Jurnal PETISI, Vol. 06, No. 02, Juli 2025
e-ISSN: 2721-6276

Implementasi ISO 27001:2022 dalam Manajemen Risiko Keamanan Informasi

Filany Cahya Arumdiya[1], Christ Rudianto[2]
Program Studi Sistem Informasi, Universitas Kristen Satya Wacana, Salatiga, Indonesia
682021104@student.uksw.edu, chris.rudianto@uksw.edu

Abstrak: Implementasi *ISO 27001:2022* merupakan langkah strategis dalam memperkuat manajemen risiko keamanan informasi di berbagai organisasi. Penelitian bertujuan menganalisis implementasi ISO 27001:2022 dalam manajemen risiko keamanan informasi di Instansi CXY dengan pendekatan studi kasus deskriptif kualitatif. serta berpedoman PermenPAN-RB No. 5 Tahun 2020. Hasil penelitian menunjukkan bahwa Instansi CXY menghadapi risiko seperti *bug* pada aplikasi, serangan siber, serta rendahnya kompetensi SDM. Penyebab utamanya antara lain adalah *human error*, kurangnya pelatihan, dan infrastruktur yang belum optimal. Upaya mitigasi yang diterapkan mencakup penggunaan autentikasi ganda, pelatihan keamanan informasi, pemantauan insiden secara *real-time*, serta pembentukan Tim Auditor Internal. Implementasi struktur RACI memperjelas pembagian peran antar unit dalam pengelolaan risiko. Temuan ini menegaskan bahwa penerapan ISO 27001:2022 secara sistematis dapat meningkatkan efektivitas kontrol keamanan informasi, transparansi pengelolaan risiko, dan ketahanan terhadap ancaman siber.
Kata Kunci: ISO 27001:2022, Manajemen Risiko, Keamanan Informasi

Abstract: *The implementation of ISO 27001:2022 is a strategic step in strengthening information security risk management in various organizations. The study aims to analyze the implementation of ISO 27001:2022 in information security risk management at the CXY Agency using a qualitative descriptive case study approach. and guided by PermenPAN-RB No. 5 of 2020. The results of the study show that the CXY Agency faces risks such as bugs in applications, cyber attacks, and low HR competency. The main causes include human error, lack of training, and suboptimal infrastructure. Mitigation efforts implemented include the use of dual authentication, information security training, real-time incident monitoring, and the formation of an Internal Audit Team. The implementation of the RACI structure clarifies the division of roles between units in risk management. These findings confirm that the systematic implementation of ISO 27001:2022 can increase the effectiveness of information security controls, transparency of risk management, and resilience to cyber threats.*
Keywords: *ISO 27001:2022, Risk Management, Information Security*

1. Pendahuluan

Penggunaan teknologi membawa risiko yang tidak dapat diabaikan, seperti ancaman keamanan dan kerentanan sistem. Manajemen risiko keamanan menjadi proses sistematis untuk mengidentifikasi, menilai, dan mengendalikan ancaman terhadap keamanan, integritas, dan ketersediaan data (B. Sinaga & & Rochmoeljati, 2024), yang jika dikelola dengan baik dapat mempercepat pengembangan sistem dan meningkatkan kinerja aparatur negara (Bisma, 2022). Manajemen risiko tidak hanya melindungi aset organisasi, tetapi juga mendukung pertumbuhan dan inovasi (Subagyo Ahmad, Simanjuntak Rusli, 2020).

Berdasarkan SOCRadar Indonesia *Threat Landscape Report* 2024, Indonesia mencatat 130 insiden ransomware, 4.046 serangan phishing, dan hampir 44.000 serangan

DDoS, menunjukkan tingginya tingkat ancaman (SOCRadar, 2024). Untuk menjawab tantangan tersebut, pemerintah mengeluarkan beberapa kebijakan strategis seperti Peraturan BRIN No. 2 Tahun 2024 tentang Pedoman Manajemen Pengetahuan SPBE, Peraturan BSSN No. 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE, serta Peraturan BSSN No. 8 Tahun 2024 tentang Standar dan Tata Cara Pelaksanaan Audit Keamanan SPBE. Oleh karena itu, implementasi ISO 27001:2022 sangat relevan dalam pengelolaan risiko keamanan informasi karena mampu meningkatkan kapabilitas organisasi publik dalam menghadapi kompleksitas ancaman digital melalui penguatan tata kelola dan prosedur yang selaras dengan kebijakan pemerintah (Novega, 2024),

Instansi CXY adalah lembaga yang bertanggung jawab dalam pengelolaan teknologi informasi, termasuk penyediaan infrastruktur TI yang handal serta perlindungan data dari berbagai ancaman seperti serangan siber, kebocoran data, dan kesalahan manusia. Sebagai lembaga yang beroperasi dalam sektor publik, Instansi CXY menghadapi tantangan yang semakin kompleks dalam menjaga keamanan informasi, seperti gangguan operasional akibat kerusakan perangkat keras, serangan keamanan berupa *spam* dan virus pada sistem layanan, serta *error* atau *bug* pada aplikasi yang menyebabkan layanan tidak dapat berjalan dengan andal. Oleh karena itu, penerapan SPBE yang ditetapkan oleh BRIN dan BSSN menjadi kunci bagi Instansi CXY untuk memastikan keamanan, keterjagaan, serta kepatuhan terhadap regulasi demi kelangsungan operasional yang aman dan efisien.

ISO 27001 adalah suatu standar keamanan yang menyediakan kerangka kerja untuk merancang, menerapkan, memelihara, dan secara berkelanjutan meningkatkan Sistem Manajemen Keamanan Informasi (SMKI) (Aurabillah et al., 2024), serta memungkinkan organisasi mengidentifikasi potensi ancaman terhadap informasi dan aset melalui penilaian risiko yang sistematis (R. Sinaga & Taan, 2024). Standar *ISO 27001:2022* juga memberikan panduan mengenai kontrol keamanan yang dapat diterapkan untuk mengurangi risiko, termasuk kebijakan, prosedur, dan teknologi yang diperlukan. Penerapan standar ini selaras dengan Permen PANRB No. 5 Tahun 2020 tentang Pedoman Manajemen Risiko SPBE, yang mendorong kesadaran keamanan di seluruh organisasi pemerintahan agar setiap individu memahami perannya dalam menjaga kerahasiaan data dan memastikan regulasi dipatuhi.

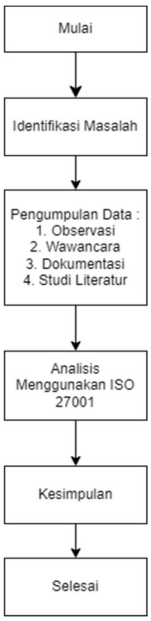
Dalam konteks implementasi *ISO 27001:2022* dalam manajemen risiko keamanan informasi, penelitian sebelumnya menunjukkan bahwa penerapan standar ini dapat secara signifikan meningkatkan keamanan dan efektivitas sistem informasi di berbagai instansi, seperti yang disoroti oleh (Sari et al., 2022) mengenai perlindungan data sensitif di institusi pendidikan dan oleh (R, 2024) terkait peningkatan keamanan data serta kepercayaan pelanggan di PT. Surveyor Indonesia. Selain itu, penelitian oleh (Fattah Ys et al., 2024) menunjukkan bahwa penerapan *ISO 27001:2022* di Perpusnas RI mampu mengidentifikasi dan mengelola risiko yang belum teratasi, sehingga memperkuat sistem manajemen keamanan informasi, sementara (Fadli, 2024) menjelaskan bahwa analisis penerapan di Pusat Data dan Sistem Informasi Badan Standardisasi Nasional menghasilkan identifikasi risiko tinggi serta rekomendasi penanganan melalui pembuatan SOP yang sesuai dengan kontrol kerangka kerja *ISO 27001:2022*. Penelitian lain oleh (Aminudin & Supriyanto, 2024) juga mengungkapkan bahwa penggunaan ISO/IEC 27001 pada BAPENDA Jawa Tengah secara signifikan membantu mengidentifikasi risiko tinggi serta memetakan mitigasinya menggunakan kontrol ISO dan NIST, sehingga implementasi ISO 27001:2022

di Instansi CXY tidak hanya akan memperkuat sistem manajemen keamanan informasi, tetapi juga meningkatkan transparansi dan akuntabilitas dalam pengelolaan informasi publik serta memberikan kerangka kerja yang efektif untuk menghadapi berbagai risiko yang mungkin muncul.

Penelitian berfokus pada implementasi ISO 27001:2022 dalam manajemen risiko keamanan informasi di Instansi CXY, dengan tujuan untuk menganalisis dan mengevaluasi penerapannya serta mengidentifikasi kekuatan dan kelemahan dari standar tersebut. Meskipun *ISO 31000* juga merupakan standar manajemen risiko internasional, *ISO 27001:2022* lebih spesifik untuk keamanan informasi karena menggunakan pendekatan sistematis melalui kebijakan, kontrol, dan mitigasi, serta mengeksplorasi tantangan yang dihadapi selama proses implementasi dan solusi efektif yang dapat diterapkan. Penelitian ini diharap dapat memberikan kontribusi nyata terhadap kebijakan serta praktik manajemen risiko yang lebih baik di lingkungan pemerintahan, terutama dalam memilih standar yang paling sesuai dengan kebutuhan keamanan informasi, sejalan dengan pentingnya pemahaman terhadap jenis-jenis risiko dan proses mitigasinya dalam konteks transformasi digital (Harahap et al., 2023).

2. Metode Penelitian

Metode kualitatif deskriptif dengan menggunakan pendekatan kualitatif guna memperoleh wawasan lebih dalam tentang implementasi *ISO 27001:2022* dalam pengelolaan risiko keamanan informasi di Instansi CXY. Penelitian ini berlangsung di Instansi CXY dengan periode pengumpulan data selama beberapa bulan untuk memastikan keakuratan dan kelengkapan informasi yang diperoleh. Untuk memperjelas dan memperluas wawasan terkait tahap penelitian, dilihat pada Gambar 1.



Gambar 1. Siklus Penelitian

1. Pertama, merumuskan masalah yang muncul dan di identifikasi menggunakan metode analisa pendukung yaitu dengan mempelajari studi literatur yang berkaitan dengan penelitian ini untuk menemukan solusi terhadap permasalahan yang dihadapi. Pada

tahapan ini menghasilkan daftar masalah yang jelas dan fokus sebagai dasar untuk analisis lebih lanjut, serta memperoleh pemahaman lebih tentang tantangan yang dihadapi dalam manajemen risiko keamanan dengan implementasi *ISO 27001:2022*.

2. Kedua, pengumpulan data melalui observasi, wawancara, dokumentasi serta memanfaatkan studi literatur.
   - Observasi dilakukan dengan cara memperhatikan secara langsung berbagai peristiwa yang memiliki keterkaitan dengan tujuan dari suatu penelitian (Malahati et al., 2023). Melakukan observasi pada lingkungan Instansi CXY. Tujuan dari observasi ini adalah untuk memperoleh pemahaman langsung mengenai proses manajemen risiko teknologi informasi pada Instansi CXY.
   - Wawancara bertujuan mendapatkan data dengan cara bertanya langsung kepada narasumber / responden (Trivaika & Senubekti, 2022). Wawancara dilakukan dengan staf Instansi CXY yang memiliki pengetahuan dan pengalaman dalam manajemen risiko teknologi informasi.
   - Dokumentasi dilakukan dengan mempelajari dokumen – dokumen seperti notulensi, buku, peraturan, jurnal, dll. Dalam penelitian kualitatif ini, dokumen yang diteliti adalah kebijakan terkait keamanan informasi, prosedur operasional, dan *risk register* yang ada di Instansi CXY.
   - Studi literatur bertujuan untuk mengungkap beberapa teori yang relevan dengan permasalahan pada penelitian yang sedang dilakukan. Studi literatur dilakukan dengan merujuk pada berbagai referensi seperti artikel ilmiah, buku, dan jurnal publikasi yang berkaitan dengan *ISO 27001:2022* dan manajemen risiko teknologi informasi. Tahapan ini menghasilkan data yang valid dan dapat diandalkan untuk melakukan analisis lebih lanjut, termasuk informasi tentang kebijakan, prosedur, dan praktik keamanan informasi yang diterapkan.
3. Ketiga, proses analisa data menggunakan metode analisis tematik untuk mengidentifikasi tema utama penerapan *ISO 27001:2022* di Instansi CXY, termasuk tantangan dan langkah mitigasi terbaik. Hasilnya memberikan pemahaman tentang penilaian risiko, pengendalian keamanan, pemantauan sistem, serta rekomendasi pengendalian yang sesuai.
4. Keempat, kesimpulan dari penelitian diharapkan menghasilkan beberapa keluaran penting terkait implementasi *ISO 27001:2022* dalam manajemen risiko keamanan informasi di Instansi CXY.

3. Hasil dan Pembahasan

Manajemen risiko keamanan informasi di Instansi CXY dimulai dengan tahap identifikasi ancaman atau risiko keamanan berdasarkan kerangka kerja *ISO 27001:2022*. Tahapan selanjutnya mencakup analisis dan penilaian Tingkat risiko yang dilakukan sesuai dengan ketentuan dalam Lampiran 1 PermenPAN-RB No. 5 Tahun 2020 tentang Pedoman Manajemen Risiko SPBE. Proses ini mencakup pemetaan Tingkat probabilitas dan dampak risiko matriks standar yang telah ditetapkan.

3.1 Identifikasi Risiko Keamanan (*Security Risk Identification)*

Dalam implementasi *ISO 27001:2022,* setiap pihak dalam Instansi CXY menjalankan fungsi serta kewajiban yang tidak sama dalam mengelola risiko keamanan informasi. RACI Chart seperti pada gambar 2, membantu mengklarifikasi peran dan

tanggung jawab masing – masing pihak agar proses manajemen keamanan informasi dapat berjalan lebih efektif dan terkoordinasi.

Aktivitas	Unit TI Pusat	Pimpinan Utama	Unit Pengguna	Unit Perencanaan	Auditor Internal	Tim Manajemen Risiko
Penyusunan dan Penetapan Kebijakan Manajemen Risiko Keamanan Informasi	R	A	C	C	I	I
Identifikasi Risiko Keamanan Informasi	R	A	C	I	I	C
Penilaian Risiko (Kemungkinan dan Dampak)	R	A	C	C	I	C
Penetapan Rencana Penanganan Risiko (Mitigasi, Transfer, dll)	R	A	C	C	I	C
Implementasi Tindakan Pengendalian Risiko Keamanan Informasi (*Annex A ISO 27001:2022*)	R	A	C	I	I	I
Monitoring dan *Review* Risiko Keamanan Informasi	R	A	C	C	C	C
Pelaporan Risiko Keamanan Informasi kepada Pimpinan	R	A	I	C	C	I
Audit Internal atas Pengelolaan Risiko Keamanan Informasi	C	I	I	I	R	C
Sosialisasi dan Pelatihan Terkait Keamanan Informasi dan Manajemen Risiko	R	A	C	I	I	I
Tinjauan Berkala dan Peningkatan Sistem Manajemen Keamanan Informasi (SMKI)	R	A	C	C	C	C

Gambar 2. RACI Chart

Dalam implementasi *ISO 27001:2022* pada aspek manajemen risiko keamanan informasi, Instansi CXY menyusun struktur tanggung jawab berdasarkan prinsip RACI (*Responsible, Accountable, Consulted, Informed*) yang mengacu pada pedoman internal. **Unit TI Pusat**, berperan sebagai pelaksana utama dalam proses identifikasi risiko, pelaksanaan kontrol dalam hal ini Instansi CXY berperan sebagai pelaksana utama (*Responsible*) dalam proses identifikasi risiko keamanan informasi, penilaian dan mitigasi risiko, pelaksanaan pengendalian keamanan informasi, serta pengelolaan teknis terhadap sistem keamanan informasi secara menyeluruh. Unit ini bertanggung jawab memastikan bahwa kontrol – kontrol dari *Annex A ISO 27001:2022* diterapkan secara efektif sesuai dengan kebutuhan instansi. **Pimpinan Utama** berperan sebagai penanggung jawab utama (*Accountable*) dalam seluruh proses manajemen risiko, keputusan akhir, pengesahan kebijakan, persetujuan atas rencana mitigasi risiko, serta komitmen terhadap peningkatan berkelanjutan berada pada tingkat ini. **Unit perencanaan, Unit Pengguna, dan Tim Manajemen Risiko** berperan sebagai **(***Consulted)* dalam penyusunan kebijakan dan evaluasi sistem. Struktur ini memperkuat kolaborasi antarunit dalam mendukung tata kelola keamanan informasi.

Unit Pengguna di lingkungan Instan CXY merupakan unit – unit non-TI yang memanfaatkan layanan teknologi informasi dalam operasional harian dan memiliki peran penting dalam proses manajemen risiko keamanan informasi. Dalam RACI Chart, unit pengguna berperan sebagai pihak yang dikonsultasikan (*Consulted*) dan diinformasikan (*Informed*), terutama dalam memberikan masukan terkait identifikasi, potensi ancaman yang dihadapi, serta efektifitas pengendalian keamanan yang diterapkan. Masukan dari unit pengguna penting untuk identifikasi risiko dan evaluasi kontrol keamanan. Mereka juga menerima informasi terkait kebijakan, kontrol, hasil monitoring dan evaluasi risiko yang relevan, sebagai bagian upaya peningkatan kesadaran dan kepatuhan terhadap sistem manajemen keamanan informasi sesuai prinsip *ISO 27001:2022.* Unit pengawasan internal (**Auditor Internal),** yang bertugas sebagai pelaksana audit internal keamanan informasi, memiliki peran penting dalam mengevaluasi efektivitas penerapan pengendalian risiko

secara independen dari fase *Check* pada siklus PDCA(*Plan-Do-Check-Act*) sebagaimana disyaratkan oleh *ISO 27001:2022.* **Tim Manajemen Risiko** dan unit – unit lainnya juga diinformasikan (*Informed*) mengenai hasil pelaksanaan dan pemantauan risiko keamanan informasi guna mendukung transparansi dan pengambilan keputusan yang lebih baik.

Identifikasi risiko keamanan yang dilakukan merupakan hasil pengumpulan data secara empiris dari narasumber di Instansi CXY. Risiko – risiko seperti *bug* atau *error* saat pengoperasian aplikasi, ancaman siber (*fraud, hacking, spam*, virus), hingga gangguan operasional akibat kerusakan sistem perangkat keras menunjukkan adanya potensi gangguan yang signifikan terhadap sistem informasi yang digunakan. Penyebab dari kejadian – kejadian tersebut antara lain adalah *human error,* kurangnya regulasi, terdapat data/informasi yang belum terstruktur dengan baik, lemahnya pemeliharaan sistem, hingga kompetensi SDM yang belum memadai. Penanganan risiko mengacu pada pendekatan RACI (Responsible, Accountable, Consulted, Informed). Struktur ini selaras dengan prinsip *ISO 27001:2022* dan regulasi internal. **Unit TI Pusat** Instansi CXY yang bertindak sebagai pelaksana utama (*Responsible*), memegang peran sentral dalam merespons langsung kejadian – kejadian tersebut melalui penerapan kontrol teknis, pemeliharaan sistem, serta pembaharuan terhadap aplikasi lama yang rentan.

Sementara itu, **Tim Manajemen Risiko** sebagai pihak yang *Accountable* memastikan proses identifikasi risiko dianalisis dan ditindaklanjuti seperti pada gambar 2. Unit pengawasan internal (**Auditor Internal)** mengevaluasi efektivitas penanganan risiko melalui audit internal. **Unit Pengguna** berkontribusi melalui laporan kejadian operasional dan evaluasi layanan yang mereka alami secara langsung. Prinsip RACI terbukti aplikatif dalam menangani kejadian nyata di lapangan. Informasi dari narasumber menegaskan pentingnya pembagian peran yang jelas. Diperlukan peningkatan kapasitas, regulasi, dan sistem untuk menjaga keberlanjutan keamanan informasi.

3.2 Analisis Risiko (*Risk Analysis)*

Dalam penelitian ini, analisis risiko dilakukan dengan mengacu pada PermenPAN-RB No. 5 Tahun 2020 tentang Pedoman Manajemen SPBE, mulai dari identifikasi risiko hingga penetapan strategi penanganannya.

Unit Pemilik Risiko (UPR) memiliki tanggung jawab dalam mengelola penerapan manajemen risiko SPBE. Terlihat pada gambar 3 yang mencakup nama unit, tugas, fungsi, dan periode waktu pelaksanaan manajemen risiko.

Informasi Umum	
Nama UPR SPBE	Unit TI Pusat
Tugas UPR SPBE	Menyediakan, mengelola, dan mengamankan infrastruktur teknologi informasi serta menyusun kebijakan keamanan informasi
Fungsi UPR SPBE	a. Penyusunan dan penetapan penilaian Risiko SPBE dan rencana pelaksanaan Manajemen Risiko SPBE b. Pelaksanaan koordinasi penerapan Manajemen Risiko SPBE kepada semua pemangku kepentingan; c. Pelaksanaan operasional Manajemen Risiko SPBE yang efektif melalui komunikasi dan konsultasi, pencatatan dan pelaporan, serta pemantauan dan evaluasi; dan d. pelaksanaan pembinaan budaya sadar Risiko SPBE melalui sosialisasi.
Periode Waktu	1 Januari – 31 Desember 2025

Gambar 3. Informasi Umum UPR SPBE

Sasaran SPBE menjelaskan tujuan yang ingin dicapai oleh UPR dalam penerapan SPBE, serta indikator dan target kinerja yang akan dijadikan acuan dalam mengelola risiko, terlihat pada gambar 4.

Sasaran UPR SPBE	Sasaran SPBE	Indikator Kinerja SPBE	Target Kinerja SPBE
Terwujudnya Pemerintahan Berbasis Elektronik	Terwujudnya tata kelola dan manajemen SPBE yang efektif dan efisien	Indeks Pelaksanaan Sistem Pemerintahan Berbasis Elektronik	5

Gambar 4. Sasaran SPBE

Struktur pelaksana risiko SPBE menampilkan susunan peran yang terlibat dalam proses manajemen risiko, mulai dari pemilik risiko, koordinator, hingga pengelola risiko. Terlihat pada gambar 5 memastikan adanya pembagian tugas yang jelas.

Struktur Pelaksana Manajemen Risiko SPBE	
Pemilik Risiko SPBE	Kepala Unit TI Pusat
Koordinator Risiko SPBE	Kepala Bidang Keamanan Informasi
Pengelola Risiko SPBE	Tim Risiko Keamanan TI

Gambar 5. Struktur Pelaksana Risiko SPBE

Daftar pemangku kepentingan berisi baik unsur internal maupun eksternal yang terkait dengan UPR SPBE dalam proses penerapan manajemen risiko. Menjelaskan hubungan dan kelompok pemangku kepentingan yang terlihat pada gambar 6.

Pemangku Kepentingan	Kelompok Pemangku Kepentingan	Hubungan
Pimpinan Utama	Unit Kerja Internal	Pengambil keputusan utama dalam kebijakan dan mitigasi risiko SPBE
Unit TI Pusat	Unit Kerja Internal	Pelaksana utama dalam pengelolaan dan pengendalian risiko SPBE
Unit Pengguna	Unit Kerja Internal	Penerima layanan TI, pelapor insiden, serta pemberi masukan atas kendala layanan
Unit Perencanaan	Unit Kerja Internal	Mendukung perencanaan strategis penanganan risiko dan alokasi sumber daya
Auditor Internal	Unit Kerja Internal	Evaluator independen atas efektivitas penerapan pengendalian risiko
Tim Manajemen Risiko	Unit Kerja Internal	Koordinator dan pengelola keseluruhan proses manajemen risiko SPBE
BSSN / Regulator Eksternal	Unit Kerja Eksternal	Pemberi regulasi dan pedoman keamanan informasi pemerintahan
Masyarakat / Pengguna Layanan Digital	Unit Kerja Eksternal	Penerima manfaat dari layanan publik berbasis elektronik; terpengaruh oleh risiko layanan TI

Gambar 6. Daftar Pemangku Kepentingan

Daftar peraturan perundang – undangan mencantumkan peraturan yang menjadi dasar hukum dan acuan dalam pelaksanaan manajemen risiko SPBE. Memuat amanat dari masing – masing peraturan yang terlihat pada gambar 7.

Peraturan Perundang-Undangan	Amanat
Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik	Pasal 7 Pasal 29 Pasal 42 Pasal 46 Pasal 47
Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Pemerintahan Berbasis Elektronik	Pasal 2 Pasal 3 Pasal 4 Pasal 5
PermenPAN-RB Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik	Pasal 8 Penjelasan lebih rinci terkait kriteria tingkat kematangan penerapan Manajemen Risiko SPBE terdapat pada Domain 3 Manajemen SPBE, Aspek 5 Penerapan Manajemen SPBE, Indikator 21 Tingkat Kematangan Penerapan Manajemen Risiko SPBE

Gambar 7. Daftar Peraturan Perundang - Undangan

Kategori risiko SPBE mengelompokkan jenis – jenis yang mungkin dihadapi berdasarkan karakteristik penyebabnya, terlihat pada gambar 8.

No	Kategori Risiko SPBE
1.	Rencana Induk SPBE Nasional
2.	Arsitektur SPBE
3.	Peta Rencana SPBE
4.	Proses Bisnis
5.	Rencana dan Anggaran
6.	Inovasi
7.	Kepatuhan terhadap Peraturan
8.	Pengadaan Barang dan Jasa
9.	Proyek Pembangunan/Pengembangan Sistem
10.	Data dan Informasi
11.	Infrastruktur SPBE
12.	Aplikasi SPBE
13.	Keamanan SPBE
14.	Layanan SPBE
15.	Sumber Daya Manusia SPBE
16.	Bencana Alam

Gambar 8. Kategori Risiko

Area dampak risiko SPBE menunjukkan area yang terdampak apabila risiko SPBE terjasi, terlihat pada gambar 9.

No	Area Dampak Risiko SPBE
1	Finansial
2	Reputasi
3	Kinerja
4	Layanan Organisasi
5	Operasional dan Aset TIK
6	Hukum dan Regulasi
7	Sumber Daya Manusia

Gambar 9. Area Dampak Risiko SPBE

Kriteria kemungkinan SPBE mengukur peluang dan frekuensi terjadinya risiko dalam periode tertentu, dinyatakan dalam level seperti hampir tidak terjadi hingga hampir pasti terjadi berdasarkan frekuensi tahunan. Dengan kriteria ini terlihat pada gambar 10, Instansi CXY dapat memperkirakan seberapa sering risiko muncul, sehingga memudahkan penentuan prioritas dan strategi pengendalian yang tepat.

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

Gambar 10. Kriteria Kemungkinan SPBE

Kriteria dampak digunakan untuk mengukur seberapa besar pengaruh dari suatu risiko terhadap area dampak yang telah ditentukan. Kriteria disusun dalam beberapa level, dari tidak signifikan hingga sangat signifikan yang terlihat pada gambar 11.

Area Dampak		Level Dampak				
		1 Tidak Signifikan	2 Kurang Signifikan	3 Cukup Signifikan	4 Signifikan	5 Sangat Signifikan
Finansial	Negatif	Jumlah kerugian negara ≤ Rp 10 Juta	Jumlah kerugian ≥ Rp 10 juta s.d Rp 50 juta	Jumlah kerugian negara lebih dari Rp 50 juta s.d Rp 100 juta	Jumlah kerugian negara lebih dari Rp 100 juta s.d Rp 500 juta	Jumlah kerugian negara lebih dari Rp 500 Juta
Reputasi	Negatif	Terdapat pemberitaan negatif namun tidak mengakibatkan penurunan kepercayaan	Terdapat pemberitaan negatif yang dapat mempengaruhi tingkat kepercayaan pihak yang berkaitan	Terdapat pemberitaan negatif yang terus menurunkan kepercayaan pihak yang berkaitan	Hilangnya kepercayaan pihak yang berkaitan	Pihak yang berkaitan sama sekali tidak percaya
Operasional dan Aset TIK	Negatif	Terdapat gangguan namun tidak mengakibatkan proses bisnis terganggu	Terdapat gangguan yang menyebabkan 1 mata rantai proses bisnis terganggu	Terdapat gangguan yang menyebabkan lebih dari 1 mata rantai proses bisnis terganggu	Terdapat gangguan yang menyebabkan seluruh proses bisnis terganggu	Terjadi kelumpuhan pada proses bisnis
Kinerja	Negatif	Menimbulkan penundaan aktivitas maksimal 24 jam	Menimbulkan penundaan aktivitas maksimal 2 x 24 jam	Menimbulkan penundaan aktivitas maksimal 7 x 24 jam	Menimbulkan penundaan aktivitas lebih dari 7 x 24 jam	Menimbulkan penundaan aktivitas secara permanen
Sumber Daya Manusia	Negatif	Berkurangnya tenaga kerja	Berkurangnya tenaga kerja yang kompeten	Berkurangnya tenaga kerja yang yang kompeten tidak tersertifikasi	Berkurangnya tenaga kerja yang tersertifikasi	Berkurangnya tenaga kerja yang berkompeten dan tersertifikasi
Layanan Organisasi	Negatif	Pelayanan tertunda ≤ 1 hari	Pelayanan tertunda diatas 1 hari s.d 5 hari	Pelayanan tertunda diatas 5 hari s.d 15 hari	Pelayanan tertunda diatas 15 hari s.d 30 hari	Pelayanan tertunda lebih dari 30 hari

Gambar 11. Kriteria Dampak SPBE

Matriks risiko merupakan alat yang sangat penting dalam membantu mengidentifikasi, menganalisis, dan mengelola risiko keamanan informasi secara efektif. Dengan menggunakan matriks risiko terlihat pada gambar 12, Instansi CXY dapat meningkatkan ketahanan terhadap ancaman keamanan dan memastikan ketepatan langkah mitigasi yang diambil untuk melindungi informasi sensitif.

Matriks Analisis Risiko 5 x 5			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 12. Matriks Risiko

Level risiko dikategorikan berdasarkan kemungkinan dan dampaknya, dari **rendah** hingga **tinggi**, seperti terlihat pada gambar 13. Risiko **rendah** berarti ancaman minimal dengan dampak terbatas, sedangkan risiko **tinggi** menunjukkan ancaman besar yang berdampak signifikan pada kerahasiaan, integritas, dan ketersediaan informasi. Evaluasi ini menjadi dasar strategi mitigasi melalui pengendalian teknis, kebijakan, dan peningkatan kesadaran pengguna untuk menjaga ketahanan sistem di Instansi CXY.

Level Risiko	Rentang Besaran Risiko	Simbol Warna
Sangat Rendah	1 - 5	Biru
Rendah	6 - 10	Hijau
Sedang	11 – 15	Kuning
Tinggi	16 – 20	Jingga
Sangat Tinggi	21 - 25	Merah

Gambar 13. Level Risiko

Selera risiko adalah tingkat risiko maksimum yang masih dapat diterima oleh suatu organisasi dalam mencapai tujuan tanpa menimbulkan kerugian yang signifikan, terlihat pada gambar 14.

No	Kategori Risiko SPBE	Besaran Risiko Minimum Yang ditangani	
		Risiko SPBE Positif	Risiko SPBE Negatif
1	Rencana Induk SPBE Nasional	x	6
2	Arsitektur SPBE	x	6
3	Peta Rencana SPBE	x	7
4	Proses Bisnis	x	7
5	Rencana dan Anggaran	x	14
6	Inovasi	x	12
7	Kepatuhan terhadap Peraturan	x	14
8	Pengadaan Barang dan Jasa	x	17
9	Proyek Pembangunan/ Pengembangan Sistem	x	13
10	Data dan Informasi	x	21
11	Infrastruktur SPBE	x	21
12	Aplikasi SPBE	x	18
13	Keamanan SPBE	x	18
14	Layanan SPBE	x	18
15	Sumber Daya Manusia SPBE	x	22
16	Bencana Alam	x	8

Gambar 14. Selera Risiko

Rencana penanganan risiko SPBE merupakan langkah strategis yang disusun supaya risiko yang dikelola tetap dalam batas toleransi yang ditunjukkan pada gambar 15.

Opsi Penanganan Risiko SPBE	Rencana Aksi Penanganan Risiko SPBE	Keluaran	Jadwal Implementasi	Penanggung Jawab
Mitigasi	Menyusun dan melakukan sosialisasi SOP keamanan informasi, penerapan *patch management* dan uji coba sistem secara rutin untuk mencegah *error/bug*	SOP Keamanan Informasi, Bukti sosialisasi	Triwulan II 2025	Unit TI Pusat, Tim, Manajemen Risiko
Mitigasi	Pengawasan dan menerapkan **multi-factor authentication (MFA)** dan peningkatan firewall untuk mencegah akses tidak sah	Log update sistem keamanan, sistem MFA aktif, laporan keamanan	Tiap bulan mulai Januari 2025	Unit TI Pusat
Mitigasi	Penyusunan standar pelaporan / SOP	Template pelaporan	Februari 2025	Unit TI Pusat, Tim SDM
Mitigasi	Penyusunan kajian kebutuhan SDM SPBE	Laporan kajian SDM	Triwulan II 2025	Unit TI Pusat, Bagian SDM
Mitigasi	Validasi dan pembersihan data secara rutin untuk mencegah data tidak valid	Form validasi, laporan koreksi data	Juli–September 2025	Auditor Internal
Mitigasi	Peningkatan sistem deteksi dini dan pengujian berkala untuk memastikan sistem berfungsi optimal	Notifikasi otomatis, laporan pengujian	Agustus–Oktober 2025	Unit TI Pusat
Mitigasi	Pelatihan SDM dan simulasi insiden keamanan informasi untuk meningkatkan kompetensi	Modul pelatihan dan sertifikat pelatihan	Triwulan II dan IV 2025	Tim Manajemen Risiko & SDM

Gambar 15. Rencana Penanganan Risiko

3.3 Pembahasan

Penelitian ini menganalisis implementasi *ISO 27001:2022* dalam manajemen risiko keamanan informasi di Instansi CXY. Identifikasi, penilaian dampak, kemungkinan terjadinya risiko, serta rencana mitigasi disusun dengan berpedoman pada *ISO 27001:2022.* Sementara itu, PermenPAN-RB No. 5 Tahun 2020 digunakan sebagai acuan dalam pengelolaan risiko secara menyeluruh, khususnya dalam konteks manajemen risiko Sistem Pemerintahan Berbasis Elektronik (SPBE), termasuk penggunaan formular berupa tabel struktur pelaksanaan risiko, pemangku kepentingan, area dampak, dan matriks risiko SPBE. Hasil penelitian menunjukkan bahwa Instansi CXY menghadapi risiko seperti *bug* aplikasi, serangan siber (*fraud, hacking, spam*, virus), kerusakan perangkat keras, serta rendahnya kompetensi SDM. Penyebab utamanya adalah *human error*, teknologi yang belum diperbarui, kurangnya pemeliharaan, serta minimnya pelatihan. Rendahnya kompetensi SDM merupakan faktor kunci dalam insiden keamanan informasi, sebagaimana dijelaskan oleh (Aurabillah et al., 2024) dan (R. Sinaga & Taan, 2024), yang menekankan pentingnya peran SDM dalam keberhasilan implementasi ISO 27001.

Upaya yang telah dilakukan antara lain pembentukan Tim Auditor Internal, enkripsi data, dan pedoman teknis keamanan, namun efektivitas sistem belum optimal akibat kurangnya sosialisasi dan pelatihan internal, yang menurunkan kesadaran staf terhadap prosedur keamanan dan meningkatkan insiden akibat human error. Hambatan pelatihan meliputi keterbatasan anggaran, belum adanya kebijakan pelatihan berkelanjutan, serta budaya organisasi yang belum sepenuhnya mendukung manajemen risiko informasi. Penelitian merekomendasikan mitigasi komprehensif seperti pelatihan dan simulasi insiden, patch management, autentikasi ganda, sistem monitoring real-time, serta evaluasi berkala, dengan penggunaan struktur RACI untuk memperkuat tata kelola risiko. Dengan pendekatan sistematis sesuai ISO 27001:2022 dan PermenPAN-RB No. 5 Tahun 2020, Instansi CXY diharapkan dapat meningkatkan efektivitas sistem manajemen keamanan informasi dan ketahanan terhadap ancaman siber. Rekomendasi ini menjadi panduan

penting bagi Instansi CXY dalam mengatasi tantangan dan memperkuat manajemen keamanan informasi. Penelitian ini berkontribusi dalam memahami implementasi *ISO 27001:2022* pada manajemen risiko TI serta wawasan bagi organisasi yang ingin menerapkan standar serupa guna mencapai tujuan keamanan informasi yang lebih baik dan melindungi aset dari berbagai ancaman.

4. Kesimpulan dan Saran

Penelitian ini menunjukkan bahwa implementasi *ISO 27001:2022* di Instansi CXY masih menghadapi beberapa tantangan, seperti *bug* pada aplikasi, serangan siber, kerusakan perangkat keras, dan rendahnya kompetensi SDM. Penyebab utama risiko meliputi *human error*, teknologi yang usang, kurangnya pemeliharaan, serta minimnya pelatihan. Meskipun telah dilakukan upaya seperti pembentukan Tim Auditor Internal, enkripsi data, dan penyusunan pedoman teknis keamanan, efektivitas sistem belum optimal karena rendahnya intensitas sosialisasi dan pelatihan internal, yang berimbas pada kurangnya kesadaran staf terhadap standar keamanan informasi. Pendekatan struktur RACI dan integrasi antara *ISO 27001:2022* dan PermenPAN-RB No. 5 Tahun 2020 telah diterapkan dalam proses identifikasi, dokumentasi, dan mitigasi risiko, sehingga menghasilkan tata kelola keamanan informasi yang lebih terstruktur dan akuntabel. Kontribusi ilmiah dari penelitian ini terletak pada pengembangan model manajemen risiko keamanan informasi yang menggabungkan pendekatan teknis *ISO 27001:2022* dengan regulasi administratif PermenPAN-RB No. 5 Tahun 2020, yang relevan diimplementasikan dalam konteks sektor publik di Indonesia. Model ini tidak hanya memperkuat ketahanan terhadap ancaman siber melalui kontrol teknis seperti *patch management*, autentikasi ganda, dan monitoring *real-time*, tetapi juga menekankan pentingnya pemetaan peran dan pemangku kepentingan dalam struktur organisasi, serta penyusunan dokumen risiko yang siap diaudit. Dengan demikian, hasil penelitian ini memberikan kontribusi nyata bagi organisasi pemerintah yang ingin meningkatkan efektivitas manajemen risiko SPBE secara menyeluruh dan selaras dengan kebijakan nasional.

Daftar Pustaka

Aminudin, A., & Supriyanto, A. (2024). Kematangan risiko keamanan informasi layanan TI menggunakan pendekatan NIST dan standar ISO 27001:2013 (Studi kasus: Bapenda Provinsi Jawa Tengah). *AITI: Jurnal Teknologi Informasi*, *21*(2), 210–229.

Aurabillah, B., Putri, L. A., Fadhlilla, N. C., & Wulansari, A. (2024). Implementasi Framework ISO 27001 Sebagai Proteksi Keamanan Informasi Dalam Pemerintahan (Systematic Literature Review). *JATI (Jurnal Mahasiswa Teknik Informatika)*, *8*(1), 454–460. https://ejournal.itn.ac.id/index.php/jati/article/download/8736/5005

Bisma, R. (2022). Risiko Aset Teknologi Informasi: Studi kasus Implementasi Manajemen Risiko SPBE Dinas Komunikasi dan Informatika Pemerintah Kota Balikpapan. *Journal of Information Engineering and Educational Technology*, *6*(2), 73–79. https://doi.org/10.26740/jieet.v6n2.p73-79

Fadli, M. R. (2024). *Analisa Penerapan Sistem Manajemen Keamanan Informasi Berdasarkan ISO 27001:2022 Di Pusat Data*. 1–23.

Fattah Ys, M. A., Parga Zen, B., & Wasitarini, D. E. (2024). Penerapan Sistem Manajemen Keamanan Informasi ISO 27001 pada Perpusnas RI dalam mendukung Keamanan Tata Kelola Teknologi Informasi. *Cyber Security Dan Forensik Digital*, *6*(2), 76–82.

https://doi.org/10.14421/csecurity.2023.6.2.4190

Harahap, L. R., Manaf, P. A., Nusantara, B., Syamil, A., & Utami, E. Y. (2023). *Manajemen Risiko Era Digital* (Issue September). https://www.researchgate.net/publication/376807892

Malahati, F., B, A. U., Jannati, P., Qathrunnada, &, & Shaleh. (2023). Analisis Penerapan Sistem Manajemen Keamanan Informasi Pada Website Official STT NF Dengan SNI ISO/IEC 27001:2022. *JURNAL PENDIDIKAN DASAR*, *11*(2), 341–348. https://doi.org/10.46368/jpd.v11i2.902

Novega, T. K. (2024). *Manajemen Risiko Pada Era Digital*. *July*. https://doi.org/10.13140/RG.2.2.21047.33448

R, T. A. P. (2024). Sistem Manajemen Keamanan Informasi (SMKI) di PT. Surveyor Indonesia Cabang Surabaya: Penerapan Standar ISO 27001:2013. *Jurnal Ilmiah Multidisiplin*, *3*(6).

Sari, M. K., Saintika, Y., & Prabowo, W. A. (2022). Penyusunan Manajemen Risiko Keamanan Informasi Dengan Standar ISO 27001 Studi Kasus Institut Teknologi Telkom Purwokerto. *Jurnal Sistem Dan Teknologi Informasi (JustIN)*, *10*(4), 423. https://doi.org/10.26418/justin.v10i4.48977

Sinaga, B., & & Rochmoeljati, R. (2024). Analisis Manajemen Risiko Aset Teknologi Informasi dan Pemeliharaan Aset Menggunakan Quantitative Risk Analysis WH-TGR. *Jurnal Teknik Industri*, *27*(1), 28–41. http://univ45sby.ac.id/ejournal/index.php/industri/index

Sinaga, R., & Taan, F. (2024). Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala. *Nuansa Informatika*, *18*(2), 46–54. https://doi.org/10.25134/ilkom.v18i2.205

SOCRadar. (2024). *THREAT LANDSCAPE REPORT Vol.1*. *Volume 1*, 1–14. https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf

Subagyo Ahmad, Simanjuntak Rusli, I. A. (2020). Dasar - Dasar Manajemen Risiko. In *Mitra Wacana Media*.

Trivaika, E., & Senubekti, M. A. (2022). PERANCANGAN APLIKASI PENGELOLA KEUANGAN PRIBADI BERBASIS ANDROID. *NUANSA INFORMATIKA*, *16*(1), 33–40. https://doi.org/10.25134/nuansa.v16i1.4670