ANALISIS TINGKAT KEMATANGAN KEAMANAN INFORMASI DATA KEPEGAWAIAN BERDASARKAN KERANGKA KERJA ISO/IEC 27001:2022

Kurnia Rubi Andini[1], Nyoman Gunantara[2], Made Sudarma[2]
[1]Mahasiswa Program Studi, Fakultas Elekto, Universitas Udayana
[2]Dosen Program Studi, Fakultas Elektro, Universitas Udayana
Jalan P.B. Sudirman, Dangin Puri Klod, Kec. Denpasar Bar., Kota Denpasar, Bali 80234
kurniarubi@gmail.com, gunantara@unud.ac.id, msudarma@unud.ac.id

ABSTRAK

Keamanan data adalah masalah kritis ketika menangani informasi pribadi karyawan, terutama jika mereka bekerja untuk organisasi pemerintah. Namun, masih banyak organisasi yang tidak memiliki kebijakan formal tentang bagaimana menerapkan Sistem Manajemen Keamanan Informasi (SMKI). Tujuan dari studi ini adalah untuk menilai tingkat kematangan SMKI yang diterapkan dalam mengelola data pribadi pegawai dan untuk mengidentifikasi kontrol untuk meningkatkan tingkat kematangan. Kuesioner, wawancara, dan observasi digunakan untuk mengumpulkan data tentang pengelolaan data pribadi. Penilaian tingkat kematangan dilakukan pada 21 kontrol sesuai dengan ISO/IEC 27001:2022. Temuan survei mencerminkan tingkat kematangan keseluruhan sebesar 3,6, menunjukkan bahwa sebagian besar kontrol sudah ada. Namun, dari hasil wawancara dan observasi menunjukkan beberapa kesenjangan terutama berkaitan dengan penyamaran data, kebijakan keamanan informasi, dan pemantauan aktivitas. Diharapkan bahwa temuan ini dapat digunakan untuk memberikan dasar bagi pembuatan kebijakan keamanan informasi dan peningkatan kemampuan sumber daya manusia oleh organisasi.
Kata kunci : Sistem Manajemen Keamanan Informasi, ISO/IEC 27001:2022, Data Pribadi, Tingkat Kematangan, Keamanan Informasi

ABSTRACT

Data security is a critical issue when handling employees' personal information, especially for those working in government organizations. However, many organizations still lack formal policies on how to implement an Information Security Management System (ISMS). The objective of this study is to assess the maturity level of ISMS implementation in managing employees' personal data and to identify controls that can enhance its maturity. Data were collected through questionnaires, interviews, and observations regarding the management of personal data. The maturity assessment was conducted on 21 controls based on ISO/IEC 27001:2022. Survey findings indicate an overall maturity level of 3.6, suggesting that most controls are already in place. However, interviews and observations revealed several gaps, particularly related to data masking, information security policies, and activity monitoring. These findings are expected to serve as a foundation for developing information security policies and improving human resource capabilities within the organization.
***Key Words** : Information Security Management System, ISO/IEC 27001:2022, Personal Data, Maturity Level, Information Security*

1. PENDAHULUAN

Pada pertumbuhan pesat teknologi informasi dan komunikasi di era Revolusi Industri 4.0, digitalisasi semakin dikembangkan di hampir semua sektor, termasuk di sektor pemerintahan.

Implementasi e-government memungkinkan pertukaran dan pemrosesan data yang efektif. Di sisi lain, penggunaannya juga membuat data pribadi lebih rentan terhadap kebocoran dan penyalahgunaan, serta diserang oleh kriminal terkait keamanan informasi.

Berbagai kasus peretasan dan pelanggaran data pada data pemerintah telah dilaporkan, termasuk di PusatData Nasional (PDN), yang menekankan perlunya peningkatan perlindungan sistem informasi. Hal ini mencerminkan betapa rentannya data pribadi pegawai pada suatu organisasi dari berbagai ancaman baik ancaman yang berasal dari luar maupun dari dalam organisasi. Untuk mengatasi risiko-risiko ini, pemerintah Indonesia telah mengeluarkan sejumlah peraturan seperti Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi, Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, dan Peraturan BSSN No. 4 tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik.

Salah satu lembaga yang terkait dengan masalah keamanan data belum menerapkan SMKI dalam pengelolaan data, terutama yang dituntut untuk melindungi privasi data para pegawai. Beberapa kontrol fisik dan teknis, seperti tindakan pengamanan dan teknologi telah diterapkan, namum belum sesuai dengan ketentuan yang dituangkan dalam standar ISO/IEC 27001:2022.

Tujuan dari penelitian ini adalah untuk menganalisis kesenjangan dalam pengelolaan data pribadi di salah satu lembaga pemerintah di Bali sesuai dengan standar ISO/IEC 27001:2022 serta untuk mengevaluasi kesesuaina pelaksanaan kontrol (sejauh mana pelaksanaan SMKI sesuai dengan standar yang relevan). Hasil data ini akan digunakan sebagai panduan untuk membuat rekomendasi perbaikan guna meningkatkan tingkat perlindungan data pribadi pegawai dan mencapai tata kelola informasi yang aman, efisien, dan sesuai dengan peraturan nasional.

Untuk memperkuat penelitian, empat subbagian berikut akan meninjau literatur terkait teori, standar, dan penelitian sebelumnya yang berkaitan dengan subjek keamanan informasi dan manajemen data pribadi.

Salah satu penelitian relevan dilakukan oleh Novianto [1], yang melakukan audit Sistem Informasi Manajemen Kepegawaian menggunakan framework COBIT 4.1. Penelitian tersebut melibatkan empat tahap, yaitu identifikasi business goals, IT goals, kontrol COBIT, dan perhitungan maturity level, dengan metode observasi dan wawancara. Hasil audit menunjukkan tingkat kematangan sebesar 2,6.

Penelitian lain dilakukan oleh Triyunsari dan Sutabri [2] yang menganalisis tingkat kematangan manajemen layanan pegawai menggunakan framework COBIT 5 pada sebuah sekolah menengah. Penelitian ini bersifat deskriptif dengan pendekatan kualitatif melalui studi kasus, yang mencakup analisis capability, serta pengumpulan data melalui observasi, wawancara, dan kuesioner. Hasil penelitian menunjukkan adanya kesenjangan sebesar satu tingkat antara kondisi saat ini (as-is) dan tingkat yang diharapkan (to-be) pada beberapa domain proses.

Penelitian sebelumnya menunjukkan berbagai pendekatan dalam audit keamanan informasi dan penilaian tingkat kematangan. Nugraha et al. [3] menggunakan framework COBIT 5 dan ISO 38500 untuk menilai tata kelola teknologi informasi, dengan metode studi pustaka, observasi, wawancara, serta kuesioner, menghasilkan nilai maturity level 2.8 dan rekomendasi untuk proses APO07.

Kamal et al. [4] melakukan audit keamanan informasi di lembaga zakat nasional menggunakan ISO 27001 dengan metode kuantitatif melalui kuesioner, fokus pada tujuh klausul utama, dan menemukan

adanya kelemahan pada manajemen risiko serta akses kontrol.

Candiawan et al. [5] menilai tingkat kematangan keamanan informasi di divisi IT sebuah perusahaan menggunakan ISO 27001:2013 dan ISO 27002:2013 melalui wawancara, observasi, dan studi dokumen, dengan hasil maturity level bervariasi di tiap domain.

Santi et al. [6] mengevaluasi keamanan sistem informasi di sebuah universitas menggunakan ISO 27002:2013 dan menemukan adanya ketidaksesuaian dengan standar tersebut.

Wijaya et al. [7] menilai maturity level risiko di perusahaan media dengan pendekatan PRISMA, menekankan pentingnya ISO 27001 untuk meningkatkan keamanan dan mencegah kebocoran data.

Susanto et al. [8] menganalisis risiko keamanan informasi di sebuah perusahaan dengan ISO/IEC 27001 dan ISO/IEC 27002, yang fokus pada kebijakan dan operasi TI perusahaan.

Nugraha et al. [9] mengintegrasikan ISO/IEC 27001:2022 dengan Undang-Undang Perlindungan Data Pribadi untuk merumuskan model perlindungan data yang sesuai dengan regulasi di Indonesia.

Ryanto et al. [10] melakukan evaluasi keamanan siber di sektor perbankan menggunakan ISO 27001:2022, dengan fokus pada pencegahan kebocoran data dan kontrol keamanan.

Dika et al. [11] mendesain sistem keamanan informasi untuk transformasi digital di sektor BPR menggunakan ISO 27001:2022 dan metode Design Science Research (DSR).

Keterbaruan dari penelitian ini terletak pada analisis tingkat kematangan Sistem Manajemen Keamanan Informasi (SMKI) yang sesuai dengan ISO/IEC 27001:2022 dalam melindungi informasi pribadi karyawan dengan metode analisi triangulasi dari hasil kuesioner, wawancara dan observasi langsung. Berbeda dengan penelitian sebelumnya yang berfokus pada versi standar yang lebih lama atau lebih kepada audit sistem informasi umum, penelitian ini mengukur kontrol keamanan informasi secara langsung terkait perlindungan data pribadi pegawai. Hasil dari analisis tingkat kematangan digunakan sebagai pedoman untuk menyusun rekomendasi yang selaras dengan peratudan perundang-undangan, yaitu Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi. Hasil dari penelitian ini diharapkan dapat menurunkan risiko terhadap keamanan informasi bagi organisasi sebagai pemenuhan kewajiban untuk melindungi data pribadi sesuai dengan perundang-undangan yang berlaku.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kuantitatif dengan tujuan untuk menganalisis kesenjangan penerapan ISO/IEC 27001:2022 pada pengelolaan data pribadi pegawai serta mengevaluasi tingkat kematangan sistem keamanan informasi pada salah satu instansi pemerintahan di Bali. Penelitian ini dilakukan melalui serangkaian tahapan sistematis, mulai dari pengumpulan data hingga penyusunan rekomendasi perbaikan.

2.1 Sumber Data

Penelitian ini menggunakan dua jenis data, yaitu kualitatif dan kuantitatif. Data kualitatif dikumpulkan melalui observasi, wawancara, dan deskripsi rinci untuk memahami konteks dan makna dari fenomena yang diteliti [12]. Sementara itu, data kuantitatif berupa angka yang dikumpulkan melalui kuesioner dan digunakan untuk menganalisis hubungan antarvariabel secara sistematis[12].

Berdasarkan sumbernya, data yang digunakan dibagi menjadi dua jenis:

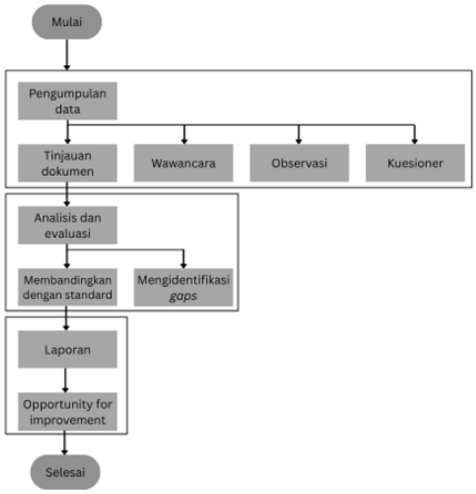
(a) Data primer: Data yang dikumpulkan dari responden melalui observasi, wawancara, dan dari kuesioner seperti persepsi pegawai terhadap keamanan informasi, wawancara dengan pemangku kepentingan terkait.

(b) Data sekunder: diperoleh dari dokumen yang tersedia seperti pedoman ISO/IEC 27001:2022, makalah ilmiah, laporan insiden keamanan, dan dokumentasi pendidikan atau

sosialisasi dalam lingkup keamanan informasi.

2.2 Alur Penelitian

Alur penelitian dibuat untuk memetakan tahap-tahap dan langkah penelitian mulai dari studi literatur hingga penyusunan laporan akhir. Setiap bagian disusun untuk memenuhi tujuan penelitian dalam menilai penerapan ISO/IEC 27001:2022 dan kematangan keamanan informasi. Alur tahapan penelitian ini diberikan pada Gambar 1.



Gambar 1. Alur Penelitian

Tahapan penelitian dimulai dengan tahap awal yaitu menetapkan tujuan dan ruang lingkup untuk audit agar dapat menilai apakah organisasi telah mematuhi ISO/IEC 27001:2022 atau tidak. Data akan dikumpulkan melalui empat metode utama:

(a) Tinjauan dokumen
(b) Wawancara
(c) Observasi langsung proses SMKI di lingkungan organisasi
(d) Kuesioner

Analisis dari data uji yang dikumpulkan bertujuan untuk menjawab apa yang sudah diterapkan pada kondisi sebenarnya sudah sesuai dengan yang dipersyaratkan dalam ISO/IEC 27001:2022. Hasil analisis ini kemudian digunakan sebagai dasar langkah atau tindakan lebih lanjut dalam merumuskan rekomendasi bagi organisasi untuk mengurangi risiko keamanan informasinya.

2.3 Metode Pengumpulan Data

Dalam penelitian ini menggunakan tiga metode yang digunakan sebagai metode pengumpulan data.

(a) Dilakukan observasi *in situ* pada pengelolaan data bagian kepegawaian, mulai dari karakteristik karyawan, prosedur, dan pengaturan hingga perubahan teknologi.
(b) Melakukan wawancara dengan kepala bagian untuk mendapatkan informasi tentang pengelolaan data dan keamanan aset di lingkungan kepegawaian.
(c) Kuesioner disusun berdasarkan kontrol yang tercantum dalam Lampiran ISO/IEC 27001:2022 dan diverifikasi sebelum dikirimkan. Kuesioner ini dikirimkan kepada 16 responden dari Bagian Tata Usaha (Kelompok Kerja Kepegawaian dan Arsip, Kelompok Kerja Keuangan dan Rumah Tangga), serta pimpinan yang terkait langsung dengan pengelolaan data kepegawaian. Responden dipilih berdasarkan kriteria tertentu: distribusi kuesioner ditunjukkan dalam Tabel 1.

Tabel 1. Responden kuesioner

No.	Responden	Jumlah
1.	Kepala Bagian Tata Usaha	1 orang
2.	Ketua Kelompok Kerja Kepegawaian dan Arsip	1 orang
3.	Ketua Kelompok Kerja Keuangan dan Rumah Tangga	1 orang
4.	Anggota Kelompok Kerja Kepegawaian dan Arsip	7 orang
5.	Anggota Kelompok Kerja Keuangan dan Rumah Tangga	6 orang

(d) Tinjauan literatur dilakukan untuk mendukung dasar teoritis sehubungan dengan perundang-undangan, karya penelitian sebelumnya, dan dokumentasi yang mendukung stadar ISO/IEC 27001:2022.

2.4 Rancangan Kuesioner

Kuesioner digunakan sebagai alat utama untuk mengumpulkan data primer dari audit SMKI sesuai dengan ISO/IEC 27001:2022. Setiap pertanyaan dipetakan ke kontrol dalam standar, dan disesuaikan dengan lingkungan organisasi. Instrumen ini menerapkan skala ordinal 4 (pengukuran data secara kuantitatif dan ilustrasi secara kualitatif) secara paralel untuk memberikan persepsi dan pengalaman yang representatif dari responden dalam bentuk terstruktur. Tabel 2 dibawah ini menunjukkan tingkat skala ordinal yang digunakan dalam kuesioner.

Tabel 2. Tingkat skala ordinal

Skala	Keterangan
1	Belum diterapkan
2	Sebagian diterapkan
3	Sudah diterapkan, tetapi belum konsisten
4	Sudah diterapkan sepenuhnya dan konsisten

Kuesioner berikut berada di bawah kontrol ISO/IEC 27001:2022 untuk keamanan informasi dalam pengelolaan data pribadi pegawai. Pilihan kontrol dipengaruhi oleh dampaknya pada organisasi dan risikonya. Kontrol yang saat ini digunakan ditunjukkan dalam Tabel 3.

Tabel 3. Daftar kontrol

No.	Kode Kontrol	Nama Kontrol
Kontrol organisasi		
1.	A.5.1	Kebijakan keamanan informasi
2.	A.5.3	Segregasi tugas
3.	A.5.7	Intelijen ancaman
4.	A.5.15	Kontrol akses
5.	A.5.18	Hak akses
6.	A.5.22	Pemonitoran, riviu, dan manajemen perubahan pelayanan pemasok
Kontrol orang		
1.	A.6.1	Skrining
2.	A.6.2	Syarat dan ketentuan ketenagakerjaan
3.	A.6.3	Kesadaran, Pendidikan dan pelatihan keamanan informasi
4.	A.6.5	Tanggung jawab setelah terminasi atau perubahan pekerjaan
Kontrol fisik		
1.	A.7.1	Perimeter keamanan fisik
2.	A.7.2	Entri fisik
3.	A.7.3	Mengamankan kantor, ruangan, dan fasilitas
4.	A.7.4	Pemonitoran keamanan fisik
5.	A.7.7	Meja bersih dan layer bersih
Kontrol Teknologi		
1.	A.8.1	Perangkat titik akhir pengguna
2.	A.8.3	Pembatasan akses informasi
3.	A.8.4	Akses ke kode sumber
4.	A.8.8	Manajemen kerentanan teknis
5.	A.8.11	Penyamaran (*masking*) data
6.	A.8.16	Pemonitoran aktivitas

Contoh kuesioner ditampilkan pada Tabel 4 berikut.

Tabel 4. Contoh kuesioner

Kontrol Standar		Uraian Pertanyaan	Nilai Skala			
			1	2	3	4
1.	A.5.3	Apakah organisasi telah menerapkan pemisahan tugas yang memadai untuk mencegash konflik kepentingan dan mengurangi risiko kesalahan atau penyalahgunaan kewenangan dalam pengelolaan data pribadi pegawai?				
2.	A.5.7	Apakah organisasi telah mengumpulkan, menganalisis dan menggunakan informasi ancaman (*threat intelligence*) untuk mengidentifikasi dan meresponspotensi ancaman terhadap keamanan data pribadi pegawai?				

2.5 Metode kuantifikasi

Penelitian ini menggunakan metode kuantifikasi, dan metode ini mengubah informasi kuesione dari data kualitatif menjadi data kuantitatif untuk dianalisis secara sistematis. Prosedur kuantisasi ini dijelaskan dalam langkah-langkah berikut.

(a) Kuesioner disusun berdasarkan kontrol ISO/IEC 27001:2022 yang sesuai dengan perlindungan data pribadi, dan diisi oleh responden menggunakan skala ordinal.

(b) Data yang terkumpul dari hasil kuesioner berbentuk angka, lalu dihitung rata-rata nilai per kontrol berdasarkan total jawaban responden. Nilai rata-rata per kontrol dihitung dengan rumus

$$\bar{X} = \frac{\sum X_i}{n} \qquad (1)$$

Dimana $\bar{X}$ adalah nilai rata-rata untuk kontrol tertentu, $\sum X_i$ adalah total nilai semua responden untuk kontrol tersebut dan n adalah jumlah responden. Nilai rata-rata per kontrol digunakan sebagai ukuran pertama dari tingkat kematangan penerapan saat ini. Nilai yang rendah menunjukkan prioritas perbaikan, sedangkan nilai yang tinggi mencerminkan penerapan yang baik.

3. HASIL DAN PEMBAHASAN

Penilaian tingkat kematangan dianalisis untuk kontrol yang relevan – yang berkaitan dengan perlindungan data pribadi seperti kontrol aset, manajemen insiden, keamanan komunikasi. Persepsi tentang sejauh mana responden menerapkan kontrol dinilai dan diberi peringkat menggunakan skala ordinal, yang kemudian dikonversi menjadi evaluasi numerik untuk merata-rata tingkat penerapan.

Temuan dalam analisis ini diterapkan untuk menilai tingkat kematangan SMKI, kesenjangan terhadap standar, dan tingkat risiko sesuai dengan dampak dan frekuensi yang diperoleh dari wawancara dan observasi. Hasil ini menunjukkan sejauh mana penerapan SMKI bekerja dan apa yang masih perlu ditingkatkan untuk mematuhi ISO/IEC 27001:2022.

3.1 Hasil Kuesioner

Pegawai yang bertugas dan bertanggung jawab atas pengelolaan data kepegawaian menerima kuesioner, dan dari hasil kuesioner yang diterima, didapat nilai rata-rata untuk setiap kontrol yang ditampilkan pada Tabel 6 berikut.

Tabel 6. Rata-rata nilai per kontrol

No	Kontrol	Rata-rata
1.	A.8.11 Penyamaran (masking) Data	3.2
2.	A.6.1 Skrining	3.4
3.	A.8.8 Manajemen Kerentanan Teknis	3.4
4.	A.7.4 Pemonitoran Keamanan Fisik	3.4
5.	A.6.2 Syarat dan Ketentuan Ketenagakerjaan	3.4
6.	A.6.3 Kesadaran, Pendidikan, dan Pelatihan Keamanan Informasi	3.5
7.	A.7.1 Perimeter Keamanan Fisik	3.6
8.	A.7.7 Meja Bersih dan Layar Bersih	3.6
9.	A.7.3 Mengamankan Kantor, Ruangan, dan Fasilitas	3.6
10.	A.7.2 Entri Fisik	3.6
11.	A.8.1 Perangkat Titik Akhir Pengguna	3.7
12.	A.5.1 Kebijakan untuk Keamanan Informansi	3.7
13.	A.5.15 Kontrol Akses	3.7
14.	A.5.7 Intelijen Ancaman	3.7
15.	A.6.5 Tanggung Jawab Setelah Terminasi atau Perubahan Pekerjaan	3.7
16.	A.8.16 Pemonitoran Aktivitas	3.7
17.	A.5.22 Pemonitoringan Riviu dan Manajemen Perubahan Pelayanan Pemasok	3.8
18.	A.8.4 Akses ke Kode Sumber	3.8
19.	A.5.18 Hak Akses	3.8
20.	A.8.3 Pembatasan Akses Informasi	3.8
21.	A.5.3 Segresi Tugas	3.9

Dari hasil kuesioner yang telah dikirimkan dan diisi oleh pegawai yang menangani pengelolaan data kepegawaian, menghasilkan nilai rata-rata untuk setiap kontrol lebih dari 4 dan nilai rata-rata untuk seluruh kontrol yang di audit senilai 3.6 yang artinya seluruh kontrol sudah diterapkan sepenuhnya dan konsisten. Namun nilai dari kuesioner ini harus dianalisis lebih lanjut dengan metode triangulasi data melalui hasil observasi dan wawancara.

Observasi langsung di lapangan menunjukkan bahwa organisasi memiliki kontrol keamanan yang ada tetapi hanya

diterapkan berdasarkan inisiatif dari inidividu tanpa adaya kebijakan dan prosedur yang formal serta tidak adanya dokumentasi penerapannya. Wawancara yang telah dilakukan dengan pemangku kepentingan menunjukkan bahwa pegawai menerapkan proses SMKI hanya berdasar inisiatif dan kebiasaan yang sudah dilakukan tanpa mengetahui proses kepatuhan ISO/IEC 27001:2022 dan penerapannya tersebut tidak selalu konsisten.

Hasil analisis triangulasi ini menunjukkan adanya kesenjangan antara pandangan subjektif dan realitas objektif dari para responden. Meskipun nilai kuesioner sangat baik, namun implementasi di lapangan masih perlu didukung dengan adanya kebijakan dan prosedur formal sebagai landasan untuk menerapkan SMKI di dalam organisasi.

3.2 Hasil Wawancara dan Observasi Lapangan

Kepala Bagian Tata Usaha dan staf kepegawaian menyatakan selama wawancara bahwa kontrol keamanan terkait akses komputer, akses ke informasi yang dilindungi kata sandi, dan penguncian perangkat komputer sudah ada tetapi belum dituangkan dalam kebijakan atau prosedur yang ditetapkan. Penerapan SMKI selama ini hanya sebatas inisiatif individu tanpa adanya acuan yang jelas.

Beberapa kerentanan akses fisik diidentifikasi melalui pengamatan langsung di lapangan, di antaranya adalah tidak adanya cakupan CCTV untuk memonitor seluruh ruangan tata usaha dan keamanan akses fisik melalui pintu yang memerlukan otentikasi yang tepat. Kurangnya cakupan CCTV membuatnya menjadi blind spot untuk pemantauan dan juga tidak ada kontrol akses fisik untuk ruangan tata usaha di mana seluruh data pegawai diarsipkan, sehingga ada risiko akses tidak sah kapan saja.

Hasil penelitian mengungkapkan pentingnya keamanan arsip dan sistem pengawasan untuk menghindari risiko kebocoran data oleh pihak yang tidak berwenang.

3.3 Analisis Kesesuaian Hasil Kuesioner dengan Hasil Wawancara dan Observasi

Hasil survei kuesioner mencerminkan tingkat kematangan yang tinggi, menunjukkan bahwa kontrol keamanan informasi juga cukup baik (rata-rata skor mencapai 3.6). Namun, wawancara dan observasi menunjukkan adanya kesenjangan antara presepsi responden dan kenyataan yang sebenarnya.

Wawancara dengan Kepala Tata Usaha menunjukkan bahwa ada beberapa langkah keamanan yang diterapkan, tetapi bersifat informal dan tidak didokumentasikan atau dituangkan dalam prosedur resmi. Bahkan ada tindakan tertentu yang dilakukan hanya berdasarkan kebiasaan.

Kesenjangan juga diamati di lapangan di mana cakupan CCTV memiliki titik buta, penyimpanan arsip tidak aman, dan komputer tidak terkunci secara otomatis.

Perbandingan dari berbagai metode pengumpulan data didapat bahwa kuesioner cenderung optimis: pegawai cenderung menganalisis berdasarkan kebiasaan mereka tetapi tidak berdasarkan presedur dan kebijakan format yang mengaturnya. Hasil ini menunjukkan bahwa dokumentasi perlu ditingkatkan, prosedur harus distandarisasi, dan pelaksanaan harus lebih konsisten.

3.4 Rekomendasi Perbaikan Risiko

Dalam penelitian ini, rekomendasi perbaikan diusulkan untuk kontrol yang memiliki nilai rata-rata kurang dari 4 sebagai prioritas untuk perbaikan guna meningkatkan tingkat kematangan sesuai dengan standar ISO/IEC 27001:2022.

Tabel 8. Tabel rekomendasi prioritas mitigasi

No.	Kontrol	Rekomendasi
1.	A.8.11	Terapkan *masking* data pribadi di seluruh aplikasi dan sistem yang menampilkan data pribadi.
2.	A.6.1	Menerapkan proses skrining latar belakang untuk pegawai yang menangani data sensitif.
3.	A.8.8	Menyusun prosedur formal untuk identifikasi, evaluasi,

		dan mitigasi kerentanan teknis secara berkala.
4.	A.7.4	Memperbaiki area *blind spot* CCTV dan melakukan permantauan fisik secara rutin.
5.	A.6.2	Memperbarui kontrak kerja pegawai dengan menambahkan klausul keamanan informasi.
6.	A.6.3	Melakukan pelatihan keamanan informasi secara rutin dan terjadwal untuk seluruh pegawai.
7.	A.7.1	Meningkatkan pengamanan perimeter, seperti pemasangan *doorlock*, sistem akses, atau penjagaan fisik.
8.	A.7.7	Menetapkan kebijakan formal tentang penerapan prinsip meja bersih dan layar bersih.
9.	A.7.3	Memperkuat pengamanan ruang kerja dan fasilitas penting dengan kontrol fisik tambahan.
10.	A.7.2	Penerapan akses otomatis (bionetrik atau kartu identitas) di area terbatas.
11.	A.8.1	Menerapkan kebijakan pengamanan perangkat *endpoint*, termasuk *password* kuat, antivirus, dan enkripsi.
12.	A.5.1	Segera menyusun dan mengesahkan kebijakan keamanan informasi yang mencakup seluruh aspek pengamanan data.
13.	A.5.15	Mendokumentasikan proses kontrol akses, termasuk pemberian, pencabutan, dan riviu hak akses.
14.	A.5.7	Melakukan analisis rutin terhadap informasi ancaman untuk memperkuat respon keamanan.
15.	A.6.5	Membuat prosedur formal untuk pencabutan hak akses dan pengembalian aset saat pegawai keluar atau pindah jabatan.
16.	A.8.16	Implementasi sistem monitoring aktivitas pengguna yang otomatis, rutin dan terdokumentasi.
17.	A.5.22	Melakukan monitoring dan reviu rutin terhadap kinerja pemasok, serta mendokumentasikan perubahannya.
18.	A.8.4	Membatasi dan mendokumentasikan akses ke kode sumber dengan prosedur formal dan sistem *version control*.
19.	A.5.18	Melakukan riviu berkala dan dokumentasi formal terkait pemberian hak akses untuk memastikan kesesuaian.
20.	A.8.3	Memperkuat pembatasan akses informasi dengan menyusun kebijakan formal yang mengatur hak akses berbasis peran.
21.	A.5.3	Menyusun dan mendokumentasikan kebijakan formal terkait segregasi tugas untuk mencegah konflik kepentingan

4. KESIMPULAN

Terkait dengan kesenjangan penelitian, tingkat kematangan penerapan SMKI di Bagian Tata Usaha mendapatkan nilai yang cukup baik (rata-rata dari semua kontrol 3,6). Hasil ini menunjukkan bahwa, secara umum, sebagian besar kontrol keamanan informasi telah diterapkan, tetapi konsistensi dan dokumentasi formal dapat ditingkatkan. Nilai terendah dari kontrol adalah 3.2 pada kontrol A.8.1 terkait penyamaran data dan nilai tertinggi adalah 3.8 pada kontrol A.5.3 terkait segregasi tugas. Urutan nilai yang didapatkan, dijadikan acuan prioritas pemberian rekomendasi dari skor yang paling rendah. Kesenjangan yang ditemukan sebagian besar disebabkan oleh tidak adanya kebijakan yang ditetapkan, ketidakmampuan untuk memantau secara berkala, dan tidak menerapkan beberapa kontrol teknis yang memadai. Oleh karena itu, rekomendasi perbaikan diberikan pada seluruh kontrol untuk mendorong tingkat kematangan secara menyeluruh.

5. DAFTAR PUSTAKA

[1] E. Novianto, "Audit Sistem Informasi pada Aplikasi Sistem Informasi Manajemen Kepegawaian (SIMPEG) menggunakan Model Framework COBIT 4.1," Jurnal Manajemen Informatika & Sistem Informasi (MISI), 2023, Vol. 6, No. 1. [Online]. Available: http://e-

journal.stmiklombok.ac.id/index.php/misi/article/view/737/234

[2] T. Triyunsari, T. Sutabri, "Analisis Tingkat Kematangan Manajemen Layanan Pegawai Berbasis Teknologi Informasi Menggunakan Framework COBIT 5 Pada SMA Negeri 19 Palembang," Indonesian Journal of Multidisciplinary on Social and Technology 2023. [Online]. Available: https://journal.ilmudata.co.id/index.php/ijmst/article/view/141

[3] I.N.A. Nugraha, G.M.A. Sasmita, A.A.K.C. Wiranatha, "Audit Tata Kelola Teknologi Informasi Pada Badan Kepegawaian XYZ," Journal of Information System and Informatics, 2024. [Online]. Available: https://www.neliti.com/publications/432041/audit-tata-kelola-teknologi-informasi-pada-badan-kepegawaian-xyz

[4] M. Kamal, M. Nasrullah, Y. Sadianto, R. Rosadi, M.A. Fauzan, Y. Anggito, W. Yasing, H. Hermawan, "Information Technology Secutiry Audit at the YDSF National Zakat Institution Using ISO 27001 Framework," Jurnal SISFOKOM (Sistem Informasi dan Komputer), 2024. [Online]. Available: https://jurnal.atmaluhur.ac.id/index.php/sisfokom/article/view/1987

[5] M.Y.D. Candiawan, Y. Priyadi, "Analysis of Information Security Audit Using ISO 27001:2013 at IT Division – X Company, In Bandung, Indonesia," International Journal of Basic and Applied Science, 2016. [Online]. Available: https://www.researchgate.net/publication/301688857_Analysis_of_Information_Security_Audit_Using_ISO_270012013_ISO_270022013_at_IT_Division_-X_Company_In_Bandung_Indonesia

[6] R. Santi, A.I. Alfresi, B. Octariana, "Audit Keamanan Sistem Informasi Menggunakan ISO/IEC 27002:2013 Pada Universitas XXX," Jurnal Teknik Informatika, 2023. [Online]. Available: https://jutif.if.unsoed.ac.id/index.php/jurnal/article/view/689

[7] A.I Wijaya, D.I. Lestiani, Y.R. Damayanti, A.A.P Sugiono, S.C. Huanggino, "Maturity Level Risk Assessment in Media Companies with ISO 27001 Framework," Journal of Digital Business and Innovation Management, 2024. [Online]. Available: https://ejournal.unesa.ac.id/index.php/jdbim/article/view/59169

[8] E. Susanto, F. Kurniasi, P. Mutiara, S.T. Afifi, "Sistem Manajemen Keamanan Informasi dengan Standar ISO/IEC 27001 dan ISO/IEC 27002 Pada PT Jasa Marga," Jurnal Ilmiah Ekonomi Manajemen Akutansi dan Bisnis, 2023.

[9] A.A. Nugraha, A.H. Nasyuha, "Integrating ISO 27001 and Indonesia's Personal Data Protection Law for Data Protection Requirement Model," Journal of Information System and Informatics, 2024.

[10] K. Ryanto, V. Tundjungsari, "Standardization of Information Security Management in the Banking Sector using the ISO 27001:2022 Framework," Journal LA Multiapp, 2024.

[11] D.D.B.R. Dika, R. Mulyana, M. Lubis, "Utilization of ISO 27001:2022 in Designing Information Security for Digital Transformation at BPRCO SME," Jurnal Penerapan Sistem Informasi (Komputer & Manajemen), 2024.

[12] A. Rachman, E. Yochanan, A.I Samanlangi, H. Purnomo, "Metode Penelitian Kuantitatif, Kualitatif dan R&D", Edisi 1, Karawang: CV Saba Jaya Publisher, 2024.