Perancangan Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan ISO 27001:2022 (Studi Kasus Data Center Dinas Komunikasi dan Informatika Kota Tangerang Selatan)

Jimmy Alberto dan Cut Maisyarah Karyati

Universitas Gunadarma

E-mail: sukajadi99@gmail.com, csyarah@gmail.com

Abstrak

Penelitian ini mengkaji perancangan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar ISO 27001:2022 dengan studi kasus yang berfokus di Data Center Dinas Komunikasi dan Informatika Kota Tangerang untuk menanggapi tantangan keamanan informasi dalam transformasi digital pemerintah. Oleh karena itu, penting untuk memiliki SMKI yang efektif sesuai dengan standar ISO 27001:2022 dapat menjadi acuan penting. ISO 27001:2022 merupakan standar internasional untuk manajemen keamanan informasi, akan tetapi pada Diskominfo Kota Tangerang Selatan belum memiliki SMKI yang terstruktur dan sesuai dengan standar ISO 27001:2022. Penelitian ini bertujuan untuk melakukan identifikasi, analisis, dan evaluasi risiko keamanan informasi serta pengukuran SMKI berdasarkan kontrol keamanan tertentu. Metode yang diterapkan dalam penelitian ini adalah metode deskriptif kualitatif, dan data dikumpulkan melalui metode survey dan wawancara. Hasil pengukuran dapat dalam penelitian ini menunjukan 59% kontrol keamanan yang *complient,* 39% *Partially Complient* dan 2% *non-complient.* Penelitian ini diharapkan dapat menjadi pedoman dalam pengelolaan keamanan informasi bagi peneliti selanjutnya dan juga institusi pemerintah lainnya.

Kata kunci :Data Center, Diskominfo, ISO 27001:2022, Manajemen Resiko Keamanan Informasi, Sistem Manajemen Keamanan Informasi (SMKI).

Pendahuluan

E-Government Indonesia adalah inisiatif transformasi digital yang dicanangkan oleh pemerintah Indonesia untuk meningkatkan pelayanan publik dan efisiensi administrasi melalui pemanfaatan teknologi informasi[4]. Dalam era digital ini, teknologi informasi dan komunikasi (TIK) telah menjadi tulang punggung pemerintahan yang modern, memungkinkan pemerintah menyediakan berbagai layanan dan informasi secara online untuk masyarakat[7]. Melalui *E-Government*, warga negara dapat dengan mudah mengakses berbagai layanan pemerintah, seperti pembayaran pajak, pengajuan dokumen, hingga layanan kesehatan, dengan cepat dan efisien[1].

Namun, dalam mengadopsi teknologi informasi dan komunikasi, pemerintah juga dihadapkan pada tantangan keamanan informasi. Ancaman-ancaman keamanan ini dapat menyebabkan kerusakan dan kerugian yang serius, serta membahayakan integritas data dan privasi individu[10]. Peretas (hacker) dan penjahat siber menggunakan berbagai metode yang canggih untuk mencuri informasi sensitif, termasuk data kartu kredit, riwayat medis, data pribadi, dan login ID, dengan tujuan memperoleh keuntungan finansial atau merugikan pihak lain. Laporan dari Symantec pada tahun 2014 menyatakan bahwa terdapat 312 pelanggaran keamanan informasi yang menyebabkan 348 juta informasi terbongkar[9]. Hal ini menyoroti pentingnya perlindungan terhadap data sensitif dan ketersediaan layanan yang kritis bagi masyarakat.

Untuk menghadapi tantangan keamanan informasi ini, penting bagi pemerintah Indonesia untuk menerapkan sistem manajemen keamanan informasi (SMKI) yang kuat dan efektif[5]. Salah satu standar internasional yang dikenal luas dalam bidang keamanan informasi adalah ISO 27001. ISO 27001 adalah standar yang diterbitkan oleh *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC) yang memberikan panduan dan persyaratan untuk

DOI : http://dx.doi.org/10.32409/jikstik.22.4.3447

membangun, menerapkan, dan memelihara sistem keamanan informasi yang terpercaya[2].

Pada tahun 2022, ISO/IEC 27001 diperbarui agar tetap relevan dengan perkembangan teknologi dan ancaman keamanan yang terus berkembang. Pembaruan standar ini mencakup restrukturisasi kategori, 11 pengendalian baru, 24 pengendalian gabungan, dan 58 pengendalian yang diperbarui dalam ISO yang baru. Oleh karena itu, pembaruan ISO/IEC 27001:2022 menjadi penting untuk memberikan panduan yang up-to-date dan efektif bagi pemerintah dalam mengatasi ancaman keamanan yang semakin kompleks[6].

Penelitian-penelitian terdahulu telah mengulas pentingnya implementasi SMKI berdasarkan ISO/IEC 27001 dalam berbagai konteks organisasi. Beberapa penelitian telah mengukur tingkat kematangan (maturity level) dan melakukan audit SMKI berdasarkan standar ISO 27001:2013[3][7][8]. Temuan dari penelitian-penelitian ini memberikan wawasan dan rekomendasi yang berharga bagi organisasi dalam memperkuat keamanan informasi dan melindungi aset-aset penting dari ancaman siber.

Penelitian ini akan melanjutkan usaha ini dengan fokus pada perancangan dan implementasi SMKI di data center Dinas Komunikasi dan Informatika Kota Tangerang Selatan sebagai studi kasus. Tujuan utamanya adalah menciptakan tata kelola keamanan informasi yang sesuai dengan kebutuhan dan konteks perangkat daerah secara menyeluruh. Diharapkan hasil dari penelitian ini akan memberikan panduan praktis bagi pemerintah daerah dan organisasi lainnya untuk memperkuat sistem keamanan informasi mereka dan menghadapi ancaman siber yang makin kompleks dan serbaguna. Dengan implementasi SMKI berdasarkan standar ISO 27001:2022, diharapkan pelayanan publik yang aman dan efektif dapat terus terwujud dalam era E-Government Indonesia.Masalah dalam Penelitian ini adalah Dinas Komunikasi dan Informatika Kota Tangerang Selatan belum memiliki sistem manajemen keamanan informasi (SMKI) yang terstruktur dan sesuai dengan standar ISO 27001 2022. Hal ini dapat menyebabkan risiko keamanan informasi yang tinggi dan meningkatkan kemungkinan terjadinya pelanggaran keamanan.

Demi menghadapi ancaman keamanan informasi, penting untuk melakukan identifikasi, analisis, dan evaluasi risiko secara menyeluruh. Namun, Dinas Komunikasi dan Informatika Kota Tangerang Selatan mungkin tidak memiliki proses yang terstruktur untuk mengidentifikasi dan menganalisis risiko keamanan informasi yang dihadapi oleh data center mereka.

Sebagai institusi yang bertanggung jawab atas pengelolaan infrastruktur teknologi informasi dan aplikasi di Pemerintah Kota Tangerang Selatan, Dinas Komunikasi dan Informatika perlu memastikan kepatuhan terhadap standar ISO 27001. Namun, belum ada sistem manajemen keamanan informasi yang dirancang berdasarkan standar tersebut di data center mereka. Dinas Komunikasi dan Informatika Kota Tangerang Selatan membutuhkan suatu kerangka kerja yang sesuai dengan kebutuhan dan konteks perangkat daerah secara menyeluruh. Dalam hal ini, diperlukan perancangan sistem manajemen keamanan informasi (SMKI) yang tepat dan relevan dengan data center mereka, dengan mempertimbangkan aspek keamanan yang unik dan spesifik.

Dengan demikian identifikasi masalah pada penelitian ini yaitu:

1. Bagaimana cara melakukan identifikasi, analisis, dan evaluasi resiko keamanan informasi yang dihadapi oleh data center Dinas Komunikasi dan Informatika Kota Tangerang Selatan?

2. Bagaimana merancang Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan SNI ISO/IEC 27001:2022 yang tepat untuk data center Dinas Komunikasi dan Informatika Kota Tangerang Selatan

Tujuan penelitian ini, yaitu:

1. Untuk mengetahui cara melakukan identifikasi, analisis, dan evaluasi risiko keamanan informasi yang dihadapi oleh Dinas Komunikasi dan Informatika Kota Tangerang Selatan

2. Untuk melakukan pengukuran dari Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan SNI ISO/IEC 27001:2022 yang tepat untuk Dinas Komunikasi dan Informatika Kota Tangerang Selatan

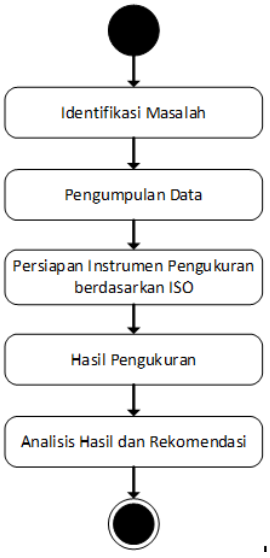
Metode Penelitian

Metode penelitian deskriptif kualitatif adalah sebuah metode yang digunakan peneliti untuk menemukan pengetahuan atau teori terhadap penelitian pada satu waktu tertentu. Metode yang diterapkan dalam penelitian ini adalah metode deskriptif kualitatif, dan data dikumpulkan melalui metode survey dan wawancara. Alur penelitian ini dimulai dengan tahap identifikasi masalah, di mana peneliti mengidentifikasi masalah keamanan informasi yang dihadapi oleh Data Center Dinas Komunikasi dan Informatika Kota Tangerang Selatan. Setelah itu, peneliti menetapkan tujuan penelitian yang spesifik dan metodologi penelitian yang akan digunakan. Selanjutnya, peneliti menentukan sumber data yang relevan seperti kebijakan keamanan informasi, prosedur operasional standar (SOP), dan dokumen audit sebelumnya. Tahap analisis kebutuhan melibatkan analisis kebutuhan keamanan informasi yang sesuai dengan standar ISO 27001:2022 dan identifikasi gap yang perlu diperbaiki. Peneliti

juga menganalisis kebijakan dan SOP yang ada untuk menentukan kebijakan dan prosedur yang diperlukan dalam pengukuran SMKI.

Analisis Kebutuhan

Dalam menganalisis kebutuhan perancangan dan pengukuran Sistem Manajemen Keamanan Informasi (SMKI), pertama-tama penting untuk memahami konteks organisasi serta menilai ruang lingkup dan batasannya. Hal ini melibatkan identifikasi semua aset informasi yang relevan dan pemahaman terhadap potensi risiko keamanan informasi yang dihadapi. Langkah selanjutnya dalam perancangan SMKI adalah menetapkan kebijakan keamanan informasi, tujuan, serta target yang jelas dan terukur. Mencakup Ruang Lingkup, Rujukan Normatif, Istilah dan Definisi, Konteks Organisasi, Kepemimpinan, Perancanaan, Penunjang, Operasional, Evaluasi Kinerja, dan Peningkatan. Struktur kontrol yang efektif harus dirancang dan diimplementasikan untuk mengelola dan mengurangi risiko keamanan, mencakup kontrol organisasi, kontrol orang, kontrol fisik, dan kontrol teknologi. Dalam pengukuran kinerja SMKI, metode pengukuran yang jelas harus didefinisikan dan diterapkan untuk memantau efektivitas SMKI secara berkelanjutan. Ini melibatkan pemantauan, pengukuran, analisis, dan evaluasi kontrol keamanan informasi. Hasil dari proses pengukuran ini harus secara rutin ditinjau untuk memastikan bahwa SMKI tetap efektif dalam mengatasi risiko keamanan informasi dan memenuhi tujuan dan target yang ditetapkan. Proses tinjauan ini juga harus mencakup pembaruan berkala atas SMKI untuk menanggapi perubahan lingkungan, risiko, dan kebutuhan bisnis organisasi. Gambaran dari keseluruhan tahapan penelitian ini digambarkan pada Gambar 1.



Gambar 1: Peta Pikiran

Tahap perngukuran SMKI melibatkan merancang sistem manajemen keamanan informasi berdasarkan standar ISO 27001:2022 yang sesuai dengan kebutuhan Data Center Dinas Komunikasi dan Informatika Kota Tangerang Selatan. Setelah itu melakukan analisa berdasarkan hasil pengukuran SMKI serta memberikan rekomendasi terhadap kontrol yang kurang patuh.

Melakukan tahap ini karena berguna untuk memastikan data ataupun informasi yang didapatkan cocok digunakan pada riset (SLR) atau tidak. Standar studi yang memenuhi syarat ialah sebagai berikut:

Detail penjelasan dalam tiap tahap pada gambar 1 adalah sebagai berikut:

1. Identifikasi Masalah Identifikasi masalah keamanan informasi yang dihadapi oleh Data Center Dinas Komunikasi dan Informatika Kota Tangerang Selatan serta menetapkan tujuan penelitian yang spesifik dan terukur untuk merancang sistem manajemen keamanan informasi (SMKI) berdasarkan ISO 27001:2022.

2. Pengumpulan Data Identifikasi sumber data yang relevan seperti kebijakan keamanan informasi, prosedur operasional standar (SOP), dokumen audit sebelumnya serta melakukan wawancara dengan personil terkait di Data Center Dinas Komunikasi dan Informatika Kota Tangerang Selatan untuk memahami lebih lanjut tentang kebutuhan dan persyaratan keamanan informasi.

3. Persiapan Instrumen Pengukuran berdasarkan ISO Melakukan persiapan Instrumen pengukuran dalam konteks ISO 27001:2022 merujuk kepada alat yang digunakan untuk mengevaluasi efektivitas kontrol keamanan informasi. Ada empat aspek utama dalam mengukur kontrol keamanan, yaitu Organizational, People, Physical, dan Technological.

4. Hasil Pengukuran Melakukan analisa kebutuhan keamanan informasi yang sesuai dengan standar ISO 27001:2022 dan mengidentifikasi gap yang perlu diperbaiki serta menganalisis kebijakan dan SOP yang ada untuk menentukan kebijakan dan prosedur yang diperlukan dalam perancangan SMKI, serta melakukan pengukuran pada SMKI tersebut.

5. Analisis Hasil dan Rekomendasi Melakukan analisa berdasarkan hasil pengukuran yang telah didapat pada sistem manajemen keamanan informasi (SMKI) berdasarkan standar ISO 27001:2022 yang sesuai dengan kebutuhan Data Center Dinas Komunikasi dan Informatika Kota Tangerang Selatan serta memberikan rekomendasi terhadap kontrol yang kurang patuh untuk meningkatkan kualitas kepatuhan.

Hasil dan Pembahasan

Hasil Analisis

Berdasarkan penelitian yang telah penulis lakukan di lapangan, penulis menyimpulkan bahwa permasalahan-permasalahan yang ditemukan dalam Diskominfo Kota Tangerang Selatan adalah sebagai berikut:

1. Dinas Komunikasi dan Informatika Kota Tangerang Selatan belum memiliki sistem manajemen keamanan informasi (SMKI) yang terstruktur dan sesuai dengan standar ISO 27001 2022. Hal ini dapat menyebabkan risiko keamanan informasi yang tinggi dan meningkatkan kemungkinan terjadinya pelanggaran keamanan.

2. Demi menghadapi ancaman keamanan informasi, penting untuk melakukan identifikasi, analisis, dan evaluasi risiko secara menyeluruh. Namun, Dinas Komunikasi dan Informatika Kota Tangerang Selatan mungkin tidak memiliki proses yang terstruktur untuk mengidentifikasi dan menganalisis risiko keamanan informasi yang dihadapi oleh data center mereka.

3. Sebagai institusi yang bertanggung jawab atas pengelolaan infrastruktur teknologi informasi dan aplikasi di Pemerintah Kota Tangerang Selatan, Dinas Komunikasi dan Informatika perlu memastikan kepatuhan terhadap standar ISO 27001. Namun, belum ada sistem manajemen keamanan informasi yang dirancang berdasarkan standar tersebut di data center mereka.

4. Dinas Komunikasi dan Informatika Kota Tangerang Selatan membutuhkan suatu kerangka kerja yang sesuai dengan kebutuhan dan konteks perangkat daerah secara menyeluruh. Dalam hal ini, diperlukan pengukuran sistem manajemen keamanan informasi (SMKI) yang tepat dan relevan dengan data center mereka, dengan mempertimbangkan aspek keamanan yang unik dan spesifik.

Hasil Pengukuran

Pada Pengukuran SMKI ini juga memuat kuesioner tentang Kontrol Keamanan Informasi (Information Security Controls) seperti yang ada di dalam standar ISO 27001 tahun 2002. Information Security Controls (Kontrol Keamanan Informasi) sebagaimana dalam ISO/IEC 27001:2022 dibagi menjadi empat bagian, yaitu: organization controls (kontrol organisasi), people controls (kontrol terkait sumber daya manusia), physical controls (kontrol fisik), dan technological controls (kontrol teknologi). Pada sub bab ini akan dibahas masing-masing kontrol tersebut sekaligus penulis akan memberikan penilaian terhadap masing-masing standar dalam kontrol terkait dengan penerapannya di dalam Data Center Diskominfo Kota Tangerang Selatan. Penilaian dibagi menjadi 4 kategori yaitu:

1. *Compliant* (Patuh): Kategori "compliant" digunakan ketika Data Center Diskominfo Kota Tangerang Selatan dinilai sepenuhnya mematuhi persyaratan standar yang diberlakukan. Ini berarti bahwa kontrol yang ditetapkan oleh standar telah diimplementasikan dengan baik, sesuai dengan kebijakan dan prosedur yang ditetapkan, dan mencapai tingkat kepatuhan yang diharapkan. Instansi telah menjalankan langkah-langkah yang diperlukan untuk melindungi keamanan informasi sesuai dengan standar yang relevan.

2. *Partially Compliant* (Sebagian Patuh): Kategori "partially compliant" digunakan ketika Data Center Diskominfo Kota Tangerang Selatan dinilai memenuhi sebagian besar persyaratan standar, tetapi masih ada beberapa area di mana ada kekurangan atau kepatuhan yang belum sepenuhnya terpenuhi. Dalam hal ini, langkah-langkah telah diambil untuk memenuhi sebagian besar persyaratan, tetapi masih ada ruang untuk perbaikan atau pengembangan lebih lanjut dalam hal implementasi kontrol yang belum sepenuhnya sesuai dengan standar.

3. *Non-compliant (*Tidak Patuh): Kategori "non-compliant" digunakan ketika Data Center Diskominfo Kota Tangerang Selatan dinilai tidak mematuhi persyaratan standar yang diberlakukan. Ini berarti bahwa kontrol yang ditetapkan oleh standar tidak diimplementasikan atau dilaksanakan dengan benar, atau tidak mencapai tingkat kepatuhan yang diharapkan. Instansi perlu melakukan tindakan perbaikan untuk memenuhi persyaratan standar yang relevan.

4. *Not Applicable* (Tidak Berlaku): Kategori "not applicable" digunakan ketika persyaratan standar tidak berlaku atau tidak relevan untuk Data Center Diskominfo Kota Tangerang Selatan. Hal ini mungkin terjadi jika Data Center Diskominfo Kota Tangerang Selatan tidak memiliki aset atau lingkungan yang relevan untuk persyaratan tertentu dalam standar. Dalam hal ini, penilaian tidak diterapkan pada persyaratan yang tidak berlaku, dan organisasi tidak diharapkan untuk memenuhi persyaratan tersebut.

Penomoran pada setiap standar dalam pengukuran SMKI ini penulis buat dengan format sesuai dengan penomoran dalam ISO/IEC 27001:2022, yaitu dari nomor 5.1 dengan tujuan memudahkan Diskominfo

Tangerang Selatan dalam mencocokan SMKI ini dengan standar ISO/IEC 27001:2022 yang asli.

Organizational controls

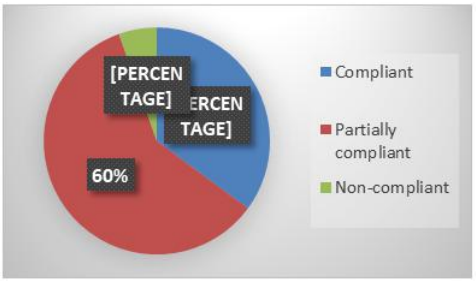
Kontrol ini berkaitan dengan kebijakan, prosedur, dan struktur organisasi yang digunakan untuk mengelola keamanan informasi. Tujuan dari kontrol ini adalah untuk memastikan bahwa kebijakan dan prosedur keamanan informasi yang sesuai telah ditetapkan, dan tanggung jawab terhadap keamanan informasi telah distribusikan dengan jelas di dalam organisasi. Pada Data Center Diskominfo Kota Tangerang Selatan, organization controls mencakup pengembangan dan penerapan kebijakan keamanan informasi, penetapan peran dan tanggung jawab terkait keamanan informasi, serta prosedur operasional yang terkait dengan pengamanan sistem dan data. Tabel 1 adalah kuesioner tentang organization controls untuk Data Center Diskominfo Kota Tangerang Selatan beserta hasilnya.

Berdasarkan Tabel 1 terlihat bahwa tidak semua domain kontrol keamanan yang patuh (compliant). Rincian dari Rancangan Alat Evaluasi SMKI Organizational Controls adalah 9 kontrol keamanan yang patuh, 5 kontrol keamanan yang hanya sebagian patuh (partially compliant), 5 kontrol keamanan yang tidak patuh (non-compliant), dan 5 kontrol keamanan yang tidak dapat diterapkan (not applicable). Presentasi Rancangan Alat Evaluasi SMKI Organizational Controls yang datanya merujuk pada Tabel 1 dapat dilihat pada Gambar 2.

Tabel 1: Rancangan Alat Evaluasi SMKI: Organizational Controls

No	Standar	Kategori
5.1	Kebijakan Keamanan Informasi	*Partially compliant*
5.2	Peran dan Tanggung Jawab Keamanan Informasi	*Compliant*
5.3	Pemisahan Tugas	*Compliant*
5.4	Tanggung Jawab Manajemen	*Partially compliant*
5.5	Kontak dengan Otoritas	*Compliant*
5.6	Kontak dengan Kelompok Kepentingan Khusus	*Partially compliant*
5.7	Intelijen Ancaman	*Partially compliant*
5.8	Keamanan Informasi dalam Manajemen Proyek	*Partially compliant*
5.9	Inventaris Informasi dan Aset Terkait Lainnya	*Partially compliant*
5.10	Penggunaan yang Dapat Diterima dari Informasi dan Aset Terkait Lainnya	*Compliant*
5.11	Pengembalian Aset	*Compliant*
5.12	Klasifikasi Informasi	*Compliant*
5.13	Pelabelan Informasi	*Compliant*
5.14	Transfer Informasi	*Partially compliant*
5.15	Kontrol Akses	*Compliant*
5.16	Manajemen Identitas	*Compliant*
5.17	Informasi Otentikasi	*Compliant*
5.18	Hak Akses	*Compliant*
5.19	Keamanan Informasi dalam Hubungan dengan Pemasok	*Partially compliant*
5.20	Pemenuhan Persyaratan Keamanan Informasi dalam Perjanjian dengan Pemasok	*Partially compliant*
5.21	Manajemen Keamanan Informasi dalam Rantai Pasok Teknologi Informasi dan Komunikasi (TIK)	*Partially compliant*
5.22	Pemantauan, Tinjauan, dan Pengelolaan Perubahan Layanan Pemasok	*Partially compliant*
5.23	Keamanan Informasi dalam Penggunaan Layanan Cloud	*Non-compliant*
5.24	Perencanaan dan Persiapan Manajemen Kejadian Keamanan Informasi	*Non-compliant*
5.25	Penilaian dan keputusan tentang peristiwa keamanan informasi	*Partially compliant*
5.26	Respon terhadap keamanan informasi insiden	*Partially compliant*
5.27	Belajar dari insiden keamanan informasi	*Partially compliant*
5.28	Pengumpulan bukti	*Partially compliant*
5.29	Keamanan informasi selama gangguan	*Compliant*
5.30	Kesiapan TIK untuk kelangsungan bisnis	*Partially compliant*
5.31	Persyaratan hukum, undang-undang, peraturan dan kontrak	*Partially compliant*
5.32	Hak kekayaan intelektual	*Partially compliant*
5.33	Perlindungan catatan	*Partially compliant*
5.34	Privasi dan perlindungan informasi identitas pribadi (PII)	*Partially compliant*
5.35	Tinjauan independen atas keamanan informasi	*Partially compliant*
5.36	Kepatuhan terhadap kebijakan, aturan, dan standar untuk keamanan informasi	*Compliant*
5.37	Prosedur operasi yang terdokumentasi	*Partially compliant*

Berdasarkan penilaian standar keamanan informasi di atas, Dinas Komunikasi dan Informatika Kota Tangerang Selatan menunjukkan tingkat kepatuhan yang bervariasi dalam berbagai aspek. Standar seperti peran dan tanggung jawab keamanan informasi, pemisahan tugas, kontak dengan otoritas, penggunaan yang dapat diterima dari informasi dan aset terkait lainnya, pengembalian aset, klasifikasi informasi, pelabelan informasi, kontrol akses, manajemen identitas, informasi otentikasi, hak akses, dan kepatuhan terhadap kebijakan, aturan, dan standar untuk keamanan informasi, telah sepenuhnya dipenuhi oleh Dinas Komunikasi dan Informatika Kota Tangerang Selatan.



Gambar 2: Presentasi Rancangan Alat Evaluasi SMKI: Organizational Controls

Namun, beberapa aspek seperti kebijakan keamanan informasi, tanggung jawab manajemen, kontak dengan kelompok kepentingan khusus, intelijen ancaman, keamanan informasi dalam manajemen proyek, inventaris informasi dan aset terkait lainnya, transfer informasi, keamanan informasi dalam hubungan dengan pemasok, pemenuhan persyaratan keamanan informasi dalam perjanjian dengan pemasok, manajemen keamanan informasi dalam rantai pasok TIK, pemantauan, tinjauan, dan pengelolaan perubahan layanan pemasok, penilaian dan keputusan tentang peristiwa keamanan informasi, respon terhadap keamanan informasi insiden, belajar dari insiden keamanan informasi, pengumpulan bukti, kesiapan TIK untuk kelangsungan bisnis, persyaratan hukum, undang-undang, peraturan dan kontrak, hak kekayaan intelektual, perlindungan catatan, privasi dan perlindungan PII, tinjauan independen atas keamanan informasi, dan prosedur operasi yang terdokumentasi, telah dipenuhi secara parsial.

Selain itu, Dinas Komunikasi dan Informatika Kota Tangerang Selatan ini belum mematuhi standar seperti keamanan informasi dalam penggunaan layanan cloud dan perencanaan dan persiapan manajemen kejadian keamanan informasi. Dari hasil penilaian ini, Dinas Komunikasi dan Informatika Kota Tangerang Selatan perlu meningkatkan kualitas kepatuhan mereka dalam beberapa area, khususnya yang berstatus non-compliant dan partially compliant, untuk mencapai standar keamanan informasi yang lebih baik.

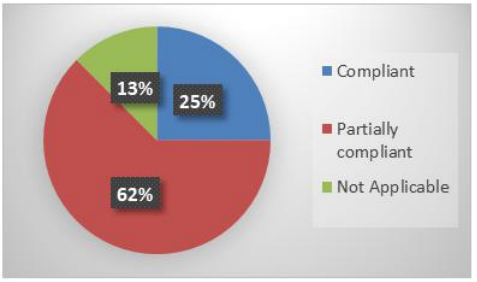
People controls

Kontrol ini berkaitan dengan aspek-aspek terkait SDM (Sumber Daya Manusia) dalam konteks keamanan informasi. Tujuan dari kontrol ini adalah untuk memastikan bahwa SDM yang terlibat dalam pengelolaan keamanan informasi memiliki pengetahuan, keterampilan, dan kesadaran yang cukup untuk melaksanakan tugas-tugas keamanan informasi dengan baik. Di Data Center Diskominfo Kota Tangerang Selatan, people controls mencakup kebijakan pelatihan dan kesadaran keamanan informasi bagi para staf, pemilihan karyawan yang sesuai untuk posisi terkait keamanan informasi, serta penerapan prosedur pengelolaan akses dan keamanan fisik terhadap personil yang memiliki akses ke pusat data. Tabel 2 adalah kuesioner tentang people controls untuk Data Center Diskominfo Kota Tangerang Selatan beserta hasilnya.

Tabel 2: Rancangan Alat Evaluasi SMKI: People Controls

No	Standar	Kategori
6.1	Pemeriksaan Latar Belakang	*Partially compliant*
6.2	Syarat dan Ketentuan Kerja	*Partially compliant*
6.3	Kesadaran, Pendidikan, dan Pelatihan Keamanan Informasi	*Compliant*
6.4	Proses Disiplin	*Partially compliant*
6.5	Tanggung Jawab Setelah Pemberhentian atau Perubahan Kerja	*Partially compliant*
6.6	Perjanjian Kerahasiaan atau Non-Disclosure	*Compliant*
6.7	Pekerjaan Jarak Jauh	*Not applicable*
6.8	Pelaporan Kejadian Keamanan Informasi	*Partially compliant*

Berdasarkan Tabel 2 terlihat bahwa tidak semua domain standar keamanan yang patuh (compliant). Rincian dari Rancangan Alat Evaluasi SMKI People Controls adalah 2 standar keamanan yang patuh, 5 standar keamanan yang hanya sebagian patuh (partially compliant), 1 standar keamanan yang tidak relevan (Not Applicable). Presentasi Rancangan Alat Evaluasi SMKI People Controls yang datanya merujuk pada Tabel 2 dapat dilihat pada Gambar 3.



Gambar 3: Presentasi Rancangan Alat Evaluasi SMKI: People Controls

Dari hasil penilaian standar keamanan informasi yang dijalankan, Dinas Komunikasi dan In-

formatika Kota Tangerang Selatan menunjukkan tingkat kepatuhan yang bervariasi. Dinas Komunikasi dan Informatika Kota Tangerang Selatan telah mencapai tingkat kepatuhan penuh dalam aspek Kesadaran, Pendidikan, dan Pelatihan Keamanan Informasi serta Perjanjian Kerahasiaan atau Non-Disclosure. Ini menunjukkan bahwa Dinas Komunikasi dan Informatika Kota Tangerang Selatan telah berhasil menerapkan pendidikan dan pelatihan keamanan informasi yang sesuai dan berkelanjutan serta telah mendokumentasikan dan menandatangani perjanjian kerahasiaan atau non-disclosure dengan baik.

Namun, masih ada ruang untuk peningkatan dalam aspek Pemeriksaan Latar Belakang, Syarat dan Ketentuan Kerja, Proses Disiplin, Tanggung Jawab Setelah Pemberhentian atau Perubahan Kerja, dan Pelaporan Kejadian Keamanan Informasi, yang semuanya hanya patuh sebagian. Ini berarti bahwa sementara beberapa langkah telah diambil dalam setiap area ini, lebih banyak lagi yang perlu dilakukan untuk mencapai tingkat kepatuhan penuh.

Untuk standar Pekerjaan Jarak Jauh, ini tidak berlaku, yang dapat berarti bahwa Dinas Komunikasi dan Informatika Kota Tangerang Selatan saat ini mungkin tidak memiliki pegawai yang bekerja dari jarak jauh atau belum ada kebijakan yang diimplementasikan dalam konteks ini. Selanjutnya, Dinas Komunikasi dan Informatika Kota Tangerang Selatan harus berusaha untuk mencapai tingkat kepatuhan yang lebih tinggi dalam semua area untuk memastikan keamanan informasi yang optimal.

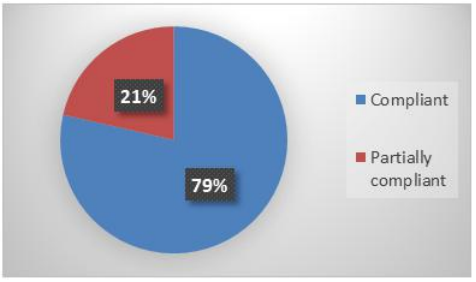
Physical controls

Kontrol ini berkaitan dengan perlindungan fisik terhadap aset informasi dan infrastruktur yang digunakan untuk mengelola keamanan informasi. Tujuan dari kontrol ini adalah untuk mencegah akses tidak sah, kerusakan, atau kehilangan terhadap aset-aset informasi yang vital. Di Data Center Diskominfo Kota Tangerang Selatan, physical controls mencakup langkah-langkah keamanan fisik seperti pengendalian akses ke ruangan server, penggunaan pengunci dan pengawasan pada perangkat keras, perlindungan terhadap kebakaran dan bencana alam, serta tata letak yang aman dan terorganisir di pusat data. Tabel 3 adalah kuesioner tentang physical controls untuk Data Center Diskominfo Kota Tangerang Selatan beserta hasilnya.

Berdasarkan Tabel 3 terlihat bahwa tidak semua domain standar keamanan yang patuh (compliant). Rincian dari Rancangan Alat Evaluasi SMKI Physical Controls adalah 11 standar keamanan yang patuh dan 3 standar keamanan yang hanya sebagian patuh (partially compliant). Presentasi Rancangan Alat Evaluasi SMKI Physical Controls yang datanya merujuk pada Tabel 3 dapat dilihat pada Gambar 4.

Tabel 3: Rancangan Alat Evaluasi SMKI: Physical Controls

No	Standar	Kategori
7.1	Perimeter keamanan fisik	*Compliant*
7.2	Entri fisik	*Compliant*
7.3	Mengamankan kantor, ruangan dan fasilitas	*Compliant*
7.4	Pemantauan keamanan fisik	*Compliant*
7.5	Perlindungan terhadap Ancaman Fisik dan Lingkungan	*Compliant*
7.6	Bekerja di Area Aman	*Compliant*
7.7	Aturan Meja Bersih dan Layar Bersih	*Partially compliant*
7.8	Penyusunan dan Perlindungan Peralatan	*Compliant*
7.9	Keamanan Aset di Lokasi Tidak Berada di Tempat	*Partially compliant*
7.10	Media Penyimpanan	*Compliant*
7.11	Utilitas Pendukung	*Compliant*
7.12	Keamanan Kabel	*Compliant*
7.13	Pemeliharaan Peralatan	*Compliant*
7.14	Pembuangan atau Penggunaan Ulang Peralatan dengan Keamanan Terjamin	*Partially compliant*



Gambar 4: Presentasi Rancangan Alat Evaluasi SMKI: Physical Controls

Berdasarkan penilaian standar keamanan fisik dan digital yang dijelaskan, tampak bahwa kebanyakan standar keamanan telah memenuhi standar. Hal ini mencakup penentuan dan penerapan perimeter keamanan, kontrol akses, perlindungan terhadap ancaman fisik dan lingkungan, hingga keamanan kabel dan pemeliharaan peralatan. Namun, beberapa standar masih belum memenuhi standar atau tingkat kepatuhan hanya sebagian, seperti aturan meja bersih dan layar bersih, perlindungan aset di luar lokasi, dan proses pembuangan atau penggunaan ulang peralatan. Meski demikian, secara umum, standar keamanan tampak baik dan telah memenuhi kebanyakan kriteria. Untuk mencapai keamanan yang lebih optimal, diperlukan peningkatan dan perbaikan pada aspek-aspek yang masih sebagian memenuhi standar.

Technological controls

Kontrol ini berkaitan dengan penggunaan teknologi dan mekanisme keamanan teknis untuk melindungi aset informasi dan sistem yang digunakan. Tujuan dari kontrol ini adalah untuk memastikan bahwa infrastruktur teknologi yang digunakan memiliki

tingkat keamanan yang memadai untuk melindungi data dan sistem informasi. Di Data Center Diskominfo Kota Tangerang Selatan, technological controls mencakup penggunaan firewall, enkripsi data, pengelolaan akses dan otentikasi, pemantauan jaringan dan sistem, serta kebijakan backup dan pemulihan data. Tabel 4 adalah kuesioner tentang technological controls untuk Data Center Diskominfo Kota Tangerang Selatan beserta hasilnya.

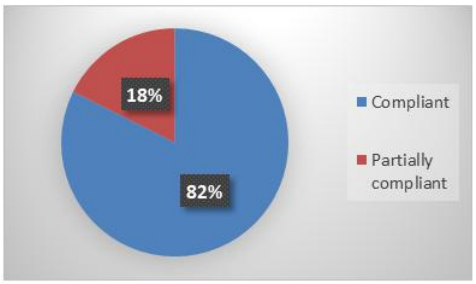
Tabel 4: Rancangan Alat Evaluasi SMKI: Technological Controls

No	Standar	Kategori
8.1	Kontrol Perangkat Pengguna Akhir	*Compliant*
8.2	Hak Akses Privileged	*Compliant*
8.3	Pembatasan Akses Informasi	*Compliant*
8.4	Akses ke Kode Sumber	*Compliant*
8.5	Autentikasi Aman	*Compliant*
8.6	Manajemen Kapasitas	*Partially compliant*
8.7	Pengamanan terhadap Malware	*Compliant*
8.8	Manajemen Kerentanan Teknis	*Compliant*
8.9	Manajemen Konfigurasi	*Compliant*
8.10	Penghapusan Informasi	*Partially compliant*
8.11	Penyamaran Data	*Compliant*
8.12	Prevensi Kebocoran Data	*Compliant*
8.13	Pencadangan Informasi	*Compliant*
8.14	Redundansi Fasilitas Pengolahan Informasi	*Compliant*
8.15	Pencatatan	*Partially compliant*
8.16	Pemantauan Aktivitas	*Compliant*
8.17	Sinkronisasi Jam	*Compliant*
8.18	Penggunaan Program Utilitas Berhak Akses	*Compliant*
8.19	Instalasi Perangkat Lunak pada Sistem Operasional	*Compliant*
8.20	Keamanan Jaringan	*Compliant*
8.21	Keamanan Layanan Jaringan	*Compliant*
8.22	Segregasi Jaringan	*Compliant*
8.23	Filterisasi Web	*Compliant*
8.24	Penggunaan Kriptografi	*Compliant*
8.25	Siklus Hidup Pengembangan Aman	*Compliant*
8.26	Persyaratan Keamanan Aplikasi	*Compliant*
8.27	Arsitektur dan Prinsip Rekayasa Sistem yang Aman	*Partially compliant*
8.28	Pengodean aman	*Compliant*
8.29	Pengujian keamanan dalam pengembangan dan penerimaan	*Compliant*
8.30	Pengembangan outsourcing	*Partially compliant*
8.31	Pemisahan lingkungan pengembangan, pengujian, dan produksi	*Compliant*
8.32	Perubahan manajemen	*Compliant*
8.33	Informasites	*Compliant*
8.34	Perlindungan sistem informasi selama pengujian audit	*Partially compliant*

Berdasarkan Tabel 4 terlihat bahwa tidak semua domain standar keamanan yang patuh (compliant). Rincian dari Rancangan Alat Evaluasi SMKI Technological Controls adalah 28 standar keamanan yang patuh dan 6 standar keamanan yang hanya sebagian patuh (partially compliant). Presentasi Rancangan Alat Evaluasi SMKI Technological Controls yang datanya merujuk pada Tabel 4 dapat dilihat pada Gambar 5.

Berdasarkan hasil penilaian terhadap standar yang ditetapkan, Dinas Komunikasi dan Informatika Kota Tangerang Selatan secara umum telah mematuhi berbagai elemen keamanan informasi yang penting. Perlindungan data dan kontrol akses, manajemen hak akses yang istimewa, batasan akses ke kode sumber, autentikasi yang aman, dan pencegahan malware telah diimplementasikan dengan baik. Selain itu, manajemen kerentanan tek-

nis, konfigurasi, dan pemantauan aktivitas juga telah sesuai standar, begitu pula dengan penggunaan kriptografi, pengembangan perangkat lunak yang aman, dan segregasi jaringan.

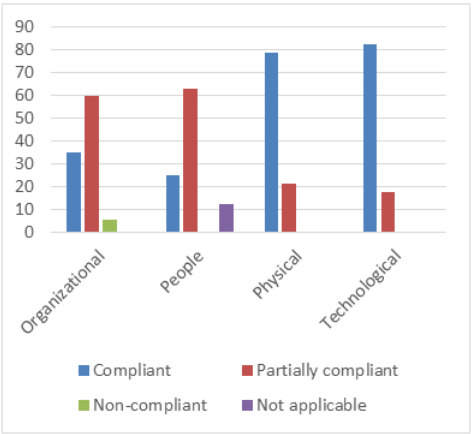


Gambar 5: Presentasi Rancangan Alat Evaluasi SMKI: Technological Controls

Namun, terdapat beberapa area yang memerlukan perbaikan. Manajemen kapasitas, yang melibatkan pemantauan dan penyesuaian penggunaan sumber daya terhadap persyaratan kapasitas, hanya sejalan sebagian dengan standar yang ditentukan. Penghapusan informasi yang sudah tidak diperlukan dan pencatatan aktivitas juga hanya mematuhi standar secara parsial.

Selain itu, standar arsitektur dan prinsip rekayasa sistem yang aman hanya dipatuhi sebagian, yang berarti ada ruang untuk peningkatan dalam penerapan arsitektur sistem dan prinsip rekayasa yang aman. Pengembangan outsourcing, yang melibatkan pengarahan, pemantauan, dan peninjauan kegiatan terkait pengembangan sistem yang dialihdayakan, juga hanya sejalan sebagian dengan standar. Terakhir, perlindungan sistem informasi selama pengujian audit memerlukan peningkatan.

Dalam kesimpulannya, Dinas Komunikasi dan Informatika Kota Tangerang Selatan secara keseluruhan telah melaksanakan praktik keamanan informasi yang baik, namun ada beberapa area yang memerlukan peningkatan untuk memenuhi sepenuhnya standar yang ditentukan.



Gambar 6: Presentasi Perbandingan Rancangan Alat Evaluasi SMKI

Gambar 6 merupakan presentasi perbandingan rancangan alat evaluasi SMKI berdasarkan 4 control yaitu Organization control, People Control, Physical Control dan Technological Control.

Tabel 5: Tabel Analisi Kesenjangan Rancangan Alat Evaluasi SMKI: Compliant

No Annex	Domain Kontrol Keamanan	Jumlah		
		Standar	Compliant	Jumlah/Total (%)
A5	Organizational	37	13	35,14%
A6	People	8	2	25%
A7	Physical	14	11	78,57%
A8	Technological	34	28	82,35%
Hasil Jumlah		93	54	58,06%
Hasil Akhir Tingkat Kesenjangan (Not Applicable -1)		92	54	58,70%

Tabel 6: Tabel Analisi Kesenjangan Rancangan Alat Evaluasi SMKI: Partially Compliant

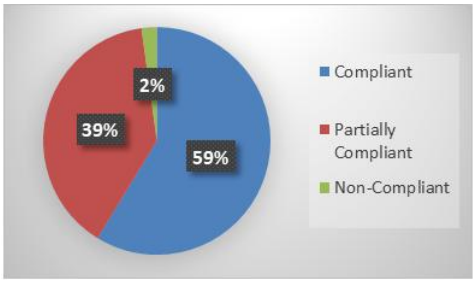
No Annex	Domain Kontrol Keamanan	Jumlah		
		Standar	Partially Compliant	Jumlah/Total (%)
A5	Organizational	37	22	59,46%
A6	People	8	5	62,50%
A7	Physical	14	3	21,43%
A8	Technological	34	6	17,65%
Hasil Jumlah		93	36	38,71%
Hasil Akhir Tingkat Kesenjangan (Not Applicable -1)		92	36	39,13%

Tabel 7: Tabel Analisi Kesenjangan Rancangan Alat Evaluasi SMKI: Non-Compliant

No Annex	Domain Kontrol Keamanan	Jumlah		
		Standar	Non-Compliant	Jumlah/Total (%)
A5	Organizational	37	2	5,41%
A6	People	8	0	0%
A7	Physical	14	0	0%
A8	Technological	34	0	0%
Hasil Jumlah		93	2	2,15%
Hasil Akhir Tingkat Kesenjangan (Not Applicable -1)		92	2	2,17%

Berdasarkan Tabel 5, Tabel 6, dan Tabel 7 terlihat bahwa tidak semua domain kontrol keamanan yang compliant. Rincian dari hasil Analisis kesenjangan rancangan alat evaluasi SMKI adalah

54 kontrol keamanan yang compliant, 36 kontrol keamanan yang partially compliant, 2 kontrol keamanan yang non-compliant, dan 1 kontrol keamanan yang not applicable. Persentasi jumlah tingkat kesenjangan sesudah yang datanya merujuk pada Tabel diatas dapat dilihat pada Gambar 7.



Gambar 7: Persentasi Jumlah Tingkat Kesenjangan

Penutup

Beberapa poin kesimpulan yang dapat penulis tarik dari penelitian ini, yaitu:

1. Berdasarkan penelitian yang dilakukan, metode identifikasi, analisis, dan evaluasi risiko keamanan informasi untuk Dinas Komunikasi dan Informatika Kota Tangerang Selatan telah berhasil diidentifikasi. Pengelolaan Data Center Diskominfo Tangsel saat ini masih menggunakan Indeks KAMI berbasis ISO 27001:2013 sebagai alat evaluasi untuk menganalisis tingkat keamanan informasi di dalam instansi tersebut. Evaluasi ini memberikan gambaran kesiapan keamanan informasi di data center dan membantu mengidentifikasi area yang perlu diperbaiki. Hasil evaluasi ini digunakan untuk menyusun langkah perbaikan demi meningkatkan keamanan informasi.

2. Dalam penelitian ini, penulis berhasil merancang Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan ISO 27001:2022 untuk Data Center Diskominfo Kota Tangerang Selatan serta melakukan pengukuran dari SMKI tersebut. Rancangan SMKI ini terdiri dari 10 bagian berisi pedoman keamanan ditambah dengan kuesioner tentang Kontrol Keamanan Informasi (Information Security Control) untuk menguji seberapa jauh keamanan informasi di Data Center Diskominfo Kota Tangerang Selatan telah diterapkan. Pedoman keamanan terdiri dari 10 bagian yaitu Ruang Lingkup, Rujukan Normatif, Istilah dan Definisi, Konteks Organisasi, Kepemimpinan, Perancanaan, Penunjang, Operasional, Evaluasi Kinerja, dan Peningkatan. Sedangkan kuesioner yang digunakan sebagai alat evaluasi keamanan terdiri dari 4 jenis evaluasi yaitu kontrol organisasi, kontrol orang, kontrol fisik, dan kontrol teknologi. Dari hasil pengukuran dengan menggunakan SMKI ini, diketahui bahwa ada banyak aspek perlindungan keamanan yang telah dipenuhi oleh Data Center Diskominfo Kota Tangerang Selatan. Namun masih ada beberapa aspek yang perlu ditingkatkan perlindungan keamanannya. Implementasi dan pengukuran ini memungkinkan untuk terus memperbaiki prosedur dan kebijakan keamanan informasi di Dinas Komunikasi dan Informatika Kota Tangerang Selatan untuk memastikan keamanan informasi yang berkelanjutan.

Daftar Pustaka

[1] Diana Anggraini dan Rahadian Bisma. "Perencanaan Tata Kelola Keamanan Informasi dalam Penerapan Cloud Computing Menggunakan ISO 27001: 2013 pada PT. SPINDO, Tbk.", Journal of Informatics and Computer Science (JINACS), Vol. 3, No. 01, 46-54, 2021.

[2] Arya Pratama Damanik, Alfasyahri Zaki, Syaidah Fiddarain dan Adnan Buyung Nasution, "Implementas ISO 27001: 2013 Dalam Pengamanan Sistem Informasi Pada Yayasan Pendidikan Islam ANNUR PRIMA", Jurnal Sains dan Teknologi (JSIT), Vol. 3, No.1, Padang, 68-73, 2023.

[3] Andy Nur Hidayat, "Peningkatan Cyber Security Dengan Penerapan Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005", Teknik Elektro Universitas Mercu Buana Jakarta, Jakarta, 2020.

[4] Musyarofah, Sitta Rif'atul dan Rahadian Bisma, "Pembuatan Standard Operating Procedure (SOP) Keamanan Informasi Berdasarkan Framework ISO/IEC 27001: 2013 dan ISO/IEC 27002: 2013 pada Dinas Komunikasi dan Informatika Pemerintah Kota Madiun", Journal of Emerging Information System and Business Intelligence (JEISBI), Vol. 1, No.1, 43-50, 2020.

[5] Silvia Paramita, Sandy Akbar Siregar, Rissa Azzahra Damanik dan Muhammad Dedi Irawan, "Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001: 2013", Bulletin of Information Technology (BIT), Vol. 3, No.4, 374-379, 2022.

[6] Rudiyanto, Rezky Alkais Putra dan Vera Suryani. "Analisis Sistem Manajemen Keamanan Informasi Pada Dinas Komunikasi Informasi Dan Statistik Kabupaten Lampung Tengah Menggunakan ISO/IEC 27001", eProceedings of Engineering, Vol.10, No.2, Bandung, 2023.

[7] Ito Setiawan, Aldistya Riesta Sekarin, Retno Waluyo dan Fiby Nur Afiana, "Manajemen Risiko Sistem Informasi Menggunakan ISO 31000 dan Standar Pengendalian ISO/EIC 27001 di Tripio Purwokerto", MATRIK: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, Vol.20, No.2, Mataram, 389-396, 2021.

[8] Edy Soesanto, , dkk. "Sistem manajemen keamanan informasi dengan standar ISO/IEC 27001 dan ISO/ICE 27002 pada PT Jasa Marga", Co-Creation: Jurnal Ilmiah Ekonomi Manajemen Akuntansi dan Bisnis, Vol. 1, No. 4, 169-179, 2023.

[9] Anonym, “Internet Security Threat Report Vol.20", Symantec, 2015, diakses daring pada: https://www.govloop.com/wp-content/uploads/2015/09/Government-Internet-Secrutiy-Threat-Report-Volume-20.pdf.

[10] Anonym, “Cyber Crime Costs Indonesia More Than Rp33 M", Tempo, 2018, diakses daring pada : https://en.tempo.co/read/695173/cyber-crime-costs-indonesia-more-than-rp33-m.