PERANCANGAN MANAJEMEN RISIKO KEAMANAN INFORMASI PADA ASET IT PT. SUPER PEMBAYARAN INDONESIA BERDASARKAN ISO/IEC27005:2022

1st Muh. Alfian Asri
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
alfianasri@student.telkomuniversity.ac.id

2nd Ryan Adhitya Nugraha
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
ranugraha@telkomuniversity.ac.id

3rd Widyatasya Agustika Nurtrisha
Fakultas Rekayasa Industri
Universitas Telkom
Bandung, Indonesia
nurtrisha@telkomuniversity.ac.id

Penelitian ini bertujuan untuk menganalisis dan menerapkan ISO/IEC 27005:2022 dalam manajemen risiko keamanan informasi pada aset IT di PT. Super Pembayaran Indonesia (PT. SPI). Saat ini, PT. SPI memiliki manajemen risiko yang belum terstruktur khususnya terkait dengan aset IT, seperti *hardware*, *software*, dan data sensitif yang akan sangat berisiko terhadap operasional dan reputasi perusahaan. Penelitian ini melakukan evaluasi terhadap risiko yang ada pada aset IT PT. SPI dengan mengacu pada tahapan *Context Establishment, Risk Assessment, dan Risk Treatment* berdasarkan ISO/IEC27005:2022. Hasil evaluasi menunjukkan bahwa perusahaan memiliki 47 risiko untuk ditangani. Dari 47 risiko tersebut, penelitian ini mengidentifikasi 9 risiko dengan grade A sebagai prioritas utama yang perlu segera ditangani. Risiko-risiko ini mencakup ancaman pada aset utama dan perangkat keras yang dapat mempengaruhi data sensitif serta infrastruktur fisik perusahaan. Rekomendasi mitigasi yang diberikan mengacu pada kontrol annex A pada ISO/IEC/ IEC 27001:2022 yang mencakup langkah-langkah penting seperti peningkatan kontrol akses, penggunaan enkripsi untuk data sensitif, serta penguatan pengamanan infrastruktur fisik untuk mencegah kerusakan dan kebocoran data. Penelitian ini juga memberikan panduan yang berharga bagi perusahaan fintech lainnya dalam meningkatkan manajemen risiko keamanan informasi di dunia digital yang terus berkembang.

Kata kunci : Manajemen Risiko, Keamanan Informasi, ISO/IEC27005:2022, ISO/IEC27001:2022, Aset IT, PT. Super Pembayaran Indonesia, *Fintech*.

I. PENDAHULUAN

Digitalisasi yang semakin pesat menimbulkan berbagai ancaman siber sehingga perusahaan perlu untuk menyiapkan startegi mitigasi yang efektif [1]. Menurut laporan dari Badan Siber dan Sandi negara, tercatat bahwa pada tahun 2023 ditemukan 279,84 juta serangan siber dan dalam paruh kedua 2023, tercatat 43 serangan siber per detik di berbagai sektor, termasuk pemerintahan dan perusahaan [2]. PT. SPI sebagai perusahaan yang beroperasi di bidang solusi pembayaran digital sejenis *fintech* menghadapi tantangan besar dalam memastikan keamanan informasi dan aset IT termasuk data konfidensial yang mereka kelola. Beberapa regulasi nasional juga mengatur terkait manajemen risiko IT di sektor jasa keuangan atau bermitra dengan bank seperti, POJK No. 38/POJK.03/2016 [3], PBI No. 9/15/2007 [4] dan PP N0.71 Tahun 2019 terkait PSTE [5]. PT. SPI yang belum menerapkan standar manajemen risiko IT khususnya pada aset IT sangat berisiko untuk mengalami kerugian dari segi finansial dan reputasi perusahaan.

Penerapan standar internasional seperti ISO/IEC 27005:2022 menjadi penting bagi PT. SPI yang belum menerapkan Sistem Manajemen Keamanan Informasi (SMKI). ISO/IEC 27005:2022 memberikan pedoman yang komprehensif untuk manajemen risiko keamanan informasi, khususnya dalam pengelolaan aset IT. Standar ini membantu perusahaan untuk mengidentifikasi, menganalisis, dan mengelola risiko yang terkait dengan aset teknologi informasi yang ada, serta untuk meningkatkan ketahanan terhadap ancaman siber. Penerapan ISO/IEC 27005:2022 diharapkan dapat memperkuat perlindungan data sensitif dan membangun kepercayaan klien serta mitra bisnis.

Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis dan menerapkan ISO/IEC 27005:2022 sebagai metode untuk mengidentifikasi, menganalisis, mengevaluasi, dan mengelola risiko keamanan informasi, terutama pada aset IT di PT. SPI. Fokus utama dari penelitian ini adalah pada tahapan *Context Establishment, Risk Assessment*, dan *Risk Treatment* yang berhubungan dengan pengelolaan risiko keamanan informasi di perusahaan. Dengan demikian, penelitian ini bertujuan untuk memberikan wawasan yang lebih baik bagi manajemen PT. SPI dalam mengambil keputusan strategis yang berbasis informasi terkait keamanan sistem informasi. Selain itu, hasil dari penelitian ini juga diharapkan dapat memberikan kontribusi signifikan terhadap praktik manajemen risiko di sektor *fintech*, khususnya dalam menghadapi tantangan yang ada di dunia digital.

Penelitian ini menggunakan pendekatan **Design Science Research (DSR)** yang berfokus pada penciptaan dan evaluasi solusi untuk mengatasi masalah pengelolaan risiko keamanan informasi [6]. Metode penelitian yang diterapkan bersifat kualitatif, dengan pengumpulan data melalui wawancara, observasi, dan analisis dokumen perusahaan. Wawancara dilakukan dengan pihak terkait, seperti Kepala Unit Sistem Informasi PT. SPI, untuk menggali kondisi pengelolaan risiko yang ada, sementara analisis dokumen termasuk kebijakan, aset IT, dan struktur organisasi dilakukan untuk memperkaya pemahaman. Data yang dikumpulkan kemudian dianalisis menggunakan perangkat lunak untuk memvisualisasikan dan mengelompokkan risiko, serta mengembangkan rekomendasi mitigasi berdasarkan kerangka ISO/IEC 27005:2022. Pendekatan ini memungkinkan peneliti untuk memberikan solusi praktis yang relevan bagi perusahaan dan memberikan kontribusi bagi pengembangan manajemen risiko di sektor *fintech*.

II. KAJIAN TEORI

A. Keamanan Sistem Informasi

Keamanan sistem informasi didefinisikan sebagai upaya untuk melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, pengoperasian, modifikasi, atau penghancuran oleh pihak yang tidak berwenang, guna menjaga kerahasiaan, integritas, dan ketersediaan informasi [7].

B. Manajemen Risiko

Manajemen risiko adalah bentuk upaya terstruktur untuk mengidentifikasi, menganalisis dan memonitor risiko serta melindungi aset organisasi. Dalam aspek IT, penggunaan IT dalam suatu organisasi memunculkan beragam risiko. Risiko terdiri dari segala peristiwa yang berkaitan dengan implementasi IT yang dapat menimbulkan suatu risiko [8].

C. Manajemen Risiko Pada Perusahaan *Fintech*

Kematangan manajemen risiko perusahaan *fintech* di Indonesia, dengan menggunakan *Risk and Insurance Management Society - Risk Maturity Model* mengungkapkan sumber utama kematangan manajemen risiko perusahaan, serta masalah dalam menjalankan manajemen risiko yang berkualitas. Studi ini merekomendasikan peningkatan praktik manajemen risiko perusahaan, menyoroti pentingnya pendekatan yang terstruktur dan proaktif [9].

D. Aset IT

Aset adalah sumber daya ekonomi yang dimiliki dan/atau dikuasai oleh pemerintah sebagai hasil dari peristiwa masa lalu, di mana manfaat ekonomi dan sosial di masa depan diharapkan dapat diperoleh oleh pemerintah maupun Masyarakat [10]. Aset informasi, sebagai bagian inti dari aset IT, mencakup data dan informasi yang relevan dengan proses bisnis organisasi [11]. Adapun aset IT yang mencakup *hardware*, *software* dan data merupakan elemen penting dalam operasional PT. SPI. Risiko yang mengancam aset ini sangat bervariasi, mulai dari kerusakan fisik, kebocoran data, hingga pencurian informasi.

E. ISO/IEC 27005:2022

ISO/IEC 27005:2022 merupakan standar internasional yang berfokus pada penanganan proses Manajemen Risiko Keamanan Informasi (ISRM) berupa dokumen yang diterbitkan oleh *International Standard Organization* (ISO/IEC) dan *International Electrotechnical Commission* (IEC) yang bertujuan untuk mendukung organisasi/perusahaan di seluruh belahan dunia dalam pengelolaan risiko siber [12]. Pada penelitian ini, proses manajemen risiko keamanan informasi dibatasi hanya pada tahap *Context Establishment, Risk Assessment* dan *Risk Treatment*.

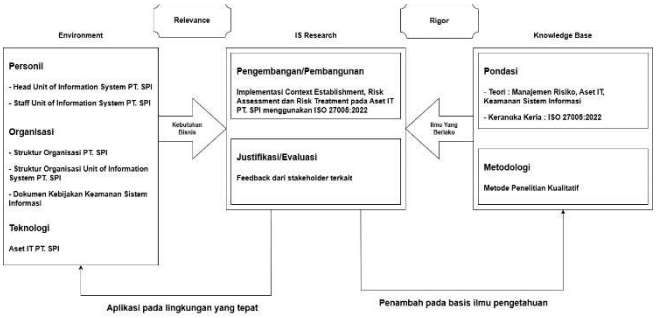
F. Alasan Pemilihan Kerangka Kerja

ISO/IEC 27005:2022 adalah opsi yang terbaik dengan mempertimbangkan kebutuhan penelitian ini. Kerangka kerja ini menyediakan pendekatan komprehensif dan berkelanjutan untuk manajemen risiko aset IT. Ini fleksibel untuk disesuaikan dengan berbagai situasi bisnis. ISO/IEC 27005:2022 adalah kerangka kerja yang ideal untuk mencapai tujuan penelitian ini dalam pengelolaan risiko keamanan informasi aset IT karena mencakup pedoman khusus yang berkaitan dengan aset IT, yang memungkinkan penelitian ini berkonsentrasi pada analisis risiko yang mendalam terhadap aset-aset tersebut tanpa meluas ke area tata kelola strategis atau kontrol teknis yang berlebihan.

III. METODE

A. Model Konseptual

Model konseptual adalah alat atau kerangka kerja yang penting dalam proses penelitian, karena membantu peneliti mengorganisir pemikiran, memandu penyelidikan dan mengkomunikasikan temuan mereka dengan cara yang jelas dan koheren [13]. Pada penelitian ini, penulis menggunakan *Design Science Research* yang berfokus pada penciptaan dan evaluasi artefak yang inovatif untuk mengatasi masalah tertentu. Pendekatan pemecahan masalah ini mampu merincikan kinerja penelitian melalui ilmu desain dalam sistem informasi secara ringkas dan memiliki panduan yang jelas dalam pemahaman, pelaksanaan dan evaluasi penelitian melalui kerangka konseptual [6].



Gambar 1 Model Konseptual DSR

Aspek pertama, *Environment*, menggambarkan konteks organisasi tempat penelitian dilakukan, dengan fokus pada *Head Unit of Information System* PT. SPI dan staf yang mendukung implementasi sistem. Struktur organisasi PT. SPI dan kebijakan keamanan sistem informasi menjadi dasar untuk pengelolaan aset informasi, sementara teknologi seperti aplikasi dan infrastruktur mendukung operasional sistem. Masalah utama yang dihadapi adalah pengelolaan risiko keamanan aset IT dan rekomendasi strategi untuk meningkatkan manajemennya.

Aspek kedua, *IS Research*, berfokus pada pengembangan dan evaluasi solusi. Penelitian ini mengimplementasikan *Context Establishment, Risk Assessment, dan Risk Treatment* berdasarkan ISO/IEC 27005:2022 pada aset IT PT. SPI. Tujuan dari proses ini adalah mengidentifikasi, mengevaluasi, dan merancang tindakan mitigasi yang sesuai, dengan umpan balik dari stakeholder untuk memastikan solusi relevan dan efektif dalam konteks organisasi.

Aspek terakhir, *Knowledge Base*, memberikan landasan teoritis dan metodologis untuk penelitian ini. Berdasarkan teori manajemen risiko, pengelolaan aset IT, dan ISO/IEC 27005:2022, penelitian ini menggunakan pendekatan kualitatif untuk menganalisis data dan konteks organisasi, serta merancang solusi berbasis praktik terbaik. *Knowledge Base* memperkuat validitas penelitian dan memberikan kontribusi pada pengembangan pengetahuan di bidang keamanan informasi.

B. Sistematika Penyelesaian Masalah

Sistematika penyelesaian masalah adalah proses atau tahapan yang terstruktur dan terorganisir yang digunakan untuk mengidentifikasi dan menyelesaikan suatu masalah. Pada penelitian ini, peneliti menggunakan 4 tahapan pemecahan masalah dalam menyusun rekomendasi panduan manajemen risiko keamanan informasi aset IT pada PT. SPI, di antaranya inisiasi, pengumpulan data dan penilaian risiko (*risk assessment*) serta kesimpulan dan saran (*risk treatment*).

Gambar 2 Diagram Alur Penyelesaian Masalah

C. Pengumpulan Data

Pada tahap pengumpulan data, data yang dibutuhkan terdiri dari data primer dan data sekunder. Data primer didapatkan dengan melakukan wawancara ke pihak *Unit Information System* untuk mengetahui pengelolaan risiko keamanan informasi yang diterapkan oleh perusahaan dan melakukan validasi terkait dokumen yang telah dianalisis sebelumnya.

Adapun untuk data sekunder, peneliti berfokus pada analisis dokumen-dokumen perusahan, wawancara yang dilakukan ke pihak-pihak terkait serta studi pustaka untuk mengumpulkan informasi yang dapat mendukung penelitian ini.

Dokumen yang akan dianilisis meliputi, dokumen daftar aset IT perusahaan, dokumen kebijakan keamanan informasi, dokumen struktural perusahaan secara umum dan spesifik di Unit Information System dan dokumen lainnya yang terkait. Data sekunder berikutnya dikumpulkan melalui proses pengumpulan data dilakukan secara kualitatif melalui studi pustaka melalui buku, jurnal maupun artikel sebelumnya yang relevan sebagai acuan dalam menentukan alur penelitian ini.

D. Pengolahan Data

Penelitian ini dimulai dengan pengumpulan data mentah dari berbagai sumber, termasuk dokumen perusahaan, wawancara dengan narasumber, dan observasi langsung terhadap aset IT PT. SPI. Data tersebut kemudian dirapikan melalui penyusunan ulang dokumen, transkripsi wawancara, dan pengorganisasian hasil observasi. Selanjutnya, data diklasifikasikan dalam kategori relevan seperti aset IT, kebijakan keamanan informasi, dan kerentanan yang teridentifikasi, dengan tujuan memetakan data sesuai dengan kerangka kerja ISO/IEC 27005:2022.

Pada tahap analisis, penulis menggunakan pendekatan kualitatif untuk menilai risiko berdasarkan skala low, medium, dan high sesuai ISO/IEC 27005:2022. Data yang telah diklasifikasikan dikelompokkan dan divisualisasikan menggunakan perangkat lunak seperti Microsoft Excel, dengan pembuatan diagram dan matriks risiko. Tahapan Context Establishment, Risk Assessment, dan Risk Treatment juga dimodelkan untuk mengidentifikasi ancaman, kerentanan, dan rekomendasi mitigasi risiko.

Dengan proses pengolahan data yang berbasis pada ISO/IEC 27005:2022, penelitian ini diharapkan dapat memberikan kontribusi penting dalam pengelolaan risiko keamanan informasi dan memberikan rekomendasi mitigasi yang efektif bagi PT. SPI.

IV. HASIL DAN PEMBAHASAN

A. *Context Establishment*

Pada tahap penetapan konteks (*Context Establishment)*, peneliti membuat batasan ruang lingkup sebagai acuan dalam pelaksanaan proses *risk assessment*. Penilaian risiko difokuskan pada infrastruktur IT yang dimiliki oleh PT. SPI, dengan titik berat pada aset-aset IT perusahaan yang bersifat fundamental. Aset tersebut mencakup aset utama (data, informasi, dokumen) dan aset pendukung mencakup perangkat lunak (*software*) dan perangkat keras (*hardware*) yang memiliki peran penting dalam keberlangsungan operasional bisnis perusahaan.

Tabel 1 Klasifikasi Aset

No	Kategori Aset	Jenis Aset
1	Aset Utama	• Data • Informasi • Dokumen
2	Aset Pendukung	• *Hardware* • *Software*

Langkah selanjutnya, menyusun kriteria penilaian risiko berdasarkan hasil analisis dua paramater utama, yaitu tingkat kemungkinan terjadinya risiko (*likelihood*) dan tingkat dampak risiko terhadap perusahaan (*impact*). Penetapan kriteria ini menjadi acuan dalam proses evaluasi dan perhitungan tingkat risiko terhadap masing-masing aset IT.

Kriteria tingkat kemungkinan risiko (*likelihood*) merupakan klasifikasi tingkatan berdasarkan kemungkinan terkecil sampai terbesar dari sebuah risiko terjadi. Berikut *likelihood* yang disusun oleh penulis mengacu pada ISO/IEC 27005:2022 dan referensi dari jurnal yang relevan [14] untuk diterapkan oleh perusahaan terdapat pada Tabel 2 di bawah :

Tabel 2 Tingkat Kemungkinan Risiko (*Likelihood*)

Level	Kemungkinan	Deskripsi
1	Sangat Rendah	Kemungkinan terjadinya kecil yaitu 1 kali dalam setahun pada beberapa kondisi yang tidak normal atau tidak pernah terjadi sama sekali pada beberapa kondisi. Presentasi kemungkinan terjadinya adalah ≤10%.
2	Rendah	Kemungkinan terjadinya kecil yaitu 1 – 2 kali dalam setahun pada banyak keadaan dengan tingkat presentasi kemungkinan terjadinya adalah 13% > x ≤ 25% dalam setahun.
3	Sedang	Pada setiap kondisi atau keadaan kemungkinan terjadi yaitu 4-8 kali dengan tingkat presentasi kemungkinan terjadinya adalah 25% > x ≤ 35% dalam setahun.
4	Tinggi	Akan ada kemungkinan terjadi dalam 1 tahun sebanyak >15 kali pada setiap kondisi atau banyak keadaan. Persentasi kemungkinan terjadinya adalah 35% > x ≤ 65%.
5	Sangat Tinggi	Kemungkinan terjadi dapat berturut-turut pada banyak keadaan atau kondisi.Persentasi kemungkinan terjadi dalam 1 tahun >65%.

Adapun kriteria dampak risiko merupakan klasifikasi tingkatan dampak risiko terhadap aspek tertentu yang menjadi prioritas bisnis perusahaan. Berikut penentuan *impact* yang telah disusun oleh penulis mengacu pada ISO/IEC 27005:2022 dan studi literatur yang relevan [14] dan hasil rekomendasi dari pihak perusahaan untuk diterapkan oleh perusahaan terdapat pada Tabel 3 di bawah :

Tabel 3 Tingkat Dampak Risiko (*Impact*)

Level	Dampak	Deskripsi
1	Sangat Ringan	Tidak ada pengaruh yang signifikan terhadap proses kegiatan operasional serta tidak mengancam atau mengganggu proses bisnis.Dampak operasional serta biaya yang ditimbulkan pada skala ini sangatkecil sehingga pengaruh terhadap keamanan aset sangat tidak berpengaruh sama sekali.
2	Ringan	Dampak yang ditimbulkan pada sistem operasional tidak terlalu serius dan sangat kecil atau hanya berpengaruh pada jaringan tidak secara menyeluruh.Pada skala ini pengaruh dampak yang ditimbulkan pada sistem operasional hanya sekitaer 5-10% dan hal ini dapat ditangani langsung dengan cara di maintanance.
3	Sedang	Dampak yang ditimbulkan pada skala ini dari segi proses kegiatan operasional sudah cukup besar yaitu sekitar 10-15%. Kegiatan operasional sudah mengalami kelumpuhan dan data atau informasi yang terdapat didalamnya mengalami error.Untuk akses hanya dapat dilakukan oleh satu pihak yaitu admin atau pihak yang diizinkan untuk memegang akses terhadap sistem.Pada skala ini sama dengan skala rendah untuk mengenai data atau aset akan ada yang hilang,rusak atau tidak dapat digunakan atau diakses sehingga diperlukan data backup dan membutuhkan waktu yang cukup lama untuk mengembalikan/memulihkannya.
4	Berat	Pada skala ini kemampuan kegiatan operasional sudah dapat dikatakan kehilangan kontrol yang sangat besar yaitu sekitar 15-20% tetapi belum hampir secara menyeluruh dan untuk pengaksesan masih sama dengan skala sedang yaitu hanya pihak admin atau pihak yang diberikan memegang kendali akses terhadap sistem. Untuk mengenai data atau aset pada skala ini sama seperti pada skala sedang tetapi untuk pemulihan butuh waktu yang sangat cukup lama atau tidak dapat sama sekali dipulihkan. Hal ini juga berdampak pada kerahasiaan dan kejaminan data yang terdapat didalamnya.
5	Sangat Besar	Skala ini adalah skala yang sangat sangat besar yaitu sistem mengalami kegagalan atau kelumpuhan total pada kegiatan operasional dan tingkat kegalalan ini sebesar >20%. Hal ini mengakibatkan kegiatan operasional sistem tidak dapat dilanjutkan atau dengan kata lain terhenti total.Untuk data atau aset sama seperti pada skala signifikan yaitu data atau aset tidak dapat dipulihkan atau dikembalikan sama sekali. Data atau aset informasi dicuri oleh pihak tertentu sehingga kerahasiaan dan kejaminan data sama sekali tidak terjaga dengan baik. Hal ini mengakibatkan kepercayaan terhadap instansi menurun akibat dari dampak yang ditimbulkan.

Langkah berikutnya ialah penetapan kriteria evaluasi risiko yang risiko akan menjadi landasan PT. SPI untuk menentukan respon terhadap tiap risiko dari aset IT. Adapun klasifikasi respon/tindakan yang akan diputuskan oleh perusahaan untuk menangani risiko berdasarkan *risk appetite* perusahaan berikutnya disebut sebagai *risk response.*

Istilah *risk response* tidak disebutkan secara eksplisit di ISO/IEC27005:2022. Pada standar ISO/IEC27005:2022, istilah yang digunakan namun memiliki kesetaraan dengan konsep *risk response* dalam manajemen risiko pada umumnya adalah *risk treatment*. Mengacu pada ISO/IEC27005:2022, *Risk Treatment* merupakan upaya-upaya yang diambil untuk meminimalkan dampak dari risiko, bahkan menghilangkan dampaknya yang dilakukan setelah tahap *risk evaluation* pada proses manajemen risiko. Menurut ISO/IEC 27005:2022 terdapat beberapa pilihan *risk treatment*, di antaranya :

- *Risk Modification* diterapkan untuk mengurangi kemungkinan terjadinya atau dampak dari suatu risiko dengan menerapkan kontrol teknis, administratif, atau prosedural.
- *Risk Retention* diterapkan ketika risiko yang tersisa (*residual risk*) dinilai dapat diterima (*acceptance*) oleh perusahaan berdasarkan kriteria risiko yang telah ditetapkan, dengan mempertimbangkan biaya mitigasi dan dampaknya terhadap bisnis.
- *Risk Avoidance* diterapkan menghindari aktivitas yang menimbulkan risiko tinggi terhadap aset IT dengan cara menghapus, menghentikan, atau mengganti proses teknologi yang memiliki potensi ancaman serius.
- *Risk Sharing* diterapkan dengan mentransfer risiko kepada pihak ketiga.

Tabel 4 Matriks Level Risiko

Kemungkinan	Dampak				
	Sangat Ringan (1)	Ringan (2)	Sedang (3)	Tinggi (4)	Sangat Tinggi (5)
Sangat Rendah (1)	E1	E2	E3	D4	D5
Rendah (2)	E2	E4	D6	C8	B10
Sedang (3)	E3	D6	C9	B12	A15
Tinggi (4)	D4	C8	B12	A16	A20
Sangat Tinggi (5)	D5	B10	A15	A20	A25

Langkah terakhir pada tahap *Context Establishment* yang dilakukan pada penelitian ini adalah penetapan *risk acceptance criteria. Risk Acceptance Criteria* menurut ISO/IEC 27005:2022 merupakan acuan secara kuantitatif untuk menentukan tingkat atau nilai dari sebuah risiko yang berikutnya disebut sebagai *level* risiko [12]. *Level* risiko ini merupakan hasil akumulasi perkalian antara *likelihood* dan *impact*. Berikut *risk acceptance criteria* yang disusun berdasarkan rekomendasi dari perusahaan :

Tabel *5 Risk Acceptance Criteria*

Grade	Level Risiko	Action Plan	Risk Response
A (Sangat Tinggi)	15-25	Membutuhkan intervensi segera, kerentanan kritis harus dimitigasi untuk	*Modification*
B (Tinggi)	10-12	Harus segera diatasi dengan kontrol keamanan yang ketat, pengalihan risiko, atau perubahan operasional.	*Modification /Sharing*
C (Sedang)	8-9	Membutuhkan strategi mitigasi seperti pemantauan yang lebih baik, kontrol tambahan, atau perencanaan kontinjensi.	*Modification /Avoidance*
D (Rendah)	4-6	Dapat diterima dengan kontrol minimal, dipantau secara berkala.	*Retention*
E (Sangat Rendah)	1-3		

B. *Risk Assessment*

Menurut panduan ISO/IEC27005:2022, *Risk Assessment* terdiri dari beberapa tahapan yang saling berhubungan dan bertujuan untuk mengidentifikasi serta mengevaluasi risiko secara sistematis. Tahap pertama, yaitu *Risk Identification*, dimulai dengan identifikasi aset utama dan pendukung yang dimiliki oleh PT. SPI. Dalam konteks ini, penulis melakukan pemetaan terhadap aset-aset IT yang krusial bagi kelangsungan operasional perusahaan, baik yang bersifat fundamental maupun pendukung. Setelah identifikasi aset dilakukan, penulis melanjutkan dengan mengidentifikasi potensi ancaman dan kerentanan yang dapat memengaruhi masing-masing aset IT tersebut. Proses identifikasi ini merujuk pada pedoman yang tercantum dalam ISO/IEC27005:2022, yang mengharuskan penilaian terhadap ancaman yang sudah ada serta ancaman potensial yang mungkin timbul di masa depan.

Tahap kedua dalam *Risk Assessment* adalah *Risk Analysis*, di mana penulis melakukan evaluasi lebih lanjut terhadap kemungkinan terjadinya risiko (*likelihood*) dan dampak yang mungkin ditimbulkan oleh setiap ancaman dan kerentanan yang telah diidentifikasi. Penilaian ini dilakukan melalui pengisian kuesioner yang disediakan oleh PT. SPI, yang berfungsi untuk mengumpulkan data yang diperlukan dalam proses analisis risiko. Pada tahap ini, setiap potensi ancaman dan kerentanan dinilai berdasarkan dua parameter utama, yakni *likelihood* dan *impact*, untuk menentukan tingkat risiko yang dihadapi oleh setiap aset IT yang ada di perusahaan.

Tahap ketiga dari *Risk Assessment* adalah *Risk Evaluation* (evaluasi risiko), yang bertujuan untuk memetakan nilai risiko berdasarkan hasil penilaian yang telah dilakukan pada tahap sebelumnya. Pada tahap ini, nilai risiko dari setiap ancaman yang teridentifikasi dipetakan ke dalam *matriks risiko*, dengan mempertimbangkan tingkat *likelihood dan impact* yang diperoleh. Pemetaan risiko ini dilakukan dengan mengalikan nilai dari kedua parameter tersebut untuk setiap risiko yang ada, yang menghasilkan *level* dan *grade* risiko masing-masing. Hasil evaluasi ini memberikan gambaran yang jelas mengenai tingkat prioritas setiap risiko, serta

membantu dalam pengambilan keputusan untuk menentukan langkah-langkah mitigasi yang perlu diambil. Dengan demikian, proses *Risk Assessment* yang dilakukan di PT. SPI mengikuti prosedur yang sistematis dan terstruktur sesuai dengan pedoman ISO/IEC27005:2022, yang bertujuan untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko secara menyeluruh untuk meningkatkan keamanan sistem informasi perusahaan.

Tabel 6 Hasil *Risk Assessment* Pada Aset Utama

ID Aset	Ancaman	Kerentanan	Kemungkinan	Dampak	Level (Grade)	ID Risiko
A01	TH10	VS14	4	5	20(A)	R02
A01	TP01	VH06	4	4	16(A)	R03
A04	TP01	VH06	4	4	16(A)	R09
A07	TP01	VH06	4	4	16(A)	R14
A10	TH10	VS06	3	5	15(A)	R20
A01	TP01	VH03	3	4	12(B)	R04
A04	TP01	VH03	3	4	12(B)	R10
A07	TP01	VH03	3	4	12(B)	R15
A07	TP01	VH04	3	4	12(B)	R16
A09	TH15	VN02	3	4	12(B)	R17
A04	TN05	VS02	2	5	10(B)	R13
A02	TH15	VN02	3	3	9(C)	R06
A04	TH11	VS13	2	4	8(C)	R07
A04	TH11	VS14	2	4	8(C)	R08
A04	TP01	VH04	2	4	8(C)	R11
A10	TP01	VS06	2	4	8(C)	R22
A01	TH10	VS13	2	3	6(D)	R01
A09	TH15	VS13	2	3	6(D)	R18
A09	TH15	VS14	2	3	6(D)	R19
A04	TN05	VH02	1	5	5(D)	R12
A02	TH15	VS14	1	4	4(D)	R05
A10	TP01	VS01	1	4	4(D)	R21

Tabel 7 Hasil *Risk Assessment* Pada Aset *Software*

ID Aset	Ancaman	Kerentanan	Kemungkinan	Dampak	Level (Grade)	ID Risiko
S03	TP01	VN03	3	4	12(B)	R28
S07	TH06	VS10	3	4	12(B)	R35
S02	TH10	VS06	2	5	10(B)	R24
S03	TP05	VS13	3	3	9(C)	R26
S06	TH14	VS01	3	3	9(C)	R30
S07	TH06	VS05	2	4	8(C)	R34
S01	TH14	VS02	2	3	6(D)	R23
S02	TH10	VS14	2	3	6(D)	R25
S06	TH14	VS14	2	3	6(D)	R29
S06	TH14	VN03	2	3	6(D)	R31
S06	TH15	VN07	2	3	6(D)	R33
S03	TP01	VN01	1	4	4(D)	R27
S06	TH15	VS08	1	4	4(D)	R32

Tabel 8 Hasil *Risk Assessment* Pada Aset *Hardware*

ID Aset	Ancaman	Kerentanan	Kemungkinan	Dampak	Level (Grade)	ID Risiko
H01	TH07	VH08	4	5	20(A)	R36
H01	TH07	VH01	3	5	15(A)	R37
H04	TH07	VH08	3	5	15(A)	R44
H04	TN05	VS02	3	5	15(A)	R47
H02	TP05	VH01	4	3	12(B)	R41
H04	TP02	VH07	3	4	12(B)	R45
H04	TP02	VH08	3	4	12(B)	R46
H01	TH07	VS06	2	5	10(B)	R38
H01	TH10	VS06	2	5	10(B)	R39
H03	TI05	VN07	2	5	10(B)	R43
H02	TP05	VH02	3	3	9(C)	R42
H02	TH07	VH10	2	4	8(C)	R40

C. *Risk Treatment*

Berdasarkan pemaparan sebelumnya bawah *Risk Treatment* merupakan upaya-upaya yang diambil untuk meminimalkan dampak dari risiko, bahkan menghilangkan dampaknya yang dilakukan setelah tahap *Risk Evaluation* pada proses manajemen risiko. Pada tahap ini, berdasarkan hasil diskusi mendalam antara peneliti dan pihak perusahaan, disimpulkan bahwa peninjauan lebih lanjut akan difokuskan pada risiko yang dikategorikan dalam ***Grade* "A"**, yaitu risiko dengan tingkat dampak dan kemungkinan yang sangat tinggi. Langkah ini diambil sebagai prioritas awal dalam perencanaan manajemen risiko PT. SPI terkait aset IT perusahaan. Fokus utama pada risiko *Grade* A bertujuan untuk memberikan perhatian lebih terhadap ancaman yang paling signifikan, yang dapat mengancam keberlanjutan operasional, integritas data, dan reputasi perusahaan. Pada tahap *Risk Treatment*, penulis mengidentifikasi *Risk Response* berdasarkan ISO/IEC 27005:2022 dan tipe kontrol berdasarkan ISO/IEC 27001:2022, serta rekomendasi penanganan risiko *Grade* A pada aset IT PT. SPI. Dengan demikian, langkah-langkah penanganan yang diambil akan lebih terarah dan efektif, sesuai dengan urgensi dan dampak yang ditimbulkan oleh risiko-risiko tersebut.

Tabel 9 *Risk Treatement* & Kontrol Risiko Aset Utama

ID Risiko	Risk Response	Tipe Kontrol	Kontrol ISO/IEC 27001:2022
R02	*Risk Modification*	*Preventive*	*5.15. Access control*
R03	*Risk Modification*	*Preventive*	*7.5. Protecting against physical and environmental threats 8.13. Information backup*
R09	*Risk Modification*	*Preventive, Corrective*	*7.5. Protecting against physical and environmental threats 8.13. Information backup*
R14	*Risk Modification*	*Preventive, Corrective*	*7.5. Protecting against physical and environmental threats 8.13. Information backup*
R20	*Risk Modification*	*Preventive*	*5.15. Access control*

Tabel 10 *Risk Treatment* & Kontrol Risiko Aset *Hardware*

ID Risiko	Risk Response	Tipe Kontrol	Kontrol ISO/IEC 27001:2022
R36	*Risk Modification*	*Preventive*	*7.1. Physical security perimeters*
R37	*Risk Modification*	*Preventive*	*7.1. Physical security perimeters*
R44	*Risk Modification*	*Preventive*	*7.1. Physical security perimeters* *5.15. Access control*
R47	*Risk Modification*	*Preventive, Corrective*	*7.1. Physical security perimeters*

			8.13. Information backup

Tabel 11 Rekomendasi Penanganan Risiko Aset Utama

ID Risiko	Rekomendasi
R02	• Menerapkan enkripsi untuk melindungi data sensitif. • Melakukan pembaruan kebijakan pengaturan akses dan pengamanan.
R03	• Pemasangan alat pemadam kebakaran otomatis. • Melakukan backup data secara berkala dan menyimpannya secara terenkripsi di lokasi *cloud* yang aman.
R09	• *Backup* data secara rutin dan simpan di lokasi yang aman. • Mengimplementasi pengamanan fisik yang kuat di pusat data.
R14	Peningkatan sistem *backup* data dan pengamanan fisik lokasi penyimpanan.
R20	• Implementasikan kontrol akses berbasis peran (RBAC) untuk membatasi akses ke dokumen keuangan sensitif. • Gunakan enkripsi pada dokumen keuangan untuk melindunginya.

Tabel 12 Rekomendasi Penanganan Risiko Aset *Hardware*

ID Risiko	Rekomendasi
R36	• Mengimplementasi pengamanan fisik yang ketat pada area server. • Penggunaan sistem pemantauan CCTV dan kontrol akses.
R37	• Pastikan adanya pengamanan fisik yang ketat di area server, seperti pengawasan dengan CCTV dan kontrol akses yang terbatas. • Terapkan sistem *backup* data yang aman.
R44	• Penggunaan kunci fisik dan kontrol akses untuk membatasi siapa yang dapat mengakses perangkat penyimpanan cadangan. • Menyimpan perangkat cadangan di lokasi aman dan terjaga.
R47	Pastikan perangkat *backup* disimpan di lokasi yang tidak berisiko terhadap bencana alam seperti banjir.

V. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa kondisi pengelolaan risiko pada PT. SPI diidentifikasi terdapat 119 potensi ancaman dari kerentanannya pada aset IT PT. SPI berdasarkan panduan ISO/IEC 27005:2022. Setelah dianalisis, dari 119 potensi ancaman dan kerentanan tersebut menghasilkan 72 risiko tidak relevan dan 47 risiko relevan yang ditinjau berdasarkan kemungkinan (*likelihood*) tiap risiko pada aset IT perusahaan. Pada hasil evaluasi dari 47 risiko tersebut, ditemukan 9 risiko dengan *Grade* A yang telah dikonfirmasi oleh pihak perusahaan khususnya Departement IT bahwa perlu menjadi fokus utama untuk ditinjau lebih lanjut sebagai langkah awal perancangan manajemen risiko pada aset IT perusahaan.

Adapun risiko pada kategori *Grade* A yang menjadi prioritas penanganan, ditemukan 5 risiko yang dapat mempengaruhi aset utama (informasi/data/dokumen) perusahaan dengan ID R02, R03, R09, R14, R20 dan 4 risiko yang dapat mempengaruhi aset *hardware* perusahaan dengan ID R36, R37, R44, R47.

Maka dari itu untuk meminimalisir dampak dari risiko-risiko tersebut penulis merekomendasikan berbagai tindakan pengamanan, termasuk penggunaan enkripsi, pembaruan kebijakan akses, pengamanan fisik area server, sistem pemantauan CCTV, pemasangan alarm pemadam kebakaran otomatis, *backup* data rutin, dan kontrol akses berbasis peran untuk meminimalkan risiko dan dampaknya pada data sensitif dan infrastruktur IT.

REFERENSI

[1] M. E. Whitman and H. J. Mattord, “Manegement Of Informationn Security,” 2019.

[2] BSSN, “Lanskap Keamanan Siber Indonesia,” 2023.

[3] OJK RI, “Peraturan Otoritas Jasa Keuangan Manajemen Risiko Teknologi Informasi,” 2016. Accessed: Jun. 25, 2025. [Online]. Available: https://www.ojk.go.id/id/kanal/perbankan/regulasi/peraturan-ojk/Documents/Pages/POJK-tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-Oleh-Bank-Umum/POJK MRTI.pdf

[4] Bank Indonesia, “Peraturan-Bank-Indonesia-Tentang-Disaster-Recovery”.

[5] Peraturan Pemerintah, “Peraturan Pemerintah Republik Indonesia Penyelenggaraan Sistem dan Transaksi Elektronik,” Jakarta, Oct. 2019.

[6] Hevner, March, Park, and Ram, “Design Science in Information Systems Research,” *MIS Q.*, pp. 75–105, 2004, Accessed: Dec. 18, 2024. [Online]. Available: https://doi.org/10.2307/25148625

[7] S. Nurul, S. Anggrainy, and S. Aprelyani, “Faktor-Faktor yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi, dan Jaringan (Literature Review SIM),” *J. Ekon. Sist. Inf.*, vol. 3, no. 5, 2022, doi: 10.31933/jemsi.v3i5.

[8] E. Nursetyawati, R. Fauzi, and R. A. Nugraha, “Perancangan Manajemen Keamanan Informasi Menggunakan Metode Analisis Risiko ISO 27005:2008 Pada Dinas Komunikasi Dan Informatika Jawa Barat,” 2020.

[9] F. Antonius Alijoyo, I. Bonita, K. Bastian, and K. Bastian Sirait, “Evaluation of Risk Management Maturity of a Fintech Firm in Indonesia,” *Eduvest-Journal Univers. Stud.*, vol. 1, no. 12, pp. 1478–1487, 2021, [Online]. Available: http://eduvest.greenvest.co.id

[10] Peraturan Pemerintah, “Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2010 Tentang Standar Akuntansi Pemerintahan,” 2010.

[11] K. Dewantara, “Identifikasi, Penilaian, dan Mitigasi Risiko Keamanan Informasi Berdasarkan Standar ISO 27001:2005 dan ISO 27002:2013 Menggunakan Metode FMEA (Studi Kasus: ISNET),” 2016.

[12] ISO 27005, “Information security, cybersecurity and privacy protection-Guidance on managing

information security risks," 2022.

[13] E. Jaakkola, "Designing Conceptual Articles: Four Approaches," *AMS Rev.*, vol. 10, no. 1–2, pp. 18–26, Jun. 2020, doi: 10.1007/s13162-020-00161-0.

[14] R. Rambe, A. Gandhi, and M. K. Sabariah, "Implementasi Manajemen Risiko pada Aplikasi XYZ dengan Pendekatan SNI ISO/IEC 27005:2018," 2023.