SABER: Jurnal Teknik Informatika, Sains dan Ilmu Komunikasi
Volume. 3 Nomor. 3 Juli 2025
e-ISSN: 3025-342X; p-ISSN: 3025-2776, Hal. 350-362
DOI: https://doi.org/10.59841/saber.v3i3.3127
Available online at: https://jurnal.stikes-ibnusina.ac.id/index.php/SABER

Analisis Manajemen Risiko Teknologi Informasi Menggunakan Framework Iso 31000
(Studi Kasus : Aplikasi Kehadiran Mobile (K-MOB))

Rafli Ahmad Zulfikri[1], Dwi Yuniarto[2], David Setiadi[3],
[1,2,3] Universitas Sebelas April

Alamat: Jl. Anggrek Situ No. 19, Sumedang Jawa Barat
Email: *A22100098@mhs.stmik-sumedang.ac.id*

Abstract. *Th Advances in information technology have had a significant impact on various aspects of life, including organizational operations. The Mobile Attendance Application (K-Mob) is one implementation of information technology designed to simplify the process of recording attendance in real-time. However, this application is vulnerable to risks that can hamper operations, such as hacking, system failures, and data security issues. This study aims to identify, analyze, and evaluate risks that may affect K-Mob's performance using the ISO 31000 framework. The analysis process is carried out through communication with stakeholders, risk identification, and risk evaluation based on the frequency of occurrence and impact. The results show that significant risks faced include hardware damage, server disruptions, and data misuse. Risk management is carried out through mitigation strategies, such as system updates, infrastructure strengthening, and increasing human resource capacity. With this approach, risks can be minimized, ensuring the sustainability of K-Mob's operations, and improving system reliability. This study recommends regular risk evaluation and the development of adaptive strategies to address evolving threats. The implementation of ISO 31000 has been proven to provide effective guidance in information technology risk management.is*

Keywords: *K-MOB application, Flexible Working Arrangement (FWA), ASN discipline, ASN performance, attendance technology.*

Abstrak. Kemajuan teknologi informasi telah membawa dampak signifikan terhadap berbagai aspek kehidupan, termasuk operasional organisasi. Aplikasi Kehadiran Mobile (K-Mob) adalah salah satu implementasi teknologi informasi yang dirancang untuk mempermudah proses pencatatan kehadiran secara real-time. Namun, aplikasi ini rentan terhadap risiko yang dapat menghambat operasional, seperti peretasan, kegagalan sistem, serta masalah keamanan data.Penelitian ini bertujuan untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko yang mungkin memengaruhi kinerja K-Mob dengan menggunakan kerangka kerja ISO 31000. Proses analisis dilakukan melalui komunikasi dengan pemangku kepentingan, identifikasi risiko, serta evaluasi risiko berdasarkan frekuensi kejadian dan dampaknya.Hasil penelitian menunjukkan bahwa risiko signifikan yang dihadapi meliputi kerusakan perangkat keras, gangguan server, dan penyalahgunaan data. Penanganan risiko dilakukan melalui strategi mitigasi, seperti pembaruan sistem, penguatan infrastruktur, dan peningkatan kapasitas sumber daya manusia. Dengan pendekatan ini, risiko dapat diminimalkan, memastikan keberlanjutan operasional K-Mob, dan meningkatkan keandalan sistem.Studi ini menyarankan evaluasi risiko secara berkala serta pengembangan strategi adaptif untuk mengatasi ancaman yang terus berkembang. Penerapan ISO 31000 terbukti memberikan panduan yang efektif dalam manajemen risiko teknologi informasi.

Kata kunci: Aplikasi K-MOB, Flexible Working Arrangement (FWA), disiplin ASN, kinerja ASN, teknologi presensi.

1. LATAR BELAKANG

Pada era digital sekarang ini kemajuan dalam dunia teknologi informasi terus berkembang yang berdampak pada segala aspek kehidupan manusia. Semua termasuk pendidikan, bisnis, pemerintahan, dll. Pada awal 1990-an, aplikasi komputerisasi masih merupakan satu hal yang jarang digunakan atau dikembangkan di banyak departemen, namun pada millennium baru, karena biaya operasi yang tinggi dan keuntungan yang cukup rendah. Aplikasi komputerisasi mulai diterapkan di berbagai bidang dan berkembang pesat. Berbagai

Received: Juni 10, 2025; Revised: Juni 30, 2025; Accepted: Juli 10, 2025;
Online Available: Juli 15, 2025;

sistem dikembangkan melalui penggunaan media komputer dan pendukungnya, memungkinkan sebagai besar departemen mulai mengembangkan sistem informasi unruk proses bisnis yang dilakukan bersama.

Perkembangan teknologi informasi merupakan bagian penting dari sistem informasi dan pengembnagan adalah pada salah satu aspek keamanan dan manajemen risiko. Dengan berkembangnya sistem operasi yang benar, karena selain dampak positif dari perkembangan sistem informasi, masalahnya keamanan dan manajemen sumber daya teknologi informasi juga terjadi.

Risiko adalah potensi bahaya, yang mengarah pada aktitivasi bisnis instansi yang kurang ideal. Risiko adalah sesuatu yang tidak pasti dan memperngaruhi peluang instansi untuk mencapai suatu tujuan atau ambisi(Mahardika et al., 2019). Risiko adalah bagian yang tidak terpisahkan dari aktifitas manusi, ibarat seperti tidak ada kehidupan tanpa adanya risiko(). Ketika sistem yang dikerahkan tidak berfungsi secara efektif, sebuah instansi yang bergantung pada sistem informasi untuk sebagai besar proses bisnisnya dapat mengalami gangguan serius(Pertiwi, 2017). Jika timbul bahaya dalam penggunaan perangkat lunak dan perangkat keras, instansi harus siap mengalami kemungkinan terjadinya risiko dengan mengidentifikasi penyebab dan mencari solusi yang tepat(Nurbaya et al., 2017). Analisi manajemen risiko merupakan suatu proses yang dilakukan pada tingkat manajemen pelaksana, yaitu berupa proses analisis sistematis dari setiap kerugian yang data dihadapi oleh sebuah perusahaan, akibat dari suatu risiko juga cara pengendalian yang tepat guna mengatasi kerugian pada instansi(Harimurti, 2006).

Dalam penggunana teknologi informasi dapat menimbulkan kemungkinan risiko. Banyak penelitian yang menunjukkan bahwa teknologi informasi dan asetnya rentan terhadap kerusakan fisik dan logis. Risiko kerusakan fisik terkait dengan perangkat keras seperti bencana alam, pencurian, kebakaran, lonjakan listrik dan vandalism. Risiko kerusakan logis mengacau pada akses yang tidak sah, kerusakan yang disengaja atau tidak disengaja terhadap informasi dan asset informasi dan asset informasi yang terkandung di dalamnya. Untuk itu diperlukan identifikasi ancaman dan analysis risiko untuk meningkatkan keamanan dan mengurangi risiko kerusakan sistem informasi.

Aplikasi Kehadiran Mobile (K-Mob) merupakan salah satu penerapan dari pengguna teknologi informasi untuk memudahkan pengguna dalam melakukan kehadiran real time untuk menggunakan pegawai di kantor maupun luar kantor secara real rime memanfaatkan teknologi Wifi dan GPS untuk memastikan kehadiran dilakukan dalam radius yang diperolehkan secara

fitur foto swafoto untuk memvalidasi kehadiran, cukup hubungi pihak K-Mob melalui aplikasi android dan IOS atau melalui hotline resmi mereka atau PlayStore atau App Store.

Setiap aplikasi pasti memiliki berbagai kemungkinan risiko interfarensi yang menyebabkan aplikasi tidak berjalan dengan optimal. Tidak terkecuali aplikasi pada K-Mob ini, aplikasi ini uga dapat menghadapi potensi risiko di sekitarnya. Berdasarkan permasalahan tersebut perlu dilakukan penelitian untuk mencatat berbagai kemungkinan risiko dan prioritasnya bagi pemerintah. Oleh karena itu, untuk tujuan ini, ISO 31000 dapat digunakan untuk analisis manajemen risiko.

2. KAJIAN TEORITIS

Lembaga penelitian pendidikan tinggi juga menggunakan ISO 31000 untuk melakukan penelitian analisis risiko teknologi informasi. Hasil dari penelitian ini adalah memberikan serangkaian risiko dan factor, risiko dan factor tersebut membantu atau memicu kejadian tertentu yang mengancam penggunaan teknologi informasi oleh lembaga penelitian pendidikan tinggi(Agustinus et al., 2017).

Analisis menajemen risiko merupakan kegiatan yang dilakukan pada tingkat pimpinan ekseklutif, yaitu menemukan dan menganalisis secara sistematis bentuk kerugian yang mungkin dihadapi perusahaan akibat risiko dan metode pengendalian yang paling tepat untuk menangani kerugian terkait bisnis. Tingkat keuntungan perusahaan(Agustinus et al., 2017).
Analisis risiko memiliki beberapa tujuan yaitu:

a. Tujuan sebelum kerugian meningkatkan kepercayaan dalam bentuk efisiensi dan menyelesaikan tanggung jawab pihak luar.
b. Setelah mengalami kerugian dalam bentuk operasi yang berkelanjutan, tujuannya adalah agar dapat terus bertahan, dengan pendapatan dan pertumbuhan yang stabil (Rilyani, n.d.).

ISO 31000 adalah standar terkait manajemen risiko yang dikembangkan oleh Organisasi Internasional untuk Standardisasi (ISO). Tujuan dari ISO itu sendiri adalah untuk memberikan prinsip dan pedoman yang diterima untuk manajemen risiko. Manajemen risiko merupakan suatu proses pengkuran atau penilaian risiko serta pengembangan strategi pengelolaannya, salah satu manajemen risiko yang dapat digunakan adalah dengan menggunakan ISO 31000(Atmojo & Manuputty, 2020).

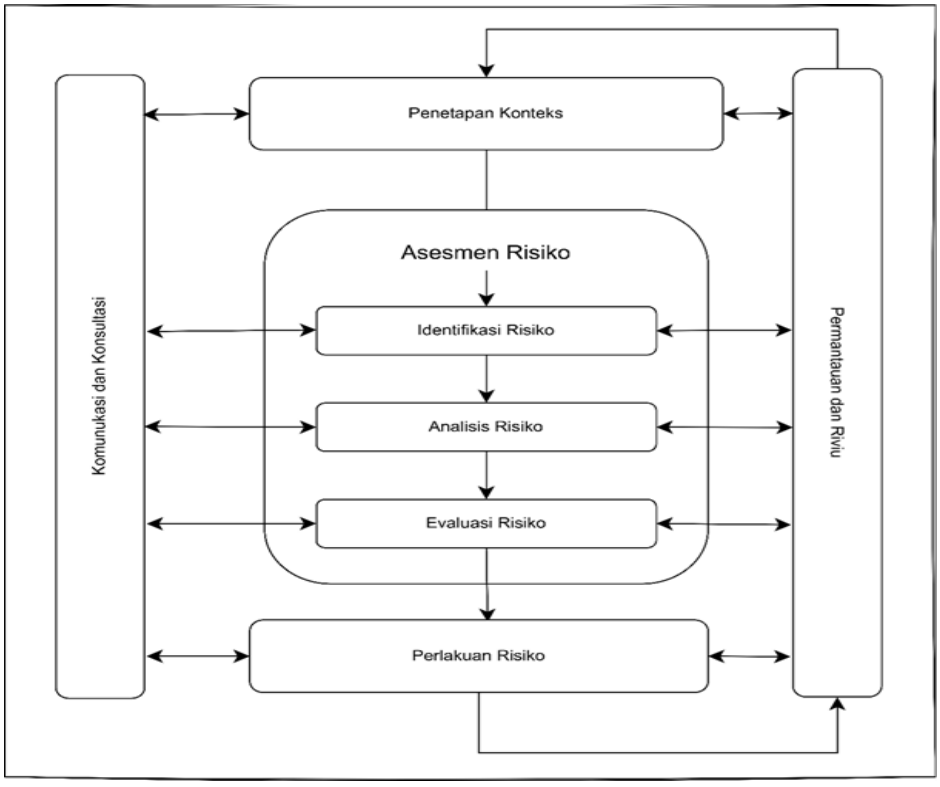
3. METODE PENELITIAN

Metode yang akan digunakan dalam penelitian ini adalah metode studi kasus, yaitu hanya satu kasus, dan sampel yang digunakan berupa individu atau kelompik. Dengan acara ini penulis dapat mengumpulkan lebih banyak data tentang objek yang diteliti untuk menjawab pertanyaan yang ada. Data dala penelitian ini adalah data mentah, dimana sumber datanya dikumpulkan dalam bentuk dokumen yang telah diverifikasi dan diverifikasi oleh sumber data. Makalah atau sumber data kertas tidak dapat digunakan karena berisi data tingkat ketiga.

Manajemen Risiko IT

Manajemen Risiko Teknologi Informasi (TI) adalah suatu proses penting dalam berbagai aspek, terutama aspek kehidupan pribadi, keuangan, bisnis da bahkan dalam mengalami keputusan, dengan menimimalisir risiko kita akan mencegah hal-hal yang buruk terjadi bahkan tujuan kita akan lebih mudah tercapai. Manajemen resiko TI adalah gabungan beberapa proses yang terdiri dari identifikasi, pengkajian, pengembangan strategi mitigasi dan komunikasi yang berpotensi menimbulkan dampak negatif serta berpengaruh pada kerugian sebuah organisasi.

Manajemen risiko merupakan suatu proses pengkuran atau penilaian risiko serta pengembangan strategi pengelolaannya, salah satu manajemen risiko yang dapat digunakan adalah dengan menggunakan ISO 31000(Mahardika et al., 2019), secara umum proses menejemen risiko yang terdapat pada ISO 31000 dapat dijelaskan melalui gambar 3.1. proses manajemen Risiko 31000 (2018).



Gambar 3.1 Proses Manajemen Risko ISO 31000

Proses manajemen risiko terdiri atas rangkain apliaksi logis dan metode sistemasis yang saling berkaitan, yaitu :

a. Kemunikasi dan Konsultasi (*Communication and Consultation*)
b. Menentukan Konteks (*Establishing the context*)
c. Penilaian Risiko (*Risk Assestment*), meliputi : Identifikasi Risiko (*Risk identification*), Abalisis Risiko (*Risk analysis*) adan Evaluasi Risiko (*Risk evaluation*)
d. Perlakuan terhadap Risiko (*Risk treatment*)
e. *Monitoring and Review*

Proses manajeman risiko membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Manajemen risiko bertujuan untuk mengelola risiko tersebut agar memperoleh hasil yang terbaik. Pada tahap yang pertama adalah risk assessment atau asesmen risiko yang dapat menggaggu perusahaan dalam mencapai tujuan bisnisnya. Pada tahap penilaian risiko terdapat 3 proses yaitu identifikasi risiko, analisis risiko dan penilaian risiko. Identifikasi potensi risiko yang dapat menghambat perkembangan perusahaan Analisis risiko adalah proses mengidentifikasi risiko yang dapat menghambat perusahaan dalam mencapai tujuan bisnisnya. Penilaian risiko adalah proses mengevaluasi semua kemungkinan proses. Risiko didasarkan pada tingkat gravitasi, berdasarkan standar yang ditetapkan. Langkah selanjutnya adalah risk treatment atau perlakuan risiko, dimana peneliti akan menyeleksi kemungkinan risiko sebelumnya. Hal ini dapat meningkatkan atau mengurangi kemungkinan risiko dan dampak risiko.

4. HASIL DAN PEMBAHASAN

Proses manajemen risiko berbasis ISO 31000 meliputi beberapa kegiatan yaitu lomunikasi dan konsultasi, penentuan konteks, penilaian risiko, perlakuan risiko, monitoring dan review.

Komunikasi dan Konsultasi

Membuat rencana komunikasi merupakan langkah awal dalam berinteraksi dengan pihak internal maupun eksternal yang akan berpartisipasi dalam tahapan ini. Setelah itu, dibuat rencana baru mengenai data yang dikumpulkan dan informasi yang akan disampaikan(Lany F.2016).

Wawancara dengan pemangku kepentingan yang terlibat dalam keberlanjutan teknologi dan sistem di K-Mob dilakukan sebagai dari penelitian dengan menggunakan pendekatan komunikasi langsung. Selain itu juga dilakukan observasi guna memperoleh informasi bagaimana proses bisnis yang diterapkan dalam K-Mob (Miftakhatun, 2020)..

Tahap Menetukan Konteks

Penelitian ini, dilakukan tahapan penetapan konteks. Di mana manajemen risiko, ruang lingkup, dan kriteria risiko akan diperhitungkan. Temuan penetapan konteks manajemen risiko adalah sebagai berikut:

a. Alam atau lingkungan.
b. Manusia.
c. Sistem dan infrastruktur

Tahap Kriteria Risiko

Setelah ditemukan faktor apa saja yang dijadikan konteks risiko yang terjadi, berdasarkan kemungkinan dan dampak maka berikutnya terlebih dahulu disusun kriteria kemungkinan dan kriteria dampak risiko.

Tabel 2. Kriteria Frekwensi kejadian (*Likelihood*)

Rating	Kreteria	Keteangan	frekuensi
1	Rare	Risiko yang sangat jarang/hamper tidak pernah terjadi	>2 Tahun
2	Unixely	Risiko jarang terjadi	1-2 Tahun
3	Possible	Risiko biasa/kadang-kadang terjadi	7-12 Bulan/Tahun
4	Lixely	Risiko sering terjadi	4-6 Bulan/Tahun
5	Certair	Risiko sangat sering/pasti terjadi	1-3 Bulan/Tahun

Tabel 3.Kriteria Dampak (*Impact*)

Rating	Kriteria	Keterangan
1	Significant	Sangat kecil/tidak menggunakan operasional dan aktivitas pengguna.
2	Minor	Kecil/proses bisnis dan aktivitas mengalami gangguan, namun tidak menghambat tugas pokok atau axtiritas pengguna.
3	Moderate	Biasa/proses bisnis mengalami gangguan sehingga aktivitas terhambat dan mengalami penundaan.
4	Mayor	Besar/menghambat hampir seluruh proses bisnis dan aktivitas.
5	Cotostrophic	Sangat besar/proses bisnis mengalami gangguan total sehinggaaktivitas berhenti total dan proses binis tidak bisa tercapai.

Analisis Risiko

Analisis risiko dilakukan dengan cara memberikan nilai dari setiap risiko yang muncul. Dari tiap-tiap risiko yang muncul akan dilakukan penilaian (bobot) dari sisi frekuensi kejadian dan dampak yang diakibatkan. Pada layanan Aplikasi K-Mob, kriteria pengukuran nilai/bobot untuk frekwensi kejadian dan dampak yang diakibatkan dapat dilihat pada Tabel 4.4.

Tabel 4. Nilai/bobot frekwensi kejadian dan dampak risiko

Frekuensi kejadian		Dampak yang diakibatkan	
Nilai	**Keterangan**	**Nilai**	**Keterangan**
1	Sangat jarang terjadi	1	Sangat kecil
2	Jarang terjadi	2	Kecil
3	Biasa terjadi	3	Biasa
4	Sering terjadi	4	Besar
5	Sangat sering terjadi	5	Sangat besar

Langkah selanjutnya adalah melakukan penilaian atai pembobotan setiap risiko dari masing-masing sumber daya TI yang telah diindentifikasi tersebut (Tabel 3.) berdasarkan pengelompokkan kriteria frekwensi kejadian (*Likelihood*) dan kriteria dampak (*Impact*) yang diakibtkan untuk setiap riaiko yang telah diidentifikasi. Hasil penilaian/pembobotan frekwensi kejadian dan kriteria dampak yang diakibatkan untuk setiap risiko tersebut secraa detail dapat dilihat pada Tabel 5.

Tabel 5. Penilaian idientifikasi risiko menurut frekwensi dan kriteria dampak

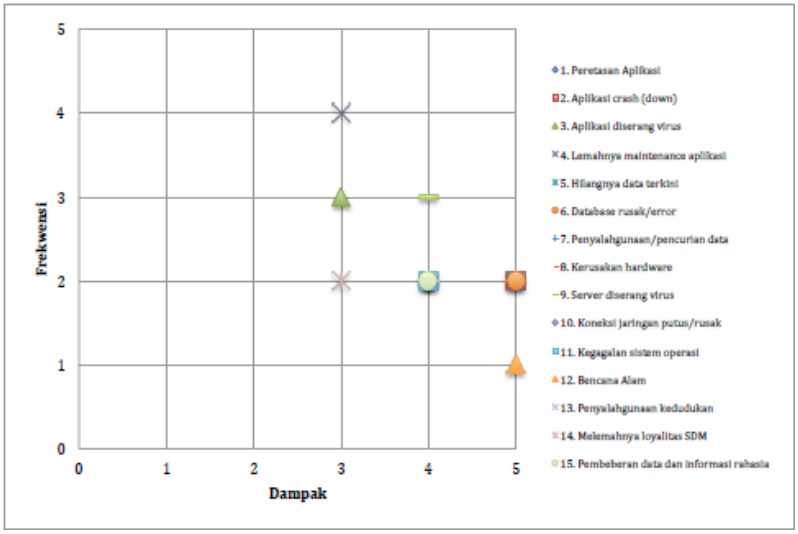
No	IT Resources	Identifikasi Risiko	Frekwensi	Dampak
1	*Application*	1. Perentasan Apliaksi	2	4
		2. Aplikasi *crash* (down)	2	5
		3. Apliaksi diserrang virus	3	3
		4. Lemahnya *maintenance* Apliaksi	4	3
2	*Information*	5. Hilangnya data terkini	2	5
		6. *Database* rusak/error	2	5
		7. Penyalahgunaan/pencurian data	1	4
3	*Infrastructure*	*8.* Kerusakan *hadware*	2	4
		9. *Server* diserang virus	3	4
		10. Koneksi jaringan putus/rusak	2	4
		11. Bencana Alam	2	4
		12. Kerusakan *hadware*	1	5
4	*People*	13. Penyalgunaan kedudukan	2	4
		14. Malemanhya loyalitas SDM	2	3
		15. Pembeberan data dan informasi rahasia	2	4

Evaluasi Risiko

Evaluasi risiko dilakukan dengan menerapkan proses mamping pada grafik (x,y) yang menggambarkan hubungan antara frekwensi kejadian risko dengan dampak yang diakibatkan oleh setiap risiko. Grafik hasil evaluasi risko tersebut dikategorikan menjadi 3 area yaitu Low, Medium dan Higt berdasarkan matriks hasil kombinasi antara *likelihood* (*frekwensi* kejadian) dengan dampak yang ditimbulkan sebagai berikut:

frekuensi						
	5	Medium	Medium	High	High	High
	4	Low	Medium	High	High	High
	3	Low	Low	Medium	High	High
	2	Low	Low	Medium	Medium	High
	1	Low	Low	Low	Medium	Medium
		1	2	3	4	5
				dampak		

Gambar 2. Matriks Evaluasi Risiko



Gambar 3. Sebaran Risiko TI berdasarkan Frekwensi dan Dampak

frekuensi						
	5					
	4			R4		
	3			R3	R9	
	2			R14	R1,R7,R8, R10,R11, R13,R15	R2,R5,R6
	1					R12
		1	2	3	4	5
				dampak		

Keterangan R: Risiko TI

Gambar 4. Matriks Evaluasi Risiko TI berdasarkan Frekwensi dan Dampak

Gambar 3. memperlihatkan sebara risiko sumber daya TI yang telah diidentifikasi sebelumnya berdasarkan *mapping* antara nilai frekwensi kejadian risiko dengan nilai dampak yang diakitkan oleh risiko tersebut. Sesuai dengan pengelompokkan kategori evaluasi risiko, maka jenis risiko yang diakibatkan dari kombinasi *mapping* nilai frekwensi dan dampak risiko dapat dilihat pada Gambar 4. dan Tabel 6.

Tabel 6. Evaluasi Risiko berdasarkan *mapping* Risiko dengan Frekwensi- Dampak

Identifikasi Risiko	Frekwensi	Dampak	Evaluais Risiko
1. Perentasan Apliaksi	2	4	Medium
2. Aplikasi *crash* (down)	2	5	High
3. Apliaksi diserrang virus	3	3	Medium
4. Lemahnya *maintenance* Apliaksi	4	3	High
5. Hilangnya data terkini	2	5	High
6. *Database* rusak/error	2	5	High
7. Penyalahgunaan/pencurian data	1	4	Medium
8. Kerusakan *hadware*	2	4	Medium
9. *Server* diserang virus	3	4	High
10. Koneksi jaringan putus/rusak	2	4	Medium
11. Bencana Alam	2	4	Medium
12. Kerusakan *hadware*	1	5	Medium
13. Penyalgunaan kedudukan	2	4	Medium
14. Malemanhya loyalitas SDM	2	3	Medium
15. Pembeberan data dan informasi rahasia	2	4	Medium

Penanganan Risiko

Tahapan selanjutnya adalah menentukan strategi perlakuan risiko. Terdapar empat jenis strategi perlakukan risiko, yaitu :

1. *Risk avoidance* (menghindari risiko)
2. Risk reduction (mengurangi/mitigasi risiko berupa pengurangan likelihood, pengurangan dampak dan pengurangan likelihood dan dampak sekaligus)
3. Risk sharing (berbagi risiko)
4. Risk acceptance (menrima risiko)

Strategi perlakuan risiko yang paling tepat dsalam mengatasi permasalahan yang sesuai dengan pembahasan ini adalah dengan risk reduction, Adapun program penanganan risiko yang dapat dilakukan dapat dilihat pada Tabel 7.

Tabel 7. Program Penanganan Risiko

No	IT Resources	Identifikasi Risiko	Program Penanganan Risiko
	Application	1. Perentasan Apliaksi	Perbaikan sistem aplikasi melalui *update patch* dan penerapan sistem *firewall* disertai dengan peningkatan sistem keamanan (*security*)
		2. Aplikasi *crash* (down)	Perbaikan sistem aplikasi melalui *update patch* dan pencegahan instalasi aplikasi lain yang bisa menyebabkan aplikasi utama *crash*

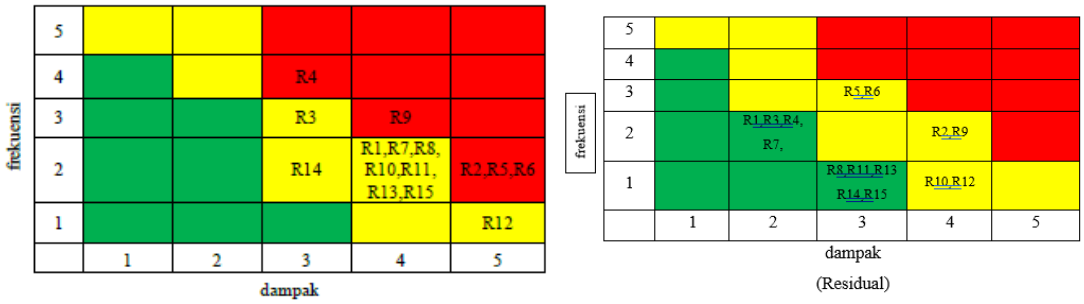
No	IT Resources	Identifikasi Risiko	Program Penanganan Risiko
		3. Apliaksi diserrang virus	Review kinerja antivirus untuk komputer *client*, baik *update* antivirus maupun scan antivirus secara periodik
		4. Lemahnya *maintenance* Aplikasi	Sementara aplikasi sedang dalam proses *maintenance* jangan sampai mengganggu sistem pelayanan terhadap pengguna data Lakukan *maintenance* pada *non-busy hour* atau gunakan mekanisme aplikasi cadangan
	Information	5. Hilangnya data terkini	Data harus senantiasa memiliki backup melalui mekanisme syncronizing secara otomatis. Sehingga kehilangan data pada satu periode waktu tidak akan menjadi alasan bagi sitem untuk berhenti bekerja
		6. *Database* rusak/error	Database harus senantiasa memiliki backup melalui mekanisme mirroring dan lokasi *backup database* diterapkan pada beberapa lokasi *device*. Kerusakan *database* tidak akan menjadi alasan bagi sitem untuk berhenti bekerja
		7. Penyalahgunaan/pencurian data	Review manajemen puncak dalam hal mekanisme *security* data
	Infrastructure	*8.* Kerusakan *hadware*	Review kinerja tim pemeriksaan fisik, perbaiki bila memungkinkan jika tidak segera lakukan penggantian
		9. *Server* diserang virus	Review kinerja antivirus, lakukan pembersihan (*scan*) secara periodik
		10. Koneksi jaringan putus/rusak	Review kinerja jaringan dengan pihak penyedia jaringan. Lakukan monitoring sistem dan kinerja jaringan secara periodik, baik instalasi jaringan maupun *bandwith*
		11. Bencana Alam	Usahakan memiliki lokasi penyimpanan *backup* yang memiliki risiko terkena bencana alam yang lebih kecil dibandingkan lokasi penyimpanan data utama.
		12. Kerusakan *hadware*	Terapkan mekanisme Disaster Recovery Planning (DRP) untuk mengantisipasi kerusakan infrastruktur TI dikarenakan bencana alam
	People	13. Penyalgunaan kedudukan	Sosialisasikan penerapan sanksi berat kepada setiap pegawai yang menyalahgunakan wewenang dan kedudukan. Berikan sanksi pada pegawai yang bersangkutan. Review manajemen puncak terhadap *fit and proper test* jabatan.
		14. Malemanhya loyalitas SDM	Review manajemen puncak terhadap tata kelola SDM Pengkajian kesesuaian hak dan kewajiban pegawai
		15. Pembeberan data dan informasi rahasia	Sosialisasikan penerapan sanksi berat kepada setiap pegawai yang melakukan pembeberan data dan informasi rahasia Berikan sanksi pada pegawai yang bersangkutan. Review manajemen puncak terhadap penilaian dan penempatan pegawai.

Tabel 8. Evaluasi Hasil Mitigasi Risiko (Residual)

Identifikasi Risiko	Frekwensi	Dampak	Evaluais Risiko
1. Perentasan Apliaksi	2	2	Low
2. Aplikasi *crash* (down)	2	4	Medium
3. Apliaksi diserrang virus	2	2	Low
4. Lemahnya *maintenance* Apliaksi	2	2	Low
5. Hilangnya data terkini	3	3	Medium
6. *Database* rusak/error	3	3	Medium
7. Penyalahgunaan/pencurian data	2	2	Low
8. Kerusakan *hadware*	1	3	Low
9. *Server* diserang virus	2	4	Medium

10. Koneksi jaringan putus/rusak	1	4	Medium
11. Bencana Alam	1	3	Low
12. Kerusakan *hadware*	1	4	Medium
13. Penyalgunaan kedudukan	1	3	Low
14. Malemanhya loyalitas SDM	1	3	Low
15. Pembeberan data dan informasi rahasia	1	3	Low

Tabel 8. menunjukan evaluasi risiko setelah dilakukan proses mitigasi risiko melalui program penanganan risiko (*risk reduction*) yang berdampak terhadap penurunan nilai *likelihood* dan dampak risiko. Perbandingan mengenai evaluasi risko sebelum (inheren) dan sesudah dilakukan mitigasi risiko (residual) dapat dilihat Gambar 2.6 berikut ini.



Keterangan R: Risiko

Gambar 5 Matriksd Evaluasi Risiko Kondisi Sebelum dan Susudah Mitigasi Risiko

Berdasarkan Gmabar 5. terlihat perubahan area risiko setelah dilakukan program penanganan risiko (mitigasi risiko), dimana keberhasilan pelaksanaan program penanganan risiko tersebut diharapkan menjadi tanggung jawab seluruh pegawai Dinas Kehutanan pada umumnya dan unit organisasi penyedia layanan K-Mob pada khususnya. Pelaksanaan program penanganan risiko tersebut harus sesuai dengan Standard Operating Procedure Manajemen Risiko yang sudah ditetapkan.

Monitoring dan review

Monitoring merupakan kegiatan pemantauan rutin terhadap kinerja aktual proses manajemen risiko dibandingkan dengan rencana atau harapan yang telah ditetapkan. *Review* adalah peninjauan atau pengkajian berkala atas kondisi saat ini dan dengan fokus tertentu. *Monitoring* dan *review* merupakan bagian dari proses manajemen risiko yang memastikan bahwa seluruh tahapan proses dan fungsi manajemen risiko memang berjalan dengan baik.

Monitoring dan review sebaiknya dilaksanakan secara simultan (bersamaan) ketika setiap langkah dari proses penilaian risiko dilakukan. Proses *monitoring* ini selayaknya melibatkan berbagai pihak termasuk *stakeholder*. Terdapat tiga macam bentuk *monitoring* dan

review yang harus dilakukan terus menerus oleh instansi sebagai bagian yang tidak terpisahkan dari tanggung jawab pekerjaan pada level jabatan masing-masing, yaitu:

1. Pemeriksaan berkala dan pemantauan berkelanjutan. Dilaksanakan harian dan menjadi bagian dari pekerjaan.
2. Pemeriksaan oleh atasan. Dilaksanakan secara berkala dan didorong oleh profil risiko serta lingkup tanggungjawab pejabat bersangkutan.
3. Audit pihak ketiga. Verifikasi oleh internal dan eksternal auditor bertujuan untuk melihat kepatuhan terhadap Standar dan Peraturan yang berlaku.

5. KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa penerapan proses manajemen risiko berbasis ISO 31000 pada Aplikasi Kehadiran Mobile (K-Mob) mampu mengidentifikasi, menganalisis, dan mengevaluasi berbagai risiko yang memengaruhi operasional aplikasi. Beberapa potensi risiko yang teridentifikasi meliputi peretasan aplikasi, kerusakan perangkat keras, gangguan server, dan risiko terkait SDM seperti rendahnya loyalitas atau penyalahgunaan kedudukan. Evaluasi risiko dilakukan dengan memetakan tingkat frekuensi kejadian dan dampak risiko pada matriks evaluasi untuk menentukan kategori risiko, yaitu rendah, menengah, atau tinggi.

Hasil penelitian mengungkapkan bahwa sebagian besar risiko signifikan yang ditemukan, seperti aplikasi crash, hilangnya data terkini, dan kerusakan database, termasuk dalam kategori risiko tinggi. Penanganan terhadap risiko-risiko tersebut melibatkan strategi yang sesuai, termasuk mitigasi risiko melalui penguatan infrastruktur, peningkatan proses maintenance, serta edukasi dan pelatihan SDM untuk meningkatkan keandalan sistem dan loyalitas pengguna.

Dengan analisis risiko ini, instansi dapat lebih proaktif dalam mengelola risiko-risiko yang muncul, memprioritaskan langkah-langkah perlakuan risiko, dan memastikan kelangsungan operasional aplikasi K-Mob dalam mendukung proses bisnis. Proses ini juga memberikan panduan strategis dalam pengelolaan risiko teknologi informasi yang adaptif terhadap perubahan lingkungan, sehingga dapat menjadi referensi bagi pengembangan sistem informasi lainnya.

Penelitian ini menyarankan agar evaluasi risiko dilakukan secara berkala, mengingat dinamika teknologi dan ancaman yang terus berkembang. Selain itu, penerapan metode dan standar manajemen risiko seperti ISO 31000 dapat terus disesuaikan dengan kebutuhan organisasi untuk meningkatkan efisiensi dan keamanannya..

DAFTAR REFERENSI

Agustinus, S., Nugroho, A., & Cahyono, A. D. (2017). Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Program HRMS. *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)*, *1*(3), 250–258. Https://Doi.Org/10.29207/Resti.V1i3.94

A. Novia Rilyani, Y. A. Firdaus W ST, And D. S. Dwi Jatmiko, "Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus : Igracias Telkom University) Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study : Igracias Telkom University)," *E-Proceeding Eng*., Vol. 2, No. 2, Pp. 6201–6208, 2015.

Atmojo, S. A., & Manuputty, A. D. (2020). Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 Pada Aplikasi AHO Office. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *7*(3), 546–558. Https://Doi.Org/10.35957/Jatisi.V7i3.525

Angraini, A., Dan Pertiwi, I. D. (2017). Analisa Pengelolaan Risiko Penerapan Teknologi Informasi Menggunakan Iso 31000. Jurnal Ilmiah Rekayasa Dan Manajemen Sistem Informasi, 3(2), 70–76.

AS/NZS ISO 31000, *Risk Management – Principles And Guidelines*, 1st Ed. New Zealand: International Standard, 2009

Ernawati, T., Suhardi, & Nugroho, D. R. (2012). IT Risk Management Framework Based On ISO 31000:2009. *2012 International Conference On System Engineering And Technology (ICSET)*, 1–8. Https://Doi.Org/10.1109/Icsengt.2012.6339352

Grey, Manson, S., & Louise, C. (2015). The *Audit Process: Principles, Practice And Cases,6th Edition*. Cengage Learning.

Harimurti, F. (2006). *Manajemen Risiko, Fungsi Dan Mekanismenya*. *6*(1).

Mahardika, K. B., Wijaya, A. F., & Cahyono, A. D. (2019). Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000: 2018 (STUDI KASUS: CV. XY). *Sebatik*, *23*(1), 277–284. Https://Doi.Org/10.46984/Sebatik.V23i1.572

Miftakhatun, M. (2020). Analisis Manajemen Risiko Teknologi Informasi Pada Website Ecofo Menggunakan ISO 31000. *Journal Of Computer Science And Engineering (JCSE)*, *1*(2), 128–146. Https://Doi.Org/10.36596/Jcse.V1i2.76

Nurbaya, F., Witanti, W., & Umbara, F. R. (2017). *Manajemen Risiko Sistem Informasi Akademik Di Universitas Jenderal Achmad Yani Menggunakan Committee Of Sponsoring Organizations Of The Treadway Commission's (COSO)*.

Pertiwi, I. D. (2017). *Analisa Pengelolaan Risiko Penerapan Teknologi Informasi Menggunakan ISO 31000*. *3*(2).

Rilyani, A. N. (N.D.). *Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO 31000 (Studi Kasus: I-Gracias Telkom University)*.