Analisis Penerapan SMKI Berdasarkan Standar Iso 27001:2013 Pada Lembaga XYZ

1st Daffa Ilham Fikri
S1 Sistem Informasi
Telkom University
Bandung, Indonesia
dffailhmfkri@student.telkomuniversity.ac.id

2nd Umar Yunan Kurnia Septo Herdiyanto, S.T., M.T
S1 Sistem Informasi
Telkom University
Bandung, Indonesia
umaryunan@telkomuniversity.ac.id

3rd Rd. Rohmat Saedudin, S.T., M.T., Ph.D
S1 Sistem Informasi
Telkom University
Bandung, Indonesia
rdrohmat@telkomuniversity.ac.id

Lembaga XYZ merupakan entitas pemerintahan yang memiliki perananan dalam mengelola data informasi pribadi pengguna yang berperan penting dalam mendukung proses administrasi serta memberikan layanan public, Oleh karena itu, untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi, instansi ini telah mengadopsi Sistem Manajemen Keamanan Informasi (SMKI) sesuai dengan pedoman ISO 27001:2013. Penelitian ini bertujuan untuk menilai sejauh mana penerapan standar tersebut dilaksanakan, dengan fokus pada penerapan klausa dan kontrol keamanan yang diatur pada ISO 27001:2013. Metodologi yang digunakan adalah Design Science Research (DSR), dengan cara pengumpulan data dengan cara wawancara serta analisis terhadap dokumen kebijakan internal dan eksternal yang relevan. Evaluasi dilakukan pada klausa inti ISO 27001:2013 dan Annex A, yang meliputi kebijakan keamanan, pengelolaan aset, kontrol akses, keamanan fisik, serta penanganan insiden keamanan. Hasil analisis menunjukkan bahwa sebagian besar persyaratan telah diterapkan dengan tingkat kepatuhan yang baik. Namun, beredasarkan evaluasi ditemukan beberapa kontrol yang belum diimplementasikan, seperti kontrol perlindungan aplikasi pada jaringan publik, keamanan layanan berbasis cloud, dan pengendalian kriptografi. Oleh karena itu, hasil penelitian ini dapat menjadi dasar dalam pengambilan keputusan untuk memperkuat efektivitas kontrol keamanan informasi dan meningkatkan kualitas SMKI agar lebih adaptif dan profesional.

Kata kunci— ISO 27001, ISO 27001:2013, Klausa ISO 27001:2013, Kontrol ISO 27001:2013, SMKI.

I. PENDAHULUAN

Seiring bertambahnya volume data yang disediakan oleh pemerintah untuk mendukung pelayanan publik, masalah keamanan data menjadi semakin kompleks. Keamanan data atau informasi terdiri dari tiga komponen utama yaitu kerahasiaan data, integritas data, dan ketersediaan data. Oleh karena itu, seluruh pihak yang terlibat, terutama pihak yang bertanggung jawab strategis, harus memahami pentingnya perlindungan informasi serta potensi bahaya yang dapat mengganggu operasi sistem informasi dan komunikasi yang digunakan [1].

Untuk mendukung pengelolaan, perlindungan, dan penerapan prinsip keamanan pada sistem informasi di lingkungan instansi pemerintah, ISO 27001:2013 dapat berguna sebagai referensi utama. Standar ini merupakan kerangka kerja SMKI yang telah digunakan secara global dan dirancang guna memenuhi kebutuhan perlindungan terhadap informasi, baik yang berasal dari lembaga pemerintahan maupun informasi penting lainnya [2].

ISO 27001:2013 adalah standar yang telah digunakan dan diakui secara global yang berguna membantu organisasi dalam proses identifikasi serta pengelolaan risiko terkait keamanan informasi. Standar ini memberikan panduan dan prosedur yang sistematis dan ketat untuk menjaga keamanan data. ISO 27001 berfungsi untuk membantu organisasi dalam menentukan kebutuhan SMKI secara tepat. Sebagai kerangka kerja, ISO 27001 memudahkan organisasi dalam merancang dan menerapkan Sistem Manajemen Keamanan Informasi (ISMS) secara efisien. Penerapannya dapat meningkatkan kepercayaan para pemangku kepentingan serta meningkatkan performa organisasi melalui strategi analisis risiko yang sistematis, sembari memastikan sistem informasi tetap aman dari berbagai potensi ancaman. Dengan demikian, ISO 27001 sangat berperan penting dalam organisasi untuk memenuhi persyaratan standar dan kebutuhan yang berhubungan dengan keamanan informasi [3].

II. KAJIAN TEORI

Bab ini membahas teori yang digunakan pada penelitian dan mencakup ruang lingkup utama yang relevan dengan ruang lingkup studi.

A. Keamanan Informasi

Keamanan informasi merupakan suatu pendekatan terstruktur yang bertujuan melindungi data dan sistem informasi dari berbagai ancaman seperti akses yang tidak sah, penyalahgunaan, modifikasi tanpa izin, dan gangguan dari pihak luar [4]. Tujuan utama dari perlindungan ini adalah untuk memastikan tiga pilar utama keamanan informasi: kerahasiaan, integritas, dan ketersediaan. Pendekatan ini juga dikenal sebagai Triad CIA untuk melindungi data dan sistem informasi dari ancaman [5].

B. Sistem Manajemen Keamanan Informasi (SMKI)

SMKI beguna untuk memastikan bahwa informasi terlindungi dari risiko yang dapat mengganggu kerahasiaan, integritas, dan ketersediaannya. SMKI melibatkan tahapan *plan*, *do*, *check*, dan *act* untuk mencapai tujuan organisasi dalam aspek keamanan informasi. Implementasi SMKI menghasilkan dokumen penting seperti prosedur keamanan, manual, instruksi kerja, dan kebijakan pengendalian. Dengan mengadopsi pendekatan ini, organisasi dapat meningkatkan perlindungan data dan meminimalkan ancaman yang mungkin timbul [6].

C. ISO 27001:2013

ISO 27001:2013 merupakan pedoman yang berguna membantu organisasi dalam mengelola keamanan informasi serta risiko yang terkait. Standar ini memberikan panduan dalam membentuk SMKI yang efektif dan sesuai dengan kebijakan yang telah ditetapkan [7]. ISO 27001 mendukung pengembangan SMKI secara terstruktur untuk melindungi aset informasi dan menjaga kelangsungan proses bisnis dengan meminimalkan potensi kerugian dan gangguan akibat insiden keamanan [6].

D. Klausa ISO 27001

Klausa pada ISO 27001 mengacu pada bagian yang menetapkan persyaratan penting bagi organisasi dalam membangun dan mengelola SMKI secara berkelanjutan. ISO/IEC 27001:2013 terdiri dari beberapa klausa utama, antara lain konteks organisasi, kepemimpinan, perencanaan, dukungan, operasional, evaluasi kinerja, serta peningkatan. Seluruh klausa dirancang agar organisasi dapat memenuhi kebutuhan keamanan informasi secara menyeluruh. ISO 27001 juga memiliki *Annex* A yang memuat pengendalian keamanan tambahan untuk memperkuat perlindungan terhadap risiko. Secara keseluruhan, klausa-klausa tersebut menjadi panduan komprehensif bagi organisasi dalam mengelola keamanan informasi secara berkesinambungan [8].

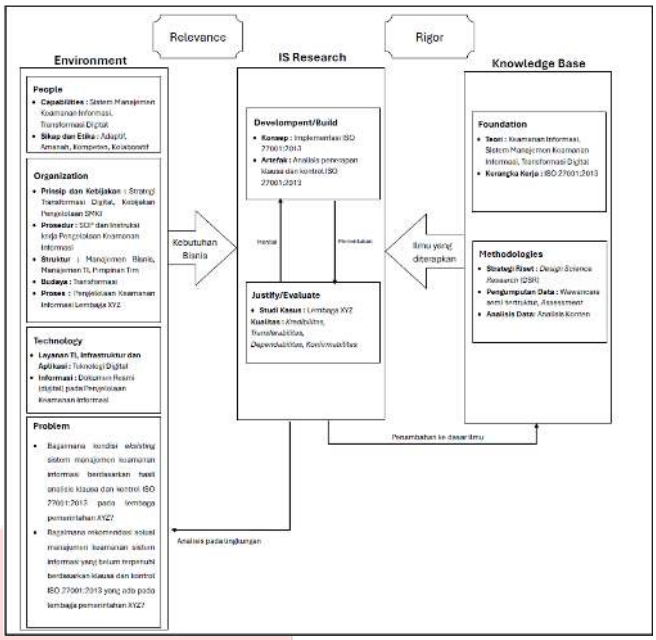
E. *Annex* A ISO 27001

Annex A dalam ISO 27001 menyediakan pedoman khusus untuk pengendalian keamanan informasi. *Annex* A terdiri dari 14 kategori kontrol yang dimaksudkan untuk membantu organisasi dalam merancang, menetapkan, serta memelihara SMKI. Kategori-kategori ini mencakup berbagai hal penting, seperti kebijakan keamanan informasi, manajemen aset, kontrol akses, dan penanganan insiden keamanan. Melalui pemanfaatan *Annex* A, organisasi dapat menyesuaikan kontrol keamanan yang tepat berdasarkan kebutuhan serta tingkat risiko yang dihadapi, sehingga pengelolaan risiko keamanan informasi menjadi lebih efektif dan terarah [9].

III. METODE

A. Kerangka Berpikir

Penelitian ini menggunakan pendekatan DSR, yang berguna untuk acuan merancang, melaksanakan, dan mengevaluasi penelitian di bidang sistem informasi. Pendekatan ini memberikan kerangka kerja sistematis yang menjelaskan proses penelitian dengan menerapkan prinsip-prinsip ilmu desain, dan memberikan pedoman konseptual yang jelas dan ringkas untuk bagaimana metode ini dapat diterapkan [10].



GAMBAR 1
Metode DSR

Model konseptual DSR Hevner mencakup tiga komponen utama, yaitu konteks *environment*, penelitian dalam bidang *IS research*, serta sumber pengetahuan *knowledge base*. Ketiga elemen ini membentuk dasar pemahaman terhadap pendekatan yang digunakan. Berikut adalah uraian dari model konseptual yang diterapkan:

1. *Environment*

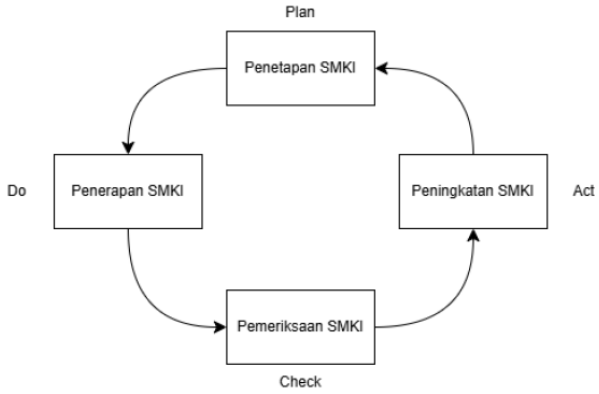
   Komponen *environment* terdiri dari empat elemen utama, yaitu *people*, *organization*, *technology*, dan *problem*. Setiap elemen dianalisis dan dipetakan sesuai dengan ruang lingkup penelitian yang dilakukan. Tujuannya adalah untuk merancang sistem manajemen keamanan informasi yang dapat mendukung pencapaian sertifikasi ISO 27001 serta meningkatkan peran transformasi digital dalam mewujudkan tujuan strategis organisasi.
2. *IS Research*

   Pada bagian ini terdiri atas dua elemen utama, yaitu pengembangan dan evaluasi. Pengembangan menjelaskan konsep implementasi ISO 27001 serta pemilihan klausa prioritas dan rancangan rekomendasi yang diutamakan. Sementara itu, evaluasi mencakup studi kasus pada Lembaga XYZ yang menilai aspek kredibilitas, transferabilitas, dependabilitas, dan konfirmabilitas.
3. *Knowledge Base*

   Terdapat dua komponen dalam bagian ini, yakni *Foundation* dan *Methodologies*. *Foundation* mencakup teori-teori terkait keamanan informasi, *IT Governance*, SMKI, dan transformasi digital. Adapun pada bagian *Methodologies*, digunakan pendekatan riset melalui metode *design science research* dan studi kasus. Cara atau teknik pengumpulan data dilaksanankan dengan cara wawancara semi-terstruktur serta penilaian (*assessment*), yang selanjutnya dilakukan analisis menggunakan pendekatan analisis konten.

B. Penyelesaian Masalah

Penelitian ini mengadopsi pendekatan penyelesaian masalah melalui penerapan siklus PDCA. Siklus ini mencakup empat langkah utama, yaitu perencanaan (*Plan*), pelaksanaan (*Do*), evaluasi atau pemeriksaan (*Check*), serta tindakan perbaikan atau peningkatan (*Act*).



GAMBAR 2
PDCA

1. *Plan*
   Tahap ini mencakup proses perencanaan dalam penerapan SMKI yang mengikuti panduan pada kerangka kerja ISO 27001:2013. Kegiatan ini dilakukan dengan meliputi analisis terhadap kebutuhan klausa dan kontrol yang akan digunakan sebagai dasar dalam penerapan sistem tersebut.
2. *Do*
   Pada tahap pelaksanaan, dilakukan evaluasi terhadap SMKI berdasarkan standar ISO 27001:2013. Evaluasi ini mencakup identifikasi terhadap klausa dan kontrol yang relevan guna memastikan bahwa kebutuhan dalam implementasi sistem di Lembaga XYZ telah terpenuhi. Selain itu, dilakukan pula analisis penerapan berdasarkan hasil kajian sebelumnya.
3. *Check*
   Tahap ini bertujuan untuk meninjau hasil implementasi guna memastikan bahwa seluruh komponen dalam SMKI telah memenuhi ketentuan yang ditetapkan dalam ISO 27001:2013.
4. *Act*
   Pada tahap ini dilakukan perbaikan berdasarkan hasil evaluasi sebelumnya, serta diberikan rekomendasi guna memenuhi ketidaksesuaian yang ditemukan terhadap klausa dan kontrol yang ditentukan dalam standar ISO 27001:2013.

C. Pengumpulan Data

TABEL 1
Pengumpulan Data

Metode Pengumpulan	Jenis Data	Kegiatan	Alat
Semi sstructured interview	Primer	Melaksanakan wawancara dengan serangkain topik pertanyaan yang telah tersusun untuk memenuhi penelitian dari pihak yang bersangkutan.	*Offline dan Online meeting*
Internal dan *External Document*	Sekunder	Mengumpulkan dan mengkaji data.	Dokumen *internal* dan dokumen *eksternal*.

IV. HASIL DAN PEMBAHASAN

A. Hasil Penerapan Klausa

Berikut merupakan hasil evaluasi penerapan SMKI berdasarkan analisis kondisi eksisting terhadap implementasi klausa ISO 27001:2013 di Lembaga XYZ.

TABEL 2
Hasil Penerapan Klausa

Judul Klausa	Status
Klausa 4 Konteks Organisasi	Sudah Diterapkan
Klausa 5 Kepemimpinan	Sudah Diterapkan
Klausa 6 Perencanaan	Sudah Diterapkan
Klausa 7 Dukungan	Sudah Diterapkan
Klausa 8 Operasional	Sudah Diterapkan
Klausa 9 Evaluasi Kinerja	Sudah Diterapkan
Klausa 10 Peningkatan	Sudah Diterapkan

Hasil analisis atas kondisi aktual di Lembaga XYZ menunjukkan bahwa instansi tersebut telah mampu secara efektif membangun, mengimplementasikan, mempertahankan, dan secara berkelanjutan meningkatkan SMKI yang selaras dengan standar ISO 27001:2013.

B. Hasil Penerapan *Annex* A

Berikut disajikan hasil evaluasi imlementasi atau penerapan SMKI berdasarkan analisis terhadap kondisi eksisting kontrol ISO 27001:2013 di Lembaga XYZ.

TABEL 3
Hasil Penerapan *Annex* A

Annex A	Status	Catatan
A.5 Kebijakan Keamanan Informasi	Semua kontrol sudah diterapkan.	Semua kontrol pada A.5 sudah diterapkan dan diatur

A.6 Organisasi Kemanan Informasi	Semua kontrol sudah diterapkan.	Semua kontrol pada A.6 sudah diterapkan dan diatur
A.7 Keamanan Sumber Daya Manusia	Semua kontrol sudah diterapkan.	Semua kontrol pada A.7 sudah diterapkan dan diatur
A.8 Manajemen Aset	Semua kontrol sudah diterapkan.	Semua kontrol pada A.8 sudah diterapkan dan diatur
A.9 Kontrol Akses	Semua kontrol sudah diterapkan.	Semua kontrol pada A.9 sudah diterapkan dan diatur
A.10 Kriptografi	Semua kontrol sudah diterapkan.	Semua kontrol pada A.10 sudah diterapkan dan diatur
A.11 Keamanan Fisik dan Lingkungan Pengolahan Informasi	Semua kontrol sudah diterapkan.	Semua kontrol pada A.11 sudah diterapkan dan diatur
A.12 Keamanan Operasional	Semua kontrol sudah diterapkan.	Semua kontrol pada A.12 sudah diterapkan dan diatur
A.13 Keamanan Komunikasi	Semua kontrol sudah diterapkan.	Semua kontrol pada A.13 sudah diterapkan dan diatur
A.14 Sistem Akuisi, Pengembangan, dan Pemeliharaan Sistem	Semua kontrol sudah diterapkan.	Belum diterapkanya kontrol A.14.1.2 dan A.14.2.6
A.15 Hubungan dengan pemasok	Semua kontrol sudah diterapkan.	Semua kontrol pada A.15 sudah diterapkan dan diatur
A.16 Manajemen Insiden Kemanan Informasi	Semua kontrol sudah diterapkan.	Semua kontrol pada A.16 sudah diterapkan dan diatur
A.17 Aspek Kemanan Informasi dalam Manjemen Keberlanjutan Bisnis	Semua kontrol sudah diterapkan.	Belum diterapkanya kontrol A.17.1.1, A.17.1.2, dan A.17.1.3
A.18 Kepatuhan	Semua kontrol sudah diterapkan.	Belum diterapkanya kontrol A.18.1.5

Dari hasil evaluasi implementasi SMKI serta analisis terhadap kondisi aktual dalam implementasu atau penerapan kontrol ISO 27001:2013 di Lembaga XYZ, dapat disimpulkan bahwa instansi tersebut telah memperlihatkan komitmen yang tinggi dalam menerapkan pengendalian keamanan informasi sesuai dengan standar yang berlaku. Meskipun demikian, masih terdapat beberapa kontrol yang belum sepenuhnya terpenuhi sebagaimana yang disyaratkan dalam ISO 27001:2013.

C. Rekomendasi

Merujuk pada hasil kajian terhadap implementasi klausa dan kontrol di Lembaga XYZ, berikut disampaikan beberapa rekomendasi sebagai tindak lanjut atas temuan terkait penerapan yang belum berjalan secara optimal.

TABEL 4
Rekomendasi

Kontrol ISO 27001:2013	Rekomendasi yang diberikan
A.6.1.5	Kontrol A.6.1.5 mewajibkan organisasi untuk mempertimbangkan aspek perlindungan informasi dalam seluruh proyek yang dilaksanakan, terlepas dari tipe atau kategori proyek tersebut. Untuk meningkatkan efektivitas penerapan kontrol ini, disarankan agar organisasi menambahkan kebijakan atau standar pendukung ke dalam dokumen pedoman terkait khususnya pada BAB VIII yang membahas Pengendalian Keamanan Komunikasi dan Operasional.
A.14.1.2	Kontrol A.14.1.2 mewajibkan organisasi untuk memastikan bahwa bahwa data atau informasi yang disalurkan melalui aplikasi layanan pada jaringan publik terlindungi dari risiko penipuan, pelanggaran perjanjian, akses tidak sah, serta modifikasi data yang tidak diotorisasi. Untuk mengoptimalkan penerapan kontrol ini, disarankan agar organisasi menambahkan kebijakan atau standar pendukung ke dalam dokumen pedoman terkait khususnya pada BAB VIII yang membahas tentang Pengendalian Keamanan Komunikasi dan Operasional.
A.14.2.6	Kontrol A.14.2.6 mengatur bahwa organisasi wajib menciptakan serta menjaga keamanan lingkungan tempat pengembangan sistem. Untuk meningkatkan efektivitas penerapannya, disarankan penambahan kebijakan atau standar yang relevan ke dalam dokumen pedoman terkait khususnya pada BAB IX tentang Pengendalian Keamanan Informasi dalam Pengembangan dan Pemeliharaan Sistem Informasi.
A.17.1.1	Kontrol A.17.1.1 menuntut organisasi untuk menetapkan persyaratan yang menjamin keberlangsungan dan

	perlindungan keamanan informasi dalam situasi darurat, seperti bencana atau krisis. Untuk mendukung efektivitas kontrol ini, direkomendasikan penambahan kebijakan atau standar pendukung ke dalam dokumen Pedoman terkait khususnya pada BAB II tentang Pengendalian Umum.
A.17.1.2	Kontrol A.17.1.2 mewajibkan organisasi untuk merancang, mendokumentasikan, menerapkan, serta memelihara prosedur dan pengendalian yang diperlukan guna menjamin keberlanjutan keamanan informasi ketika menghadapi situasi tak terduga. Untuk meningkatkan efektivitas pelaksanaan kontrol ini, disarankan agar organisasi menambahkan kebijakan atau standar pendukung ke dalam dokumen Pedoman terkait khususnya pada BAB II mengenai Pengendalian Umum.
A.17.1.3	Kontrol A.17.1.3 mengharuskan organisasi untuk secara berkala melakukan verifikasi terhadap pengendalian keberlanjutan keamanan informasi yang sudah ada. Tujuannya adalah untuk menjamin bahwa kontrol tersebut tetap relevan dan berfungsi dengan baik dalam mengatasi kondisi yang merugikan. Untuk meningkatkan efektivitas pelaksanaannya, disarankan agar organisasi menambahkan kebijakan atau standar pendukung ke dalam dokumen Pedoman terkait khususnya pada BAB II tentang Pengendalian Umum.
A.18.1.5	Kontrol A.18.1. mengatur bahwa organisasi memiliki kewajiban untuk memastikan penggunaan teknologi kriptografi selaras dengan ketentuan hukum, perjanjian, dan regulasi yang berlaku. Guna mengoptimalkan penerapan kontrol ini, disarankan agar organisasi menyusun kebijakan atau standar tambahan yang dimuat dalam dokumen Pedoman terkait khususnya khususnya pada BAB XIII mengenai Pengendalian Kepatuhan.

Berdasarkan hasil penelitian dan analisis terhadap implementasi SMKI di Lembaga XYZ yang mengacu pada pedoman ISO 27001:2013, diperoleh kesimpulan bahwa Lembaga XYZ telah berhasil menetapkan, menerapkan, serta memelihara sistem keamanan informasi secara berkelanjutan, dan terus meningkatkan penerapannya sesuai dengan ketentuan standar tersebut. Komitmen dari pihak organisasi dalam menerapkan pengendalian keamanan informasi menjadi elemen penting dalam mendukung tercapainya kondisi saat ini. Namun demikian, masih ditemukan sejumlah kontrol yang belum sepenuhnya diimplementasikan, terutama yang berkaitan dengan keamanan layanan aplikasi berbasis jaringan publik, perlindungan lingkungan pengembangan, pengelolaan keberlangsungan informasi, serta penggunaan kriptografi yang sesuai dengan regulasi. Temuan ini menunjukkan bahwa masih terdapat kebutuhan penyesuaian kebijakan dan prosedur agar pengelolaan SMKI dapat berjalan secara optimal dan sejalan dengan standar ISO 27001:2013. Oleh karena itu, disarankan agar organisasi menambahkan kebijakan maupun standar pendukung yang sesuai untuk mengatasi kekurangan tersebut, khususnya pada aspek-aspek yang telah diidentifikasi, serta memastikan dokumentasi pelaksanaan tercantum dalam *Pedoman Standar Keamanan Informasi Lembaga XYZ*.

REFERENSI

[1] H. A. Pratiwi and L. Wulandari, “Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor,” *J. Ind. Eng. Manag. Res.*, vol. 2, no. 5, pp. 146–163, 2021.

[2] 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 Mhs. Tek. Inform.*, vol. 8, no. 1, pp. 454–460, 2024, doi: 10.36040/jati.v8i1.8736.

[3] M. R. Aditama, F. Dewi, and D. Praditya, “SEIKO : Journal of Management & Business Perancangan Proses Keamanan Informasi Berdasarkan Framework ISO27001:2022,” *SEIKO J. Manag. Bus.*, vol. 6, no. 2, pp. 362–376, 2023.

[4] S. Nurul, Shynta Anggrainy, and Siska Aprelyani, “Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim),” *J. Ekon. Manaj. Sist. Inf.*, vol. 3, no. 5, pp. 564–573, 2022, doi: 10.31933/jemsi.v3i5.992.

[5] A. Hermawan, T. Hartati, and Y. A. Wijaya, “Analisa Keamanan Data Melalui Website Zahra Software Menggunakan Metode Keamanan Informasi CIA Triad,” *J. Inform. J. Pengemb. IT*, vol. 7, no. 3, pp. 125–130, 2022, doi: 10.30591/jpit.v7i3.3428.

[6] 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, 2021, doi: 10.26594/teknologi.v11i1.2152.

[7] A. P. Damanik, A. Zaki, S. Fiddarain, and A. B. Nasution, “Implementasi ISO 27001:2013 Dalam Pengamanan Sistem Informasi Pada Yayasan Pendidikan Islam ANNUR PRIMA,” *J. Sains dan Teknol.*, vol. 3, no. 1, pp. 68–73, 2023, doi: 10.47233/jsit.v3i1.488.

[8] M. Bakri and N. Irmayana, “Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi Simhp Bpkp Menggunakan Standar Iso 27001,” *J. Tekno*

Kompak, vol. 11, no. 2, p. 41, 2017, doi: 10.33365/jtk.v11i2.162.

[9] Y. C. Pradipta, Y. Rahardja, and M. N. N. Sitokdana, "Audit Sistem Manajemen Keamanan Informasi Pusat Teknologi Informasi Dan Komunikasi Penerbangan Dan Antariksa (Pustikpan) Menggunakan Sni Iso/Iec 27001:2013," *Sebatik*, vol. 23, no. 2, pp. 352–358, 2019, doi: 10.46984/sebatik.v23i2.782.

[10] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Research 1," *Des. Sci. IS Res. MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004.