Analisis Manajemen Risiko Menggunakan Framework ISO 31000 Pada *Smart Parking Gate* UKSW

Jesica Mambrasar dan Penidas Fiodinggo Tanaem

Universitas Kristen Satya Wacana,
Jl. Diponegoro No.52-60,Salatiga, Kec. Sidorejo, Kota Salatiga, Jawa Tengah
E-mail : jessikadesyah0412@gmail.com, penidas.fiodinggo@uksw.edu*)

Abstrak

Pada era kemajuan teknologi sangat pesat, hampir seluruh aspek kehidupan sudah menerapkan teknologi informasi, selain karena efisien dan efektif tetapi banyak juga kemudahan yang didapatkan. Penerapan teknologi informasi tidak terlepas dari ancaman risiko yang dapat berdampak dalam penggunaannya. Oleh sebab itu, penting pengelolaan yang baik dan benar dengan menerapkan manajemen risiko untuk melihat kemungkinan atau dampak risiko. Penelitian ini bertujuan untuk mengalisis risiko menggunakan kerangka kerja International Organization for Standardization (ISO) 31000. Penelitian ini juga menerapkan metode penelitian kualitatif dengan pendekatan case study research serta Teknik pengumpulan data melalui wawancara. Hasil yang didapatkan dari sistem smart parking gate di UKSW teridentifikasi memiliki 17 kemungkinan risiko yang dapat terjadi diantaranya 4 kemungkinan level risiko high, 10 kemungkinan level risiko medium, dan 3 kemungkinan level risiko low.

Kata kunci : manajemen risiko, smart parking gate, ISO 31000

Pendahuluan

Teknologi informasi mengalami kemajuan sangat luar biasa dan telah menjadi kebutuhan penting di masa sekarang. Hampir seluruh aktivitas sehari-hari maupun sektor bisnis sudah menerapkan teknologi informasi [1]. Dengan teknologi informasi, mampu mempermudah setiap kegiatan menjadi efektif dan efisien. Selain itu, teknologi informasi juga mampu memperoleh, mengelola, dan mengolah data dengan berbagai cara sehingga menghasilkan informasi berkualitas, seperti informasi yang relevan, akurat, dan tepat waktu. Informasi ini dapat digunakan untuk keperluan pribadi atau organisasi, serta dapat menjadi landasan strategis dalam pengambilan keputusan. Salah satu revolusi teknologi informasi yaitu Internet of Things (IoT). IoT menggambarkan objek jaringan yang mampu melakukan komunikasi data dengan dikontrol antara objek, sistem, ataupun server lain [2]. Hal ini mengacu pada konektivitas internet dari perangkat standar seperti komputer desktop, laptop, ponsel, dan tablet ke beberapa perangkat fisik atau objek sehari-hari yang menggunakan internet dengan atau tanpa akses manual [3]. *IoT* menjadi inovasi yang sering digunakan saat ini karena dampaknya yang banyak dan sangat memudahkan kehidupan sehari-hari maupun dunia kerja.

Dalam perkembangannya, inovasi teknologi informasi dan berbagai kemudahan yang ditawarkan tidak terlepas dari risiko. Risiko tersebut dapat didefinisikan sebagai kemungkinan munculnya ancaman atau dampak dari berbagai faktor yang dapat menimbulkan masalah, atau bahkan bahaya yang serius, terhadap proses bisnis yang berjalan [4]. Risiko-risiko ini memiliki potensi untuk mengganggu, menghambat, atau bahkan melumpuhkan aktivitas bisnis secara total, yang pada akhirnya dapat berujung pada kerugian besar bagi organisasi .

Berbagai faktor dapat menjadi sumber risiko dalam operasional pelayanan. Di antaranya adalah human error, yang bisa terjadi kapan saja dan menyebabkan gangguan signifikan; kejahatan siber (*cybercrime*), yang semakin meningkat seiring dengan ketergantungan pada teknologi digital; serta faktor-faktor lingkungan sekitar, seperti bencana alam atau perubahan kondisi fisik yang tidak terduga. Selain itu, masih ada risiko-risiko lain yang dapat mempengaruhi kelancaran dan optimalisasi dari proses bisnis yang sedang berlangsung. Jika tidak dikelola dengan baik, risiko-risiko ini dapat menyebabkan penurunan efisiensi, kehilangan data penting, kerusakan infrastruktur, atau bahkan kebangkrutan.

Mengingat potensi dampak yang besar tersebut, diperlukan upaya pengelolaan yang komprehensif melalui penerapan manajemen risiko. Manajemen risiko adalah pendekatan yang sistematis untuk mengidentifikasi, menganalisis, mengevaluasi,

DOI : http://dx.doi.org/10.32409/jikstik.23.4.3661, *) Penulis Korespondensi

dan mengantisipasi berbagai kemungkinan risiko yang dapat mengancam keberlangsungan proses bisnis. Dengan manajemen risiko yang baik, organisasi mampu mengenali sejak dini kemungkinan terjadinya masalah dalam proses bisnis, memahami akar penyebabnya, dan mengukur seberapa besar dampak yang mungkin terjadi. Selain itu, manajemen risiko juga memberikan kerangka kerja untuk mengevaluasi risiko-risiko tersebut, sehingga dapat diambil langkah-langkah preventif atau korektif yang tepat sebelum risiko-risiko tersebut berkembang menjadi masalah yang lebih besar.

Dengan demikian, penerapan manajemen risiko tidak hanya berfungsi sebagai alat untuk meminimalkan kerugian, tetapi juga sebagai mekanisme untuk memastikan bahwa setiap aspek dari proses bisnis dapat berjalan secara optimal, terlepas dari berbagai tantangan yang mungkin muncul. Dalam dunia bisnis yang semakin kompleks dan berisiko tinggi, manajemen risiko menjadi kunci untuk menjaga stabilitas operasional, meningkatkan daya tahan terhadap krisis, serta memberikan kepercayaan kepada para pemangku kepentingan bahwa organisasi siap menghadapi dan mengelola segala bentuk ancaman dengan efektif.

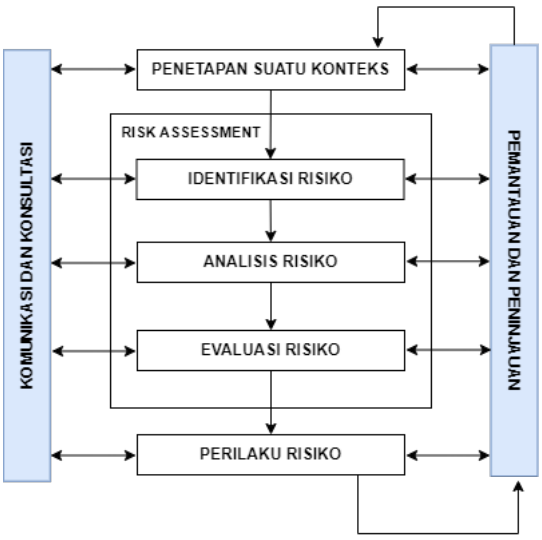
Beberapa penelitian sebelumnya yang membahas terkait dengan manajemen risiko TI yaitu penelitian pertama yang dilakukan Wirawan Harefa, dkk. Penelitian ini menjelaskan kemungkinan risiko yang dapat terjadi dari segi SI/TI dengan menggunakan framework ISO 31000. Dari 3 tahapan yaitu *Risk Identification, Risk Analyst*, dan *Risk Evaluation*. Maka didapati ada 26 risiko yang menyebabkan aplikasi ERP CV. Ribka Furniture terhambat dalam menjalankan bisnis yaitu 3 kemungkinan risiko tingkatan High, 13 kemungkinan risiko tingkatan Medium, dan 10 kemungkinan risiko tingkatan Low [5]. Penelitian kedua dilakukan oleh Ferro G Punusingon, dkk. Penelitian ini menggunakan kerangka kerja ISO 31000 dengan menerapkan beberapa tahapan yaitu identifikasi masalah, studi literatur, pengumpulan data, analisis risiko . Hasil yang ditemukan peneliti ada 14 kemungkinan risiko terdapat 4 tingkat Risk Level high, 4 tingkat Risk Level Medium, dan 6 tingkat Risk Level Low [6]. Penelitian ketiga dilakukan oleh Kristoforus Charmindo Delazega Jayonata, dkk. Analisis ini menerapkan 3 tahapan besar yaitu identifikasi risiko (*Risk Identification*), analisis risiko (Risk Analsyt), dan evaluasi risiko (*Risk Evaluation*), dan perlakuan risiko (*Risk Treatment*). Hasilnya ditemukan terdapat 21 kemungkinan risiko yang terbagi dalam 4 risiko level high, 7 risiko level medium, dan 10 risiko level low [7].

Instansi perguruan tinggi menjadi lembaga pendidik yang harus terus melakukan peningkatan pelayanan baik secara akademik maupun non-akademik bagi para civitas academica agar selalu merasa nyaman dan aman. Hal serupa juga terjadi di UKSW, salah satu upaya untuk memberi rasa aman maka kini pihak kampus telah menerapkan sistem IoT smart parking gate. Dengan sistem ini mampu melakukan tracking, menjaga keamanan, dan memberikan kenyamanan. Dalam penerapannya juga telah mendapatkan tanggapan positif dari para pengguna. Berdasarkan hal tersebut, penting bagi pemangku tanggung jawab untuk menerapkan manajemen risiko guna meminimalisir masalah di lapangan. Ketika sumber daya teknologi informasi terkena ancaman atau serangan secara internal atau eksternal, maka proses bisnis dapat berisiko mengalami gangguan dan bahkan penghentian aktivitas secara menyeluruh [8]. Oleh karena itu, penting untuk menghindari kerugian yang ditimbulkan bagi penggunaan *smart parking gate* UKSW, maka perlu dilakukannya evaluasi menggunakan manajemen risiko.

Berdasarkan dari beberapa penelitian sebelumnya terkait manajemen risiko maka penelitian ini akan melakukan analisis risiko dengan menerapkan kerangka kerja *International Organization for Standardization* (ISO) 31000 yang menjadi standar atau pedoman dalam melakukan manajemen risiko [9]. Dengan ISO 31000 menjadi kebijakan standar, instruksi, dan persyaratan bagi organisasi untuk memberikan landasan dan kerangka kerja bagi program manajemen risiko mereka. Tujuan dari standarisasi ini adalah untuk memberikan prinsip-prinsip dan bahan referensi kepada organisasi untuk program manajemen risiko [10]. Proses manajemen risiko mencakup penerapan yang sistematis dari kebijakan, prosedur, dan praktik dalam aktivitas komunikasi dan konsultasi, penetapan konteks, serta penilaian, peninjauan, hingga pelaporan risiko [11]. Penelitian terkait analisis risiko pada sistem smart parking gate belum pernah dilakukan oleh peneliti sebelumnya maka hasil dari penelitian ini diharapkan dapat menjadi acuan bagi pemangku tanggung jawab untuk dapat terus memperhatikan dan meningkatkan terus teknologi informasi, sehingga dapat memberikan pelayanan terbaik bagi civitas academica kampus. Selain itu, dapat menjadi acuan bagi penelitian-penelitian selanjutnya

Metode Penelitian

Penelitian yang dilakukan terkait manajemen risiko pada sistem smart parking gate UKSW menggunakan pendekatan *case study research*, yaitu pendekatan yang berfokus pada satu objek tertentu. Dalam penelitian ini, yang menjadi fokus utama adalah sistem *IoT* yang digunakan dalam sistem *smart parking gate*. Metode yang digunakan dalam penelitian ini adalah metode kualitatif, yang menekankan pada pentingnya pengumpulan data melalui observasi secara langsung di lapangan. Observasi ini dilakukan untuk memperoleh data asli yang akurat dan dapat dipertanggungjawabkan secara ilmiah. Dalam manajemen risiko, penelitian ini acuan untuk mengukur kemungkinan dan dampak risiko dapat lihat Gambar 1.



Gambar 1: Alur Proses ISO 31000

Tahapan awal dilakukan dengan penilaian risiko pada sistem *smart parking gate*, melakukan penilaian risiko dengan secara sistematis sesuai dengan pedoman analisis manajemen risiko ISO 31000 pada tahapan penilaian risiko terbagi lagi dalam beberapa tahapan yaitu :

1. Tahap Identifikasi Risiko (*Risk Identification*) Pada tahapan awal dalam melakukan penilaian risiko (Risk Assessment) akan dilakukan upaya pengumpulan informasi yang bertujuan untuk mengidentifikasi berbagai risiko yang mungkin akan timbul dalam kegiatan operasional yang dilakukan pemangku tanggung jawab sistem *parking gate* [12].

2. Tahap Analisis Risiko (*Risk Analyst*) Tahapan ini mempertimbangkan penilaian kemungkinan risiko dan jumlah dampak yang disebabkan oleh risiko [13]. Penentuan nilai ini akan didasari pada tabel Kriteria Kemungkinan (Likelihood). Tabel ini terdiri 5 kemungkinan yaitu : Jarang Sekali (*Rare*), Jarang Terjadi (*Unlikely*), Cukup Sering Terjadi (*Moderate*), Sering Terjadi (*Likely*) dan Selalu Terjadi (*Certain*) [10] lihat Tabel 1.

Tabel 1: Nilai Likelihood

Likelihood			
Nilai	**Kriteria**	**Deskripsi**	**Frekuensi Kejadian**
1	*Rare*	Risiko sangat jarang sekali terjadi	>2 Tahun
2	*Unlikely*	Risiko jarang sekali terjadi	1-2 Tahun
3	*Moderate*	Risko cukup sering sekali terjadi	7-12 Bulan
4	*Likely*	Risiko sering sekali terjadi	4-6 Bulan
5	*Certain*	Risiko pasti selalu terjadi	1-3 Bulan

Tahap selanjutnya dapat menentukan dampak (*Impact*) yang terjadi pada objek kasus terhadap kemungkinan risiko tersebut. Dampak dibedakan berdasarkan bagaimana akan mempengaruhi kerja sistem *smart parking gate* [6] lihat Tabel 2.

.

Tabel 2: Nilai Impact

Impact		
Nilai	**Kriteria**	**Deskripsi**
1	*Insignificant*	Risiko tidak mengganggu aktivitas dan proses bisnis pada instansi.
2	*Minor*	Aktivitas pada instansi sedikit terhambat, namun tidak mengganggu aktivitas inti pada instansi.
3	*Moderate*	Risiko tersebut mengganggu jalannya proses bisnis pada instansi, sehingga aktivitas bisnis sedikit terhambat.
4	*Major*	Risiko tersebut menghambat hampir seluruh jalannya proses bisnis pada instansi.
5	*Catastrophic*	Risiko mengganggu jalannya proses bisnis yang ada secara menyeluruh dan menghentikan aktivitas instansi secara total.

3. Tahap Evaluasi Risiko (*Risk Evalution*) Tahapan ketiga dalam penilaian risiko dengan mengevaluasi risiko. Dilakukan untuk menetapkan manajemen risiko dengan membandingkan tingkat risiko yang ada dengan standar yang ditentukan [7]. Berdasarkan pada skala prioritas risiko terendah hingga tertinggi. Evaluasi ini akan berdasarkan pengelompokkan dari *Likelihood* Tabel 1 dan impact Tabel 2 sebelumnya pada. Dalam penentuan ini akan menggunakan tabel matriks risiko sebagai pengukuran.

Hasil dan Pembahasan

Identifikasi Risiko

Tahapan pertama dalam proses manajemen risiko ini dimulai dengan mengidentifikasi berbagai aspek yang terkait dengan sistem *smart parking gate* UKSW. Tahap awal akan melibatkan wawancara mendalam dengan Kepala Bagian Direktorat Keamanan, Ketertiban, dan Data Siber (D2KDS) untuk mendapatkan informasi yang komprehensif mengenai kondisi sistem yang ada. Dalam proses ini, fokus utama akan diberikan pada tiga hal penting: pertama, identifikasi aset-aset yang terkait dengan sistem smart parking gate, termasuk perangkat keras, perangkat lunak, data, dan infrastruktur pendukung lainnya. Kedua, identifikasi berbagai kemungkinan risiko yang dapat muncul, seperti ancaman keamanan, gangguan operasional, atau potensi kegagalan sistem. Ketiga, penilaian dampak yang mungkin ditimbulkan oleh risiko-

risiko tersebut terhadap operasional sistem, keamanan data, serta kenyamanan pengguna. Dengan demikian, tahapan ini akan memberikan landasan yang kuat untuk langkah-langkah mitigasi risiko selanjutnya yang akan diterapkan dalam upaya menjaga keandalan dan keamanan sistem *smart parking gate* di UKSW.

Identifikasi Aset

Tahapan ini akan dilakukan identifikasi terkait aset-aset diantaranya ada data, perangkat lunak (*Software*) dan perangkat kerang (*Hardware*) lihat Tabel 3.

.

Tabel 3: Identifikasi Aset

Komponen SI/TI	Aset
Data	Data mahasiswa, Data pegawai
Software	Parkways
Hardware	Komputer, keyboard, mouse, processor

Dari hasil yang ada pada identifikasi aset sistem *smart parking gate* UKSW terdapat aset-aset penting diantaranya terdapat data mahasiswa dan pegawai,U software parkways, hardware seperti komputer, keyboard, mouse, dan processor.

.

Tabel 4: Identifikasi Kemungkinan Risiko

ID	Kemungkinan Risiko
R01	Bencana Alam
R02	Kebakaran
R03	Human Error
R04	Penyalahgunaan Hak Akses
R05	Kurangnya Tenaga SDM
R06	Gagal Backup/Backup Failure
R07	Data Corrupt
R08	Sistem Crash
R09	Overhead
R10	Overload
R11	Debu/Kotoran
R12	Kegagalan Update
R13	Koneksi Tidak Stabil
R14	Kerusakan Hardware
R15	Listrik Padam
R16	Maintance Tidak Terjadwal
R17	Database Tidak Sinkron dengan Sistem

Identifikasi Kemungkinan Risiko

Setelah langkah awal berupa identifikasi aset berhasil dilakukan, tahapan selanjutnya dalam proses manajemen risiko adalah mengidentifikasi kemungkinan dan dampak dari berbagai risiko yang mungkin terjadi. Identifikasi ini dilakukan dengan tujuan untuk menemukan dan memahami secara mendalam berbagai potensi risiko yang dapat timbul dari berbagai faktor, baik internal maupun eksternal, yang dapat mempengaruhi kelangsungan dan keamanan operasional sistem. Dalam proses ini, risiko-risiko yang diidentifikasi mencakup berbagai aspek, termasuk faktor alam atau lingkungan, manusia, sistem dan infrastruktur. Semua potensi risiko ini dianalisis dengan cermat untuk menilai sejauh mana dampaknya terhadap operasional sistem secara keseluruhan. Hasil dari identifikasi kemungkinan risiko dan dampaknya ini disusun dalam lihat Tabel 4.

Dari identifikasi kemungkinana ditemukan faktor-faktor yang mempengaruhi penggunaan sistem *smart parking gate* UKSW. Terindentifikasi faktor alam atau lingkungan memiliki 2 kemungkinan, faktor manusia memiliki 3 kemungkinan, dan faktor sistem atau infrastruktur memiliki 12 kemungkinan yang dapar mengganggu kegiatan oprasional setiap harinya.

Tabel 5: Identifikasi Dampak Risiko

ID	Identifikasi Risiko	Dampak
R01	Bencana Alam	Merusak gedung, fasilitas, dan kerugian secara finansial
R02	Kebakaran	Merusak infrastruktur, proses pelayanan terhenti, kerugian secara finansial
R03	Human Error	Tidak dapat menjalankan sistem dan mengganggu pelayanan
R04	Penyalahgunaan Hak Akses	Kehilangan data dan kebocoran informasi
R05	Kurang Tenaga SDM	Pelayanan menjadi relatif lambat
R06	Gagal Backup/Backup Failure	Kehilangan data dan tidak lengkap
R07	Data Corrupt	Kehilangan informasi penting, gangguan operasional, kerugian finansial, krisisnya kepercayaan
R08	Sistem Crash	Kerusakan sistem sehingga tidak dapat diakses dalam jangka waktu sementara
R09	Overhead	Kinerja hardware tidak optimal dan mengalami kerusakan akibat suhu yang panas
R10	Overload	Data hilang dan proses loading menjadi lambat
R11	Debu/Kotoran	Hardware dapat mengalami kerusakan
R12	Kegagalan Update	Tidak dapat beroperasi secara optimal karena tidak sesuai kebutuhan
R13	Koneksi Tidak Stabil	Gagal melakukan koneksi dengan database
R14	Kerusakan Hardware	Menghambat proses pelayanan dan kerugian secara finansial
R15	Listrik Padam	Proses pelayanan tidak dapat berjalan optimal terhenti sementara
R16	Maintenance Tidak Terjadwal	Melemahnya kemampuan atau daya komputasi dan database
R17	Database Tidak Sinkron Dengan Sistem	Mengakibatkan sistem sensor parking tidak mampu membaca data

Identifikasi Dampak Risiko

Berdasarkan hasil pada tahap identifikasi kemungkinan risiko, maka ditemukan bahwa terdapat 17 kemungkinan risiko yang berpotensi terjadi pada sistem *smart parking gate* di UKSW. Setiap risiko yang teridentifikasi ini mencakup berbagai aspek,

mulai dari gangguan teknis hingga ancaman keamanan yang dapat mempengaruhi operasional sistem secara keseluruhan. Proses ini akan berlanjut dengan analisis mendalam terhadap dampak dari masing-masing dari 17 risiko tersebut. Tujuan identifikasi ini untuk memahami secara detail konsekuensi yang mungkin dihadapi jika risiko-risiko ini benar-benar terjadi. Dampak yang dianalisis akan mencakup berbagai dimensi, seperti kerugian operasional, penurunan efisiensi, gangguan terhadap keamanan data, serta potensi kerugian finansial atau reputasi bagi institusi. Semua hasil analisis dampak dari risiko-risiko tersebut akan disusun secara sistematis lihat Tabel 5.

Dari 17 risiko di identifikasi memiliki risiko dan beberapa diantara dapat menyebabkan masalah serius dapat mengganggu aktivitas. kerusakan secara fisik, dapat menjadi hambatan kinerja oprasional. Selai iru terdapat ancaman keamanan informasi dan data serta kerusakan pada *hardware.*

Analisis Resiko

Dari tahap identifikasi aset, kemungkinan, beserta dampak risiko maka dapat dilakukan proses analisis risiko yang berdasarkan pada penentuan nilai kemungkinan *(Likelihood)* dan dampak *(impact)* lihat Tabel 6.

Tabel 6: Analisis Nilai Likelihood dan Impact

ID	Kemungkinan Risiko	*Likelihood*	*Impact*
R01	Bencana Alam	1	5
R02	Kebakaran	1	5
R03	Human Error	4	3
R04	Penyalahgunaan Hak Akses	2	2
R05	Kurang Tenaga SDM	4	3
R06	Gagal Backup/Backup Failure	5	2
R07	Data Corrupt	3	5
R08	Sistem Crash	4	4
R09	Overhead	5	1
R10	Overload	2	3
R11	Debu/Kotoran	4	1
R12	Kegagalan Update	2	3
R13	Koneksi Tidak Stabil	3	1
R14	Kerusakan Hardware	2	4
R15	Listrik Padam	5	3
R16	Maintenance Tidak Terjadwal	4	5
R17	Database Tidak Sinkron Dengan Sistem	2	4

Tabel 7: Matriks Evaluasi Risiko

Likelyhood							
	Certain	5	**R09**	**R06**	**R15**		
	Likely	4	**R11**		**R03, R05**	**R08**	**R16**
	Moderate	3	**R13**				**R07**
	Unlikely	2		**R04**	**R10, R12**	**R14, R17**	
	Rare	1					**R01, R02**
Impact			1	2	3	4	5
			Insignificant	*Minor*	*Moderate*	*Major*	*Catastrophic*

Evaluasi Risiko

Tahapan akhir dalam proses penilaian risiko adalah melakukan evaluasi risiko, yang merupakan langkah krusial dalam menentukan bagaimana organisasi akan mengelola dan merespon berbagai ancaman yang telah diidentifikasi. Pada tahap ini, dilakukan pemetaan risiko dari setiap risiko yang telah teridentifikasi sebelumnya maka memperoleh dari hasil lihat Tabel 7.

Tabel 8: Usulan Perlakuan Risiko

ID	Identifikasi Risiko	*Risk Level*	Tindakan Risiko
R07	*Data Corrupt*		Melakukan penyimpanan data dengan baik dan backup secara berkala min 1 bulan skali.
R08	Sistem Crash		Membuat jadwal *maintance* untuk sistem dan backup secara berulang-ulang.
R15	Listrik Padam		Menyediakan fasilitas genset.
R16	*Maintenance Tidak Terjadwal*		*Melakukan penjadwalan maintenance secara rutin min 1 bulan skali.*
R01	Bencana Alam		Menaruh hardware pada tempat yang lebih aman, tinggi, terhindar dari benda-benda yang mungkin dapat terjatuh meinpah hardware.
R02	Kebakaran		Menyediakan 1-2 alat pemadam kebakaran di setiap ruangan
R03	*Human Error*		Memberikan pelatihan terhadap karyawan sesuai Kemampuan dan menerapkan SOP
R05	Kurangnya Tenaga SDM		Menambah pegawai khusus menangani sistem *smart parking gate*
R06	Gagal *Backup/Backup Failure*		Pastikan penggunaan memori selalu di bawah kapasitas maks dan lakukan *maintance* data rutin min 1 bulan skali
R09	*Overhead*		Menjaga ruangan dingin dan memiliki sirkulasi udara yang cukup baik
R10	*Overload*		Melakukan maintance data secara berkala dan sering min 1 bulan skali
R12	Kegagalan Update		Dapat melakukan request kepada pengampu tanggung jawab untuk menambah fitur yang dibutuhkan atau menambah pegawai khusus menangani bagian ini
R14	Kerusakan *Hardware*		Melakukan perawatan secara berkala dan membeli hardware berkualitas
R17	Database Tidak Sinkron Dengan Sistem		Menerapkan sistem monitoring, backup, dan optimalkan koneksi
R11	Debu/Kotoran		Menjaga kebersihan untuk meminimalisir kerusakan dengan rutin membersihkan sebeluan 2x
R04	Penyalahgunaan Hak Akses		Melakukan penggantian hak akses secara berkala min 3 bulan sekali
R13	Koneksi Tidak Stabil		Menerapkan metode retry otomatis, penggunaan bandwidth atau buffering, dan peningkatan jaringan

Berdasarkan hasil pemetaan kemungkinan risiko yang telah disusun dalam tabel matriks evaluasi risiko, dipetakkan dalam tabel matriks evaluasi risiko dilakukan pengelompokan terhadap 17 kemungkinan risiko yang teridentifikasi Risiko-risiko ini dikelompokkan ke dalam tiga tingkatan utama,

yaitu *High* (tinggi), *Medium* (sedang), dan *Low* (rendah), berdasarkan probabilitas terjadinya serta potensi dampak yang mungkin ditimbulkan. Tahapan ini diharapkan dapat memberikan saran yang tepat mengenai langkah-langkah yang perlu diambil untuk meminimalisir kemungkinan dan dampak risiko yang mungkin dapat terjadi lihat Tabel 8.

Tabel 8 memberikan rekomendasi perlakuan risiko yang dapat menghambat operasional, dengan menekankan pada risiko-risiko yang telah diidentifikasi dalam sistem *smart parking gate* UKSW. Rekomendasi ini mencakup berbagai aspek, seperti memastikan ketersediaan dan keandalan jaringan, menjaga kontinuitas operasional, melindungi data dari ancaman, dan meningkatkan efisiensi sistem. Penelitian ini menyoroti langkah-langkah untuk pengelolaan dan pemeliharaan infrastruktur teknologi informasi.

Penutup

Berdasarkan tahapan-tahapan penilaian risiko (Risk Assessment) pada sistem s*mart parking gate* di UKSW yang sudah dilakukan sesuai dengan standar International Organization for Standardization ISO 31000. Dengan melewati proses analisis risiko yang dilakukan melalui 3 langkah dalam tahapan evaluasi risiko, yaitu risk identification, risk analysis, dan risk evaluation. Pada tahapan ini dilakukan juga proses perlakuan risiko dengan memberikan saran pencegahan akan kemungkinan dan dampak risiko-risiko tersebut. Hasil yang didapatkan dari Analisis Manajemen Risiko dengan menggunakan framework ISO 31000 pada sistem *smart parking gate* di UKSW teridentifikasi memiliki 17 kemungkinan risiko yang dapat terjadi diantaranya 4 kemungkinan level risiko high, 10 kemungkinan level risiko medium, dan 3 kemungkinan level risiko low. Tingkatan risiko yang tinggi merupakan tingkat risiko yang pasti akan terjadi secara langsung dan mempengaruhi kegiatan pelayanan. Dari hasil ini selanjutnya, Diharapkan dapat menjadi acuan tolak ukur bagi pengampu sistem *smart parking gate* di UKSW untuk terus dapat berbena dan memberikan pelayanan yang terbaik bagi civitas academica.

Ucapan Terimakasih

Ucapan terima kasih kepada Bapak/Ibu atas dukungan, bimbingan, dan fasilitas yang diberikan selama proses penelitian ini. Terima kasih juga kepada semua pihak-pihak yang sudah ikut berkontribusi dan masukan berharga yang membantu penyelesaian penelitian ini.

Daftar Pustaka

[1] Anindhita Ari Putri dan Deva Istifadhah Irnanda Syafi'i, "Analisis Risiko Teknologi Informasi menggunakan ISO31000 (Studi Kasus: Aplikasi J&T Express Indonesia)", Aisyah Journal of Informatics and Electrical Engineering, vol. 4, no. 1, 2022.

[2] A. Nurain, R. A. G. Gultom, dan R. E. Indrajit, "Manajemen Ketahanan Risiko Siber pada Internet of Things dan Cyber Physical System", Journal on Education, vol. 06, no. 02, pp. 13271–13281, 2024.

[3] N. Nasution, M. Rizal, D. Setiawan, dan M. A. Hasan, "IoT Dalam Agrobisnis Studi Kasus : Tanaman Selada Dalam Green House", IT Journal Research and Development, vol. 4, no. 2, Oct. 2019, doi: 10.25299/itjrd.2020.vol4(2).3357.

[4] T. Widy Chrisanty dan J. Tambotoh, "Analisis Manajemen Risiko Sistem Informasi Menggunakan ISO 31000:2018 di PT. XYZ", ZONASI : Jurnal Sistem Informasi, vol. 5, no. 2, pp. 372-381, 2018.

[5] W. Harefa dan K. D. Hartomo, "Analisis Manajemen Risiko Dengan Menggunakan Framework ISO 31000:2018 Pada Sistem Informasi Gudang", JATISI : Jurnal Teknik Informatika dan Sistem Informasi, vol. 9, no. 1, pp. 407-420, 2022.

[6] F. G. Punusingon dan M. N. N Sitokdana, "Analisis Manajemen Risiko Aplikasi Simfoni pada Dinas PPA di Kab. Minahasa Tenggara Menggunakan ISO 31000", ZONASI : Jurnal Sistem Informasi, vol. 4, no. 2, pp 26-38, 2022.

[7] K. C. D. Jayonata dan M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi Menggunakan ISO31000 pada Aplikasi CUPK Mobile (Studi Kasus: KSP CU Pancur Kasih)", JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika), vol. 9, no. 1, pp. 16–25, doi: 10.29100/jipi.v9i1.4291, Feb. 2024.

[8] M. I. Fachrezi, A. Dwika Cahyono, dan P. F. Tanaem, "Manajemen Risiko Keamanan Aset Teknologi Informasi Menggunakan ISO 31000:2018 Diskominfo Kota Salatiga", JATISI (Jurnal Teknik Informatika dan Sistem Informasi), vol. 8, no. 2, 2021.

[9] D. Yudha Andika dan A. Fritz Wijaya, "Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000:2018 pada PT. Trust Lerinvital Timur", Mnemonic: Jurnal Teknik Informatika, Vol. 5, no. 2, 2022.

[10] S. P. Zagoto dan M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi di Organisasi XTZ Cabang Salatiga Menggunakan ISO 31000 ", Mnemonic: Jurnal Teknik Informatika, vol. 4, no. 1, 2021.

[11] H. I. Pribadi dan E. Ernastuti, "Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000:2018 Dengan

FMEA (Studi Kasus PT Pertamina)", Jurnal Sistem Informasi Bisnis , vol. 10, no. 1, pp. 28–35, doi: 10.21456/vol10iss1pp28-35, May 2020.

[12] Syahrul Syahrul, Ramdan Satra, dan Farniwati Fattah, "Analisis Risiko Sistem Informasi Menggunakan ISO 31000 Sebagai Upaya Manajemen Risiko", Buletin Sistem Informasi dan Teknologi Islam, vol. 4, no. 1, pp. 51–58, 2023.

[13] J. Rambi dan M. Sitokdana, "Analisis Manajemen Resiko Aplikasi Rene Kasir Di Restoran Oemah Djari Salatiga Menggunakan ISO 31000", Journal of Computer and Information Systems Ampera, vol. 3, no. 2, 2022.

Halaman ini sengaja dikosongkan.