NUANSA INFORMATIKA
Volume 18 Nomor 2, Juli 2024
p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

Penerapan ISO/IEC 27001:2022 dalam Tata Kelola Keamanan Sistem Informasi: Evaluasi Proses dan Kendala

Frangky*[1], Rudolf Sinaga[2]
[1,2]Universitas Dinamika Bangsa, Jambi, Indonesia
E-mail: *[1]frangky.taan@gmail.com, [2]rudolfverdinan@gmail.com

Penerapan ISO/IEC 27001:2022 dalam tata kelola sistem keamanan informasi sangatlah mendesak dan relevan mengingat perkembangan ancaman siber, kebutuhan akan kepatuhan regulasi, serta pentingnya keamanan informasi sebagai keunggulan kompetitif. Revisi terbaru dari standar ini juga menuntut adanya adaptasi dan implementasi yang tepat untuk memastikan efektivitas pengelolaan keamanan informasi di berbagai organisasi. Penelitian ini menganalisis komponen utama dari ISO/IEC 27001:2022 , termasuk konteks organisasi, kepemimpinan, perencanaan, dukungan, operasi, evaluasi kinerja, dan perbaikan. Dalam hal ini akan mengeksplorasi penerapan ISO/IEC 27001:2022 dalam tata kelola sistem keamanan, dengan fokus pada bagaimana standar informasi ini dapat meningkatkan manajemen risiko dan keamanan informasi pada sebuah organisasi. Studi kasus pada perusahaan ekspedisi yang mulai mengadopsi standar ini dilakukan untuk mengidentifikasi praktik terbaik, tantangan penerapan, serta dampaknya terhadap keamanan dan kepatuhan regulasi. Hasil penelitian menunjukkan bahwa penerapan ISO/IEC 27001:2022 secara efektif meningkatkan postur keamanan informasi organisasi dengan mengintegrasikan kebijakan, prosedur, dan kontrol keamanan ke dalam proses bisnis. Temuan ini memberikan rekomendasi sebagai panduan praktis bagi organisasi yang berupaya memperkuat tata kelola sistem keamanan informasi melalui penerapan standar internasional yang diakui secara global.

Kata Kunci: ISO/IEC 27001:2022, SMKI, Tata Kelola Keamanan, Keamanan Sistem Informasi

Abstract

Implementing ISO/IEC 27001:2022 in information security management is crucial and timely due to the increasing cyber threats, the necessity for regulatory compliance, and the significance of information security as a competitive edge. The latest revision of this standard demands proper adaptation and implementation to ensure effective information security management across various organizations. This study examines the key components of ISO/IEC 27001:2022, including organizational context, leadership, planning, support, operations, performance evaluation, and improvement. It delves into the application of ISO/IEC 27001:2022 in security system governance, emphasizing how this standard can enhance risk management and information security within an organization. A case study on a logistics company adopting this standard was conducted to identify best practices, implementation challenges, and its impact on security and regulatory compliance. The study's findings demonstrate that implementing ISO/IEC 27001:2022 effectively improves an organization's information security posture by integrating security policies, procedures, and controls into business processes. These findings offer recommendations as practical guidelines for organizations aiming to strengthen their information security management through the adoption of globally recognized international standards.

Keywords*: ISO/IEC 27001:2022, SMKI, Security Governance, Information Systems Security*

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

Diajukan: 28 Juni 2024 *Disetujui: 3 Juli 2024* *Dipublikasi: 20 Juli 2024*

1. PENDAHULUAN

Di era digital saat ini, keamanan informasi menjadi salah satu aspek krusial dalam keinginan dan kesuksesan organisasi. Ancaman terhadap keamanan informasi semakin kompleks dan beragam, mulai dari serangan siber hingga kebocoran data internal.[1,2] Untuk menghadapi tantangan ini, organisasi perlu mengadopsi kerangka kerja yang sistematis dan terstandarisasi untuk melindungi aset informasi mereka.[3] ISO/IEC 27001:2022, sebagai standar internasional untuk sistem manajemen keamanan informasi (ISMS), menawarkan panduan yang komprehensif untuk mengidentifikasi, mengelola, dan mengurangi risiko keamanan informasi.[4,5] ISO/IEC 27001:2022 merupakan revisi terbaru yang memperbarui dan menyempurnakan standar sebelumnya, mencakup perubahan signifikan yang relevan dengan dinamika ancaman siber saat ini. Standar ini dirancang untuk memastikan bahwa keamanan informasi bukan hanya tanggung jawab departemen TI, tetapi juga menjadi bagian integral dari tata kelola organisasi secara keseluruhan.[6] Dengan pendekatan berbasis risiko, ISO/IEC 27001:2022 membantu organisasi dalam mengidentifikasi risiko keamanan yang potensial dan menetapkan kontrol yang tepat untuk mengelola risiko tersebut.[7,8]

Namun, meskipun ISO 27001:2022 dirancang untuk memberikan kerangka kerja yang kuat dalam mengelola risiko keamanan informasi, implementasinya tidak selalu berjalan mulus.[9–11] Beberapa organisasi menghadapi tantangan signifikan dalam mengadopsi standar ini, seperti keterbatasan sumber daya, kurangnya dukungan dari manajemen puncak, serta resistensi terhadap perubahan dalam budaya organisasi.[12] Selain itu, ada juga pandangan skeptis yang berpendapat bahwa kepatuhan terhadap standar tidak selalu menjamin keamanan yang efektif, melainkan hanya menghasilkan dokumentasi yang berlebihan tanpa penerapan yang nyata. Penelitian ini dilakukan dan bertujuan untuk mengeksplorasi penerapan ISO/IEC 27001:2022 dalam tata kelola sistem informasi keamanan, dengan fokus pada implementasi praktis, tantangan, dan manfaat yang diperoleh.

Beberapa penelitian terkait telah dilakukan oleh beberapa peneliti sebelumnya, diantaranya adalah penelitian yang dilakukan oleh Fatiha Djebbar dan Kim Nordstrom, dengan topik *A Comparative Analysis of Industrial Cybersecurity Standards*, mereka menyampaikan bahwa standar ISO/IEC 27001:2022 memberikan kontrol keamanan untuk membangun, menerapkan, memelihara, dan terus meningkatkan Sistem Manajemen Keamanan Informasi (ISMS) dan juga memberikan daftar lengkap dari semua kontrol yang diperlukan untuk memastikan keamanan informasi yang efektif.[13]

Penelitian lain yang dilakukan oleh Azizi Algi, dkk yang menemukan masih terdapat banyak masalah dalam upaya mencapai tujuan keamanan informasi di Pushansiber, seperti akses jarak jauh oleh vendor, kurangnya kebijakan internal, keterbatasan anggaran, dan kurangnya edukasi keamanan informasi bagi personel. Dengan assesment menggunakan Standar ISO 27001 maka dapat ditemukan belum ada peraturan yang mengikat dan memberikan hukuman bagi pelanggan, meskipun telah dilakukan edukasi informasi keamanan.[14]

Selanjutnya penelitian yang dilakukan oleh Yevhenii O. Kurii dan Ivan R. Opirskyy menyampaikan bahwa perusahaan-perusahaan perlu mengadaptasi sistem manajemen keamanan informasi mereka sesuai dengan persyaratan baru dari standar ISO/IEC 27001:2022. Langkah-langkah yang disarankan termasuk memperbarui registrasi risiko, Pernyataan Kepatuhan, dan dokumentasi lainnya untuk memastikan kepatuhan dengan kontrol baru yang ditambahkan dalam standar tersebut.[15]

Penelitian lainnya yang dilakukan oleh Juan Vicente, dkk mengidentifikasi langkah-langkah dalam melakukan penilaian risiko, yaitu mengidentifikasi risiko, menganalisis risiko, mereka menyebutkan bahwa penanganan risiko harus dilakukan secara iteratif dengan mengimplementasikan kontrol atau mengambil tindakan lain untuk mengurangi kemungkinan

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

atau dampak risiko, pentingnya membangun proses manajemen risiko yang terdokumentasi dan mengintegrasikannya dengan sistem manajemen lainnya salah satunya dengan meggunakan standar ISO/IEC 27001:2022 karena standar ini memberikan penekanan bahwa pemilihan kontrol harus didasarkan pada hasil dan kesimpulan yang diperoleh dari proses analisis dan penilaian risiko.[16]

Dari beberapa penelitian tersebut dapat disimpulkan bahwa sebuah organisasi sangat perlu menerapkan kebijakan kepatuhan dan penegakan standar kemanan, adaptasi terhadap standar baru yang sangat efektif, integrasi manajemen risiko, keterbatasan sumber daya sangat mempengaruhi kualitas keamanan sistem informasi, serta sangat perlunya penerapan kontrol dan kebijakan internal. Namun beberapa penelitian yang dilakukan masih menggunakan standar ISO/IEC 27001:2013 sedangkan yang menggunakan ISO/IEC 27001:2022 belum memaparkan implementasi ISO/IEC 27001 dilihat dari aspek yang menjadi penekanan standar tersebut.

Penelitian ini dilakukan melalui studi kasus pada sebuah perusahaan ekspedisi yang memulai mengadopsi standar ini. Perusahaan tersebut adalah perusahaan ekspedisi XX didirikan di Kota Jambi, berdasarkan informasi yang diberikan perusahaan bahwa bisnis mereka hadir dengan fokus untuk memenuhi kebutuhan pengiriman barang yang efisien, aman, dan membangun reputasi perusahaan mereka dalam hal keandalan dan kecepatan layanan. Perusahaan berkembang seiring dengan meningkatnya permintaan akan layanan pengiriman sebagai akibat pertumbuhan perdagangan dan e-commerce.

Skala operasional dari perusahaan ekpedisi ini adalah skala nasional, dimana proses bisnis dibangun untuk menjangkau pengiriman ke seluruh wilayah Indonesia. Penanganan data yang efisien dan aman sangat penting bagi perusahaan ekspedisi untuk memastikan kelancaran operasional dan kepuasan pelanggan, oleh sebab itu perusahaan memberikan prioritas pada jenis data yang dikelola dan menjadi pusat perhatian perusahaan. Adapun jenis data yang dikelola merupakan data-data yang terkategori aset yang krusial diantaranya adalah:

1. Data Pelanggan terdiri dari informasi pribadi dan kontak pelanggan yang menggunakan layanan pengiriman,
2. Data Pengiriman terdiri dari rincian pengiriman termasuk nomor pelacakan, alamat pengiriman, status pengiriman, dan rincian paket.
3. Data Transaksi terdiri dari informasi terkait pembayaran dan biaya pengiriman.
4. Data Operasional terdiri dari Informasi tentang armada kendaraan, rute pengiriman, dan jadwal pengiriman.
5. Data Keamanan terdiri dari rekaman CCTV, data logistik, dan informasi lain yang digunakan untuk memastikan keamanan pengiriman.
6. Data Kinerja terdiri dari statistik mengenai waktu pengiriman, tingkat keberhasilan pengiriman, dan umpan balik pelanggan.

Penelitian ini berupaya mengidentifikasi praktik terbaik (*best practice*) dan memberikan panduan bagi organisasi lain yang ingin mengimplementasikan ISO/IEC 27001:2022 . Pendekatan ini diharapkan dapat membantu organisasi dalam memperkuat postur keamanan informasi mereka dan memastikan kepatuhan terhadap peraturan yang berlaku. Dengan semakin meningkatnya ancaman keamanan informasi dan kompleksitas regulasi yang harus dipatuhi, penelitian ini menjadi sangat relevan dan penting untuk memberikan wawasan yang mendalam mengenai peran ISO/IEC 27001:2022 dalam membangun tata kelola informasi keamanan yang efektif dan berkelanjutan.

2. METODE PENELITIAN

2.1. Tahapan Penelitian

Penelitian ini menggunakan pendekatan kualitatif dan kuantitatif untuk mengeksplorasi penerapan ISO 27001:2022 dalam tata kelola sistem keamanan informasi. Metodologi yang digunakan meliputi tahapan-tahapan berikut:

1. Desain Penelitian
   Penelitian ini dirancang sebagai studi kasus, dengan tujuan untuk memperoleh pemahaman mendalam tentang bagaimana sebuah organisasi menerapkan ISO 27001:2022 dan tantangan serta manfaat yang dihadapi dalam proses ini.
2. Pemilihan Sampel
   Sampel penelitian terdiri dari sebuah perusahaan ekspedisi yang mulai akan

p-ISSN :1858-3911* , *e-ISSN : 2614-5405
https://journal.fkom.uniku.ac.id/ilkom

mengadopsi ISO 27001:2022. Organisasi ini dipilih berdasarkan kriteria salah satunya bersedia berpartisipasi dalam wawancara dan survei penelitian.

3. Pengumpulan Data

   Data dikumpulkan melalui beberapa metode berikut seperti wawancara mendalam dilakukan dengan manajer keamanan informasi, auditor internal, dan staf kunci lainnya yang terlibat dalam penerapan ISO 27001:2022. Wawancara ini bertujuan untuk memahami pengalaman, tantangan, dan manfaat yang dirasakan dari penerapan standar ini.

   Selanjutnya dilakukan survei berupa penyebaran Kuesioner kepada personel informasi keamanan dan karyawan lainnya untuk mengumpulkan data kuantitatif tentang pemahaman mereka terhadap kebijakan keamanan, efektivitas pelatihan, dan kepatuhan terhadap standar.

4. Analisis Data

   Data yang dikumpulkan dianalisis menggunakan metode analisis tematik, data kualitatif dari wawancara dianalisis untuk mengidentifikasi tema-tema utama yang muncul terkait penerapan ISO 27001:2022, tantangan yang dihadapi, dan praktik terbaik. Sementara data kuantitatif dari survei dianalisis menggunakan deskriptif statistik untuk menggambarkan distribusi tanggapan dan mengidentifikasi pola umum dalam pemahaman dan kepatuhan terhadap standar.

5. Pelaporan dan Diskusi

   Hasil penelitian akan disajikan dalam bentuk laporan komprehensif yang mencakup analisis data, diskusi temuan, dan rekomendasi praktis untuk organisasi yang ingin mengimplementasikan ISO 27001:2022 dalam tata kelola keamanan informasi mereka. Laporan ini juga akan membahas pengungkapan temuan penelitian untuk praktik keamanan informasi secara umum dan kontribusinya terhadap literatur yang ada.

2.2. ISO/IEC 27001:2022

ISO/IEC 27001 adalah standar internasional yang memberikan persyaratan untuk Sistem Manajemen Keamanan Informasi (ISMS). Edisi terbaru dari standar ini adalah ISO/IEC 27001:2022, yang diterbitkan pada bulan Oktober 2022. Standar ini adalah hasil revisi terhadap ISO/IEC 27001:2013 dan dirancang untuk membantu organisasi melindungi informasi mereka melalui penerapan kontrol keamanan yang memadai dan proporsional. [7]

ISO/IEC 27001 pertama kali diterbitkan pada tahun 2005 oleh International Organization for Standardization (ISO) dan International Electrotechnical Commission (IEC). Standar ini telah mengalami beberapa kali revisi untuk menyesuaikan dengan perkembangan teknologi dan ancaman keamanan informasi yang semakin kompleks. Revisi pada tahun 2022 bertujuan untuk meningkatkan relevansi dan efektivitas standar dalam konteks ancaman dan praktik keamanan informasi yang terus berkembang.

Struktur dan Isi ISO/IEC 27001:2022

ISO/IEC 27001:2022 mengikuti struktur tingkat tinggi yang umum digunakan dalam standar ISO lainnya, seperti ISO 9001 dan ISO 14001. Struktur ini mencakup 10 klausa utama:

1. Lingkup: Menjelaskan cakupan dari SMKI yang diterapkan.
2. Referensi Normatif: Mengacu pada dokumen-dokumen standar lain yang menjadi acuan.
3. Istilah dan Definisi: Menjelaskan istilah-istilah yang digunakan dalam standar.
4. Konteks Organisasi: Mengidentifikasi isu-isu internal dan eksternal yang relevan dengan tujuan ISMS.
5. Kepemimpinan: Memperkuat komitmen manajemen puncak terhadap ISMS.
6. Perencanaan: Meliputi penilaian risiko keamanan dan rencana informasi penanganannya.
7. Dukungan: Menyediakan sumber daya, kompetensi, dan kesadaran yang diperlukan untuk ISMS.
8. Operasi: melibatkan proses operasional untuk mengelola risiko keamanan informasi.
9. Evaluasi Kinerja: Memantau, mengukur, dan menganalisis kinerja ISMS.
10. Perbaikan: mengambil tindakan untuk terus meningkatkan ISMS.

Manfaat Implementasi ISO/IEC 27001:2022

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

Implementasi ISO/IEC 27001:2022 memberikan berbagai manfaat bagi organisasi, antara lain:

1. Meningkatkan Keamanan Informasi: Melalui penerapan kontrol yang sistematis dan terstruktur.
2. Kepatuhan Regulasi: membantah bahwa organisasi mematuhi persyaratan hukum dan regulasi terkait keamanan informasi.
3. Mengurangi Risiko: Mengidentifikasi dan mengelola risiko keamanan dengan informasi yang lebih efektif.
4. Meningkatkan Kepercayaan Pelanggan: Menunjukkan komitmen terhadap informasi keamanan kepada pelanggan dan mitra bisnis.
5. Peningkatan Operasional: Membantu dalam mengelola dan mengoptimalkan proses bisnis yang terkait dengan keamanan informasi.

Studi Kasus dan Implementasi Nyata

Berbagai organisasi dari sektor publik dan swasta telah mengimplementasikan ISO/IEC 27001:2022. Studi kasus menunjukkan bahwa organisasi yang berhasil menerapkan standar ini tidak hanya meningkatkan keamanan informasi mereka tetapi juga memperoleh keuntungan kompetitif. Misalnya, sebuah perusahaan teknologi besar melaporkan penurunan kejadian keamanan setelah menerapkan standar ini dan meningkatkan kepercayaan pelanggan, yang berdampak positif pada pendapatan mereka.

Tantangan dalam Implementasi

Meskipun banyak manfaatnya, penerapan ISO/IEC 27001:2022 juga menghadapi sejumlah tantangan, termasuk:

1. Biaya dan Sumber Daya: Standar implementasi ini memerlukan investasi yang signifikan dalam waktu, biaya, dan sumber daya manusia.
2. Perubahan Budaya: Memerlukan perubahan budaya organisasi untuk meningkatkan kesadaran dan komitmen terhadap keamanan informasi.
3. Kompleksitas Teknis: Beberapa organisasi mungkin menghadapi kesulitan dalam memahami dan menerapkan kontrol teknis yang disyaratkan oleh standar tersebut.

3. HASIL PENELITIAN

Penerapan standar ISO/IEC 27001:2022 pada salah satu perusahaan ekspedisi dilakukan dengan mengikuti tahapan penelitian yang dirumuskan diawal. Untuk menyusun indikator sebagai dasar evaluasi dan kendala yang ada pada perusahaan tersebut maka penelitian ini dilakukan dengan mengukur tingkat kepatuhan terhadap ISO 27001:2022 dalam berbagai bidang tata kelola sistem informasi keamanan. Berikut merupakan daftar pernyataan yang digunakan dalam pengumpulan data melalui pengisian kuesioner.

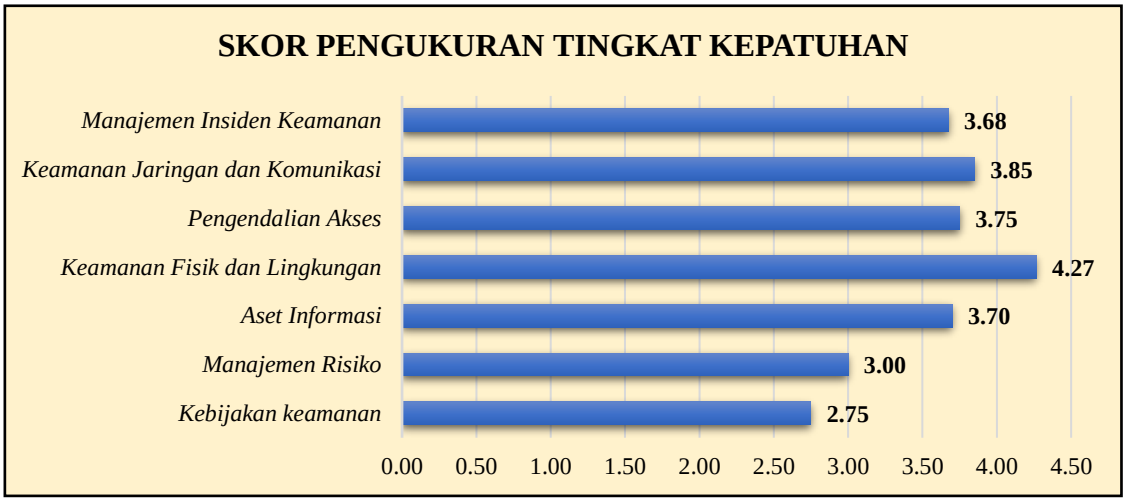
1. Perusahaan Ekspedisi XX telah mengadopsi kebijakan keamanan informasi sesuai dengan standar ISO 27001-2022.
2. Perusahaan Ekspedisi XX memiliki tim atau individu yang bertanggung jawab atas manajemen keamanan sistem informasi secara khusus.
3. Prosedur telah ditetapkan oleh Perusahaan Ekspedisi XX untuk mengidentifikasi dan mengevaluasi risiko keamanan sistem informasi.
4. Perusahaan Ekspedisi XX telah mengimplementasikan mekanisme untuk menerapkan pengendalian keamanan yang relevan dengan standar ISO 27001-2022.
5. Audit keamanan sistem informasi secara rutin dilakukan oleh Perusahaan Ekspedisi XX untuk memastikan kepatuhan terhadap ISO 27001-2022.
6. Kebijakan dan prosedur yang jelas telah ditetapkan oleh Perusahaan Ekspedisi XX untuk mengelola akses dan penggunaan data sensitif.
7. Perusahaan Ekspedisi XX memiliki kebijakan untuk melindungi informasi rahasia yang dimiliki oleh pihak ketiga.
8. Prosedur telah ditetapkan oleh Perusahaan Ekspedisi XX untuk melaporkan dan menangani insiden keamanan yang terjadi.
9. Langkah-langkah telah diambil oleh Perusahaan Ekspedisi XX untuk memastikan keamanan fisik terhadap akses yang tidak sah ke fasilitasnya.
10. Kebijakan telah ditetapkan oleh Perusahaan Ekspedisi XX untuk meningkatkan kesadaran keamanan informasi di kalangan pengguna dan memberikan pelatihan terkait.
11. Prosedur telah ditetapkan oleh Perusahaan Ekspedisi XX untuk mengelola patch dan

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

pembaruan keamanan sistem operasi dan perangkat lunak.

12. Kebijakan dan prosedur telah ditetapkan oleh Perusahaan Ekspedisi XX untuk memastikan keamanan saat mengoperasikan sistem informasi secara jarak jauh.
13. Prosedur telah ditetapkan oleh Perusahaan Ekspedisi XX untuk memantau dan mendeteksi ancaman keamanan seperti serangan malware atau intrusi.
14. Kebijakan dan prosedur yang jelas telah ditetapkan oleh Perusahaan Ekspedisi XX untuk mengelola penghentian akses dan penghapusan data.
15. Perusahaan Ekspedisi XX mengelola perubahan dalam kebijakan dan persyaratan kepatuhan, serta menyusun rencana tindak lanjut untuk meningkatkan tingkat kepatuhan.
16. Kebijakan dan prosedur keamanan informasi secara berkala ditinjau dan diperbarui oleh Perusahaan Ekspedisi XX sesuai dengan perkembangan teknologi dan ancaman keamanan terbaru.
17. Evaluasi rutin dilakukan oleh Perusahaan Ekspedisi XX untuk memastikan kepatuhan terhadap kebijakan keamanan informasi yang telah ditetapkan.

Selanjutnya pengukuran dilakukan dengan menghitung skor untuk masing-masing Area standar, untuk mengukur Skor kepatuhan dinilai pada skala 1 sampai dengan 5, dimana 1 menunjukkan tingkat kepatuhan yang sangat rendah dan 5 menunjukkan tingkat kepatuhan yang sangat tinggi. Berikut adalah hasil skor kepatuhan untuk setiap area, seperti pada gambar 1:



Gambar 1. Hasil Skor Pengukuran Tingkat Kepatuhan

4. PEMBAHASAN

Hasil evaluasi menunjukkan bahwa penerapan standar ini telah berhasil meningkatkan kesadaran dan kepatuhan terhadap praktik informasi keamanan di berbagai tingkat organisasi. Namun, penelitian ini juga mengidentifikasi sejumlah kendala yang menghadang selama proses implementasi. Kendala utama meliputi kurangnya pemahaman dan kompetensi teknis di kalangan staf, keterbatasan anggaran, serta resistensi terhadap perubahan budaya kerja yang diperlukan untuk mendukung standar penerapan.

Selain itu, penelitian ini menyoroti pentingnya dukungan manajemen puncak dan keterlibatan seluruh pemangku kepentingan dalam proses penerapan. Tanpa dukungan yang kuat dari manajemen dan kolaborasi antar departemen, penerapan ISO/IEC 27001:2022 sulit mencapai keberhasilan yang optimal. Oleh karena itu, rekomendasi yang diberikan meliputi peningkatan pelatihan dan kesadaran, penyediaan sumber daya yang memadai, serta pengembangan strategi komunikasi yang efektif untuk mengatasi resistensi terhadap perubahan.

Berikut adalah tabel pembahasan terhadap hasil pengukuran skor tingkat

kepatuhan yang dilakukan terhadap area cakupan standar:

Tabel 1. Hasil pengukuran pada area cakupan standar

No	Area	Skor	Pembahasan
1	Kebijakan Keamanan	2,75	Skor ini menunjukkan bahwa kebijakan keamanan belum sepenuhnya diadopsi dan diimplementasikan dengan baik. Organisasi masih dalam tahap awal kebijakan pengembangan atau belum berhasil mengkomunikasikannya secara efektif kepada semua pemangku kepentingan.
2	Manajemen Risiko	3,00	Skor manajemen risiko menunjukkan bahwa praktik manajemen risiko sudah mulai diterapkan, tetapi masih memerlukan perbaikan lebih lanjut. Organisasi perlu memperkuat proses, identifikasi, dan mitigasi risiko untuk mencapai pemenuhan yang lebih tinggi.
3	Informasi Aset	3,70	Dengan skor 3,70, pengelolaan aset informasi berada pada tingkat yang cukup baik. Hal ini menunjukkan bahwa sebagian besar telah memiliki inventaris aset informasi yang lengkap dan telah menerapkan langkah-langkah untuk melindunginya..
4	Keamanan Fisik dan Lingkungan	4,27	Keamanan fisik dan lingkungan mendapatkan skor tertinggi sebesar 4,27, yang menunjukkan bahwa sebagian besar telah berhasil mengimplementasikan kontrol fisik yang kuat untuk melindungi informasi dan sistem mereka dari ancaman fisik dan lingkungan.
5	Pengendalian Akses	3,75	Skor 3,75 untuk pengendalian akses menunjukkan bahwa organisasi telah menerapkan kontrol akses yang cukup baik. Namun, masih ada ruang untuk perbaikan dalam memastikan bahwa hanya personel yang berwenang yang memiliki akses ke informasi dan sistem kritis.
6	Keamanan Jaringan dan Komunikasi	3,85	Skor 3,85 pada keamanan jaringan dan komunikasi menunjukkan bahwa organisasi telah mengimplementasikan langkah-langkah yang efektif untuk melindungi jaringan dan komunikasi mereka.
7	Manajemen Insiden Keamanan	3,68	Dengan skor 3,68, manajemen insiden keamanan menunjukkan bahwa organisasi telah memiliki prosedur untuk menangani insiden keamanan. Namun, peningkatan lebih lanjut diperlukan dalam hal respons yang cepat dan efektif terhadap kejadian untuk meminimalkan resiko.

Secara keseluruhan, skor kepatuhan terhadap ISO 27001:2022 di berbagai area menunjukkan bahwa meskipun ada implementasi yang baik dalam beberapa aspek, seperti keamanan fisik dan lingkungan serta keamanan jaringan dan komunikasi, masih ada area yang memerlukan perbaikan signifikan. Kebijakan keamanan dan manajemen risiko, khususnya, memerlukan perhatian lebih untuk memastikan bahwa organisasi dapat mencapai tingkat kepatuhan yang optimal dan melindungi informasi mereka secara menyeluruh

Rekomendasi

Berdasarkan temuan tersebut, beberapa rekomendasi yang diberikan untuk meningkatkan kualitas tata kelola keamanan sistem informasi dengan meningkatkan kepatuhan terhadap standar ISO/IEC 27001:2022 meliputi:

1. Penguatan Kebijakan Keamanan
   Organisasi perlu mengembangkan, mengomunikasikan, dan menerapkan kebijakan keamanan yang jelas dan komprehensif.
2. Peningkatan Manajemen Risiko
   Organisasi harus mengadopsi pendekatan manajemen risiko yang lebih sistematis dan terstruktur, termasuk pelatihan bagi personel untuk memahami dan menerapkan proses manajemen risiko dengan baik.
3. Peninjauan dan Penyempurnaan Kontrol Akses
   Melakukan audit rutin dan peninjauan kontrol terhadap akses untuk memastikan

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

kesesuaiannya dengan kebutuhan keamanan saat ini.

4. Peningkatan Pelatihan dan Kesadaran Keamanan
   Mengadakan program pelatihan yang berkelanjutan untuk meningkatkan kesadaran dan pemahaman personel mengenai praktik informasi keamanan yang baik.

Dengan menerapkan rekomendasi-rekomendasi ini, diharapkan organisasi dapat meningkatkan tingkat kepatuhan mereka terhadap ISO 27001:2022 dan memperkuat tata kelola keamanan sistem informasi secara keseluruhan.

5. KESIMPULAN

Berdasarkan hasil evaluasi, dapat disimpulkan bahwa organisasi telah mencapai kemajuan yang signifikan dalam penerapan informasi keamanan, terutama dalam aspek-aspek seperti keamanan fisik, pengendalian akses, dan manajemen insiden keamanan. Skor tinggi yang diperoleh dalam keamanan fisik dan lingkungan, serta keamanan jaringan dan komunikasi, menunjukkan bahwa kontrol yang kuat telah diterapkan untuk melindungi infrastruktur fisik dan jaringan komunikasi organisasi. Meskipun demikian, terdapat beberapa bidang yang memerlukan perhatian lebih lanjut. Kebijakan keamanan dan manajemen risiko, meskipun sudah diimplementasikan, mendapat skor yang lebih rendah dibandingkan dengan bidang lainnya. Hal ini menunjukkan perlunya perbaikan dalam kebijakan pengembangan yang lebih ketat dan komprehensif, serta penguatan strategi manajemen risiko untuk mengidentifikasi dan mengatasi potensi ancaman keamanan dengan lebih efektif.

6. SARAN

Secara keseluruhan penerapan kebijakan keamanan sistem informasi telah memberikan hasil yang baik namun organisasi masih memerlukan upaya perbaikan terutama pada aspek kebijakan keamanan dan manajemen risiko untuk menjaga keamanan informasi secara optimal.

UCAPAN TERIMAKASIH

Terimakasih kepada seluruh pihak yang terlibat dan mendukung kegiatan penelitian ini, seluruh pimpinan dan staf perusahaan ekspedisi XX yang dengan terbuka mulai dari kegiatan wawancara, pengisian kuesioner serta memberikan data yang diperlukan.

REFERENSI

[1] Yuwono ST, Pratama N, Afifah V, Minggu P, Selatan J. Re-Assessment Konsistensi Dokumen Kontrol Sertifikasi ISO 27001:2013 (ISMS) di Bagian Komunikasi Satelit Monitoring PT. Bank BRI, TBK. 2020.

[2] Risna R, Amaliah Y, Yunita S. Implementasi Kriptografi Pada Pengamanan Data Pembayaran Piutang Pelanggan Menggunakan Vigener Cipher. Sebatik 2022;26:525–34. https://doi.org/10.46984/sebatik.v26i2.2061.

[3] Nasiri A. Evaluasi Tingkat Kapabilitas Keamanan Sistem Informasi Menggunakan Kerangka Kerja Cobit 2019 2023;9:34–41.

[4] Glavan AF, Gheorghica D, Croitoru V. MULTI-ACCESS EDGE COMPUTING ANALYSIS OF RISKS AND SECURITY MEASURES. vol. 68. 2023.

[5] Syani M, Mahestro Tresna R, Firdaus EA, Faisal Nugraha F, Bandung PT. PENERAPAN NETWORK ACCESS CONTROL AUTENTIKASI INTERNAL NETWORK SECURITY PROTOKOL 802.1 X. Nuansa Informatika 2022;16.

[6] Budhiningtias Winanti M, Dzulhan I. AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK DENGAN KERANGKA KERJA ISO 27001 DI PROGRAM STUDI SISTEM INFORMASI UNIKOM. 2020.

[7] WATKINS SG. ISO/IEC 27001:2022. IT Governance Publishing; 2022. https://doi.org/10.2307/j.ctv30qq13d.

p-ISSN :1858-3911 **,** ***e-ISSN : 2614-5405***
https://journal.fkom.uniku.ac.id/ilkom

[8] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection-Information security management systems-Requirements. 2022.

[9] Syarif RA, Nugroho A. ANALISIS TINGKAT KEMATANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI DIREKTORAT JENDERAL PERBENDAHARAAN DIUKUR DENGAN MENGGUNAKAN INDEKS KEAMANAN INFORMASI (STUDI KASUS: APLIKASI SPAN) 1) 2). 2020.

[10] Hidaya N, Jatnika I. PERANCANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI DATA CENTER STANDART SNI ISOIEC 27001 2013. Jurnal Sistem Informasi Musirawas 2022.

[11] Kurniasih S, Masitoh S. AUDIT SISTEM INFORMASI HUMAN RESOURCE INFORMATION SYSTEM (HRIS) PADA BAGIAN HUMAN RESOURCE (HR) MENGGUNAKAN FRAMEWORK COBIT 5 DOMAIN DSS01. Nuansa Informatika 2021;15.

[12] Parama Yoga T, Maharani V, Maulana ND. Audit Keamanan Sistem Informasi Puskesmas Dengan Standar ISO/IEC 27001:2013 Dan Framework COBIT 5. Nuansa Informatika 2024;18:2614–5405.

[13] Djebbar F, Nordstrom K. A Comparative Analysis of Industrial Cybersecurity Standards. IEEE Access 2023;11:85315–32. https://doi.org/10.1109/ACCESS.2023.3303205.

[14] Algi A, S Reksoprodjo AH, Agus Gultom RG. ANALISIS STANDAR ISO/IEC 27001: 2013 SEBAGAI STRATEGI KEAMANAN INFORMASI DI PUSAT PERTAHANAN SIBER KEMENTERIAN PERTAHANAN REPUBLIK INDONESIA. 2020.

[15] Kurii Y, Opirskyy I. ISO 27001: ANALYSIS OF CHANGES AND COMPLIANCE FEATURES OF THE NEW VERSION OF THE STANDARD. Cybersecurity: Education, Science, Technique 2023;3:46–55. https://doi.org/10.28925/2663-4023.2023.19.4655.

[16] Barraza de la Paz JV, Rodríguez-Picón LA, Morales-Rocha V, Torres-Argüelles SV. A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0. Systems 2023;11. https://doi.org/10.3390/systems11050218.