Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 10, Nomor 1, Februari 2025, pp 226-235
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Perancangan Manajemen Risiko Keamanan Informasi Menggunakan SNI ISO/IEC 27005: Studi Kasus Integrated School Management System milik PT XYZ

Rizky Muhamad Rasyid[1], Rizal Fathoni Aji[2]
[1,2]Universitas Indonesia, Indonesia
Email: rizkym.rasyid@gmail.com[1], rizal@cs.ui.ac.id[2]

Abstract

The existence of information technology has provided various conveniences and opportunities for conducting business online, one of which is the Software as a Service (SaaS) industry. PT XYZ is one of the startups focused on the SaaS business as a provider of integrated school management system (ISMS) solutions. IT plays a vital role in the operational activities of ISMS. PT XYZ is aware of this and has implemented a zero-security incident policy for its ISMS. However, the ISMS still experiences security incidents due to vulnerabilities in the system that result in losses for PT XYZ. This indicates the need for information security risk management for the ISMS. The purpose of this study is to obtain a design for information security risk management for ISMS. This study uses a qualitative method where data collection is conducted through interviews, observations, and literature reviews. SNI ISO/IEC 27005:2022 is used as the information security risk assessment, while risk control recommendations utilize SNI ISO/IEC 27001:2022. This study resulted in 28 risk scenarios, namely: 12 High risks, 10 Moderate risks, two Low risks, and four Very Low risks. The outcome of this study is the design of information security risk management for PT XYZ's ISMS.

Keywords*: ISMS, information security risk management, SNI ISO/IEC 27005:2022, SNI ISO/IEC 27001:2022*

Abstrak

Keberadaan teknologi informasi telah memberikan berbagai kemudahan dan peluang melakukan bisnis secara online, salah satunya adalah industri Software as a Service (SaaS). PT XYZ merupakan salah satu startup yang berfokus pada bisnis SaaS sebagai penyedia solusi integrated school management system (ISMS). IT memiliki peran yang vital pada kegiatan operasional ISMS. PT XYZ sadar akan hal tersebut dan menerapkan zero security incident pada ISMS miliknya. Namun pada kenyataannya, ISMS tersebut masih mengalami insiden keamanan karena terdapat celah pada sistem yang mengakibatkan kerugian bagi PT XYZ. Hal tersebut menandakan perlunya manajemen risiko keamanan informasi bagi ISMS. Tujuan dari penelitian ini adalah untuk memperoleh desain manajemen risiko keamanan informasi ISMS. Penelitian ini menggunakan metode kualitatif dimana pengumpulan data dilakukan melalui wawancara, observasi, dan tinjauan pustaka. SNI ISO/IEC 27005:2022 digunakan sebagai penilaian risiko keamanan informasi, sementara rekomendasi pengendalian risiko menggunakan SNI ISO/IEC 27001:2022. Penelitian ini menghasilkan 28 skenario risiko, yaitu: 12 risiko Tinggi, 10 risiko Sedang, dua risiko Rendah, dan empat risiko Sangat Rendah. Hasil dari penelitian ini adalah desain manajemen risiko keamanan informasi ISMS milik PT XYZ.

Kata kunci*: ISMS, manajemen risiko keamanan informasi, SNI ISO/IEC 27005:2022, SNI ISO/IEC 27001:2022*

1. PENDAHULUAN

Keberadaan teknologi informasi telah memberikan berbagai kemudahan dan peluang melakukan bisnis secara *online*, salah satunya adalah industri *Software as a Service* (SaaS). Perusahaan yang bergerak pada industri SaaS menyediakan

perangkat lunak sebagai layanan dan berfokus pada solusi perangkat lunak spesifik ke target pasar yang dituju serta sering menggunakan model bisnis *freemium* dan *subscription* untuk menarik pengguna [1]. Semua *startup* SaaS memiliki tujuan yang sama untuk menyediakan perangkat lunak yang mudah digunakan dan dapat diakses oleh khalayak luas [2]. Menurut *Boston Consulting Group* (BCG), dalam tingkat tahunan, bisnis SaaS di Indonesia tumbuh sebesar 31,9%. Pesatnya pertumbuhan ini disebabkan juga oleh pandemi COVID-19 yang membuat bisnis SaaS di Indonesia diprediksi akan bernilai US$1 miliar atau sekitar Rp14,8 triliun pada tahun 2025 [3]. Hingga saat ini sudah ada 954 startup yang bergerak dibidang SaaS di Indonesia dan salah satunya adalah PT XYZ [4].

PT XYZ didirikan pada tahun 2020 sebagai perusahaan startup yang berfokus pada bisnis SaaS penyedia solusi *integrated school management system* (ISMS) untuk sekolah islam dan pesantren di Indonesia. ISMS merupakan aplikasi yang bisa digunakan institusi pendidikan untuk melakukan manajemen operasional terhadap institusinya [5]. ISMS milik PT XYZ ini telah digunakan oleh 40 pondok pesantren dan sekolah islam yang ada di Indonesia. PT XYZ memiliki target pada tahun 2025 untuk dapat memperluas target pasarnya tidak hanya terbatas pada institusi pendidikan swasta, tetapi juga institusi pemerintah dengan menggandeng sekolah negeri yang ada di pulau Jawa. PT XYZ sadar bahwa IT memegang peranan yang vital terhadap operasional ISMS sehari-hari sehingga mengharapkan terciptanya *zero-incident security* setiap harinya. Hal ini menjadi risiko apabila terjadi insiden dan permasalahan pada operasional ISMS.

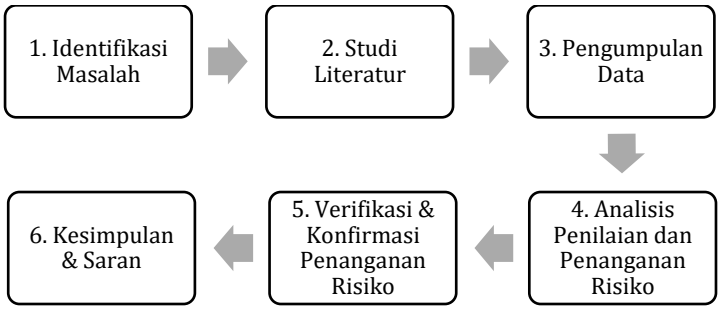
Pada tahun 2023, Kementrian Komunikasi dan Informatika (Kominfo) sendiri telah menindak 35 insiden kasus kebocoran data dimana hal ini menandakan bahwa kebocoran data kerap terjadi [6]. Kebocoran data sendiri membidik berbagai lini bisnis di berbagai industri. Menurut ketua lembaga Communication and Information System Security Research Center (CISSReC), selama satu periode dimulai dari Januari hingga Desember, Indonesia mengalami 403 juta percobaan serangan siber [7]. Pada 20 Agustus 2023 dan 11 Januari 2024 terjadi insiden *hacking* dan *ransomware* pada ISMS milik PT XYZ. Insiden tersebut menyebabkan kerugian yang signifikan bagi PT XYZ pasalnya *Service Level Agreement* (SLA) dengan pelanggan turun karena ISMS tidak dapat diakses pada hari tersebut. Insiden tersebut juga berpotensi menurunkan kepercayaan para pelanggannya untuk tetap menggunakan ISMS jika terjadi lagi dikemudian hari. PT XYZ sadar terhadap dampak dari insiden tersebut namun penanganan insiden masih bersifat *accidental*. Dengan kata lain, pengelolaan insiden keamanan informasi saat ini belum dilakukan dengan tata kelola keamanan informasi yang baik.

Berdasarkan latar belakang yang telah dijelaskan, terdapat kesenjangan antara harapan PT XYZ berupa *zero-incident security* ISMS dengan kenyataan implementasi penanganan insiden yang bersifat *accidental* serta belum adanya tata kelola insiden berupa manajemen risiko keamanan informasi ISMS. Penelitian ini bertujuan untuk merancang manajemen risiko keamanan informasi pada ISMS milik PT XYZ berdasarkan SNI ISO/IEC 27005:2022. Hasil penelitian ini adalah perancangan manajemen risiko keamanan informasi ISMS yang diharapkan dapat dijadikan acuan dalam penerapan manajemen risiko keamanan informasi di PT

XYZ. Sementara itu, terdapat keterbatasan penelitian berupa tidak dilakukannya analisis risiko sisa dan biaya mitigasi risiko.

2. METODOLOGI PENELITIAN

Penelitian ini merancang manajemen risiko keamanan informasi pada ISMS PT XYZ dengan menggunakan metodologi klasifikasi *action research*. Dalam penelitian ini, peneliti berkolaborasi dengan praktisi di PT XYZ untuk mencapai pemahaman bersama mengenai masalah organisasi yang kompleks, melakukan intervensi untuk memperbaiki situasi secara langsung, serta menyampaikan pengetahuan yang diperoleh setelah investigasi [7]. Selain klasifikasi, data yang dikumpulkan bersifat kualitatif, dan proses pengumpulan data dilakukan melalui wawancara, studi dokumen PT XYZ, serta observasi langsung. Gambar 1 menggambarkan alur penelitian yang dilakukan.



Gambar 1. Alur Penelitian

Penelitian ini dilakukan dalam beberapa tahap, seperti yang ditunjukkan pada Gambar 1. Tahap pertama adalah mengidentifikasi masalah dengan melakukan wawancara awal, observasi, dan analisis laporan insiden yang pernah terjadi. Pada tahap kedua, dilakukan studi literatur baik teoritis maupun penelitian terdahulu yang relevan untuk mendapatkan metode yang tepat. Tahap ketiga adalah melakukan wawancara dengan menggunakan kerangka teori pada tahap kedua. Wawancara bersifat semi terstruktur, artinya pewawancara memiliki panduan saat melakukan kegiatan wawancara [8]. Wawancara dilakukan dengan metode semi terstruktur dengan mengikuti instrumen Lampiran A pada SNI ISO/IEC 27005:2022 [9]. Tahap keempat menganalisis penilaian risiko berdasarkan SNI ISO/IEC 27005:2022, dan penanganan risiko menggunakan SNI ISO/IEC 27001:2022 [10]. Pada tahap keempat juga dilakukan penetapan kriteria dasar penggunaan Peraturan Menteri Pan&RB No.5 Tahun 2020 sebagai acuan pendukung sebagai bentuk kepatuhan terhadap peraturan pemerintah [11]. Tahap kelima adalah melakukan verifikasi dan konfirmasi kepada pemilik risiko atas hasil yang didapatkan pada tahap keempat untuk memastikan analisis yang dilakukan dengan wawancara yang dilakukan telah sesuai. Tahap keenam merupakan pembuatan kesimpulan dan saran atas hasil yang didapatkan pada tahap keempat.

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 10, Nomor 1, Februari 2025, pp 226-235
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

3. HASIL DAN PEMBAHASAN

Pada tahap ini dilakukan proses perancangan manajemen risiko keamanan informasi ISMS meliputi pengumpulan data, penetapan konteks, penilaian risiko dan penanganan risiko.

3.1. Penetapan Konteks

Penetapan konteks merupakan aktivitas awal yang dilakukan untuk melaksanakan proses manajemen risiko. Pada tahap ini akan ditetapkan pesyaratan dasar dan kriteria risiko**.**

3.1.1. Penetapan Persyaratan Dasar

Penelitian ini dilakukan menggunakan pendekatan Peraturan Menteri PAN&RB No.5 Tahun 2020 tentang pedoman manajemen risiko sistem pemerintahan berbasis elektronik. Hal ini didasari oleh adanya kebutuhan perusahaan terkait kepatuhan dengan peraturan pemerintah dikarenakan perusahaan ingin melakukan diversifikasi pasar dengan menyediakan layanan untuk sekolah negeri yang merupakan instansi pemerintah. Kaidah ini cocok untuk digunakan oleh instansi pemerintahan maupun instansi swasta yang menyediakan layanan terhadap instansi pemerintah untuk menerapkan manajemen risiko keamanan informasi.

3.1.2. Penetapan Kriteria Risiko

Berdasarkan persyaratan dasar yang telah ditentukan, Penelitian mengadopsi beberapa kriteria risiko menggunakan pendekatan Peraturan Menteri PAN&RB No.5 Tahun 2020. Kriteria risiko yang diadopsi antara lain kriteria dampak, kriteria kemungkinan, kriteria analisis risiko, kriteria level risiko, dan kriteria akseptansi risiko.

a) Kriteria Dampak: Kriteria Dampak yang diserap dalam penelitian ini meliputi tiga area dampak berdasarkan Peraturan Menteri PAN&RB No.5 Tahun 2020 yaitu Layanan, Reputasi, dan Kinerja. Gambar 2 menyajikan kriteria dampak penelitian.

Area Dampak		Level Dampak				
		1	2	3	4	5
		Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat signifikan
Layanan	Positif	Peningkatan <20%	Peningkatan 20% s.d.<40%	Peningkatan 40% s.d.<60%	Peningkatan 60% s.d.<80%	Peningkatan ≥ 80%
	Negatif	Penurunan <20%	Penurunan 20% s.d.<40%	Penurunan 40% s.d.<60%	Penurunan 60% s.d.<80%	Penurunan ≥ 80%
Reputasi	Positif	Peningkatan <20%	Peningkatan 20% s.d.<40%	Peningkatan 40% s.d.<60%	Peningkatan 60% s.d.<80%	Peningkatan ≥ 80%
	Negatif	Penurunan <20%	Penurunan 20% s.d.<40%	Penurunan 40% s.d.<60%	Penurunan 60% s.d.<80%	Penurunan ≥ 80%
Kinerja	Positif	Peningkatan <20%	Peningkatan 20% s.d.<40%	Peningkatan 40% s.d.<60%	Peningkatan 60% s.d.<80%	Peningkatan ≥ 80%
	Negatif	Penurunan <20%	Penurunan 20% s.d.<40%	Penurunan 40% s.d.<60%	Penurunan 60% s.d.<80%	Penurunan ≥ 80%

Gambar 2. Kriteria Dampak

b) Kriteria Kemungkinan: Kriteria Kemungkinan yang diserap dalam penelitian ini sesuai dengan Peraturan Menteri PAN&RB No.5 Tahun 2020 yaitu *probabilistic* (oportunitas peristiwa terjadi pada waktu tertentu) atau *frequentist* (jumlah

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 10, Nomor 1, Februari 2025, pp 226-235
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

rata-rata kejadian dalam waktu tertentu). Gambar 3 menyajikan kriteria kemungkinan penelitian.

Level Kemungkinan		Persentase Kemungkinan Terjadinya dalam Satu Tahun	Jumlah Frekuensi Kemungkinan Terjadinya dalam Satu Tahun
1	Hampir Tidak Terjadi	X ≤ 5%	X < 2 kali
2	Jarang Terjadi	5% < X ≤ 10%	2 kali ≤ X ≤ 5 kali
3	Kadang-kadang Terjadi	10% < X ≤ 20%	6 kali ≤ X ≤ 9 kali
4	Sering Terjadi	20% < X ≤ 50%	10 kali ≤ X ≤ 12 kali
5	Hampir Pasti Terjadi	X > 50%	X > 12 kali

Gambar 3. Kriteria Kemungkinan

c) Kriteria Analisis: Untuk dapat menetapkan besaran risiko yang direpresentasikan dalam bentuk angka, dilakukan kombinasi antara level dampak dan level kemungkinan dalam matriks analisis risiko. Gambar 4 menyajikan matriks analisis risiko penelitian.

Matriks Analisis Risiko			Level Dampak				
			1	2	3	4	5
			Tidak Signifikan	Kurang Signifikan	Cukup Signifikan	Signifikan	Sangat Signifikan
Level Kemungkinan	5	Hampir Pasti Terjadi	9	15	18	23	25
	4	Sering Terjadi	6	12	16	19	24
	3	Kadang-kadang Terjadi	4	10	14	17	22
	2	Jarang Terjadi	2	7	11	13	21
	1	Hampir Tidak Terjadi	1	3	5	8	20

Gambar 4. Matiks Analisis Risiko

d) Kriteria Level Risiko: Setelah matriks analisis risiko didapatkan maka level risiko dapat ditentukan. Gambar 5 menyajikan level risiko penelitian berserta keterangan warna dari setiap level risikonya berdasarkan pedoman Peraturan Menteri PAN&RB No.5 Tahun 2020.

Level Risiko		Rentang Besaran Risiko	Keterangan Warna
1	Sangat Rendah	1-5	**Biru**
2	Rendah	6-10	**Hijau**
3	Sedang	11-15	**Kuning**
4	Tinggi	16-20	**Jingga**
5	Sangat Tinggi	21-25	**Merah**

Gambar 5. Kriteria Level Risiko

e) Kriteria Akseptansi Risiko: Berdasarkan wawancara dengan pemilik risiko, penelitian ini menetapkan kriteria penerimaan risiko sebagai berikut: risiko tingkat tinggi dan sangat tinggi harus dimitigasi, risiko tingkat sedang dapat dimitigasi, risiko tingkat rendah dan sangat rendah dapat diterima.

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 10, Nomor 1, Februari 2025, pp 226-235
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

3.2. Penilaian Risiko

Berdasarkan kerangka kerja SNI ISO/IEC 27005:2022, terdapat tiga tahap asesmen risiko yang dilakukan pada penelitian ini yaitu identifikasi, analisis, dan evaluasi terhadap risiko.

3.2.1. Identifikasi Risiko

Pada tahap ini terdapat beberapa prosedur yang dilakukan yaitu identifikasi aset, ancaman, kerentanan, serta dampak risiko. Luaran pada tahap ini berupa daftar risiko yang disajikan pada Tabel 1. Berikut ini adalah hasil yang didapatkan dari setiap tahapan pada identifikasi risiko:

a) Identifikasi Aset: Aset yang telah teridentifikasi terdiri dari aset utama dan aset pendukung. Aset utama terdiri dari proses bisnis dan informasi, sedangkan aset pendukung meliputi jaringan, perangkat lunak, perangkat keras, personel, dan organisasi.
b) Identifikasi Ancaman: Terdapat setidaknya 7 ancaman terhadap aset yang telah teridentifikasi baik yang bersumber dari kecelakaan (*accident*), kesengajaan (*deliberate*), maupun lingkungan (*environment*).
c) Identifikasi Kerentanan: Terdapat 28 kerentanan yang teridentifikasi, dengan dua kerentanan pada perangkat keras, 16 kerentanan pada perangkat lunak, dua kerentanan pada jaringan, empat kerentanan pada personel, dan empat kerentanan pada organisasi.
d) Identifikasi Dampak: Pada setiap kerentanan, dampak yang didapat disesuaikan dengan kriteria dalam kriteria dampak risiko yaitu layanan menurun, reputasi menurun, dan kinerja menurun.

Tabel 1. Daftar Risiko

Kode Risiko	Aset	Kerentanan	Dampak
R1	Perangkat Keras	Kartu absensi diganti ketika rusak	Layanan & Reputasi
R2		Server Cloud Alibaba Rentan Terbakar	
R3	Perangkat Lunak	Tidak pernah *vulnerability assesment* & *penetration testing* aplikasi	Reputasi
R4		Menggunakan *Node Package Manager* versi lama	Layanan & Reputasi
R5		Tampilan antarmuka membingungkan	Layanan & Kinerja
R6		*JSON Web Token* kadaluarsa lama	Reputasi
R7		Response API menyertakan ID primitif	Kinerja & Reputasi
R8		Salah record tahun transaksi	Layanan & Kinerja
R9		Tidak muncul notifikasi Whatsapp saat tanggal penagihan	
R10		Pengguna tidak mengubah *password default*	Reputasi
R11		Mekanisme *backup* belum efektif	
R12		Gagal unduh laporan keuangan	Layanan & Kinerja
R13		Transaksi berhasil dilakukan namun data tidak tersimpan	
R14		Tidak optimalnya kinerja server	
R15		Terjadi duplikasi data	
R16		Data antar modul tidak konsisten	

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 10, Nomor 1, Februari 2025, pp 226-235
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Kode Risiko	Aset	Kerentanan	Dampak
R17		Terdapat formulir isian data yang ambigu	
R18		Bahasa pada aplikasi tidak konsisten	
R19	Jaringan	Mengembalikan seluruh data dari database dalam respons API	Reputasi & Kinerja
R20		Tidak pernah *vulnerability assesment* & *penetration testing* jaringan	Reputasi
R21	Personel	Ketergantungan terhadap seorang pegawai terkait infrastruktur	Layanan & Kinerja
R22		Tidak ada pelatihan kemanan informasi untuk pegawai	Reputasi
R23		Kurangnya kesadaran pegawai	
R24		Kurangnya kesadaran pengguna	
R25	Organisasi	Proses *review* hak akses bagi pengguna belum efektif	Reputasi
R26		Mekanisme formal pencatatan keluhan belum efektif	
R27		Tidak memiliki *Business Continuity Plan* (BCP)	Layanan & Reputasi
R28		Mekanisme peninjauan log jaringan tidak efektif	Layanan &Reputasi

3.2.2. Analisis Risiko

Berdasarkan daftar risiko yang telah teridentifikasi, dilakukan analisis berupa pemberian skor terhadap dampak dan kemungkinan serta level risiko. Hasil analisis disajikan dalam Tabel 2.

Tabel 2. Analisis Risiko

No	Kode Risiko	Level Dampak	Level Kemungkinan	Skor Risiko	Level Risiko
1	R1	3	4	16	Tinggi
2	R2	4	1	8	Rendah
3	R3	4	3	17	Tinggi
4	R4	4	3	17	Tinggi
5	R5	3	2	11	Sedang
6	R6	4	4	19	Tinggi
7	R7	4	4	19	Tinggi
8	R8	3	2	11	Sedang
9	R9	3	3	14	Sedang
10	R10	4	4	19	Tinggi
11	R11	4	2	13	Sedang
12	R12	3	2	11	Sedang
13	R13	3	2	11	Sedang
14	R14	3	1	5	Sangat Rendah
15	R15	3	1	5	Sangat Rendah
16	R16	3	2	11	Sedang
17	R17	3	2	11	Sedang
18	R18	3	1	5	Sangat Rendah
19	R19	4	4	19	Tinggi
20	R20	4	3	17	Tinggi

Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 10, Nomor 1, Februari 2025, pp 226-235
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

No	Kode Risiko	Level Dampak	Level Kemungkinan	Skor Risiko	Level Risiko
21	R21	3	5	18	Tinggi
22	R22	2	2	7	Rendah
23	R23	4	3	17	Tinggi
24	R24	4	4	19	Tinggi
25	R25	4	3	17	Tinggi
26	R26	2	4	12	Sedang
27	R27	4	2	13	Sedang
28	R28	1	1	1	Sangat Rendah

3.2.3. Evaluasi Risiko

Berdasarkan hasil analisis risiko, risiko yang telah diberi skor dibandingkan dengan kriteria penilaian risiko sehingga mendapatkan prioritas risiko untuk proses penanganan risiko. Tabel 3 menunjukkan hasil evaluasi risiko.

Tabel 3. Evaluasi Risiko

Kode Risiko	Skor Risko	Akseptansi Risiko	Prioritas Risiko
R19	19	Tidak Diterima	1
R7	19	Tidak Diterima	2
R24	19	Tidak Diterima	3
R6	19	Tidak Diterima	4
R10	19	Tidak Diterima	5
R21	18	Tidak Diterima	6
R3	17	Tidak Diterima	7
R4	17	Tidak Diterima	8
R20	17	Tidak Diterima	9
R23	17	Tidak Diterima	10
R25	17	Tidak Diterima	11
R1	16	Tidak Diterima	12
R9	14	Tidak Diterima	13
R11	13	Tidak Diterima	14
R27	13	Tidak Diterima	15
R26	12	Tidak Diterima	16
R5	11	Tidak Diterima	17
R16	11	Tidak Diterima	18
R8	11	Tidak Diterima	19
R12	11	Tidak Diterima	20
R13	11	Tidak Diterima	21
R17	11	Tidak Diterima	22
R2	8	Diterima	23
R22	7	Diterima	24
R14	5	Diterima	25
R15	5	Diterima	26
R18	5	Diterima	27
R28	1	Diterima	28

3.3. Penanganan Risiko

Berdasarkan hasil evaluasi risiko, 22 risiko yang tidak diterima akan diberikan mitigasi berupa rekomendasi penanganan terhadap setiap risiko dan

telah dikonfirmasi serta diverifikasi oleh setiap pemilik risiko. Rekomendasi ini tidak mempertimbangkan risiko sisa dan analisis *cost-benefit*. Rekomendasi pengendalian risiko dilakukan menggunakan instrumen format Lampiran A pada SNI ISO/IEC 27001:2022. Detail rekomendasi dapat dilihat pada Tabel 4.

Tabel 4. Rekomendasi Penanganan Risiko

Kode Risiko	Rekomendasi	Referensi SNI ISO/IEC 27001:2022
R19	*Filtering* dan *pagination* respon API	A.8.3 Pembatasan Akses Informasi
R7	Enkripsi data menggunakan hashing	A.8.24 Penggunaan Kriptografi
R24, R23	Sosialisasi dan pelatihan keamanan informasi secara berkala	A.6.3 Kesadaran, Pendidikan & Pelatihan Keamanan Informasi
R6	Mempercepat kadaluarsa token autentikasi	A.8.5 Autentikasi Aman
R10	Pemaksaan perubahan password saat pertama login	A.5.18 Hak Akses
R25	Pembuatan prosedur *review* hak akses	
R21	Penambahan pegawai	A.5.2 Peran & tanggung jawab keamanan informasi
R3, R20	*Vulnerability Assessment* dan P*enetration Testing*	A.8.29 Pengujian keamanan dalam pengembangan & penerimaan
R5, R17	UI/UX testing	
R4	Pembaruan *library* yang usang	A.8.27 Prinsip-prinsip arsitektur dan rekayasa sistem yang aman
R1	Kartu diganti secara berkala	A.7.11 Utilitas pendukung
R9, R16, R8, R12, R13	Perbaikan Code / Konfigurasi	A.8.9 Manajemen konfigurasi
R11	Perbaikan Prosedur *Backup*	A.8.13 Pencadangan Informasi
R27	Pembuatan dokumen *business continuity plan*	A.5.30 Kesiapan TIK untuk kontinuitas bisnis
R26	Pembuatan prosedur pencatatan keluhan	A.5.24 Perencanaan dan persiapan manajemen insiden keamanan informasi

4. SIMPULAN

Penelitian ini menghasilkan rancangan manajemen risiko keamanan informasi ISMS milik PT XYZ. Rancangan ini terdiri dari penetapan konteks, penilaian risiko, dan penanganan risiko. Penelitian ini menghasilkan rancangan dengan menggunakan pendekatan kualitatif, SNI ISO/IEC 27005:2022 untuk penilaian risiko dan SNI ISO/IEC 27001:2022 untuk penanganan risiko. Dalam analisis risiko, ditemukan 12 risiko tinggi, 10 risiko sedang, dua risiko rendah, dan empat risiko sangat rendah. Penanganan risiko dilakukan terhadap 22 risiko yang memiliki risiko level tinggi dan sedang. Penelitian ini memiliki dampak praktis dan akademis. Dampak praktisnya adalah untuk membantu organisasi dalam meningkatkan kualitas manajemen risiko keamanan informasi ISMS. Secara akademis, penelitian ini dapat memberikan referensi tambahan bagi organisasi, terutama pada industri SaaS penyedia layanan ISMS untuk instansi pemerintah, dalam mengelola manajemen risiko keamanan informasi aplikasi ISMS mereka.

Penelitian ini juga menyarankan melakukan analisis risiko sisa, analisis *cost-benefit*, dan analisis kelayakan sebelum menentukan kontrol rekomendasi sebagai topik potensial di masa depan.

DAFTAR PUSTAKA

[1] M. Seifert, S. Kuehnel, dan S. Sackmann, "Hybrid Clouds Arising from Software as a Service Adoption: Challenges, Solutions, and Future Research Directions," *ACM Comput Surv*, vol. 55, no. 11, Nov 2023.

[2] W. T. Tsai, X. Y. Bai, dan Y. Huang, "Software-as-a-service (SaaS): Perspectives and challenges," *Science China Information Sciences*, vol. 57, no. 5, hlm. 1–15, Mei 2014.

[3] Finfolk, "Berkembang Pesat, Bisnis SaaS di Indonesia Diprediksi Bernilai Rp14,8 Triliun Pada 2025." [Daring]. Tersedia pada: https://finfolk.co/article/news/berkembang-pesat-bisnis-saas-di-indonesia-diprediksi-bernilai-rp148-triliun-pada-2025

[4] Tracxn, "Global SaaS sector in Indonesia overview." [Daring]. Tersedia pada: https://tracxn.com/d/explore/global-saas-startups-in-indonesia

[5] Z. Yildirim, C. M. Reigeluth, S. Kwon, Y. Kageto, dan Z. Shao, "A comparison of learning management systems in a school district: searching for the ideal personalized integrated educational system (PIES)," *Interactive Learning Environments*, vol. 22, no. 6, hlm. 721–736, Nov 2014.

[6] I. S. Syarief, "Kominfo Tangani 94 Kasus Kebocoran Data Pribadi dalam Tiga Tahun." [Daring]. Tersedia pada: https://www.suarasurabaya.net/kelanakota/2023/kominfo-tangani-94-kasus-kebocoran-data-pribadi-dalam-tiga-tahun

[7] E. V. Beskaravainaya dan T. N. Kharybina, "Characteristics of Information Flow in Scientific Research," *Scientific and Technical Information Processing*, vol. 51, no. 3, hlm. 206–214, Sep 2024.

[8] L. Setiyani, "Research Methods Information Technology". Karawang: Jatayu Catra Internusa, 2018.

[9] Badan Standarisasi Nasional, "SNI ISO/IEC 27005:2022," 2023.

[10] Badan Standarisasi Nasional, "SNI ISO/IEC 27001:2022," 2023.

[11] Menteri PAN&RB, "Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020," Jakarta, Mar 2020.