Koneksi jaringan tidak stabil	5	4	High
R19	Data dan informasi yang tidak sesuai	4	4	High
R20	Dokumentasi data tidak lengkap	4	4	High
R21	Proses <i>maintenance</i> tidak terjadwal	5	5	High
R14	Kerusakan <i>Hardware</i>	2	3	Medium

ID	Kemungkinan Resiko	Likelihood	Impact	Level Resiko
R15	Kerusakan <i>Software</i>	3	3	Medium
R16	Data <i>Corrupt</i>	2	3	Medium
R22	Serangan Virus	3	3	Medium
R23	<i>Backup Failure</i>	3	2	Medium
R01	Gempa bumi	2	1	Low
R02	Kebakaran	2	1	Low
R03	Banjir	2	1	Low
R04	Petir	2	1	Low
R09	UI Desain yang susah di pahami	5	2	Low

Dari hasil evaluasi resiko yang sudah dikelompokan setiap tingkatan resiko yang sesuai dengan menggunakan matrix evaluasi resiko. Terdapat 13 kemungkinan tingkatan resiko yang tinggi (*High*) yaitu pada R05, R06, R07, R08, R10, R11, R12, R13, R17, R18, R19, R20, R21. Dan terdapat 5 tingkatan kemungkinan resiko yang sedang (*Medium*) yaitu pada R14, R15, R16, R22, R23. Dan 5 tingkatan resiko yang rendah (*Low*) yaitu pada R01, R02, R03, R04, R09.

Perlakuan Resiko

Perlakuan resiko merupakan suatu masukan atau suatu perlakuan agar dapat meminimalisir dan mencegah setiap kemungkinan – kemungkinan resiko yang sudah diidentifikasi dan di kelompokkan sebelumnya. Dari 23 kemungkinan resiko dapat dilihat tingkatan resiko yang tinggi terdapat 13 kemungkinan, 5 tingkatan sedang, dan 5 tingkatan rendah. Dari hasil tingkatan resiko tersebut selanjutnya dengan memberikan perlakuan resiko yang sesuai dengan setiap kendala yang ada.

ID	Kemungkinan Resiko	Level Resiko	Perlakuan Resiko/Usulan
R05	Penyalahgunaan Hak Akses	High	Meningkatkan tingkat keamanan dan memberikan batasan hak akses pada tiap pengguna
R06	<i>Human Error</i>	High	Memberikan training pada setiap pengguna
R07	<i>Hacking</i>	High	Meningkatkan tingkat keamanan dan selalu mengupdate password secara berkala
R08	Pencurian Data/Perangkat Keras	High	Meningkatkan tingkat keamanan dengan memasang dan memantau CCTV, dan memantau data server atau database secara berkala
R10	<i>Trouble Web Server</i>	High	Melakukan pengecekan secara rutin pada server maupun database dan melakukan maintenance dengan tepat waktu

ID	Kemungkinan Resiko	Level Resiko	Perlakuan Resiko/Usulan
R11	<i>Server Down</i>	High	Melakukan pengecekan berkala pada server web atau pun database
R12	Listrik padam secara tiba-tiba	High	Melakukan antisipasi dengan menyediakan generator Listrik atau genset agar dapat menyuplai listrik saat listrik padam
R13	Koneksi jaringan gangguan	High	Menyediakan Wifi dengan kecepatan internet yang bagus pada setiap pengguna
R17	Koneksi jaringan terputus	High	Menyediakan koneksi jaringan alternatif
R18	Koneksi jaringan tidak stabil	High	Menyediakan koneksi jaringan alternatif yang lebih memadai dan stabil
R19	Data dan informasi yang tidak sesuai	High	Melakukan pengecekan secara menyeluruh sebelum melakukan pengiriman data
R20	Dokumentasi data tidak lengkap	High	Selalu melakukan pengecekan pada setiap berkas ataupun dokumentasi secara berkala agar dapat meminimalisir data yang tidak lengkap
R21	Proses <i>maintenance</i> tidak terjadwal	High	Selalu melakukan penjadwalan <i>maintenance</i> secara teratur dan rutin baik itu tiap minggu maupun tiap bulan
R14	Kerusakan <i>Hardware</i>	Medium	Melakukan perawatan secara rutin dan menyediakan jaminan asuransi pada tiap <i>hardware</i> yang digunakan
R15	Kerusakan <i>Software</i>	Medium	Melakukan pengecekan pada tiap <i>software</i> yang digunakan maupun pengecekan pada driver perangkat dan jika diperlukan untuk menginstal kembali <i>windows</i>
R16	<i>Data Corrupt</i>	Medium	Menyediakan secara berkala backup data
R22	Serangan Virus	Medium	Meningkatkan <i>internet security</i> atau <i>firewall</i> , dan melakukan <i>scanning antivirus</i> secara berkala
R23	<i>Backup Failure</i>	Medium	Memperhatikan penggunaan memori yang dibutuhkan dan menyediakan penyimpanan alternatif lain untuk melakukan <i>backup data</i>
R01	Gempa bumi	Low	Menyediakan tempat yang aman untuk penyimpanan perangkat keras
R02	Kebakaran	Low	Menyediakan alat pemadam kebakaran

ID	Kemungkinan Resiko	Level Resiko	Perlakuan Resiko/Usulan
R03	Banjir	Low	Membangun saluran air dan menyediakan tempat yang aman untuk perangkat keras agar dapat terhindar banjir
R04	Petir	Low	Menyediakan dan memasang alat penangkal petir
R09	UI Desain yang susah di pahami	Low	Melakukan training atau bimtek (Bimbingan teknis)

KESIMPULAN

Berdasarkan penelitian analisis manajemen resiko pada aplikasi SRIKANDI dengan menggunakan metode ISO 31000 dengan melalui beberapa tahap yang sudah dilalui baik itu tahap pengumpulan data, tahap identifikasi resiko, analisis resiko, evaluasi, dan perlakuan resiko yang mana menentukan tiap kemungkinan resiko yang ada dengan menentukan *likelihood* dan *impact* pada aplikasi SRIKANDI dengan menentukan tiap faktor – faktor yang mungkin dapat terjadi baik itu faktor alam, faktor manusia, maupun faktor *system* atau infrastruktur yang bisa saja mengganggu aktivitas dan kinerja pada aplikasi SRIKANDI sehingga tidak dapat digunakan secara maksimal. Penelitian ini dilakukan dengan harapan dapat meminimalisir dan mencegah setiap kemungkinan resiko dan dampak yang terjadi. Dimana terdapat 23 kemungkinan resiko yang bisa saja terjadi dimana memiliki 13 kemungkinan resiko yang tinggi (*High*), 5 kemungkinan yang sedang (*Medium*), dan 5 kemungkinan resiko yang rendah (*Low*). Kemungkinan resiko yang memiliki tingkatan tinggi (*High*) yaitu penyalahgunaan hak akses, *human error*, *hacking*, pencurian data/perangkat keras, *trouble web server*, *server down*, listrik padam secara tiba-tiba, koneksi jaringan gangguan, koneksi jaringan terputus, koneksi jaringan tidak stabil, data dan informasi yang tidak sesuai, dokumentasi data yang tidak lengkap, dan proses maintenance tidak terjadwal. Kemungkinan resiko yang sedang (*Medium*) yaitu kerusakan *hardware*, kerusakan *software*, *data corrupt*, serangan virus, *backup failure*. Lebih lanjut kemungkinan resiko rendah (*Low*) yaitu gempa bumi, kebakaran, banjir, petir, UI desai susah dipahami.

Dapat dilihat bahwa faktor kemungkinan resiko yang tinggi (*High*) terdapat pada faktor manusia dan faktor sistem maupun infrastruktur sedangkan faktor alam memiliki kemungkinan resiko yang rendah (*Low*) dan Sebagian sistem dan infrastruktur memiliki kemungkinan resiko yang sedang (*Medium*). Kiranya dengan hasil penelitian ini dapat membantu dan bermanfaat baik itu pada penggunaan aplikasi SRIKANDI pada Diskominfo Kota Manado dan dapat meminimalisir dampak kemungkinan resiko yang dapat terjadi kedepannya.

DAFTAR PUSTAKA

Atmojo, S. A., & Manuputty, A. D. (2020). Analisis Manajemen Resiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi AHO Office. *Jurnal Informatika dan Sistem Informasi*, 546-558.

- Hidayat, E. W. (2013). Risk Assessment pada Manajemen Resiko Penerapan Teknologi Cloud Computing bagi Pemerintah Daerah. *Jurnal Komputer Bisnis*, 2(2).
- Irawati, A., Fadholi, H. B., Alamsyah, A. N., Dwipayana, D. P., & Muslih, M. (2021). Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia Di Era Digital. In *Proceeding of Conference on Law and Social Studies*.
- Miftakhatun. (2020). Analisis Manajemen Resiko Teknologi Informasi Pada Website Ecofo Menggunakan ISO 31000. *Journal Of Computer Science an Engineering*, 129-145.
- Munawwaroh, Z. (2017). Analisis Manajemen Risiko pada pelaksanaan program pendidikan dalam upaya meningkatkan mutu pendidikan. *Jurnal Administrasi Pendidikan*, 24(2).
- Qintharah, Y. N. (2019). Perancangan Penerapan Manajemen Risiko. *JRAK: Jurnal Riset Akuntansi Dan Komputerisasi Akuntansi*, 10(1), 67-86.
- Priadana, M. S., & Sunarsi, D. (2021). *Metode Penelitian Kuantitatif*. Pascal Books.
- Pusung, R. E., Manggopa, H. K., & Takaredase, A. (2021). Analisis Kendala dan Alternatif Pembelajaran Daring pada Masa Pandemi Covid-19. *EduTIK: Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, 1(6), 719-730.
- Ramadhan, D. L., Febriansah, R., & Dewi, R. S. (2020). Analisis Manajemen Resiko Menggunakan ISO 31000 pad Smart Canteen SMA XYZ. *JURIKOM (Jurnal Riset Komputer)*, 91-96.
- Rambi, J., & Sitikodna, M. (2022). Analisis Manajemen Resiko Aplikasi Rene Kasir di Restoran Oemah Djari Salatiga Menggunakan ISO 31000. *Journal of Computer and Information Systems Ampera*, 66-83.
- Ratnaningtyas, E. M., Ramli, S. S., Suliwati, D., Nugroho, B. T., & Jahja, A. S. (2023). *Metodologi Penelitian Kualitatif*. Aceh: Yayasan Penerbit Muhammad Zaini.
- Rilyani, A. N., Wibowo, Y. F. A., & Suwawi, D. D. J. (2015). Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus: i-Gracias Telkom University). *eProceedings of Engineering*, 2(2).
- Sandre, H. I., Paat, W. R. L., & Pratasik, S. (2021). Analisis Pembelajaran Daring Pada SMK. *EduTIK: Jurnal Pendidikan Teknologi Informasi dan Komunikasi*, 1(1), 90-96.
- Utamajaya, J. N., Afrina, A., & Fitriah, A. N. (2021). Analisis Manajemen Risiko Teknologi Informasi Pada Perusahaan Toko Ujung Pandang Grosir Penajam Paser Utara Menggunakan Framework Iso 31000: 2018. *Sebatik*, 25(2), 326-334.
- Wahidmurni. (2017). Pemaparan Metode Penelitian Kualitatif. *Jurnal Penelitian*, 1-17.