 ISSN:2302-8149
e-ISSN:2540-9719

Audit Kepatuhan Internal Sistem Manajemen Keamanan Informasi pada Perusahaan Keamanan Siber berbasis ISO/IEC 27001

Internal Compliance Audit of the Information Security Management System in a Cybersecurity Company based on ISO/IEC 27001

[1]Sterevania Rambu Muna, [2]Halim Budi Santoso*, [3]Jong Jek Siang
[1,2,3]Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Duta Wacana, Yogyakarta, Indonesia
*e-mail: hbudi@staff.ukdw.ac.id

(***received*:** 23 May 2026, ***revised*:** 31 May 2026, ***accepted*:** 1 June 2026)

Abstrak

Penerapan Sistem Manajemen Keamanan Informasi perlu dilakukan evaluasi untuk mengetahui tingkat kepatuhan terhadap suatu kerangka kerja yang ada. Pada penelitian ini, tim peneliti melakukan evaluasi sistem manajemen keamanan informasi pada sebuah perusahaan jasa keamanan siber di Indonesia, khususnya pada Divisi *Compliance* dan Divisi *Security Operation Center*. Tim peneliti menggunakan studi kasus perusahaan jasa keamanan siber dikarenakan sistem manajemen keamanan informasi yang diterapkan belum sepenuhnya konsisten, khususnya pada pembaharuan kebijakan dan prosedur kerja. Selain itu, sebagai perusahaan jasa keamanan siber, perusahaan ini sebaiknya melakukan evaluasi secara berkala untuk mengetahui tingkat kepatuhan pada suatu standar sistem manajemen keamanan informasi, seperti ISO/IEC 27001:2022. Penelitian ini menggunakan metode *Gap Analysis* dengan menggabungkan data kualitatif dan kuantitatif. Selain itu, tim peneliti juga melakukan observasi langsung dan melakukan telaah terhadap dokumen internal setelah mendapatkan persetujuan dari perusahaan. Sebagai hasilnya, tim peneliti menemukan bahwa tingkat kepatuhan secara keseluruhan sebesar 77,5%. Selain itu, terdapat tiga control yang memenuhi tingkat kepatuhan penuh, yaitu pelaksanaan audit internal sesuai jadwal, dokumentasi insiden, dan penyimpanan log. Hasil gap analysis yang didapatkan digunakan untuk menyusun beberapa rekomendasi perbaikan yang dapat dilakukan perusahaan agar lebih patuh terhadap standard ISO/IEC 27001:2022. Penelitian ini memberikan kontribusi praktis terkait dengan audit kepatuhan internal sistem manajemen keamanan informasi dengan menggunakan kerangka kerja ISO/IEC 27001:2022.

Kata kunci: keamanan siber, *gap analysis*, sistem manajemen keamanan informasi, audit kepatuhan internal, ISO 27001

Abstract

Information Security Management Systems (ISMSs) require periodic evaluation to assess their level of compliance with established standards and frameworks. This study evaluates the implementation of an Information Security Management System in an Indonesian cybersecurity services company, with a particular focus on the Compliance Division and the Security Operations Center (SOC). The case study was selected because the organization's ISMS had not been implemented consistently, particularly regarding the regular updating of security policies and operational procedures. As a cybersecurity service provider, the company is expected to conduct periodic compliance assessments to ensure alignment with recognized information security management standards, such as ISO/IEC 27001:2022. The study employed a Gap Analysis approach that combined qualitative and quantitative data. Data were collected through direct observation and a review of internal documentation after obtaining the company's authorization. The results indicate an overall compliance level of 77.5%. Three control areas achieved full compliance: the timely execution of internal audits, incident documentation, and log management. Based on the identified gaps, a set of improvement recommendations was developed to assist the organization in achieving greater compliance with the requirements of ISO/IEC 27001:2022. This study provides practical contributions by demonstrating the application of the ISO/IEC 27001:2022 framework for conducting

 ISSN:2302-8149
e-ISSN:2540-9719

internal compliance audits of Information Security Management Systems and offering actionable recommendations for strengthening organizational information security governance.

Keywords: *cyber security, gap analysis, information security management system, Internal compliance audit, ISO 27001*

1 Pendahuluan

Sistem Manajemen Keamanan Informasi (SMKI) merupakan kerangka kerja sistematis yang digunakan organisasi untuk melindungi aset informasi melalui pengelolaan risiko yang terstruktur. SMKI mencakup kebijakan, prosedur, serta kontrol keamanan yang terintegrasi untuk menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Penerapan SMKI juga berperan dalam meningkatkan tata kelola keamanan informasi serta memastikan bahwa pengendalian yang diterapkan dapat berjalan secara efektif dan berkelanjutan [1], [2].

Kebutuhan terhadap penerapan SMKI menjadi semakin penting pada organisasi yang bergerak di bidang keamanan siber. Aktivitas seperti monitoring keamanan, pengelolaan insiden, serta pengendalian akses memerlukan penerapan kontrol yang konsisten dan terintegrasi. Namun, beberapa penelitian menunjukkan bahwa masih terdapat kendala dalam menjaga keselarasan antara kebijakan dan implementasi, terutama pada aspek dokumentasi, evaluasi keamanan, dan tata kelola sistem informasi [3], [4].

Penerapan SMKI diperlukan dan dilakukan audit secara berkala untuk mengetahui tingkat kepatuhan terhadap standar yang berlaku. Penelitian ini melakukan observasi audit keamanan informasi pada sebuah perusahaan jasa kemanan siber di Indonesia yang bergerak di bidang *managed security services*, meliputi layanan monitoring kamanan 24/7, respons insiden, dan konsultasi keamanan informasi. Perusahaan ini memiliki dua divisi yang menjadi fokus pada penelitian ini, yaitu divisi *Compliance* dan divisi *Security Operation Center* (SOC). Divisi compliance bertanggung jawab atas pengelolaan kebijakan dan kepatuhan, sedangkan divisi SOC melakukan pemantauan kemanan secara aktif yang meliputi *syslog*, *firewall*, aplikasi, database, dan *Windows Event* secara berkelanjutan. SMKI juga telah diterapkan oleh perusahaan, akan tetapi audit internal belum pernah dilakukan [5].

Suatu perusahaan keamanan informasi diharapkan memiliki mekanisme peninjauan yang terjadwal secara formal, dokumentasi insiden keamanan yang terstandardisasi, serta pencatatan ketidaksesuaian (*non-conformity*) yang terstruktur [6], [7]. Selain itu, perusahaan keamanan siber juga diharapkan memiliki standar keamanan informasi untuk meningkatkan kepercayaan klien dan menjaga kualitas layanan yang diberikan. Oleh karena itu, beberapa pustaka menyarankan untuk melakukan audit kepatuhan internal agar memperoleh gambaran yang terukur mengenai tingkat kesesuaian implementasi SMKI serta mengidentifikasi area yang memerlukan perbaikan [8], [7].

Akan tetapi, objek penelitian yang digunakan dalam studi ini belum melakukan audit internal kepatuhan secara berkala. Hal ini tentunya membutuhkan suatu usaha untuk membantu dalam mengetahui tingkat kepatuhan terhadap audit internal kepatuhan. Oleh karena itu, penelitian ini mencoba untuk melakukan audit kepatuhan internal dengan menggunakan metode *Gap Analysis* pada Divisi *Compliance* dan Divisi *Security Operation Center* (SOC) berdasarkan ISO/IEC 27001:2022. Tim peneliti mendapatkan persetujuan untuk melakukan audit internal dari perusahaan yang akan digunakan sebagai studi kasus pada penelitian ini.

Hasil evaluasi menunjukkan bahwa tingkat kepatuhan Divisi *Compliance* sebesar 75%, Divisi SOC sebesar 80%, dan tingkat kepatuhan gabungan sebesar 77,5%. Penelitian ini juga menghasilkan 17 rekomendasi perbaikan diklasifikasikan berdasarkan prioritas. Penelitian ini diharapkan dapat mem berikan gambaran kondisi implementasi SMKI secara terukur serta menjadi dasar dalam peningkatan kepatuhan secara berkelanjutan [9], [10].

2 Tinjauan Pustaka

2.1 Sistem Manajemen Keamanan Informasi berdasarkan ISO/IEC 27001

Sistem Manajemen Keamanan Informasi (SMKI) merupakan pendekatan sistemasi dalam mengelola keamanan informasi melalui proses identifikasi risiko, penerapan kontrol, serta evaluasi

 ISSN:2302-8149
e-ISSN:2540-9719

berkelanjutan terhadap efektivitas pengaman informasi [1], [2], [11]. Implementasi SMKI mencakup pengelolaan kebijakan, prosedur, serta kontrol keamanan yang terintegrasi dalam mendukung tata kelola organisasi yang baik.

ISO/IEC 27001:2022 menyediakan kerangka kerja dalam penerapan SMKI berbasis risiko yang menekankan pada pengelolaan risiko sebagai dasar dalam penentuan kontrol keamanan informasi [5], [12]. Standar ini digunakan untuk membantu organisasi dalam mengidentifikasi ancaman serta menentukan langkah pengendalian yang sesuai dengan kebutuhan organisasi [13]. Beberapa penelitian menunjukkan bahwa penerapan standar ini dapat meningkatkan pengendalian keamanan informasi serta memperkuat tata kelola sistem informasi [8], [14].

Annex A dalam ISO/IEC 27001:2022 merupakan bagian penting yang memuat daftar kontrol keamanan informasi yang dapat diterapkan oleh organisasi berdasarkan hasil penilaian risiko. Annex A terdiri dari 93 kontrol yang dikelompokkan dalam empat tema: kontrol organisasi (A.5), kontrol manusia (A.6), kontrol fisik (A.7), dan kontrol teknologi (A.8) [15]. Setiap kontrol memiliki tujuan spesifik yang harus dipenuhi, di mana standar yang harus diterapkan mencakup penyediaan bukti implementasi, konsisten penerapan, serta kesesuaian dengan kebijakan yang telah ditetapkan organisasi.

Kontrol yang relevan dalam penelitian ini antara lain: A.5.1 yang mengharuskan kebijakan keamanan informasi disetujui manajemen, dikomunikasikan, dan ditinjau secara berkala; Klausul 9.2 yang mewajibkan pelaksanaan audit internal pada interval terencana dengan laporan yang terdokumentasi; Klausul 10.1 yang mewajibkan setiap ketidaksesuaian ditindaklanjuti dengan tindakan korektif yang mencakup analisis akar masalah; A.5.24 hingga A.5.27 yang mengatur manajemen insiden dari perencanaan hingga pembelajaran pasca insiden; serta A.8.15 dan A.8.16 yang mengharuskan log kejadian direkam,dilindungi, dan dipantau secara aktif [14]. Dalam menerapkan kontrol-kontrol ini pada data yang dimiliki, organisasi perlu memetakan setiap kontrol ke kondisi aktual yang ada, kemudian menilai sejauh mana bukti implementasi tersedia dan sesuai dengan standar yang ditetapkan dalam Annex A.

Statement of Applicability (SoA) merupakan dokumen penting dalam implementasi ISO/IEC 27001:2022 karena berfungsi sebagai dasar penetapan kontrol keamanan yang diterapkan oleh organisasi beserta justifikasinya. Evaluasi terhadap SoA dilakukan dengan memeriksa kesesuaian antara kontrol Annex A, bukti implementasi, serta kebutuhan operasional organisasi. Audit *surveilans* secara berkala diperlukan untuk memastikan bahwa penerapan kontrol keamanan informasi tetap berjalan secara konsisten dan efektif sesuai dengan persyaratan standar [14].

Namun, dalam implementasinya masih ditemukan berbagai kendala, terutama pada aspek operasional. Permasalahan yang sering muncul meliputi ketidakkonsistenan dokumentasi, kurangnya pembaruan kebijakan, serta lemahnya pengendalian terhadap penerapan kontrol keamanan informasi [3], [9], [4]. Hal ini menunjukkan bahwa penerapan SMKI memerlukan evaluasi yang berkelanjutan unutk memastikan kesesuaian dengan standar yang berlaku.

2.2 Audit Sistem Manajemen Keamanan Informasi

Audit SMKI merupakan proses evaluasi yang dilakukan untuk menilai kesesuaian penerapan SMKI dengan standar yang berlaku serta memastikan bahwa kontrol keamanan telah diimplementasikan secara efektif [6], [8]. Audit dilakukan secara berkala sebagai bagian dari upaya peningkatan berkelanjutan dalam pengelolaan keamanan informasi.

Dalam pelaksanaannya, audit SMKI mencakup beberapa tahapan, yaitu perencanaan audit, pengumpulan data, evaluasi bukti, serta penyusunan laporan hasil audit. Pengumpulan data dapat dilakukan melalui kuesioner, ebservasi, serta pemeriksaan dokumen untuk memastikan kesesuaian antara kebijakan dan implementasi di lapangan [7].

Salah satu metode yang digunakan dalam audit SMKI adalah *Gap Analysis*. Metode ini digunakan untuk mengidentifikasi kesenjangan antara kondisi aktual dengan standar yang ditetapkan, sehingga dapat diketahui tingkat kepatuhan organisasi [2], [13]. Proses perhitungan dilakukan dengan membandingkan nilai implementasi aktual terhadap nilai standar menggunakan rumus: *GAP* = Skor Ideal – Skor Aktual, sehingga diperoleh nilai kesenjangan yang menunjukkan tingkat kesesuaian. Skor aktual diperoleh dari penilaian kondisi implementasi menggunakan skala kematangan 0-4, di mana 0 berarti tidak diterapkan dan 4 berarti sesuai penuh dengan standar [7].

 ISSN:2302-8149
e-ISSN:2540-9719

Nilai kesenjangan yang dihasilkan kemudian digunakan untuk menentukan prioritas perbaikan secara sistematis, sehingga organisasi dapat melakukan peningkatan secara berharap dan terarah [7]. Instrumen yang digunakan dalam *Gap Analysis* umumnya berupa kuesioner yang disusun berdasarkan kontrol dalam standar ISO/IEC 27001:2022, sehingga memungkinkan evaluasi dilakukan secara lebih rinci dan terstruktur [5].

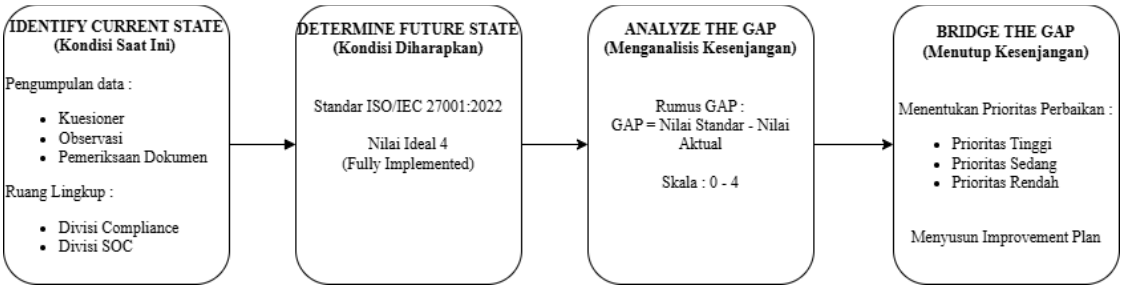
Beberapa penelitian menunjukkan bahwa *Gap Analysis* dapat dikombinasikan dengan kerangka kerja lain untuk menghasilkan evaluasi yang lebih komprehensif serta memudahkan penyusunan rencana peningkatan yang terprioritas. Intgrasi ISO 27005 dan NIST SP 800-30 pada *Security Operation Center* (SOC) menunjukkan bahwa pendekatan berbasis risiko dapat membantu meningkatkan efektivitas pengelolaan keamanan informasi [16]. Selain itu, penerapan evaluasi berbasis tingkat kematangan (*maturity level*) dan siklus PDCA (*Plan-Do-Check-Act*) juga mampu membantu organisasi dalam Menyusun rencana peningkatan keamanan informasi secara berkelanjutan [10].

Dalam konteks perusahaan yang bergerak di bidang keamanan siber, kepatuhan terhadap standar keamanan informasi menjadi aspek yang penting karenan perusahaan memiliki tanggung jawab dalam menjaga keamanan informasi klien. Oleh karena itu, pelaksanaan audit internal secara berkala menjadi bagian penting dalam memastikan bahwa seluruh proses pengelolaan keamanan informasi telah berjalan sesuai dengan standar yang berlaku [1], [5], [17].

3 Metode Penelitian

Penelitian ini menggunakan pendekatan evaluatif dengan motede *Gap Analysis* untuk mengukur tingkat kepatuhan internal penerapan SMKI pada Divisi *Compliance* dan Divisi *Security Operation Center* (SOC) di sebuah perusahaan keamanan siber di Indonesia, berdasarkan ISO/IEC 27001:2022. Sebelum pengumpulan data dimulai, tim peneliti memperoleh *informed consent* dari pimpinan perusahaan yang mencakup izin untuk melakukan observasi operasional, pembagian *Gform* dengan staff pada dua divisi yang menjadi tinjauan pada penelitian ini, yaitu divisi compliance dan divisi SOC, dan pemeriksaan secara komprehensif beberapa dokumen internal pendukung.

Implementasi *Gap Analysis* dalam penelitian ini mengikuti empat tahap diilustrasikan pada Gambar 1. Keempat tahap tersebut disesuaikan dengan konteks penelitian, di mana setiap tahap menghasilkan data yang menjadi masukan bagi tahap berikutnya hingga menghasilkan nilai *GAP* per kontrol dan persentase kepatuhan per divisi.



Gambar 1 Tahapan *gap analysis*

Tahap pertama, *Ideentify Current State*, dilakukan untuk memperoleh gambaran kondisi aktual penerapan SMKI di perusahaan. Pada tahap ini tim peneliti melakukan pengumpulan data melalui dua cara. Pertama, kuesioner berbasis *Google Form* dikirimkan kepada responden yang terlibat langsung dalam pengelolaan SMKI: 3 *staff Compliance Officer* dari Divisi *Compliance* yang bertanggung jawab atas pengelolaan kebijakan, pengendalian dokumen, dan pelaksanaan audit internal; serta 3 *staff* analisis SOC dari Divisi SOC yang menangani monitoring keamanan, penanganan insiden, dan pengelolaan log secara aktif. Selain melalui kuisioner, untuk mendapatkan data dari kasus yang ada secara lebih komprehensif, tim peneliti melakukan observasi dan pemantauan kerja di perusahaan. Observasi dilakukan dengan melakukan pengamatan pada proses operasional. Enam dokumen internal perusahaan juga turut dilakukan pemeriksaan, yaitu: Dokumen *System Operating Procedure* (SOP) SMKI, SOP Keamanan Teknologi Informasi, SOP Penggunaan Aset TI, SOP Pengembangan Aplikasi, SOP Manajemen Kerentanan, SOP SOC. Seluruh temuan dari tahap ini membentuk kondisi aktual (*as-is*) yang menjadi dasar penilaian dalam gap analysis. Dengan

 ISSN:2302-8149
e-ISSN:2540-9719

menggunakan beberapa metodologi pada proses pengamatan, diharapkan dapat memberikan pemahaman secara komprehensif terkait dengan kondisi penerapan SMKI perusahaan secara menyeluruh.

Tahap kedua, *Determine Future State*, menetapkan kondisi ideal yang menjadi acuan evaluasi berdasarkan klausul dan kontrol ISO/IEC 27001:2022 yang relevan. Untuk Divisi *Compliance*, kondisi ideal ditetapkan berdasarkan: A.5.1 (kebijakan keamanan informasi wajib disetujui manajemen dan ditinjau berkala), Klausul 7.5 (pengendalian informasi terdokumentasi), A.5.37 (prosesdur operasional terdokumentasi), Klausul 9.2 (audit internal terjadwal dan dilaporkan), serta Klausul 10.1 (ketidaksesuaian wajin ditindaklanjuti dengan *corrective action*). Untuk Divisi SOC, kondisi ideal ditetapkan berdasarkan: A.5.24 (prosedur pelaporan dan penanganan insiden), A.5.25 (penilaian dan eskalasi insiden). A.5.27 (pembelajaran dari insiden), A.8.15 (pengelolaan dan retensi *log*), dan A.8.16 (monitoring aktivitas keamanan secara aktif). Skor ideal per kontrol ditetapkan sebesar 4 berdasarkan definisi tingkat tertinggi dalam skala kematangan kontrol ISO/IEC 27001:2022 (Dioptimalkan/ Sesuai Penuh), sebagaimana disajikan pada Tabel 1.

Tabel 1 Skala penilaian *gap analysis*

Skor	Kategori	Deskripsi
0	Tidak ada / belum dilakukan	Kontrol tidak diterapkan sama sekali, tidak terdapat bukti pelaksanaan
1	Inisiasi / belum lengkap	Ada upaya penerapan namun bukti pendukung masih sangat minim.
2	Terdefinisi / sebagaian diimplementasikan	Kontrol diterapkan Sebagian, belum konsisten, kesenjangan signifikan
3	Terkelola / hampir penuh	Penerapan hampir memenuhi persyaratan standar, kesenjangan minor.
4	Dioptimalkan / sesuai penuh	Kontrol diterapkan sepenuhnya sesuai ISO/IEC 27001:2022, bukti lengkap

Tahap ketiga, *Analyze the Gaps*, dilaksanakan melalui pengisian kuesioner berbasis Google Form oleh responden dari masing-masing divisi. Kuesioner terdiri dari dua bagian: Bagian A untuk Divisi *Compliance* (10 pertanyaan) dan Bagian B untuk Divisi SOC (10 pertanyaan), sehingga total terdapat 20 item pertanyaan. Seluruh pertanyaan dikembangkan yang mengacu pada klausul dan kontrol ISO/IEC 27001:2022 yang relevan. Daftar lengkap item pertanyaan per divisi beserta sumber masing-masing pertanyaan disajikan pada Tabel 2 dan Tabel 3.

Tabel 2 Item pertanyaan penilaian divisi *compliance*

No	Area Penilaian	Pertanyaan	Kontrol ISO/IEC 27001:2022
1	Kebijakan & SOP	1. Apakah kebijakan dan SOP keamanan informasi telah diperbarui sesuai periode yang ditetapkan perusahaan ? 2. Sebutkan SOP kebijakan keamanan informasi yang digunakan saat ini dan tahun terakhir pembaruannya ?	A.5.1 – *Policies for information security*
2	Pengesahan Dokumen	1. Apakah dokumen kebijakan dan SOP memiliki tanda pengesahan resmi dari pihak berwenang? 2. Siapa pihak yang berwenang mengesahkan dokumen dan bagaimana bentuk pengesahan tersebut (tanda tangan, digital approval, dll)?	A.5.1 – *Policies for information security*
3	Versi & Revisi	1. Apakah dokumen SMKI memiliki nomor versi dan riwayat revisi yang terdokumentasi dengan jelas? 2. Di mana riwayat revisi dokumen dicatat dan bagaimana mekanisme pembaruannya?	A.5.37 – *Documented operating procedures*
4	Audit Internal	1. Apakah audit internal keamanan informasi dilaksanakan sesuai jadwal yang telah ditetapkan? 2. Kapan audit internal terakhir dilakukan dan siapa pihak yang terlibat?	Clause 9.2 – *Internal audit*
5	Laporan Audit	1. Apakah laporan hasil audit internal terdokumentasi lengkap dan dapat ditelusuri kembali? 2. Sebutkan bentuk laporan audit yang digunakan (dokumen, file, sistem) dan lokasi penyimpanannya.	Clause 9.2 – *Internal audit*

 ISSN:2302-8149
e-ISSN:2540-9719

6	Pencatatan NC	1. Apakah ketidaksesuaian (*Non-Conformity*) dicatat secara lengkap termasuk akar masalah dan tindakan perbaikan? 2. Apakah Ketidaksesuaian (*Non-Conformity*) dicatat lengkap termasuk akar masalah?	Clause 10.1 – *Nonconformity and corrective action*
7	Tindak Lanjut NC	1. Apakah setiap *Non-Conformity* memiliki bukti tindak lanjut yang terdokumentasi? 2. Sebutkan contoh bukti tindak lanjut *Non-Conformity* yang pernah dilakukan.	Clause 10.1 – *Nonconformity and corrective action*
8	Penyimpanan Dokumen	1. Apakah dokumen SOP disimpan sesuai SOP? 2. Di mana dokumen SOP disimpan dan bagaimana pengamanannya?	A.5.37 – *Documented operating procedures*
9	Distribusi Dokumen	1. Apakah distribusi dokumen dicatat sesuai prosedur? 2. Bagaimana mekanisme distribusi dokumen dilakukan kepada pihak terkait?	A.5.1 – *Policies for information security*
10	Log Perubahan	1. Apakah perubahan atau revisi dokumen dicatat dalam log perubahan atau catatan revisi? 2. Sebutkan contoh informasi yang dicatat dalam log perubahan dokumen	Clause 7.5 – *Documented information*

Tabel 3 Item pertanyaan penilaian divisi SOC

No	Area Penilaian	Pertanyaan	Kontrol ISO/IEC 27001:2022
1	Pelaporan Insiden	1. Apakah insiden keamanan informasi dilaporkan menggunakan form atau format sesuai SOP ? 2. Sebutkan jenis form atau sistem yang digunakan untuk pelaporan insiden	A.5.24 – *Information security incident management*
2	Dokumentasi Insiden	1. Apakah dokumentasi insiden mencakup informasi waktu kejadian, penyebab, tindakan, dan hasil penanganan? 2. Bagian apa saja yang wajib diisi dalam dokumentasi insiden?	A.5.24 – *Information security incident management*
3	Monitoring Log	1. Apakah monitoring log aktivitas sistem dilakukan secara rutin sesuai prosedur? 2. Sebutkan jenis log yang dimonitor dan frekuensi monitoringnya.	A.8.15 – *Logging*
4	Evaluasi Insiden	1. Apakah dilakukan evaluasi pasca insiden untuk menilai efektivitas penanganan insiden? 2. Jelaskan contoh evaluasi pasca insiden yang pernah dilakukan	A.5.27 – *Learning from information security incidents*
5	Eskalasi Insiden	1. Apakah proses eskalasi pasca insiden dilakukan untuk menilai efektivitas penanganan insiden ? 2. Jelaskan bagaimana proses eskalasi dilakukan dan siapa pihak yang terlibat dalam evaluasi pasca insiden.	A.5.25 – *Assessment and decision on information security incidents*
6	Penyimpanan Log	1. Apakah penyimpanan log aktivitas keamanan telah dilakukan sesuai prosedur yang ditetapkan? 2. Di mana log aktivitas disimpan dan berapa lama log tersebut disimpan sesuai ketentuan?	A.8.15 – *Logging*
7	Monitoring Keamanan	1. Apakah monitoring keamanan dilakukan secara aktif dan terdokumentasi ? 2. Sebutkan tools atau sistem yang digunakan untuk melakukan monitoring keamanan.	A.8.16 – *Monitoring Activities*
8	Insiden Berulang	1. Apakah insiden yang terjadi secara berulang dianalisis untuk mengetahui pola atau akar penyebabnya? 2. Berikan contoh insiden berulang yang pernah terjadi dan hasil analisis yang dilakukan.	A.5.27 – *Learning from incidents*
9	Waktu Respons	1. Apakah waktu respons insiden dicatat secara jelas sesuai tingkat keparahan insiden ? 2. Berapa target waktu respons untuk insiden dengan tingkat keparahan tinggi atau kritikal ?	A.5.24 – *Information security incident management*

 ISSN:2302-8149
e-ISSN:2540-9719

10	Bukti Teknis	1. Apakah bukti teknis insiden terdokumentasi? 2. Sebutkan jenis bukti teknis yang biasanya dikumpulkan saat terjadi insiden dan di mana bukti tersebut disimpan.	A.8.15 - *Logging* A.8.16 - *Monitoring activities*

Penilaian dilakukan per item pertanyaan menggunakan skala 0-4. Jawaban responden diverifikasi melalui observasi dan telaah dokumen (triangulasi) untuk memastikan objektivitas skor yang diberikan. Skor akhir per kontrol merupakan skor yang disepakati antara jawaban responden dan hasil verifikasi dokumen. Dalam menilai kondisi yang bersifat kualitatif, tim peneliti menggunakan kriteria operasional berikut: **Skor 1** diberikan apabila terdapat upaya implementasi namun tidak ada bukti dokumen yang dapat ditunjukkan saat telaah; **Skor 2** diberikan apabila terdapat dokumen pendukung namun hanya berlaku untuk sebagian kasus atau tidak diterapkan secara konsisten (misalnya SOP ada namun tidak semua staf mengikutinya); **Skor 3** diberikan apabila kontrol sudah berjalan konsisten namun masih terdapat satu atau dua aspek minor yang belum terpenuhi berdasarkan pembandingan langsung dengan persyaratan spesifik klausul ISO/IEC 27001:2022 misalnya laporan audit tersedia namun tidak mencantumkan status tindak lanjut secara eksplisit; **skor 4** diberikan apabila seluruh persyaratan kontrol terpenuhi dengan bukti dokumen yang lengkap dan konsisten.

Nilai *GAP* per kontrol dihitung dengan rumus: ***GAP* = Skor Ideal – Skor Aktual**. Nilai *GAP* = 0 berarti kontrol telah memenuhi standar penuh; GAP = 1 menunjukkan kesenjangan minor yang perlu ditingkatkan konsistenya; *GAP* = 2 menunjukkan kesenjangan signifikan di mana kontrol hanya terimplementasi Sebagian dan memerlukan perbaikan segera; *GAP* = 3 mengindikasikan kontrol baru dalam tahap insiasi dengan bukti yang sangat minim; sedangan *GAP* = 4 berarti kontrol sama sekali belum diterapkan. Semakin besar nilai *GAP*, semakin tinggi prioritas perbaikan yang diperlukan. Presentase kepatuhan per divisi dihitung menggunakan rumus : **Presentase Kepatuhan = (Total Skor Aktual / Total Skor Ideal) x 100%**. Total skor ideal per divisi adalah 40 (10 kontrol x skor ideal 4). Klasifikasi tingkat kepatuhan berdasarkan rentang presentase disajikan pada Tabel 4.

Tabel 4 Klasifikasi tingkat kepatuhan

Rentang Presentase	Kategori	Keterangan
76 – 100%	Patuh	Implementasi sesuai dengan standar ISO secara konsisten dengan bukti pendukung memadai.
51 – 75%	Cukup Patuh	Kontrol sudah diterapkan, namun masih terdapat kekurangan dalam konsistensi atau kelengkapan bukti.
26 – 50%	Kurang Patuh	Implementasi masih lemah, banyak kontrol belum berjalan secara optimal.
0 – 25%	Tidak Patuh	Kontrol tidak diterapkan atau tidak terdapat bukti pendukung yang memadai.

Tahap keempat, *Bridge the Gap*, dilaksanakan dengan Menyusun rekomendasi perbaikan (*Improvement Plan*) berdasarkan hasil analisis kesenjangan. Setiap rekomendasi ditetapkan prioritas dan target waktunya menggunakaan kriteria yang disajikan pada Tabel 5 dan Tabel 6. Penetapan prioritas mempertimbangkan tiga faktor: (1) dampak langsung terhadap keamanan informasi dan keterkaitan dengan kontrol utama ISO/IEC 27001:2022; (2) kompleksitas teknis perbaikan apakah memerlukan perubahan sistem atau cukup perubahan prosedur; dan (3) jumlah pihak yang harus terlibat dalam pelaksanaan perbaikan. Target waktu bersifat rekomendasi dan perlu disesuaikan dengan kapasitas aktual perusahaan.

Tabel 5 Kriteria prioritas rekomendasi perbaikan

Nilai	Keterangan
Tinggi	Berdampak langsung pada keamanan informasi dan berkaitan dengan kontrol utama ISO/IEC 27001:2022.
Sedang	Mendukung efektivitas sistem namun tidak berdampak langsung secara kritis terhadap keamanan informasi
Rendah	Bersifat administratif dan tidak berdampak signifikan terhadap risiko keamanan informasi.

 ISSN:2302-8149
e-ISSN:2540-9719

Tabel 6 Kriteria target waktu rekomendasi perbaikan

Nilai	Keterangan
1 Bulan	Perbaikan sederhana, tidak memerlukan perubahan sistem dan dapat dilakukan oleh satu divisi.
1-2 Bulan	Perbaikan dengan tingkat kompleksitas sedang dan memerlukan koordinasi terbatas antar pihak.
2-3 Bulan	Perbaikan kompleks yang melibatkan lebih dari satu divisi atau memerlukan perubahan sistem.

4 Hasil dan Pembahasan

Evaluasi Divisi *Compliance* mencakup 10 kontrol terkait kebijakan keamanan informasi, pengesahan dokumen, *versioning*, audit internal, pengelolaan *non-conformity*, penyimpanan, distribusi, dan log perubahan dokumen. Hasil penelitian disajikan pada Tabel 7.

Tabel 7 Hasil *gap analysis* divisi *compliance*

No	Kontrol ISO/IEC 27001:2022	Item Penilaian	Skor Aktual	Skor Ideal	*GAP*
1	A.5.1	Kebijakan SMKI diperbarui berkala	3	4	1
2	A.5.1	Dokumen memiliki pengesahan	3	4	1
3	A.5.37	Nomor versi & revisi jelas	3	4	1
4	Klausul 9.2	Audit internal sesuai jadwal	4	4	0
5	Klausul 9.2	Laporan audit terdokumentasi lengkap	3	4	1
6	Klausul 10.1	NC dicatat lengkap + akar masalah	2	4	2
7	Klausul 10.1	Bukti tindak lanjut NC terdokumentasi	3	4	1
8	A.5.37	Penyimpanan dokumen sesuai SOP	3	4	1
9	A.5.1	Distribusi dokumen terdokumentasi	3	4	1
10	Klausul 7.5	Log perubahan dokumen tercatat	3	4	1
	Total		30	40	-

Berdasarkan Tabel 7, total skor aktual Divisi *Compliance* adalah 30 dari skor ideal 40, menghasilkan presentase kepatuhan sebesar **75% (Cukup Patuh)**. Kontrol dengan *GAP* tertinggi (*GAP* = 2) adalah pencatatan *Non-Conformity* (Klausul 10.1) dengan skor aktual 2. Meskipun terdapat dokumen *Audit Report* dan *Corrective Action Tracker*, analisis akar masalah belum dilakukan secara komprehensif menggunakan pendekatan terstruktur. Satu-satunya kontrol yang mencapai skor ideal (*GAP* = 0) adalah pelaksanaan audit internal sesuai jadwal (Klausul 9.2), yang terbukti dengan pelaksanaan audit terakhir pada Januari 2026 yang melibatkan Direktur, Divisi *Compliance*, dan Divisi SOC. Ini merupakan praktik baik yang mencerminkan komitmen perusahaan terhadap siklus audit yang konsisten.

Divisi *Compliance* juga memiliki beberapa praktik baik yang perlu dipertahankan: proses approval dokumen oleh Direktur sudah berjalan konsisten, penyimpanan dokumen di *Google Drive* sudah terpusat, dan audit internal terlaksana sesuai jadwal dengan partisipasi seluruh divisi terkait. Adapun temuan yang memerlukan perbaikan meliputi: (1) pembaruan SOP belum terjadwal secara formal seluruh SOP termasuk SMKI belum memiliki jadwal *review* yang baku; (2) format pengesahan dokumen tidak seragam antar divisi meskipun proses *approval* oleh Direktur sudah berjalan; (3) pencatatan versi dan riwayat revisi dalam tabel history belum diterapkan secara seragam; (4) penyimpanan dokumen di *Google Drive* dengan kontrol akses berbasis peran belum sepenuhnya terstruktur; serta (5) distribusi dokumen melalui sosialisasi belum disertai catatan formal distribusi.

Evaluasi Divisi SOC mencakup 10 kontrol terkait pelaporan insiden, dokumentasi insiden, monitoring log, evaluasi dan eskalasi insiden, penyimpanan log, monitoring keamanan aktif, analisis insiden berulang, pencatatan waktu respons, dan bukti teknis. Hasil penilaian disajikan pada Tabel 8.

 ISSN:2302-8149
e-ISSN:2540-9719

Tabel 8 Hasil *gap analysis* divisi SOC

No	Kontrol ISO/IEC 27001:2022	Item Penilaian	Skor Aktual	Skor Ideal	*GAP*
1	A.5.24	Pelaporan insiden sesuai SOP	3	4	1
2	A.5.24	Dokumentasi insiden lengkap	4	4	0
3	A.8.15	Monitoring log aktivitas rutin	3	4	1
4	A.5.27	Evaluasi pasca insiden dilakukan	3	4	1
5	A.5.25	Proses eskalasi insiden berjalan	3	4	1
6	A.8.15	Penyimpanan log sesuai SOP	4	4	0
7	A.8.16	Monitoring keamanan aktif & terdokumentasi	3	4	1
8	A.5.27	Analisis insisden berulang	3	4	1
9	A.5.24	Waktu respons insiden dicatat	3	4	1
10	A.8.15	Bukti teknis insiden terdokumentasi	3	4	1
	Total		32	40	-

Berdasarkan Tabel 8, total skor aktual Divisi SOC adalah 32 dari skor ideal 40, menghasilkan presentase kepatuhan sebesar **80% (Patuh**). Dua kontrol mencapai skor penuuh (*GAP* = 0): dokumentasi insiden lengkap (A.5.24) dan penyimpanan log sesuai SOP (A.8.15). Dokumentasi insiden melalui platform internal perusahaan mencakup detail insiden, *timeline*, IOC, dampak, dan solusi. Log disimpan di *Google Cloud Platform* dan *server-on-premise* minimal 1 tahun sesuai standar PCI-DSS dan dapat diakses real-time.

Delapan kontrol lainnya memperoleh skor 3 (*GAP* = 1). Temuan utama mencakup : (1) pengisian laporan insiden di *platform* internal belum seragam antar analisis; (2) monitoring menggunakan SIEM Wazuh mencakup *syslog*, *firewall*, aplikasi, database, dan *Windows Event* secara 24/7, namun tidak semua terdokumentasi konsisten; (3) evaluasi pasca insiden (*post-mortem*) belum diformalisasi untuk semua insiden; (4) proses eskalasi L1,L2 Klien belum memiliki protokol seragam; (5) waktu respons insiden kritis berkisar 10-30 menit namun pencatatan belum detail dan konsisten per tingkat keparahan.

Tabel 9 menyajikan rekaptulasi hasil penilaian kepatuhan kedua divisi.

Tabel 9 Kriteria prioritas rekomendasi perbaikan

Komponen	*Compliance*	SOC	Total
Skor Ideal	*40*	40	80
Skor Aktual	30	32	62
Presentase Kepatuhan	75%	80%	77,5%
Kategori Kepatuhan	Cukup Patuh	Patuh	-

Presentase kepatuhan gabungan kedua divisi mencapai 77,5%. Divisi SOC (80)% masuk kategori Patuh, sedangkan Divisi *Compliance* (75%) berada pada kategori Cukup Patuh. Selisi 5 poin mengindikasikan bahwa Divisi SOC memiliki kematangan implementasi lebih tinggi, diperkuat oleh penggunaan *platform internal* perusahaan dan SIEM Wazuh yang telah beroperasi aktif. Dari 20 kontrol yang dievaluasi, 3 kontrol mencapai skor ideal (*GAP* = 0), 16 kontrol memiliki *GAP*=1, dan 1 kontrol memiliki *GAP*=2.

Berdasarkan *gap analysis*, disusun 17 rekomendasi perbaikan yang diprioritaskan berdasarkan nilai *GAP*, dampak terhadap keamanan informasi, dan kemudahan implementasi, sebagaimana disajikan pada Tabel 10.

Tabel 10 Rencana perbaikan (*improvement plan*)

No	Area Perbaikan	Temuan *Gap*	Rekomendasi Perbaikan	Divisi	Prioritas	Target
1	Kebijakan & SOP	Pembaruan SOP belum dilakukan secara berkala	Menetapkan jadwal review SOP minimal 1 tahun sekali dan mencantumkan tanggal review pada dokumen	*Compliance*	Tinggi	1-2 bulan

 ISSN:2302-8149
e-ISSN:2540-9719

2	Pengesahan Dokumen	Format pengesahan dokumen belum seragam	Menstandarkan format pengesahan (TTD/digital *approval*) dan menetapkan pihak berwenang dalam SOP	*Compliance*	Sedang	2-3 bulan
3	Versi & Revisi	Pencatatan veris dan revisi belum konsisten	Mewajibkan penggunaan *version control* dan *table revision history* pada seluruh dokumen	*Compliance*	Tinggi	1-2 bulan
4	Laporan Audit	Laporan audit belum terstruktur dan sulit ditelusuri	Menyusun template laporan audit standar dan sistem penyimpanan berbasis *indexing*	*Compliance*	Tinggi	1-2 bulan
5	Pencatatan NC	Pencatatan NC belum lengkap terutama analisis akar masalah	Menambahkan analisis *root cause* (5 *Why*) dalam form NC dan membuat *corrective action tracker*	*Compliance*	Tinggi	1 bulan
6	Tindak Lanjut NC	Dokumentasi tindak lanjut belum konsisten	Membuat sistem monitoring tindak lanjut dengan status *tracking* (*open/close*)	*Compliance*	Tinggi	1 bulan
7	Penyimpanan Dokumen	Kontrol akses dokumen belum terstruktur	Menerapkan kontrol akses berbasis peran dan penyimpanan terpusat	*Compliance*	Tinggi	1-2 bulan
8	Distribusi Dokumen	Distribusi dokumen belum terdokumentasi secara formal	Membuat log distribusi dokumen dan mencatat pihak penerima dokumen	*Compliance*	Rendah	2 bulan
9	Log Perubahan	Log perubahan belum konsisten di semua dokumen	Menstandarkan formal log perubahan dan menjadikannya wajib pada setiap dokumen	SOC	Tinggi	1-2 bulan
10	Pelaporan Insiden	Pengisian laporan insiden belum konsisten lengkap	Menstandarkan *form* pelaporan insiden dan mewajibkan *field* wajib diisi	SOC	Tinggi	1 bulan
11	Monitoring Log	Monitoring log belum dilakukan secara konsisten	Menetapkan jenis log wajib dan jadwal monitoring log	SOC	Tinggi	1-2 bulan
12	Evaluasi Insiden	Evaluasi pasca insiden belum dilakukan secara formal	Menerapkan proses *post-incident review* dan dokumentasi evaluasi	SOC	Tinggi	1 bulan
13	Eskalasi Insiden	Proses eskalasi belum terstandarisasi sepenuhnya	Menetapkan level eskalasi dan alur penanganan dalam SOP SOC	SOC	Tinggi	1-2 bulan
14	Monitoring Keamanan	Dokumentasi monitoring belum konsisten	Menggunakan *dashboard* monitoring dan menyimpan laporan monitoring	SOC	Sedang	2-3 bulan
15	Insiden Berulang	Analisis insiden berulang belum optimal	Membuat database insiden dan analisis tren untuk pencegahan	SOC	Sedang	2-3 bulan
16	Waktu	Pencatatan waktu	Menetapkan SLA	SOC	Tinggi	1-2 bulan

 ISSN:2302-8149
e-ISSN:2540-9719

	Respons	respons belum detail	insiden dan mencatat waktu deteksi, respon, dan penyelesaian			
17	Bukti Teknis Insiden	Bukti teknis belum terdokumentasi lengkap	Menstandarkan dokumen bukti teknis dan menyimpan dalam repository terpusat	SOC	Tinggi	1-2 bulan

Target waktu pada setiap rekomendasi ditetapkan oleh tim peneliti berdasarkan tiga faktor: (1) kompleksitas teknis perbaikan apakah memerlukan perubahan sistem atau cukup perubahan prosedur; (2) jumlah pihak yang terlibat perbaikan yang hanya melibatkan satu divisi dapat diselesaikan lebih cepat; dan (3) ketersediaan template atau standar yang dapat langsung diadopsi. Target ini bersifat rekomendasi dan perlu disesuaikan dengan kapasitas aktual perusahaan. Contohnya, *review* SOP yang dijadwalkan setiap akhir tahun oleh perusahaan dapat disesuaikan dengan siklus yang sudah ada. Dari 17 *item* perbaikan, 12 berkategori prioritas tinggi, 3 prioritas sedang, dan 2 prioritas rendah. Mayoritas dapat diselesaikan dalam 1-2 bulan dengan dukungan manajemen. Perbaikan paling mendesak adalah: penambahan analisis 5-*Why* dalam form NC (*Compliance*, *GAP*=2), standarisasi form pelaporan insiden di *platform internal* (SOC), formalisasi prosedur post-incident review (SOC), dan penetapan jadwal review SOP (*Compliance*). Implementasi menyeluruh diproyeksikan meningkatkan kepatuhan *Compliance* ke ≥ 90% dan SOC ke ≥ 95%, menempatkan perusahaan pada posisi siap sertifikasi ISO/IEC 27001:2022.

5 Kesimpulan

Penelitian ini telah mengevaluasi tingkat kepatuhan internal SMKI pada Divisi *Compliance* dan Divisi SOC di sebuah perusahaan keamanan siber menggunakan metode *Gap Analysis* berbasis ISO/IEC 27001:2022. Hasil evaluasi menunjukkan kepatuhan Divisi *Compliance* 75% (Cukup Patuh) dan Divisi SOC sebesar 80% (Patuh), dengan persentase kepatuhan gabungan 77,5%. Dari 20 kontrol yang dievaluasi, tiga kontrol mencapai skor ideal (*GAP* = 0), yaitu pelaksanaan audit internal, dokumentasi insiden, dan penyimpanan log; sementara kesenjangan terbesar ditemukan pada pencatatan *Non-Conformity* (*GAP*=2) di Divisi *Compliance*. Sebanyak 17 rekomendasi perbaikan telah disusun berdasarkan prioritas dan kompleksitas, yang apabila diimplementasikan secara menyeluruh diproyeksikan dapat meningkatkan kepatuhan Divisi *Compliance* menjadi ≥90% dan Divisi SOC menjadi ≥95%, sehingga perusahaan siap menuju sertifikasi ISO/IEC 27001:2022.

Ucapan Terima Kasih

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

Referensi

[1] 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.

[2] 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.

[3] L. D. A. Jelita, M. N. Al Azam, and A. Nugroho, "Evaluasi Keamanan Teknologi Informasi menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022," *Jurnal SAINTEKOM*, Vol. 14, No. 1, pp. 84–94, Mar. 2024, DOI: 10.33020/saintekom.v14i1.623.

[4] M. N. H. Siregar and Mardiah, "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.

[5] R. Sinaga, "Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala," *Nuansa Informatika*, Vol. 18, No. 2, pp. 46–54, 2024, DOI: 10.25134/ilkom.v18i2.205.

[6] D. Fatih and R. Fathoni Aji, "Evaluasi Keamanan Informasi menggunakan ISO/IEC 27001: Studi Kasus PT XYZ," *Jurnal Sains Komputer & Informatika (J-SAKTI*, Vol. 8, No. 2, pp. 58–75, 2024, DOI: 10.30996/jsakti.v8i2.12099.

[7] 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, Jan. 2024, DOI: 10.28932/jutisi.v9i3.6850.

[8] K. Ryanto and V. Tundjungsari, "*Standardization of Information Security Management in the Banking Sector using the ISO 27001:2022 Framework*," *Journal La Multiapp*, Vol. 5, No. 4, pp. 344–354, Aug. 2024, DOI: 10.37899/journallamultiapp.v5i4.1399.

[9] I. N. A. A. Wibawa, A. A. N. H. Susila, and M. A. Pasirulloh, "*Information Security Evaluation at Hospital using Index KAMI 5.0 and Recommendations based on ISO/IEC 27001:2022*," *Journal of Information Systems and Informatics*, Vol. 6, No. 4, pp. 3070–3086, Dec. 2024, DOI: 10.51519/journalisi.v6i4.949.

[10] 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.

[11] A. Ambarwati and C. Darujati, "Penilaian Risiko Data Sistem Informasi Manajemen Puskesmas dan Aset menggunakan ISO 27005," *Telp*, Vol. 10, No. 1, pp. 1–13, 2021, DOI: 10.32520/stmsi.v10i1.995.

[12] Y. Kamil, S. Lund, and M. S. Islam, "*Information Security Objectives and the Output Legitimacy of ISO/IEC 27001: Stakeholders' Perspective on Expectations in Private Organizations in Sweden*," *Information Systems and e-Business Management*, Vol. 21, No. 3, pp. 699–722, Sep. 2023, DOI: 10.1007/s10257-023-00646-y.

[13] A. Ulya, A. Karima, T. S. A. Sukiman, A. Zulfia, and R. Rahmawati, "*Information Security Risk Analysis using ISO 31000:2018 and ISO 27001:2022*," *Brilliance: Research of Artificial Intelligence*, Vol. 5, No. 2, pp. 843–853, Sep. 2025, DOI: 10.47709/brilliance.v5i2.6564.

[14] J. P. Keinsinyuran, C. Widharto, and M. A. Kartawidjaja, "Evaluasi *Statement of Applicability* ISO 27001:2022 melalui Audit Surveilans pada Pusat Data Internal," *Jurnal Praktik Keinsinyuran*, Vol. 3, No. 2, pp. 135–146, 2026, DOI: 10.25170/jpk.v3i02.7631.

[15] M. Sari *et al.*, "Analisis Tata Kelola TI Perumdam Tirta Siak menggunakan COBIT 2019 dan ISO27001 A*nalysis IT Governance of Perumdam Tirta Siak using COBIT 2019 and ISO27001*," *Sistemasi: Jurnal Sistem Informasi*, Vol. 13, pp. 324–334, 2024, DOI: 10.32520/stmsi.v13i1.

[16] M. Lubis, M. I. Luthfi, Rd. R. Saedudin, A. N. Muttaqin, and A. R. Lubis, "*The Integration of ISO 27005 and NIST SP 800-30 for Security Operation Center (SOC) Framework Effectiveness in the Non-Bank Financial Industry*," *Computers*, Vol. 15, No. 1, p. 60, Jan. 2026, DOI: 10.3390/computers15010060.

[17] A. A. Nugraha and A. H. Nasyuha, "*Integrating ISO 27001 and Indonesia's Personal Data Protection Law for Data Protection Requirement Model*," *Journal of Information Systems and Informatics*, Vol. 6, No. 2, pp. 1052–1069, Jun. 2024, DOI: 10.51519/journalisi.v6i2.754.