Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
https://ojs.stmik-banjarbaru.ac.id/index.php/jutisi/index
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0893

Analisis Kepatuhan ISO 27001 Annex A pada Perusahaan Keamanan Siber

DOI: http://dx.doi.org/10.35889/jutisi.v15i3.3696

Adelia Cristyana Dewanti[1], Halim Budi Santoso[2*], Jong Jek Siang[3]
Sistem Informasi, Universitas Kristen Duta Wacana, Yogyakarta, Indonesia
**E-mail Corresponding Author:* hbudi@staff.ukdw.ac.id

Abstract

Information Security Management System is an important aspect for cybersecurity companies in maintaining the confidentiality, integrity, and availability of information. This study evaluates the implementation of ISO 27001:2022 Annex A controls in the Compliance and IT Security divisions of a cybersecurity company using the Gap Analysis method. The evaluation covered 12 controls clusters, including security policies, compliance audits, access management, incident handling, and third party management through observation, semi structured interviews, and document analysis. Assessment results showed an actual score of 33 out of 48, indicating a compliance level of 68.75% categorized as compliant. Technical controls had generally been implemented well. However, gaps remained in compliance audits, third party management, security documentation, and employee security awareness. Recommendations include documentation standardization, stronger compliance monitoring, periodic evaluations, and formal incident handling procedures to improve ISMS implementation continuously.

Keywords: *ISO 27001:2022; Annex A; Gap Analysis; Compliance; Information Security.*

Abstrak

Sistem Manajemen Keamanan Informasi menjadi aspek penting bagi perusahaan keamanan siber dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi. Penelitian ini mengevaluasi implementasi kontrol ISO 27001:2022 Annex A pada divisi *Compliance* dan *IT Security* menggunakan metode *Gap Analysis*. Evaluasi dilakukan terhadap 12 cluster kontrol keamanan informasi melalui observasi, wawancara semi terstruktur, dan analisis dokumen perusahaan. Hasil penilaian menunjukkan skor aktual sebesar 33 dari skor maksimal 48 dengan tingkat kepatuhan 68,75% yang termasuk kategori patuh. Implementasi kontrol pada aspek teknis telah berjalan cukup baik, namun masih ditemukan kesenjangan pada audit kepatuhan, pengelolaan pihak ketiga, dokumentasi keamanan informasi, dan kesadaran keamanan SDM. Rekomendasi yang diusulkan meliputi standarisasi dokumentasi, penguatan pemantauan kepatuhan, evaluasi berkala, dan penyusunan prosedur formal penanganan insiden guna meningkatkan implementasi SMKI secara berkelanjutan.

Kata kunci: *ISO 27001:2022; Annex A; Analisis GAP; Kepatuhan; Keamanan Informasi*.

1. Pendahuluan

Perkembangan teknologi informasi meningkatkan ketergantungan organisasi terhadap sistem digital dalam mendukung proses bisnis. Kondisi tersebut menyebabkan keamanan informasi menjadi aspek penting dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi dari berbagai ancaman siber [1]. Pada tahun 2022, Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 700 juta serangan siber terjadi di Indonesia [2]. Ancaman seperti kebocoran data, *malware*, dan akses tidak sah menunjukkan bahwa organisasi memerlukan pengelolaan keamanan informasi yang terstruktur dan berkelanjutan. Ketergantungan organisasi terhadap teknologi informasi juga meningkatkan potensi risiko seperti gangguan sistem, kebocoran data, dan kegagalan integrasi, sehingga diperlukan penerapan manajemen risiko keamanan informasi yang efektif [3]. Oleh karena itu, organisasi memerlukan evaluasi keamanan informasi yang terstruktur agar implementasi kontrol keamanan dapat berjalan secara konsisten

dan sesuai standar internasional. Evaluasi keamanan informasi yang dilakukan secara berkala juga membantu organisasi dalam mengidentifikasi potensi kerentanan, meningkatkan efektivitas kontrol keamanan, serta mendukung proses mitigasi risiko keamanan informasi secara berkelanjutan [4]. Penilaian penerapan SMKI juga penting dilakukan untuk memastikan kesiapan organisasi dalam menjaga keamanan informasi secara sistematis dan berkelanjutan [5].

Kompleksitas ancaman siber menuntut perusahaan keamanan siber untuk menerapkan Sistem Manajemen Keamanan Informasi (SMKI) yang terstruktur guna menjaga keamanan layanan digital dan meningkatkan kepercayaan terhadap layanan keamanan siber, konsultasi SMKI, *penetration testing*, dan *Compliance management*. Perusahaan yang menjadi objek penelitian memiliki divisi *Compliance* dan *IT Security* yang bertanggung jawab dalam memastikan implementasi keamanan informasi berjalan sesuai standar dan regulasi yang berlaku. Namun, berdasarkan hasil observasi awal, evaluasi terhadap implementasi kontrol ISO 27001:2022 Annex A pada kedua divisi tersebut belum pernah dilakukan secara terstruktur. Kondisi tersebut berpotensi menyebabkan ketidakkonsistenan implementasi kontrol keamanan informasi serta meningkatkan risiko ketidaksesuaian terhadap standar ISO 27001:2022. Oleh karena itu, diperlukan evaluasi yang mampu mengukur tingkat kepatuhan implementasi kontrol keamanan informasi secara sistematis agar perusahaan dapat mengidentifikasi kelemahan kontrol dan menentukan prioritas perbaikan keamanan informasi.

Implementasi ISO 27001 pada manajemen risiko keamanan informasi menunjukkan bahwa penerapan kontrol keamanan mampu meningkatkan efektivitas pengendalian risiko secara sistematis [6]. Analisis SMKI menggunakan metode *Gap Analysis* juga digunakan untuk mengidentifikasi kesiapan organisasi terhadap sertifikasi ISO 27001 dan menghasilkan rekomendasi peningkatan kontrol keamanan informasi [7]. Evaluasi keamanan informasi melalui observasi, wawancara, dan analisis dokumen berdasarkan ISO 27001 dapat membantu mengidentifikasi kelemahan implementasi kontrol keamanan informasi pada perusahaan [8]. Selain itu, evaluasi keamanan informasi menggunakan indeks KAMI dan audit berbasis ISO 27001:2022 menunjukkan bahwa pendekatan evaluasi terstruktur dapat digunakan untuk mengukur tingkat kesiapan dan efektivitas penerapan keamanan informasi organisasi [4] [9]. *Framework* ISO 27001 berperan penting sebagai proteksi keamanan informasi dalam mendukung tata kelola keamanan informasi organisasi [10]. Selain itu, penelitian terkait evaluasi implementasi kontrol ISO 27001:2022 Annex A pada divisi *Compliance* dan *IT Security* secara terintegrasi masih terbatas. Analisis SMKI menggunakan metode *Gap Analysis* digunakan untuk mengidentifikasi kesiapan organisasi terhadap sertifikasi ISO 27001 [7]. Selain itu, evaluasi keamanan informasi menggunakan indeks KAMI dan audit berbasis ISO 27001:2022 digunakan untuk mengukur tingkat kesiapan dan efektivitas penerapan keamanan informasi organisasi [4]. Namun, evaluasi implementasi kontrol ISO 27001:2022 Annex A yang mengintegrasikan fungsi kepatuhan dan operasional keamanan informasi pada perusahaan keamanan siber masih belum banyak dilakukan.

Perusahaan telah menerapkan beberapa kontrol keamanan informasi pada fungsi *Compliance* dan *IT Security*, namun evaluasi terhadap tingkat kepatuhan implementasi kontrol ISO 27001:2022 Annex A belum pernah dilakukan secara terstruktur. Kondisi tersebut berpotensi menyebabkan ketidakkonsistenan implementasi kontrol keamanan informasi dan menyulitkan proses evaluasi keamanan informasi secara menyeluruh. Oleh karena itu, penelitian ini melakukan evaluasi tingkat kepatuhan implementasi kontrol ISO 27001:2022 Annex A menggunakan metode *Gap Analysis*. Evaluasi difokuskan pada 12 cluster kontrol keamanan informasi yang berkaitan dengan kebijakan keamanan informasi, audit kepatuhan, pengelolaan dokumen, manajemen hak akses, *logging* dan *monitoring*, penanganan insiden keamanan informasi, serta pengelolaan pihak ketiga. Metode *Gap Analysis* dipilih karena mampu membandingkan kondisi aktual perusahaan dengan kondisi ideal berdasarkan standar ISO 27001:2022 Annex A secara sistematis sehingga dapat mengidentifikasi tingkat kesenjangan implementasi kontrol keamanan informasi dan menentukan prioritas perbaikan. Evaluasi implementasi kontrol ISO 27001:2022 Annex A pada fungsi *Compliance* dan *IT Security* secara terintegrasi belum pernah dilakukan pada perusahaan sehingga proses pengukuran kepatuhan keamanan informasi belum memiliki acuan evaluasi yang terstruktur. Evaluasi dilakukan menggunakan pendekatan berbasis cluster kontrol Annex A agar hasil penilaian dapat menggambarkan kondisi implementasi keamanan informasi secara lebih spesifik sesuai operasional perusahaan.

2. Metodologi

Metodologi dalam penelitian ini menggunakan pendekatan kualitatif dengan metode *Gap Analysis* untuk mengevaluasi kesenjangan antara kondisi aktual dan standar ISO 27001:2022 Annex A. Gambar 1 menunjukkan metodologi yang dilakukan pada penelitian ini

Gambar 1. Tahapan Penelitian

2.1 Observasi dan Wawancara

Tahap observasi dilakukan pada divisi *Compliance* dan *IT Security* dengan menelaah kebijakan keamanan informasi, SOP keamanan, dokumen audit internal, rekaman pemantauan, pengelolaan hak akses, serta dokumen pendukung lainnya yang berkaitan dengan implementasi ISO 27001:2022 Annex A, seperti tertulis pada Tabel 1 dibawah ini.

Selain observasi dokumen, dilakukan wawancara semi terstruktur kepada pihak yang terlibat langsung dalam pengelolaan kepatuhan dan keamanan informasi perusahaan. Wawancara dilakukan untuk memvalidasi implementasi kontrol keamanan informasi yang diterapkan pada perusahaan serta memperoleh gambaran kondisi aktual implementasi ISO 27001:2022 Annex A. Analisis dokumen dan validasi melalui wawancara efektif digunakan untuk mengukur kesiapan organisasi dalam memenuhi standar keamanan informasi [11].

Tabel 1. Daftar Pertanyaan Wawancara Kepada Divisi *Compliance* dan *IT Security*

No	Cluster	Kontrol Annex A	Divisi	Pertanyaan
1	Kebijakan & Tata Kelola Keamanan Informasi	A.5.1, A.5.2, A.5.4, A.5.37	*Compliance*	Apakah perusahaan sudah memiliki dan menerapkan kebijakan serta prosedur keamanan informasi yang disusun, didokumentasikan, dan disosialisasikan oleh divisi *Compliance*, serta bagaimana penerapan kebijakan tersebut dijalankan secara konsisten dalam praktik?
2	Kepatuhan terhadap Regulasi & Standar	A.5.31, A.5.32, A.5.34	*Compliance*	Apakah divisi *Compliance* sudah memastikan kepatuhan perusahaan terhadap regulasi yang berlaku, standar keamanan informasi, perlindungan data pribadi, dan kekayaan intelektual, serta bagaimana mekanisme pemantauan kepatuhan tersebut dilakukan dalam praktik?
3	Pengelolaan Dokumen & Rekaman	A.5.33, A.5.36	*Compliance*	Apakah perusahaan sudah memiliki mekanisme pengelolaan, penyimpanan, perlindungan, dan pengendalian dokumen serta rekaman yang berkaitan dengan keamanan informasi, serta bagaimana mekanisme tersebut diterapkan dalam praktik sehari-hari?
4	Audit, Review & Evaluasi Kepatuhan	A.5.35, A.5.22	*Compliance*	Apakah divisi *Compliance* sudah melakukan audit atau peninjauan berkala terhadap penerapan keamanan informasi, serta bagaimana tindak lanjut dari hasil audit atau evaluasi tersebut dijalankan dalam praktik?
5	Kesadaran Keamanan & Disiplin SDM	A.6.3, A.6.4, A.6.8	*Compliance*	Apakah divisi *Compliance* sudah berperan aktif dalam membangun kesadaran dan disiplin karyawan terhadap keamanan informasi, termasuk pelatihan dan pengaturan sanksi pelanggaran, serta bagaimana pelaksanannya dalam praktik?

No	Cluster	Kontrol Annex A	Divisi	Pertanyaan
6	Kesiapan Keamanan Informasi & Keberlangsungan Bisnis	A.5.29, A.5.30	*Compliance* & *IT Security*	Apakah divisi *Compliance* sudah memastikan kesiapan keamanan informasi dan keberlangsungan bisnis saat terjadi gangguan operasional atau kondisi darurat, serta bagaimana kepatuhan terhadap rencana dan kebijakan tersebut dijalankan dalam praktik?
7	Manajemen Identitas & Hak Akses	A.5.15, A.5.16, A.5.17, A.5.18	*IT Security*	Apakah perusahaan sudah memiliki dan menerapkan mekanisme pengelolaan identitas dan hak akses pengguna (pemberian, peninjauan, dan pencabutan akses) sesuai kebijakan dan prosedur keamanan informasi, serta bagaimana mekanisme tersebut dijalankan dalam praktik sehari-hari?
8	Pengelolaan Akses Istimewa (Privileged Access)	A.8.2	*IT Security*	Apakah perusahaan sudah menerapkan pengendalian terhadap akun dengan hak akses istimewa (administrator), termasuk pembatasan penggunaan dan pemantauan aktivitas sesuai kebijakan keamanan informasi dan bagaimana pengendalian tersebut diterapkan dalam praktik?
9	Logging, *Monitoring* & Bukti Audit	A.8.15, A.8.16, A.5.28	IT Security	Apakah perusahaan sudah melakukan pencatatan dan pemantauan aktivitas sistem serta akses pengguna dan memanfaatkan log sebagai bukti audit atau evaluasi kepatuhan, serta bagaimana pemanfaatan log tersebut dilakukan dalam praktik?
10	Penanganan & Respons Insiden Keamanan Informasi	A.5.24, A.5.25, A.5.26, A.5.27	*IT Security*	Apakah perusahaan sudah memiliki dan menerapkan prosedur penanganan insiden keamanan informasi mulai dari pelaporan, respons, pendokumentasian, hingga evaluasi pasca insiden sesuai kebijakan yang diterapkan, serta bagaimana alur pelaksanannya dalam praktik?
11	Keamanan Layanan & Teknologi Pendukung	A.5.23, A.8.24	*IT Security*	Apakah perusahaan sudah menerapkan pengamanan informasi pada layanan dan teknologi pendukung sesuai standar dan kebijakan keamanan informasi perusahaan, serta bagaimana penerapan pengamanan tersebut dilakukan dalam praktik?
12	Manajemen Pihak Ketiga & Supplier	A.5.19, A.5.20, A.5.21	*IT Security*	Apakah perusahaan sudah memastikan pihak ketiga atau supplier memenuhi persyaratan keamanan informasi yang ditetapkan sebelum dan selama kerja sama berlangsung, serta bagaimana mekanisme pengawasan atau evaluasi kepatuhan dilakukan dalam praktik?

2.2 Analisis Dokumen berdasarkan ISO 27001:2022 Annex A

Analisis dokumen dilakukan untuk memperoleh data evaluasi terhadap penerapan kontrol keamanan informasi berdasarkan standar ISO 27001:2022 Annex A. Proses analisis dilakukan dengan menelaah berbagai dokumen perusahaan yang berkaitan dengan keamanan informasi seperti kebijakan keamanan informasi, *Standard Operating Procedure (SOP)*, dokumen audit internal, dokumentasi pengelolaan hak akses, serta dokumen penanganan insiden keamanan informasi.

Analisis dilakukan dengan membandingkan dokumen dan implementasi aktual perusahaan terhadap kontrol ISO 27001:2022 Annex A yang digunakan dalam penelitian. Penilaian dilakukan berdasarkan keberadaan kebijakan, kelengkapan dokumentasi, konsistensi penerapan, serta bukti implementasi kontrol keamanan informasi pada divisi *Compliance* dan *IT Security*. Pendekatan evaluasi berbasis dokumentasi dan implementasi kontrol tersebut digunakan untuk memastikan bahwa proses penilaian tidak hanya berfokus pada keberadaan kebijakan, tetapi juga pada efektivitas penerapan keamanan informasi di lingkungan operasional perusahaan [8].

2.3 *Gap Analysis* dan rekomendasi

Berdasarkan *Gap Analysis*, disusun rekomendasi peningkatan yang disesuaikan dengan kondisi operasional perusahaan dan praktik ISO 27001:2022, meliputi standardisasi dokumen, penguatan penyimpanan terpusat, dan evaluasi berkala terhadap SOP keamanan informasi. *Gap Analysis* efektif digunakan untuk menentukan rekomendasi perbaikan implementasi ISO 27001:2022 [12] [13].

Penilaian *Gap Analysis* dilakukan dengan membandingkan kondisi aktual dengan kondisi ideal berdasarkan standar ISO 27001:2022 Annex A. Setiap kontrol dievaluasi berdasarkan tingkat kesesuaian implementasi di lapangan. Hasil penilaian kemudian dikategorikan menjadi beberapa tingkat, yaitu:

0 = Tidak diimplementasi
1 = Diterapkan sebagian
2 = Diimplementasi namun belum konsisten
3 = Diimplementasi cukup baik
4 = Diimplementasi secara optimal dan berkelanjutan

Kategori ini digunakan untuk mengidentifikasi kesenjangan (GAP) pada setiap kontrol serta menjadi dasar dalam penyusunan rekomendasi perbaikan yang sesuai dengan kebutuhan perusahaan. Untuk mengetahui tingkat kepatuhan implementasi keamanan informasi secara keseluruhan, dilakukan perhitungan persentase tingkat kepatuhan berdasarkan total skor aktual dibandingkan skor maksimal. Perhitungan dilakukan menggunakan rumus berikut:

$$\text{Persentase Kepatuhan} = \frac{\sum_{Skor\ Aktual}}{\sum_{Skor\ Maksimal}}\ x\ 100\% \quad (1)$$

Keterangan:

Skor maksimal = jumlah kontrol x 4
Skor aktual = total skor hasil penilaian

Interpretasi hasil persentase tingkat kepatuhan mengacu pada kategori penilaian yang ditunjukkan pada tabel 2 berikut ini.

Tabel 2. Kategori Persentase

Persentase	Kategori	Keterangan
0 – 20%	Tidak patuh	Organisasi tidak menerapkan kontrol/kebijakan yang dievaluasi
21 – 40%	Kurang patuh	Sebagian kecil kontrol telah diterapkan, namun belum terstruktur dan belum konsisten
41 – 60%	Cukup patuh	Kontrol sudah diterapkan sebagian, namun masih terdapat banyak kekurangan dan ketidakkonsistenan
61 – 80%	Patuh	Sebagian besar kontrol telah diterapkan dengan baik, namun masih terdapat gap yang perlu diperbaiki
81 – 100%	Sangat patuh	Seluruh kontrol telah diterapkan secara optimal dan konsisten

3. Hasil dan Pembahasan

Pada bagian ini disajikan hasil analisis kesenjangan (*Gap Analysis*) terhadap penerapan kontrol keamanan informasi berdasarkan standar ISO 27001:2022 Annex A. Analisis dilakukan pada fungsi kepatuhan dan *IT Security* untuk mengidentifikasi tingkat kesesuaian antara kondisi aktual perusahaan dengan standar yang ditetapkan. Hasil analisis ini kemudian digunakan

sebagai dasar dalam penyusunan rekomendasi peningkatan guna memperbaiki implementasi keamanan informasi di perusahaan.

3.1. Hasil Analisis Kesenjangan Keamanan Informasi

Berdasarkan hasil wawancara, observasi, dan analisis dokumen, diperoleh gambaran kondisi aktual penerapan kontrol keamanan informasi pada perusahaan. Penilaian dilakukan terhadap 12 cluster kontrol ISO 27001:2022 Annex A dengan mempertimbangkan tingkat implementasi, dokumentasi, serta konsistensi penerapan.

Hasil analisis (lihat Tabel 3) menunjukkan bahwa sebagian besar kontrol telah diterapkan, namun belum berjalan secara optimal dan konsisten. Beberapa kontrol telah memiliki kebijakan dan prosedur yang terdokumentasi, namun belum didukung oleh evaluasi berkala dan mekanisme *monitoring* yang terstruktur. Kondisi tersebut menunjukkan bahwa keberadaan kebijakan keamanan informasi saja belum cukup tanpa adanya proses monitoring dan evaluasi yang dilakukan secara konsisten [14].

Tabel 3. Hasil Analisis *Gap Analysis* Keamanan Informasi ISO 27001:2022 Annex A

No	Cluster	Kontrol Annex A	Bukti Implementasi	Skor	Prioritas
1	Kebijakan & Tata Kelola Keamanan Informasi	A.5.1, A.5.2, A.5.4, A.5.37	Kebijakan tersedia dan terdokumentasi, namun belum dilakukan evaluasi dan implementasi secara optimal	3	Sedang
2	Kepatuhan terhadap Regulasi & Standar	A.5.31, A.5.32, A.5.34	Implementasi kepatuhan belum menyeluruh.	2	Tinggi
3	Pengelolaan Dokumen & Rekaman Keamanan Informasi	A.5.33, A.5.36	Belum ada evaluasi efektivitas secara berkala	3	Sedang
4	Audit, Review & Evaluasi Kepatuhan	A.5.35, A.5.22	Audit belum dilakukan secara rutin dan belum terdokumentasi dengan baik	2	Tinggi
5	Kesadaran Keamanan & Disiplin SDM	A.6.3, A.6.4, A.6.8	Program *awareness* belum konsisten dan belum terukur efektivitasnya	2	Tinggi
6	Kesiapan Keamanan Informasi & Keberlangsungan Bisnis	A.5.29, A.5.30	Rencana sudah tersedia, namun belum dilakukan pengujian/simulasi secara berkala	3	Sedang
7	Manajemen Identitas & Hak Akses	A.5.15, A.5.16, A.5.17, A.5.18	Kontrol akses sudah diterapkan dengan baik dan terdokumentasi, meskipun masih terdapat ruang perbaikan dalam cakupan *lifecycle* pengguna	4	Rendah
8	Pengelolaan Akses Istimewa (Privileged Access)	A.8.2	Pengelolaan akses istimewa sudah dikontrol dengan baik dan konsisten, sehingga hanya memerlukan monitoring dan evaluasi berkala	4	Rendah
9	Logging, *Monitoring* & Bukti Audit	A.8.15, A.8.16, A.5.28	Sistem pemantauan sudah berjalan optimal dan	4	Rendah

			mendukung analisis insiden		
10	Penanganan & Respons Insiden Keamanan Informasi	A.5.24, A.5.25, A.5.26, A.5.27	Proses sudah diterapkan, namun belum didukung SOP formal dan belum dijalankan secara konsisten sehingga berisiko menyebabkan proses respons insiden yang tidak terstruktur.	2	Tinggi
11	Keamanan Layanan & Teknologi Pendukung	A.5.23, A.8.24	Kontrol teknis sudah diterapkan, namun belum ada evaluasi berkala	3	Sedang
12	Manajemen Pihak Ketiga & Supplier	A.5.19, A.5.20, A.5.21	Belum terdapat proses formal dalam evaluasi dan pemantauan pihak ketiga	1	Sangat tinggi

Prioritas perbaikan ditentukan berdasarkan tingkat kesenjangan implementasi kontrol.Semakin rendah skor implementasi, semakin tinggi prioritas perbaikan yang diberikan karena menunjukkan tingkat ketidaksesuaian yang lebih besar terhadap standar ISO 27001:2022 Annex A. Penilaian pada setiap cluster dilakukan berdasarkan hasil observasi, wawancara, dan analisis dokumen pendukung perusahaan yang relevan dengan implementasi kontrol ISO 27001:2022 Annex A. Dokumen pendukung yang digunakan meliputi kebijakan keamanan informasi, SOP keamanan, contoh form *incident report* milik perusahaan.

Berdasarkan hasil penilaian terhadap 12 cluster kontrol ISO 27001:2022 Annex A, diperoleh total skor aktual sebesar 33 dari skor maksimal 48. Perhitungan tingkat kepatuhan dilakukan menggunakan rumus persentase kepatuhan sebagai berikut:

$$\frac{33}{48} \text{ x } 100\% = 68{,}75\%$$

Hasil tersebut menunjukkan bahwa tingkat kepatuhan implementasi kontrol keamanan informasi pada perusahaan berada pada kategori Patuh dengan persentase sebesar 68,75%. Hal ini menunjukkan bahwa sebagian besar kontrol telah diterapkan, namun beberapa kontrol masih belum berjalan secara optimal dan konsisten terutama pada aspek audit kepatuhan, pengelolaan pihak ketiga, dan dokumentasi keamanan informasi.

3.2. Pembahasan Hasil Analisis

Berdasarkan hasil analisis kesenjangan yang telah dilakukan, dapat diketahui bahwa tingkat implementasi kontrol keamanan informasi di perusahaan masih bervariasi pada setiap cluster. Secara umum, hasil analisis menunjukkan bahwa implementasi kontrol ISO 27001:2022 Annex A pada perusahaan telah berjalan cukup baik dengan tingkat kepatuhan sebesar 68,75% dan berada pada kategori patuh. Sebagian besar kontrol keamanan informasi telah diterapkan, khususnya pada aspek teknis dan pengelolaan akses sistem. Namun, masih ditemukan beberapa kesenjangan pada aspek audit kepatuhan, pengelolaan dokumentasi, dan pengelolaan pihak ketiga.

Pada aspek teknis, seperti manajemen identitas dan hak akses, pengelolaan akses istimewa, serta logging dan *monitoring*, perusahaan telah menunjukkan tingkat implementasi yang baik. Hal ini ditunjukkan melalui penerapan *identity management*, pembatasan akses berbasis peran (*role based access control)*, serta pemantauan aktivitas keamanan informasi secara *real time* oleh tim *IT Security*. Penerapan kontrol akses dan pemantauan secara *real time* tersebut berperan penting dalam menjaga keamanan sistem dan meminimalkan risiko akses tidak sah terhadap informasi perusahaan [6].Implementasi kontrol keamanan informasi pada divisi *IT Security* juga menunjukkan hasil yang cukup baik terutama pada pengelolaan akses sistem dan monitoring aktivitas keamanan informasi. Meskipun demikian, dokumentasi monitoring dan evaluasi log belum dilakukan secara konsisten sehingga masih diperlukan peningkatan pada aspek dokumentasi dan evaluasi berkala terhadap aktivitas keamanan informasi. Dokumentasi dan pencatatan aktivitas keamanan informasi yang tidak konsisten dapat mengurangi efektivitas

proses audit serta menyulitkan organisasi dalam melakukan evaluasi insiden keamanan informasi [11].

Pada aspek tata kelola dan kepatuhan masih ditemukan kesenjangan pada audit, kesadaran keamanan SDM, dan penanganan insiden karena implementasi kontrol belum terstruktur dan terdokumentasi secara konsisten. Hal tersebut memperlihatkan bahwa evaluasi dan pengawasan keamanan informasi yang belum dilakukan secara konsisten dapat meningkatkan potensi kerentanan sistem dan mengurangi efektivitas penerapan kontrol keamanan informasi dalam organisasi [14]. Selain itu, integrasi kebijakan keamanan, kesadaran karyawan, dan kepatuhan sangat berhubungan terhadap regulasi dalam implementasi ISO 27001:2022 [9][8]. Hasil penelitian ini turut diperkuat oleh bukti yang menunjukkan bahwa analisis Gap dapat membantu organisasi menyusun rekomendasi peningkatan tata kelola TI secara terstruktur [15]. Selain itu, pada divisi *Compliance* masih ditemukan kesenjangan pada audit kepatuhan dan pengelolaan pihak ketiga. Pengelolaan audit kepatuhan yang belum berjalan secara terstruktur dapat menyebabkan organisasi kesulitan dalam memastikan efektivitas implementasi kontrol keamanan informasi secara menyeluruh [7]. Beberapa proses audit dan evaluasi kepatuhan belum dilakukan secara terstruktur serta belum memiliki dokumentasi yang konsisten. Audit dan evaluasi keamanan informasi yang dilakukan secara berkala juga penting untuk memastikan efektivitas penerapan kontrol keamanan informasi serta mendukung peningkatan level keamanan informasi organisasi [16].

Temuan paling kritis terdapat pada manajemen pihak ketiga karena pengendalian keamanan informasi belum diterapkan secara optimal. Hubungan dengan pihak ketiga memiliki risiko signifikan terhadap keamanan informasi organisasi sehingga memerlukan pengendalian yang terstruktur [17].

Hasil penelitian menunjukkan bahwa pengelolaan dokumentasi dan audit kepatuhan belum dilakukan secara konsisten sehingga beberapa kontrol keamanan informasi belum terdokumentasi dengan baik. Implementasi SMKI masih menghadapi kendala pada aspek dokumentasi dan pengelolaan kontrol keamanan informasi [11]. Selain itu, pengelolaan pihak ketiga belum didukung oleh mekanisme evaluasi keamanan vendor secara berkala sehingga berpotensi meningkatkan risiko keamanan informasi perusahaan.

3.3. Rekomendasi Peningkatan

Rekomendasi peningkatan pada penelitian ini ditujukan untuk perusahaan keamanan siber sebagai acuan perbaikan implementasi kontrol keamanan informasi berdasarkan hasil identifikasi kesenjangan ISO 27001:2022 Annex A. Berdasarkan hasil analisis kesenjangan (*Gap Analysis*), disusun rekomendasi peningkatan (tabel 4) untuk memperbaiki efektivitas penerapan kontrol keamanan informasi di perusahaan. Rekomendasi diberikan berdasarkan tingkat kesenjangan implementasi pada setiap kontrol ISO 27001:2022 Annex A serta disesuaikan dengan praktik pengelolaan keamanan informasi yang direkomendasikan dalam standar ISO 27001:2022. Penyusunan rekomendasi juga mempertimbangkan hasil observasi, wawancara, dan analisis dokumen terhadap kondisi aktual perusahaan. Rekomendasi yang disusun difokuskan pada peningkatan tata kelola keamanan informasi, kepatuhan terhadap standar, standardisasi dokumentasi, monitoring dan evaluasi keamanan informasi, serta pengelolaan risiko pihak ketiga. Rekomendasi tersebut disesuaikan dengan hasil identifikasi kesenjangan pada setiap cluster kontrol ISO 27001:2022 Annex A. Pendekatan rekomendasi berbasis *Gap Analysis* digunakan agar prioritas perbaikan dapat disusun secara lebih terarah sesuai tingkat risiko dan kebutuhan operasional organisasi [12]. Model penilaian kepatuhan berbasis ISO 27001:2022 juga dapat digunakan sebagai acuan dalam meningkatkan proses evaluasi keamanan informasi secara sistematis [18].

Penyusunan rekomendasi peningkatan dilakukan berdasarkan hasil identifikasi kesenjangan implementasi kontrol ISO 27001:2022 Annex A serta didukung oleh penelitian sebelumnya sebagai *benchmark* implementasi keamanan informasi. Evaluasi berkala, monitoring keamanan secara *real time*, penerapan autentikasi ganda, penguatan dokumentasi, serta pengelolaan risiko pihak ketiga berperan penting dalam meningkatkan efektivitas implementasi SMKI [6] [12] [11] [17]. Selain itu, metode *Gap Analysis* dinilai efektif dalam membantu organisasi menentukan prioritas perbaikan keamanan informasi secara sistematis dan berkelanjutan [7] [4]. Rekomendasi ini menekankan pentingnya pemantauan real time, autentikasi ganda, dan evaluasi berkala sebagai bagian dari mitigasi risiko dalam implementasi ISO 27001:2022 [6].

Tabel 4. Rekomendasi Peningkatan Berdasarkan Hasil *Gap Analysis* ISO 27001:2022 Annex A

No	Cluster	Fokus Perbaikan	Rekomendasi Peningkatan
1	Kebijakan & Tata Kelola Keamanan Informasi	Penguatan tata kelola dan kebijakan keamanan informasi	Melakukan review dan pembaruan kebijakan keamanan informasi secara berkala agar tetap selaras dengan perkembangan ancaman siber; meningkatkan sosialisasi kebijakan kepada seluruh karyawan karena implementasi belum konsisten; serta menetapkan mekanisme *monitoring* kepatuhan kebijakan oleh fungsi kepatuhan [6] [19].
2	Kepatuhan terhadap Regulasi & Standar	Peningkatan kepatuhan terhadap standar dan regulasi	Menyusun *Compliance* register yang terstruktur untuk memantau kewajiban regulasi, meningkatkan peran fungsi kepatuhan dalam melakukan pemantauan dan pelaporan kepatuhan, serta melakukan evaluasi berkala untuk memastikan seluruh kontrol telah memenuhi standar ISO 27001:2022 [7] [20].
3	Pengelolaan Dokumen & Rekaman Keamanan Informasi	Standardisasi dokumentasi keamanan informasi	Menstandardisasi format dan struktur dokumen keamanan informasi, mengimplementasikan sistem penyimpanan dokumen terpusat dengan pengendalian akses, serta memastikan seluruh dokumen memiliki riwayat pembaruan yang jelas [12] [21].
4	Audit, Review & Evaluasi Kepatuhan	Penguatan audit dan evaluasi kepatuhan	Meningkatkan frekuensi audit internal karena evaluasi belum dilakukan secara terstruktur, menyusun checklist audit berbasis ISO 27001:2022 Annex A, serta memastikan adanya tindak lanjut dari setiap temuan audit [16] [22].
5	Kesadaran Keamanan & Disiplin SDM	Peningkatan kesadaran keamanan informasi SDM	Meningkatkan program awareness keamanan informasi yang sebelumnya belum berjalan optimal, melakukan pelatihan rutin terkait keamanan siber, serta memperjelas mekanisme sanksi terhadap pelanggaran kebijakan [9] [23].
6	Kesiapan Keamanan Informasi & Keberlangsungan Bisnis	Penguatan kesiapan keamanan dan keberlangsungan bisnis	Meningkatkan *Business Continuity Plan* (BCP) yang lebih terstruktur, melakukan simulasi kondisi darurat secara berkala, serta memastikan seluruh karyawan memahami peran masing-masing dalam kondisi insiden atau gangguan operasional [13] [24].
7	Manajemen Identitas & Hak Akses	Optimalisasi pengelolaan identitas dan hak akses	Memperkuat pengelolaan hak akses dengan menerapkan prinsip least privilege secara konsisten, melakukan review akses pengguna secara berkala, serta memastikan proses pemberian dan pencabutan akses terdokumentasi dengan baik [11] [25].
8	Pengelolaan Akses Istimewa (*Privileged Access*)	Penguatan pengendalian akses istimewa	Membatasi penggunaan akun *privileged* hanya untuk kebutuhan tertentu, meningkatkan *monitoring* aktivitas akun administrator, serta menerapkan *multi factor*

			authentication (MFA) untuk mengurangi risiko penyalahgunaan akses [6] [26].
9	Logging, *Monitoring* & Bukti Audit	Optimalisasi monitoring dan pencatatan aktivitas sistem	Mengoptimalkan sistem logging yang sudah ada agar lebih terpusat dan terintegrasi, meningkatkan *monitoring* aktivitas sistem secara *real time*, serta memastikan log digunakan sebagai bahan evaluasi dan audit keamanan [14] [27].
10	Penanganan & Respons Insiden Keamanan Informasi	Penguatan prosedur penanganan insiden keamanan informasi	Menyusun SOP *incident* response yang lebih terstruktur karena penanganan masih belum optimal, memperjelas alur pelaporan dan eskalasi insiden, serta melakukan evaluasi pasca insiden untuk perbaikan berkelanjutan [11] [16].
11	Keamanan Layanan & Teknologi Pendukung	Peningkatan keamanan layanan dan infrastruktur teknologi	Meningkatkan pengamanan sistem melalui *hardening system* dan *patch management* secara berkala, melakukan vulnerability assessment secara rutin, serta memastikan konfigurasi sistem telah sesuai dengan standar keamanan yang ditetapkan [12] [28].
12	Manajemen Pihak Ketiga & Supplier	Penguatan pengelolaan risiko pihak ketiga	Meningkatkan proses evaluasi keamanan terhadap pihak ketiga sebelum kerja sama, menetapkan klausul keamanan dalam kontrak, serta melakukan *monitoring* berkala terhadap kepatuhan vendor terhadap standar keamanan [17] [29].

5. Simpulan

Penelitian ini menunjukkan bahwa tingkat kepatuhan implementasi kontrol ISO 27001:2022 Annex A pada perusahaan keamanan siber mencapai 68,75% dan berada pada kategori patuh. Hasil evaluasi menunjukkan bahwa sebagain besar kontrol keamanan informasi telah diterapkan dengan baik, terutama pada aspek manajemen identitas dan hak akses, pengelolaan akses Istimewa, serta *logging* dan *monitoring*. Meskipun demikian, masih ditemukan beberapa kesenjangan pada aspek audit dan evaluasi kepatuhan, pengelolaan dokumen keamanan informasi, kesadaran keamanan SDM, penanganan insiden keamanan informasi, serta pengelolaan pihak ketiga. Kesenjangan tersebut menunjukkan bahwa implementasi kontrol keamanan informasi belum sepenuhnya konsisten dan terdokumentasi secara optimal. Melalui metode *Gap Analysis*, penelitian ini berhasil mengidentifikasi tingkat kesesuaian implementasi kontrol ISO 27001:2022 Annex A dan menentukan area prioritas yang memerlukan perbaikan. Selain itu, penelitian ini menghasilkan rekomendasi peningkatan yang dapat digunakan perusahaan sebagai acuan dalam memperkuat penerapan Sistem Manajemen Keamanan Informasi secara berkelanjutan serta meningkatkan efektivitas tata kelola keamanan informasi pada fungsi *Compliance* dan *IT Security*.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Fakultas Teknologi Informasi Universitas Kristen Duta Wacana Yogyakarta yang telah memberikan bantuan dana publikasi.

Daftar Referensi

[1] R. Vansuri *et al.*, “Peran CIA (Confidentiality, Integrity, Availability) Terhadap Manajemen Keamanan Informasi,” *JIM: Jurnal Ilmu Multidisiplin*, vol. 2, no. 1, pp. 106–113, Jun. 2023, doi: 10.38035/jim.v2i1.

[2] A. D. Saputra, F. Dione, and I. Uluputty, “Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur,” *Jurnal Teknologi dan Komunikasi Pemerintahan*, vol. 5, no. 2, pp. 159–187, Dec. 2023, doi: 10.33701/jtkp.v5i2.3735.

[3] G. H. Wicaksana and E. Maria, “Penerapan ISO 31000:2018 dalam Mitigasi Risiko Sistem Visual Hotel Program di Hotel Griya Persada,” *Jutisi : Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, vol. 14, no. 3, p. 2328, Mar. 2026, doi: 10.35889/jutisi.v14i3.3270.
[4] L. D. A. Jelita, M. N. Al Azam, and A. Nugroho, “Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/IEC 27001:2022,” *Jurnal SAINTEKOM*, vol. 14, no. 1, pp. 84–94, Mar. 2024, doi: 10.33020/saintekom.v14i1.623.
[5] I. Suryono, “Evaluasi Penilaian Mandiri Penerapan SMKI di Salah Satu Lingkungan K/L,” *JUPIK: Jurnal Penelitian Ilmu Komputer*, vol. 1, pp. 1–7, Mar. 2023, doi: 10.5281/zenodo.7720440.
[6] F. Cahya Arumdiya and C. Rudianto, “Implementasi ISO 27001:2022 dalam Manajemen Risiko Keamanan Informasi,” *Jurnal PETISI*, vol. 06, no. 02, pp. 143–155, Jul. 2025.
[7] S. R. Musyarofah and R. Bisma, “Analisis Kesenjangan Sistem Manajemen Keamanan Informasi (SMKI) sebagai Persiapan Sertifikasi ISO/IEC 27001:2013 pada Institusi Pemerintah,” *Teknologi*, vol. 11, no. 1, pp. 1–15, Jan. 2021, doi: 10.26594/teknologi.v11i1.2152.
[8] R. Rizky Junior, R. Guntur Utomo, and D. Oktaria, “Information Security Analysis in PT. XYZ Using ISO/IEC 27001:2013,” *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, vol. 12, No. 1, pp. 220–231, Apr. 2023.
[9] N. Nurbojatmiko, M. S. K. Karimiyah, N. M. Asnadi, and R. Anisyah, “ISO 27001 As Information Security Solution In Society 5.0 Era: Systematic Literature Review,” *Sinkron*, vol. 9, no. 1, pp. 484–492, Feb. 2025, doi: 10.33395/sinkron.v9i1.14448.
[10] B. Aurabillah, L. Aprillia Putri, N. Citra Fadhlilla, and A. Wulansari, “Implementasi Framework ISO 27001 sebagai Proteksi Keamanan Informasi dalam Pemerintahan (Systematic Literature Review),” *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 8, no.1, pp. 454-460. Feb. 2024.
[11] Setiawan and I. P. Wardhani, “Evaluasi Efektivitas Pemetaan Keamanan Siber dalam Penerapan Sistem Keamanan Informasi Berbasis ISO/IEC 27001:2022 PT Jasa Raharja,” *JATI (Jurnal Mahasiswa Teknik Informatika)*, vol. 10, no. 1, pp. 27887–2794, Apr. 2026.
[12] Bimantoro, “Rekomendasi Implementasi 11 Kontrol keamanan informasi baru ISO 27001:2022 di Perusahaan HealthTech XYZ,” *The Indonesian Journal of Computer Science*, vol. 13, no. 4, pp. 6398–6410, Jul. 2024, doi: 10.33022/ijcs.v13i4.4166.
[13] M. Hafidz Bahaudin and A. Wasiur Rizqi, “Evaluasi Kesesuaian Penerapan Sistem Manajemen Keselamatan dan Kesehatan Kerja (SMK3) Berdasarkan ISO 45001:2018 Menggunakan Metode Gap Analysis dan PDCA (Studi kasus: PT Swabina Gatra),” *Jurnal Teknologi dan Manajemen Industri Terapan (JTMIT)*, vol. 5, no. 2, pp. 766–773, 2026.
[14] R. Umar, I. Riadi, M. Ihya, and A. Elfatiha, “Analisis Keamanan Sistem Informasi Akademik Berbasis Web Menggunakan Framework ISSAF,” *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, vol. 12, no. 1, pp. 280–292, Apr. 2023.
[15] H. Zaenul Rahmat, F. Nurapriani, and B. Huda, “Penerapan Tata Kelola Audit Sistem Informasi Pada Shen Coffee Space Menggunakan Framework COBIT 2019,” *Tugas Akhir,* UBP Karawang, 2025
[16] E. Riana, M. E. S. Sulistyawati, and O. P. Putra, “Analisis Tingkat Kematangan (Maturity Level) Dan PDCA (Plan-Do-Check-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan Metode ISO 27001:2013,” *Journal of Information System Research (JOSH)*, vol. 4, no. 2, pp. 632–640, Jan. 2023, doi: 10.47065/josh.v4i2.2552.
[17] A. Budiyantara, P. Sita Witari, T. Marpaung, G. Jordana, and M. Hamka, “Analisis Kebijakan Keamanan Informasi di Perusahaan Distributor Mobile Phone,” *Jurnal of Business and Audit Information System (JBASE)*, vol. 8, no. 2, pp. 24–31, Sep. 2025, doi: 10.24105/jbase.v8i2.9061.
[18] R. Sinaga, “Pengembangan Model Penilaian Kepatuhan Salah Satu Perguruan Tinggi Terhadap Standar ISO 27001:2022,” *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 9, no. 3, pp. 381–394, Jan. 2024, doi: 10.28932/jutisi.v9i3.6850.
[19] I. Mardiyana *et al.*, “Penerapan Kerangka Kerja Keamanan Informasi di Rumah Sakit: Tinjauan Literatur Sistematis,” *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, vol. 12, pp. 729–738, Aug. 2023.

[20] Mardiah and M. N. H. Siregar, "Analisis Keamanan Data pada Sistem Informasi Menggunakan Metode ISO/IEC 27001," *Jurnal Ilmu Komputer dan Teknik Informatika*, vol. 1, no. 2, pp. 58–64, Jul. 2025, doi: 10.64803/juikti.v1i2.52.

[21] L. Kusnitawati and A. Kurniawati, "Analisis Kualitas Perangkat Lunak Aplikasi GT-Kalinfo pada PT. Gajah Tunggal Menggunakan ISO 25010," *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, vol. 12, no. 3, pp. 1319–1330, Dec. 2023.

[22] I. Wayan, G. Adnyana, H. Syakh Alam, I. Gede, and J. E. Putra, "Tata Kelola Audit Sistem Informasi Menggunakan Framework COBIT 5 (Studi Kasus: Dinas Kependudukan & Pencatatan Sipil Kabupaten Gianyar)," *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, Vol. 12, no. 3, pp. 1343–1354, Dec. 2023.

[23] P.S. Lestari *et al.*, "Implementasi ISO 27001 dalam Meningkatkan Kepercayaan Pengguna dalam Sektor Industri," *Jurnal Pengabdian Masyarakat dan Riset Pendidikan*, vol. 4, no. 1, pp. 1152–1167, Jul. 2025, doi: 10.31004/jerkin.v4i1.1565.

[24] R. N. J. Meimo Nakashita *et al.*, "Analisis Manajemen Risiko Teknologi Informasi dengan Metode FMEA dan Kontrol ISO 27001:2013 Pada Perusahaan Kontruksi Kapal," *Jurnal Ilmiah Media Sisfo*, vol. 18, no. 2, pp. 166–176, Oct. 2024, doi: 10.33998/mediasisfo.2024.18.2.1795.

[25] C. A. Gemawaty and Y. Yuliani, "MANAJEMEN IDENTITAS DAN AKSES DALAM KEAMANAN SISTEM INFORMASI (PENDEKATAN LITERATURE REVIEW)," *Jurnal Manajemen Informatika Jayakarta*, vol. 4, no. 4, pp. 396–403, 2024, doi: 10.52362/jmijayakarta.v4i4.1527.

[26] A. Fauzi, I. Nur Aprilla, N. Fauziyyah, and N. Fazriyanti Bachtiar, "Implementasi Multi-Faktor Authentication, Single Sign-on dan Role-Based Access Control dalam Keamanan Sistem Informasi (Studi Literature Review)," *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen, dan Keuangan*, vol. 2, no. 1, pp. 33–45, 2025, doi: 10.63217/fibonacci.v2i1.256.

[27] A. Rahmadana, R. Mulyana, and A. F. Santoso, "Pemanfaatan COBIT 2019 Information Security Dalam Merancang Manajemen Keamanan Informasi Pada Transformasi BankCo," *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, vol. 12, no. 3, pp. 1226–1239, 2023.

[28] V. P. Meylani and L. A. Fransen, "Penerapan Model ISO/IEC 25010 Dalam Mengukur Kualitas Aplikasi Shafira Holiday Mobile," *Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi*, vol. 15, no. 1, pp. 388–397, Feb. 2026, doi: http://dx.doi.org/10.35889/jutisi.v15i1.3437.

[29] F. S. Mulyadi and Rizal Fathoni Aji, "Audit Keamanan Informasi Pemasok Pada Perusahaan Penyelenggara Sistem Pembayaran XYZ," *The Indonesian Journal of Computer Science*, vol. 13, no. 4, pp. 6424-6439, Jul. 2024, doi: 10.33022/ijcs.v13i4.4167.