Jutisi: Jurnal Ilmiah Teknik Informatika dan Sistem Informasi
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0893
p-ISSN: 2089-3787

Analisis Keamanan Sistem Informasi Perdagangan Terintegrasi Menggunakan Standar ISO 27002

Haryanto Tanuwijaya
Program Studi Manajemen, Universitas Dinamika
Jl. Raya Kedung Baruk 98, Surabaya, Indonesia
*e-mail *Corresponding Author*: haryanto@dinamika.ac.id

Abstract

Along with the increasing volume and area of business, PT. XYZ implements an Integrated Trading Information System which is abbreviated Sipeter. Information leakage issues, data loss, system hangs, and so on can cause Sipeter security risks. If this is allowed, Sipeter is threatened with not being able to fulfill the aspects of confidentiality, integrity, and availability of data. In this study, Sipeter security analysis was carried out using the ISO 27002 standard in articles 8 to 14. Findings and evidence data were obtained through interviews and field observations to related departments. The results of this study showed that the approach of PT. XYZ's security at Sipeter is inconsistent and security controls are carried out informally. Which is indicated by Sipeter's maturity level is 1.55 or Initial level. PT. XYZ needs to be consistent in managing Sipeter security, develop information system security standards and be disciplined in documenting various incidents related to Sipeter to minimize the risk of data loss, information leakage and misuse, as well as internal chaos that is detrimental to the business continuity of PT. XYZ.
Keywords: *Security; Information System; Commerce; ISO 27002 standard*

Abstrak

Seiring meningkatnya volume dan luas wilayah usaha maka PT. XYZ menerapkan Sistem Informasi Perdagangan Terintegrasi yang disingkat Sipeter. Permasalahan kebocoran informasi, kehilangan data, sistem hang, dan lain sebagainya dapat menimbulkan risiko keamanan Sipeter. Apabila hal tersebut dibiarkan maka Sipeter terancam tidak dapat memenuhi aspek kerahasiaan, integritas dan ketersediaan data. Pada penelitian ini dilakukan analisis keamanan Sipeter menggunakan standar ISO 27002 pada klausul 8 sampai dengan klausul 14. Data temuan dan bukti diperoleh melalui wawancara dan observasi lapangan ke bagian terkait. Hasil penelitian menunjukkan pendekatan PT. XYZ terhadap keamanan Sipeter tidak konsisten dan kontrol keamanan dilakukan secara informal. Yang ditunjukan dengan maturity level Sipeter adalah 1.55 atau level Initial. PT. XYZ perlu konsisten dalam memanaj keamanan Sipeter, menyusun standar keamanan sistem informasi dan disiplin dalam pendokumentasian berbagai kejadian terkait Sipeter untuk meminimalisir risiko kehilangan data, kebocoran dan penyalahgunaan informasi, serta kekacauan internal yang merugikan bisnis PT. XYZ.
Kata kunci: *Keamanan; Sistem Informasi; Perdagangan; Standar ISO 27002*

1. Pendahuluan

Teknologi Informasi memiliki peranan penting dalam mendukung kesuksesan bisnis di era digital saat ini. Informasi merupakan aset yang sangat berharga bagi perusahaan bisnis, dimana pertukaran data dan informasi berlangsung dengan mudah dan cepat sehingga menimbulkan ancaman terhadap keamanan informasi [1]. Hal ini berkaitan meningkatnya transmisi data internal maupun eksternal antar perusahaan melalui jaringan komputer mengakibatkan risiko informasi perusahaan terbaca pihak luar. Apabila informasi rahasia perusahaan tersebar luas dan disalahgunakan dapat menimbulkan risiko kerugian bagi bisnis perusahaan. Namun masalah yang berkaitan dengan keamanan informasi masih kurang mendapat perhatian dari manajemen perusahaan, padahal merupakan hal penting dari sistem informasi yang diterapkan perusahaan [2]. Mengingat pentingnya masalah keamanan siber, Indonesia bahkan telah membentuk lembaga khusus yang bernama *Security Incident Response*

Team on Internet Infrastructure/Coordination Center (IDSIRTII/CC) untuk mengatasi keamanan internet. IDSIRTII melaporkan pada tahun 2021, Indonesia mengalami 1.637.973.022 anomali trafik dimana anomali tertinggi terjadi pada Desember 2021 sebanyak 242.066.168 anomali [3]. Tingginya angka serangan memberi peringatan kepada perusahaan yang menerapkan TI untuk memperhatikan masalah keamanan informasi. Hal ini penting mengingat tujuan keamanan informasi untuk melindungi informasi dan aset informasi dengan menjaga kerahasiaan (*Confidentiality*), keutuhan (*Integrity*) dan ketersediaan (*Availability*) dari Informasi [4]. Melindungi informasi dari berbagai ancaman menjadi tanggung jawab dan upaya seluruh anggota organisasi [5] bertujuan menjamin kelangsungan bisnis, meminimalkan kerusakan akibat ancaman, dan mempercepat pengembalian investasi dan peluang bisnis [6].

Objek penelitian dalam studi ini adalah PT. XYZ, perusahaan swasta nasional yang bergerak di bidang pengadaan perlengkapan dan peralatan pendukung industri. Seiring meningkatnya volume dan luas wilayah usaha dengan cabang perusahaan serta jenis dan jumlah produk yang semakin bertambah maka PT. XYZ sudah menerapkan teknologi informasi meliputi pengelolaan inventori, data pelanggan, dan data supplier, serta berbagai transaksi, pelaporan dan analisa keuangan dalam operasional yang terintegrasi yang disebut Sistem Informasi Perdagangan Terintegrasi yang dikenal di PT. XYZ dengan sebutan Sipeter. Mengingat perkembangan bisnis PT. XYZ yang semakin maju, maka pengembangan Sipeter terus dilakukan yang saat ini telah memiliki 8 buah *server*. Permasalahan yang dihadapi selama penerapan Sipeter yaitu terjadinya kebocoran informasi pada karyawan yang tidak berhak atas informasi tersebut. Hal ini tentu menjadi masalah serius karena menyangkut kerahasiaan data yang dapat merugikan PT. XYZ dalam persaingan dengan para kompetitornya. Permasalahan lain adalah sistem yang sering *hang* dan hilangnya data akibat terjadinya kerusakan perangkat Sipeter. Kejadian ini mengakibatkan Sipeter gagal memenuhi ketersediaan data dan informasi kepada pengguna sewaktu dibutuhkan. Permasalahan lain adalah semakin sering muncul gangguan yang menyebabkan kerusakan data yang menyebabkan ketidakutuhan data saat diakses pengguna. Permasalahan ini sejalan dengan pernyataan [7] bahwa semakin banyak informasi perusahaan yang disimpan, dikelola dan di-*sharing*-kan maka semakin besar pula risiko terjadi kerusakan, kehilangan atau terbukanya data ke pihak-pihak yang tidak diinginkan. Menilik permasalahan yang terjadi ada pada aspek kerahasiaan, keutuhan, dan ketersediaan data dan informasi dari Sipeter, jelas hal ini menyangkut keamanan informasi. Namun sampai sejauh ini PT. XYZ belum pernah melakukan evaluasi dan analisis keamanan informasi Sipeter tidak memiliki gambaran utuh tentang keamanan informasi Sipeter yang telah digunakan selama ini. Berdasarkan permasalahan yang dijabarkan tersebut terkait kerahasiaan, keutuhan, dan ketersediaan data dan infomasi, maka dibutuhkan analisis keamanan informasi pada Sipeter yang diterapkan PT. XYZ. untuk mengetahui sejauhmana keamanan informasi Sipeter agar dapat memenuhi aspek kerahasiaan (*confidentiality*) dengan melindungi data dan informasi dari pengaksesan orang yang tidak berhak, keutuhan (*integrity*) dengan menjaga keutuhan data dan informasi perusahaan, serta ketersediaan (*availibility*) data dan informasi perusahaan pada saat dibutuhkan [4], [7] demi kelangsungan bisnis PT. XYZ di masa mendatang [6].

Penelitian analisis keamanan informasi Sipeter ini menggunakan standar ISO 27002 kontrol keamanan TI agar analisis keamanan informasi dapat berjalan dengan baik. Pertimbangan penggunaan standar ISO 27002 dalam penelitian ini adalah standar ini memiliki fleksibelilitas untuk dikembangkan sesuai kebutuhan dan tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah karyawan serta ukuran struktur organisasi [7]. Hal ini sesuai pernyataan [8] bahwa perusahaan dapat menggunakan standar sesuai dengan kebutuhan karena secara formal tidak ada acuan baku mengenai standar yang digunakan perusahaan. Pertimbangan lain digunakannya ISO 27002 karena tersedianya sertifikat implementasi yang diakui internasional yaitu *Information Security Management Sistem certification*. Hal ini juga sejalan dengan PT. XYZ yang selama ini telah menerapkan standar manajemen mutu ISO 9001:2015. Dalam penelitian ini dilakukan penilaian *maturity level* menggunakan *Capability Maturity Model Integration* (CMMI) [9] untuk mengetahui tingkat kedewasaan dari Sipeter.

Penelitian ini bertujuan menganalisis keamanan sistem informasi perdagangan terintegrasi atau Sipeter di PT. XYZ menggunakan standar ISO 27002 untuk mengetahui tingkat keamanan informasi Sipeter agar dapat memenuhi aspek kerahasiaan, keutuhan dan ketersediaan data dan informasi dalam menunjang kelancaran operasional dan mendukung pengambilan keputusan manajemen perusahaan. Hasil penelitian dapat dijadikan pedoman

peningkatan keamanan Sipeter yang terus dikembangkan seiring dengan perkembangan bisnis perusahaan yang semakin maju.

2. Tinjauan Pustaka

Sejumlah penelitian terlalu yang berkaitan dengan analisis maupun audit keamanan informasi dengan standar ISO 27002 yang telah dilakukan banyak peneliti dijelaskan sebagai berikut.

Penelitian dengan judul *Evaluasi Keamanan Informasi Menggunakan ISO/IEC 27002: Studi Kasus Pada STMIK Tunas Bangsa Banjarnegara* oleh [10]. Penelitian ini bertujuan menganalisis keamanan informasi menggunakan ISO/IEC 27002 terkait penerapan Sistem Informasi Akademik di STMIK Tunas Bangsa Banjarnegara untuk memperoleh nilai *maturity level* dan memberikan rekomendasi perbaikan yang perlu dilakukan untuk meningkatkan keamanan informasi. Hasil penelitian menunjukkan STMIK Tunas Bangsa Banjarnegara memiliki *maturity level* sebesar 2,6 yang berarti telah melakukan pengelolaan informasi tetap belum terdefinisi dan terdokumentasi. Hasil penelitian juga menemukan bahwa institusi belum memiliki pedoman organisasi pengelolaan informasi dimana saat ini hanya memiliki pedoman di pengelola informasi. Rekomendasi yang diberikan adalah perlu perbaikan untuk memastikan keamanan informasi.

Selanjutnya penelitian tentang Audit Keamanan Sistem Informasi Manajemen Akademik (SIMAK) di Fakultas Ekonomi Universitas Udayana (FE UNUD) yang dilakukan oleh [11]. Penelitian ini bertujuan untuk menganalisis kesenjangan *maturity level* saat ini (*as-is*) dengan yang diharapkan (*to-be*). Hasil penelitian ini menunjukkan bahwa SIMAK FE UNUD berada pada *maturity level* 3 atau *Well Defined* yang berarti sudah terdapat prosedur yang standar dan telah didefinisikan secara baik.

Pada studi yang dilakukan oleh [12] dengan judul *Analisis Sistem Keamanan Informasi Menggunakan ISO/IEC 27001:2013 Pada Pemerintahan Daerah Kota Sukabumi (Studi Kasus: Di Diskominfo Kota Sukabumi)*. Penelitian ini bertujuan menganalisis sistem manajemen keamanan informasi menggunakan ISO/IEC 27001:2013 di Diskominfo untuk mengetahui ancaman keamanan informasi; mengetahui gap kinerja keamanan informasi; menghasilkan dokumen manual, instruksi kerja, prosedur dan formulir; dan pengukuran *capability maturit model integration* (CMMI). Hasil studi menunjukkan objek penelitian telah mengatur dan melaksanakan keamanan inormasi terhadap aset namun belum didokumentasikan dengan rata-rata *maturity level* 2.00. Temuan lain studi ini adalah terdapat 25 profil risiko dengan 1 risiko sangat tinggi, 1 risiko tinggi, 6 risiko sedang, dan 17 tingkat risiko rendah.

Penelitian berikutnya berjudul Keamanan Infomasi (*Information Security*) Pada Aplikasi Perpustakaan iPUSNAS [13]. Penelitian ini bertujuan untuk mengukur mengetahui keamanan informasi pada aplikasi iPusnas milih Perpustakaan nasional Republik Indonesia. Hasil analisis pada penelitian menunjukkan bahwa Aplikasi iPusnas sudah menjamin kerahasisaan data pribadi pengguna dan data koleksi yang dipinjam pengguna. Aplikasi iPusnas memiliki kebijakan lisensi dimana setiap pengguna harus registrasi untuk memperoleh akun dan diharuskan *log in* untuk mengakses iPusnas yang menyatakan pengguna menyetujui semua ketentuan yang berlaku.

Penelitian selanjutnya dilakukan oleh [14] dengan judul Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standar ISO 27002:2013 Menggunakan SSE-CMM. Penelitian ini bertujuan untuk untuk mengukur keamanan informasi pada sistem informasi akademik secara akurat dan meningkatkan kualitas keamanan informasi sesuai dengan standar ISO 27002 serta mengetahui *maturity level* sistem keamanan yang digunakan dalam sistem informasi akademik sehingga dapat dijadikan bahan pertimbangan dalam mempersiapkan perbaikan sistem manajemen keamanan informasi. Kesimpulan dari hasil analisis keamanan informasi pada penelitian ini adalah nilai 2.51 atau level Define yang berarti mekanisme perencanaan pengadaan barang kebutuhan TI memiliki prosedur dan telah didokumentasikan serta dikomunikasikan melalui pelatihan. Namun perencanaan anggaran, mekanisme pengembangan infrastuktur teknologi informasi dan menjaga hubungan kinerja vendor masih perlu ditingkatkan. Demikian pula prosedur yang digunakan belum sesuai standar.

Penelitian [15] dengan judul Audit Keamanan Informasi Menggunakan ISO 27002 Pada Data Center PT. Gigi Patra Multimedia untuk mengukur tingkat keamanan PT. Giga Patra Multimedia, mengetahui kelemahan sistem, dan memberikan rekomendasi perbaikan dalam meningkatkan keamanan informasi perusahaan. Penelitian ini menghasilkan pengukuran keamanan informasi pada klausul 7 sampai 12 dari standar ISO 27002. Temuan lain dari hasil

penelitian adalah *maturity level* pada level 2 (*limited/repeatable*) dan berbagai kelemahan yang menyebabkan kerentanan terhadap ancaman keamanan informasi.

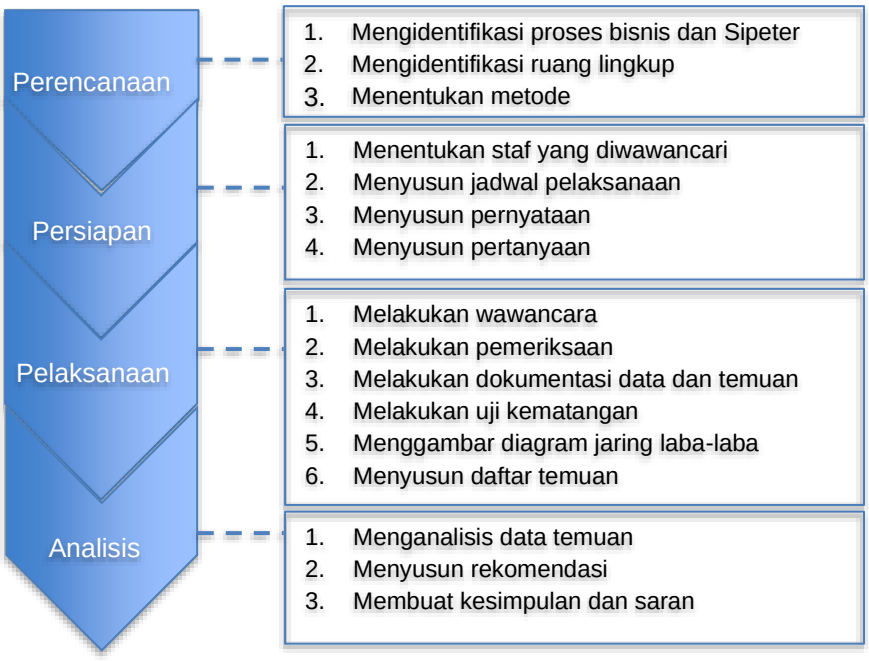
Penelitian terakhir yang dibahas adalah penelitian yang dilakukan oleh [16] dengan judul Implementasi Awal Sistem Manajemen Keamanan Informasi pada UKM Menggunakan Kontrol ISO/IEC 27002. Tujuan penelitian ini adalah melakukan implementasi awal sistem manajemen keamanan informasi pada UKM yang bergerak di bidang *engineering services* menggunakan kontrol pada ISO/IEC 27002. Hasil penelitian membuktikan bahwa perusahaan memiliki risiko keamanan tingkat sedang (*medium*). Rekomendasi prioritas program perbaikan adalah penyusunan kebijakan dan prosedur, kemudian peningkatan kesadaran keamanan informasi di kalangan manajemen dan karyawan.

Penelitian ini memiliki perbedaan dengan penelitian sebelumnya, yaitu pada objek penelitian di perusahaan swasta nasional PT. XYZ yang bergerak dibidang pengadaan perlengkapan dan peralatan pendukung industri. Selain itu pada penelitian ini menerapkan standar ISO 27002 untuk mengukur dan menganalisis keamanan informasi Sipeter dengan klausul, objektif kontrol dan kontrol keamanan yang berbeda sesuai hasil identifikasi kebutuhan PT. XYZ. Penelitian ini bertujuan menganalisis keamanan informasi Sipeter berdasarkan standar ISO 27002 untuk menemukan berbagai kelemahan pada Sipeter sehingga dapat memberi rekomendasi perbaikan guna menjamin keamanan informasi pada Sipeter. Dengan demikian hasil penelitian ini dapat menjadi pedoman bagi manajemen PT. XYZ memutuskan prioritas dan perbaikan serta pengembangan Sipeter di masa mendatang.

3. Metodologi

3.1. Tahapan Penelitian

Tahapan proses yang dilakukan dalam penelitian ini terdiri dari empat tahapan utama [4], yaitu: perencanaan, persiapan, pelaksanaan, dan analisis keamanan informasi Sipeter. Masing-masing tahapan utama tersebut memiliki sub tahapan proses yang dapat dilihat selengkapnya pada Gambar 1.



Gambar 1. Tahapan dan Sub Tahapan Penelitian

3.2. Identifikasi Ruang Lingkup

Pada tahapan identifikasi ruang lingkup diperoleh pemetaan klausul, objektif kontrol, dan kontrol keamanan yang telah disampaikan dan disepakati pimpinan PT. XYZ. Berdasarkan hasil identitifikasi melalui observasi lapangan dan interview, maka ditetapkan 7 klausul yang digunakan

dalam penelitian ini yang disajikan selengkapnya beserta objektif kontrol pada Tabel 2. Sedangkan klausul yang tidak digunakan sejumlah 7 klausul yang disajikan pada Tabel 3.

Tabel 2. Klausul Yang Digunakan Dalam Penelitian

Klausul	Objektif Kontrol	Kontrol Keamanan
8: Kemanan sumber daya Manusia (SDM)	8.1 Kemanan SDM sebelum menjadi karyawan	Aturan dan tanggung jawab; Seleksi; Persyaratan dan kondisi yang wajib dipenuhi karyawan.
	8.2 Saat menjadi karyawan	Tanggung jawab manajemen; Pendidikan dan Pelatihan keamanan informasi; Proses kedisiplinan
	8.3 Pemberhentian dan pemindahan karyawan	Tanggung jawab pemberhentian; Pengembalian aset; Penghapusan hak ases.
9: Keamanan fisik dan lingkungan	9.1 Keamanan wilayah	Pembatas keamanan fisik; Kontrol masuk fisik; Keamanan ruang dan fasilitas; Perlindungan serangan luar dan ancaman lingkungan sekitar; Wilayah aman; Akses publik dan area pengiriman dan penurunan barang.
	9.2 Keamanan peralatan	Penempatan peralatan dan perlindungannya; Utillitas pendukung; Keamanan pengkabelan; Pemeliharaan peralatan; Keamanan peralatan di luar tempat kerja; Keamanan pembuangan peralatan; Hak pemindahan peralatan
10: Manajemen komunikasi dan operasi	10.1 Prosedur dan tanggung jawab operasi	Dokumentasi prosedur operasi; Manajemen pertukaran; Pemisahan tugas; Pemisahan pengembangan, pengujian dan operasi fasilitas
	10.3 Perencanaan dan penerimaan sistem	Manajemen kapasitas; Penerimaan sistem
	10.4 Perlindungan terhdp *malicious* dan *mobile code*	Kontrol terhadap kode bahaya.
	10.5 *Back up*	*Back up* sistem inforamsi
	10.7 Penanganan media	Manajemen pemindahan media; Pemusanahan media; Prosedur penanganan informasi; Keamanan dokumen informasi
	10.8 Pertukaran informasi	Kebijakan dan prosedur pertukaran informasi; Pesan elektronik; Sistem informasi bisnis
	10.10 Monitoring	Rekaman audit; Monitoring penggunaan sistem; Proteksi catatan informasi; Catatan administrator dan operator; Catatan kesalahan; Sinkronisasi waktu
11: Kontrol akses	11.1 Persyaratan bisnis untuk kontrol akses	Kebijakan kontrol akses
	11.2 Manajemen akses *user*	Registrasi pengguna; Manajemen hak khusus; Manajemen *passwod user*; Tinjauan hak akses *user*;
	11.3 Tanggung jawab pengguna	Penggunaan *password*; Penjagaan peralatan penguna; Kebijakan *clear desk* dan *clear screen*;
	11.4 Kontrol akses jaringa	Kebijakan penggunaan layanan jaringan; Otentifikasi pengguna layanan jaringan dan koneksi keluar; Pemisahan jaringan, Kontrok koneksi jaringan; Kontrol *routing* jaringan
	11.5 Kontrol akses sistem operasi	Prosedur log-on; Identifikasi dan otentifikasi *user*; Sistem manajemen *password*; Penggunaan utilitas sistem; Sesi *time-out*; Batasan wakt koneksi
	11.6 Kontrol akses informasi dan aplikasi	Pembatasan akses informasi; Isolasi sistem yang sensitif
	11.7 Komputasi *mobile* dan *teleworking*	Komunikasi dan komputerisasi *mobile*
12: Akuisisi SI, pengembangan dan pemeliharaan	12.1 Persyaratan keamanan sistem informasi (SI)	Analisis dan spesifikasi persyaratan keamanan.
	12.2 Pemrosesan yang benar dalam aplikasi	Validasi data input; Kontrol pemrosesan internal; Validasi data ouput.
	12.5 Keamanan dlm pembangunan dan proses pendukung	Kontrol prosedur tambahan; Pembatasan perubahan paket *software*; Kelemahan informasi.
	12.6 Manajemen kelemahan secara teknis	Kontrol kelemahan secara teknis (*vurnerability*).
13: Manajemen kejadian keamanan informasi	13.1 Pelaporan kejadian & kelemahan keamanan inf.	Pelaporan kejadian keamanan informasi; Pelaporan kelemahan keamanan informasi.
	13.2 Manajemen kejadian keamanan informasi dan pengembangannya	Tanggung jawab dan prosedur; Pembelajaran kejadian keamanan informasi; Pengumpulan bukti

Klausul	Objektif Kontrol	Kontrol Keamanan
14: Manajemen kelangsungan bisnis	14.1 Aspek keamanan informasi dalam kelangsungan bisnis	Keamanan informasi proses manajemen; Kelang- sungan bisnis dan penilaian risiko; Pembangunan dan implemen- tasi keamaan inf. dlm kelangsungan bisnis; Kerangka kerja rencana kelangsung bisnis; Pengujian, pemeliharaan, dan pengkajian ulang rencana kelangsungan bisnis.

Tabel 3. Klausul Yang Tidak Digunakan

Klausul	Kontrol Keamanan	Keterangan
5: Kebijakan keamanan	Seluruh kontrol keamanan	Tidak memiliki kebijakan keamanan informasi
6: Organisasi keamanan informasi	Seluruh kontrol keamanan	Tidak ada pengaturan penanganan keamanan informasi.
7: Manajemen aset	Seluruh kontrol keamanan	Tidak diijinkan analisis keamanan aset perusahaan
10: Manajemen komunikasi dan operasi	Seluruh kontrol keamanan	Tidak menggunakan layanan oleh pihak ketiga
11: Kontrol akses	Seluruh kontrol keamanan	Tidak diijinkan analisis keamanan peralatan jaringan
12: Akuisisi sistem informasi pembangunan dan pemeliharaan	Seluruh kontrol keamanan	Tidak diijinkan analisis bagian tersebut
15: Kepatuhan	Seluruh kontrol keamanan	Perusahaan belum melakukan uji kepatutan.

3.3. Penentuan Bagian Yang Diwawancara

Untuk memperoleh hasil analisis yang akurat maka dibutuhkan wawancara dan observasi pada bagian yang bertanggungjawab sesuai klausul yang dianalisis [17]. Hasil penentuan bagian yang diwawancara selengkapnya ditampilkan pada Tabel 4.

Tabel 4. Bagian Yang Diwawancari Berdasarkan Klausul

Klausul	Deskripsi	Bagian
8	Keamanan sumber daya manusia	Sumber Daya Manusia
9	Keamanan fisik dan lingkungan	Teknologi Informasi
10	Manajemen komunikasi dan operasi	Teknologi Informasi
11	Kontrol akses	Teknologi Informasi
12	Akuisisi sistem informasi, pengembangan, dan pemeliharaan	Teknologi Informasi
13	Manajemen kejadian keamanan informasi	Teknologi Informasi
14	Manajemen kelangsungan bisnis	Teknologi Informasi

3.4. Perhitungan Maturity Level

Perhitungan *maturity level* dilakukan setelah melakukan tahapan pemeriksaan dan pendokumentasian bukti-bukti hasil analisis Sipeter. Setiap pernyataan dinilai tingkat kepatutannya sesuai hasil pemeriksaan menggunakan kriteria penilaian pada standar penilaian *maturity level* yang terdiri dari lima tingkatan proses rangkaian *maturity level* berdasarkan metode CMMI. Pendekatan CMMI digunakan sebagai pedoman perbandingan dan alat bantu untuk memahami tingkatan proses, praktik pada perusahaan [18]. Lima tingkatan kerangka CMMI, yaitu: a. Level 0 (*non-existent*), artinya tidak ada kontrol sama sekali; b. Level 1 (*initial*), artinya perusahaan memiliki pendekatan tidak konsisten, pelaksaaan kontrol keamanan masih informal (tidak ada standar dan dokumentasi); c. Level 2 (*limited/repeatable*), artinya kontrol keamanan masih taraf pengembangan dan dokumentasi masih terbatas sesuai kebutuhan; d. Level 3 (*defined*), artinya kontrol keamanan sudah didokumentasikan secara rinci dan disosialisasikan melalui pelatihan, namun belum dilakukan pengukuran tingkat kepatuhan; e. Level 4 (*managed*), artinya pengukuran efektivitas kontrol keamanan telah dilakukan namun tanpa bukti dari pengukuran kepatuhan dimana kontrol membutuhkan perbaikan untuk mencapai tingkat kepatuhan yang diharapkan; dan f. Level 5 (*optimized*), artinya kontrol keamanan sudah sesuai

dengan ISO 27002 yang menunjukkan adanya kepemimpinan yang efektif, manajemen perubahan, perbaikan berkelanjutan, dan terjalinnya komunikasi internal. Nilai *maturity level* pada setiap kontrol keamanan dari masing-masing klausul [19] dihitung menggunakan rumus berikut.

$$\textit{Maturity level} = \frac{\text{Total nilai}}{\text{Jumlah nilai}}$$

4. Hasil dan Pembahasan

4.1. Hasil Pengukuran Maturity Level

Pengukuran *maturity level* pada setiap kontrol keamanan pada masing-masing klausul menghasilkan *maturity level* yang selengkapnya ditunjukkan pada Tabel 5.

Tabel 5. Maturity Level Klausul Penelitian

Klausul	Objektif Kontrol	Kontrol Keamanan	Maturity Level	Rata-Rata
8: Kemanan sumber daya manusia (SDM)	8.1 Sebelum menjadi karyawan	Aturan dan tanggung jawab	3.29	3.72
		Seleksi	4.55	
		Persyaratan dan kondisi yg wajib dipenuhi	3.33	
	8.2 Saat menjadi karyawan	Tanggung jawab manajemen	1.67	1.89
		Pendidikan dan Pelatihan keamanan informasi	0.00	
		Proses kedisiplinan	4.00	
	8.3 Pemberhenti-an dan pemindah-an karyawan	Tanggung jawab pemberhentian	5.00	3.33
		Pengembalian aset	5.00	
		Penghapusan hak ases	0.00	
		Maturity level klausul 8 =		**2.98**
9: Keamanan fisik dan lingkungan	9.1 Keamanan wilayah	Pembatas keamanan fisik	3.00	3.18
		Kontrol masuk fisik	1.22	
		Keamanan ruang dan fasilitas	2.94	
		Perlindungan serangan luar dan ancaman lingkungan sekitar	3.56	
		Wilayah aman	3.33	
		Akses publik dan area pengiriman dan penurunan barang.	5.00	
	9.2 Keamanan peralatan	Penempatan peralatan dan perlindungannya;	5.00	2.38
		Utillitas pendukung;	2.22	
		Keamanan pengkabelan;	0.71	
		Pemeliharaan peralatan;	1.00	
		Keamanan peralatan di luar tempat kerja;	5.00	
		Keamanan pembuangan peralatan;	1.50	
		Hak pemindahan peralatan	1.25	
		Maturity level klausul 9 =		**2.78**
10: Manaje-men komuni-kasi dan operasi	10.1 Prosedur dan tanggung jawab operasi	Dokumentasi prosedur operasi	1.78	2.43
		Manajemen pertukaran	1.91	
		Pemisahan tugas	4.14	
		Pemisahan pengembangan, pengujian dan operasi fasilitas	1.89	
	10.3 Perencanaan dan penerimaan sistem	Manajemen kapasitas	0.86	0.59
		Penerimaan sistem	0.47	
	10.4 Perlindungan terhdp *malicious* dan *mobile code*	Kontrol terhadap kode bahaya	2.85	2.85
	10.5 *Back up*	*Back up* sistem inforamsi	2.69	2.69
	10.7 Penanganan media	Manajemen pemindahan media	0.00	1.97
		Pemusanahan media	2.25	
		Prosedur penanganan informasi	2.62	
		Keamanan dokumen informasi	3.00	
	10.8 Pertukaran informasi	Kebijakan dan prosedur pertukaran informasi	2.50	1.72
		Pesan elektronik	1.67	
		Sistem informasi bisnis	1.00	
	10.10 Monitoring	Rekaman audit	0.00	0.51
		Monitoring penggunaan sistem	0.05	
		Proteksi catatan informasi	1.00	
		Catatan administrator dan operator	0.00	
		Catatan kesalahan	0.00	
		Sinkronisasi waktu	2.00	
		Maturity level klausul 10 =		**1.46**

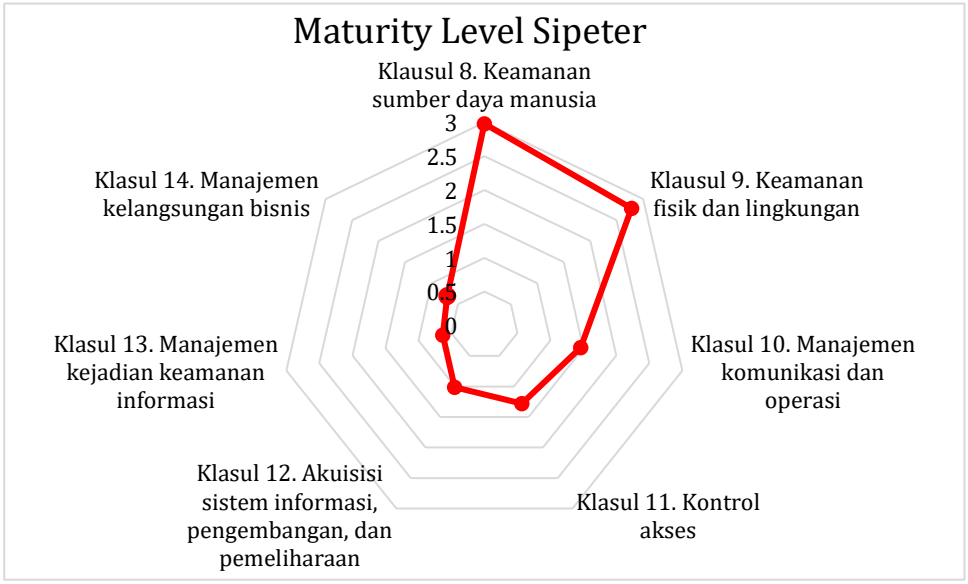
Klausul	Objektif Kontrol	Kontrol Keamanan	Maturity Level	Rata-Rata
11: Kontrol akses	11.1 Persyaratan bisnis untuk kontrol akses	Kebijakan kontrol akses	1.91	1.91
	11.2 Manajemen akses *user*	Registrasi pengguna	1.07	0.67
		Manajemen hak khusus	1.00	
		Manajemen *passwod user*	0.60	
		Tinjauan hak akses *user*	0.00	
	11.3 Tanggung jawab pengguna	Penggunaan *password*	0.78	1.51
		Penjagaan peralatan penguna	2.00	
		Kebijakan *clear desk* dan *clear screen*	1.75	
	11.4 Kontrol akses jaringan	Kebijakan penggunaan layanan jaringan;	0.40	0.08
		Otentifikasi pengguna layanan jaringan dan koneksi keluar;	0.00	
		Pemisahan jaringan,	0.00	
		Kontrok koneksi jaringan;	0.00	
		Kontrol *routing* jaringan	0.00	
	11.5 Kontrol akses sistem operasi	Prosedur log-on	1.43	1.58
		Identifikasi dan otentifikasi *user*	3.00	
		Sistem manajemen *password*	2.56	
		Penggunaan utilitas sistem	0.43	
		Sesi *time-out*	1.29	
		Batasan wakt koneksi	0.75	
	11.6 Kontrol akses inf. dan aplikasi	Pembatasan akses informasi	2.92	2.21
		Isolasi sistem yang sensitif	1.50	
	11.7 Komputasi *mobile* & telework.	Komunikasi dan komputerisasi *mobile*	1.00	1.00
		Maturity level klausul 11 =		**1.28**
12: Akuisisi SI, pengembangan dan *maintenance*	12.1 Persyaratan keamanan SI	Analisis dan spesifikasi persyaratan keamanan.	0.00	0.00
	12.2 Pemrosesan aplikasi yang benar	Validasi data input	3.00	3.16
		Kontrol pemrosesan internal	3.33	
		Validasi data ouput	2.83	
	12.5 Keamanan dlm pembang. dan proses pendukung	Kontrol prosedur tambahan;	0.00	0.89
		Pematasan perubahan paket *software*	2.67	
		Kelemahan informasi.	0.00	
	12.6 Manajemen kelemahan teknis	Kontrol kelemahan secara teknis (vurnerability).	0.00	0.00
		Maturity level klausul 12 =		**1.01**
13: Manaj. kejadian keamanan inf.	13.1 Pelaporan kejadian dan kelemahan keaman inf	Pelaporan kejadian keamanan informasi	0.50	0.59
		Pelaporan kelemahan keamanan	0.67	
	13.2 Manajemen kejadian keamanan inf. & pengembangannya	Tanggung jawab dan prosedur	0.50	0.67
		Pembelajaran kejadian keamanan informasi	1.00	
		Pengumpulan bukti	0.50	
		Maturity level klausul 13 =		**0.63**
14: Manajemen kelangsungan bisnis	14.1 Aspek keamanan inf. dlm kelangsungan bisnis	Keamanan informasi proses manajemen;	1.00	0.70
		Kelangsungan bisnis dan penilaian risiko	1.17	
		Pembangunan dan implementasi keamaan inf. dalam kelangsungan bisnis	0.58	
		Kerangka kerja rencana kelangsung bisnis	0.36	
		Pengujian, pemeliharaan, dan pengkajian ulang rencana kelangsungan bisnis	0.40	
		Maturity level klausul 14 =		**0.70**

Rekapitulasi dari *maturity level* ketujuh klausul yang digunakan dalam menganalisis keamanan informasi Sipeter dalam penelitian ini ditunjukkan pada Tabel 6 dan digambarkan dalam jaring *maturity level* Sipeter seperti tampak pada Gambar 2. Hasil rekapitulasi *maturity level* pada Tabel 6 menunjukkan klausul 8 tentang keamanan sumber daya manusia memiliki *maturity level* tertinggi sebesar 2.98 (*Limited/repeatable*) yang menunjukkan bahwa proses keamanan SDM masih dalam pengembangan dengan dokumentasi yang terbatas. Hal ini dapat dibuktikan dengan beberapa prosedur yang belum terdokumentasi dan banyak kontrol yang

belum dilaksanakan seperti pemeriksaan referensi dan kelayakan karakter, serta belum ada pelatihan keamanan informasi kepada karyawan.

Tabel 6. Rekapitulasi Maturity Level Tujuh Klausul Yang Ditetapkan

Klausul	Deskripsi	Maturity Level	Keterangan
8	Keamanan sumber daya manusia	2.98	Limited/repeatable
9	Keamanan fisik dan lingkungan	2.78	Limited/repeatable
10	Manajemen komunikasi dan operasi	1.46	Initial
11	Kontrol akses	1.28	Initial
12	Akuisisi SI, pengembangan, dan pemeliharaan	1.01	Initial
13	Manajemen kejadian keamanan informasi	0.63	Non-existent
14	Manajemen kelangsungan bisnis	0.70	Non-existent
	Maturity Level Rata-Rata	**1.55**	**Initial**



Gambar 2. Jaring Maturity Level Sipeter

Klausul 9 tentang keamanan fisik dan lingkungan memiliki maturity level tertinggi kedua sebesar 2.78 (*Limited/repeatable*) yang artinya proses keamanan fisik dan lingkungan sekitar masih dalam pengembangan dengan dokumentasi terbatas. Hal ini dibuktikan dengan belum terdokumentasinya beberapa prosedur dan banyak kontrol yang belum dilaksanakan seperti pemasangan tanda bahaya, *log* kedatangan dan kepergian pengunjung, terabaikannya pemeliharaan peralatan, tidak adanya catatan peminjaman peralatan.

Hasil pengukuran juga menunjukkan bahwa klausul 10, 11, dan klausul 12 berada pada *maturity level Initial* yang berarti bahwa proses manajemen komunikasi dan operasi (klausul 10), kontrol akses (klausul 11), akuisisi SI, pengembangan dan pemeliharaan (klausul 12) dilaksanakan secara tidak konsisten dan informal. Hal tersebut berbagai bukti kelemahan pada ketiga klausul tersebut, antara lain: belum dilaksanakannya beberapa kontrol pada klausul 10 yaitu pemisahan pengujian sistem, tidak adanya *back up* di luar perusahaan, tidak adanya pencatatan informasi dan kontrol audit trail. Klausul 11 memiliki kelemahan seperti tidak adanya pernyataan resmi perusahaan untuk menjaga *password*, tidak adanya tinjauan terhadap hak akses *user*, dan masih banyak kebijakan dilakukan secara informal, antara lain kebijakan dan otorisasi terhadap keamanan informasi, persyaratan bisnis kontrol akses, serta persyaratan keamanan. Sedangkan temuan pada klausul 12 seperti adanya modifikasi pada *software* telah diuji namun tidak dilakukan oleh badan yang independen.

Hasil pengukuran menunjukkan *maturity level* terendah pada klausul 13 sebesar 0.63, selanjutnya maturity level klausul 14 sebesar 0.70 yang berarti berada pada tingkat Non-existent. Artinya perusahaan belum memiliki kontrol keamaan pada proses manajemen kejadian keamanan informasi (klausul 13) dan manajemen kelangsungan bisnis (klausul 14). Secara keseluruhan ditemukan kelemahan yang sama yaitu belum adanya dokumentasi prosedur-prosedur di semua klausul yang telah dianalisis dalam penelitian ini.

Secara keseluruhan hasil perhitungan pada Tabel 6 menunjukkan *maturity level* Sipeter sebesar 1.55 atau level 1 yaitu initial yang artinya pendekatan yang dilakukan PT. XYZ terhadap keamanan Sipeter tidak konsisten dan kontrol keamanan masih dilakukan secara informal yang artinya tidak memiliki standar yang jadi pedoman dan tidak ada proses atau kejadian-kejadian terkait keamanan Sipeter yang terdokumentasi dengan baik dan rapi. Perusahaan bahkan tidak memiliki kontrol sama sekali pada manajemen kejadian keamanan informasi (klausul 13) dan manajemen kelangsungan bisnis (klausul 14) yang ditunjukkan dengan *maturity level non-existent*.

Hasil temuan pada penelitian ini mendukung temuan pada penelitian oleh [10] dan [14] dimana perusahaan belum memiliki standar atau pedoman pengelolaan informasi memiliki *maturity level* rendah sehingga membutuhkan perbaikan-perbaikan untuk memastikan keamanan informasi. Hal ini juga mendukung penelitian [11], [20], dan [21] yang membuktikan bahwa perusahaan yang telah menerapkan standar dengan prosedur yang terdefinisikan dengan baik memperoleh pengukuran *maturity level* lebih tinggi atau sama dengan level 3 (*defined*). Hal ini didukung [16] yang dalam penelitiannya memberikan rekomendasi penyusunan kebijakan dan prosedur sebagai prioritas perbaikan untuk meminimalisir risiko keamanan sistem informasi serta didukung [22] yang menyatakan keamanan informasi penting untuk meminimalisir risiko bisnis dan ancaman kelangsungan bisnis perusahaan. Temuan terkait kerentanan kebocoran informasi dalam penelitian ini didukung temuan penelitian [13] untuk meningkatkan keamanan sistem informasi dalam hal akses pengguna dan penelitian [16] dalam peningkatan kesadaran keamanan informasi di tingkatan manajemen dan karyawan. Temuan lain tentang belum terdokumentasinya prosedur di semua klausul dalam penelitian ini sejalan dengan hasil penelitian [10] dan [12] yang menunjukkan *maturity level* lebih rendah dari level 3 (*defined*) dengan didukung temuan penelitian [15], [16] dan [22] terkait berbagai kelemahan yang terjadi dapat menyebabkan kerentanan terhadap ancaman keamanan informasi.

5. Simpulan

Kesimpulan yang dapat diambil dari hasil penelitian ini adalah analisis keamanan Sipeter menggunakan standar ISO 27002 di PT. XYZ telah berjalan dengan sesuai tahapan penelitian. Hasil penelitian menunjukkan m*aturity level* Sipeter sebesar 1.55 atau level *Initial* yang menunjukkan PT. XYZ tidak konsisten dalam memanaj keamanan Sipeter, tidak memiliki standar keamanan sistem informasi, dan tidak melakukan dokumentasi berbagai kejadian keamanan Sipeter. Berbagai temuan pada hasil penelitian juga menunjukkan banyaknya kelemahan aturan dan prosedur keamanan sistem informasi yang rentan terhadap berbagai ancaman keamanan informasi dengan berbagai risiko antara lain kehilangan data, kebocoran informasi dan penyalahgunaan informasi, serta kekacauan internal yang pada akhirnya merugikan kelangsungan bisnis PT. XYZ. Berdasarkan hasil temuan dalam penelitian ini diketahui keamanan informasi Sipeter sangat rentan yang berisiko tidak dapat memenuhi aspek kerahasiaan, keutuhan, dan ketersediaan data dan informasi perusahaan yang dapat merugikan kelangsungan bisnis PT. XYZ.

Rekomendasi yang dapat diberikan pada PT. XYZ adalah melakukan perbaikan manajemen keamanan SI, aturan, dan prosedur keamanan SI sesuai standar ISO 27002, dan meningkatkan kedisiplinan dalam mendokumentasikan kejadian keamanan Sipeter agar dapat meminimalisir atau meniadakan berbagai ancaman keamanan informasi. Setelah seluruh temuan kelemahan pada klausul 8 sampai dengan klausul 14 pada penelitian ini selesai diperbaiki, maka PT. XYZ dapat melaksanakan tata kelola keamanan sistem informasi dan melakukan analisis keamanan SI pada seluruh klausul dan kontrol keamanan yang terdapat pada standar ISO 27002.

Daftar Referensi

[1] D. M. Budiyanto, "Keamanan Informasi Tanggung Jawab Kita Bersama", Kementerian Keuangan Republik Indonesia, 27 Mei 2020. [Online]. https:// www.djkn.kemenkeu.go.id/ kpknl-singkawang/baca-artikel/13136/Keamanan-Informasi-Tanggung-Jawab-Kita-Bersama.html [Diakses pada 30 Agustus 2022].

[2] A. R. Tanaamah dan F. J. Indira, "Analysis of Information Technology Security Management SWCU SIASAT Using ISO/IEC 27001:2013", *International Journal of Innovative Technology and Exploring Engineering*, vol. 5, no. 2, pp. 68-74, 2021.

[3] ID-SIRTII. *Laporan Tahunan ID-SIRTII*. *Indonesia Security Incident Response Team on Internet and Infrastructure*, 2021.

[4] ISO/IEC. *Information Technology-Security Techniques-Code of Practice for Information Security Management ISO/IEC 17799 (27002):2005*. Switzerland, 2005.

[5] D. C. Islami, K. Bunga I. H., dan Candiwan, "Awareness Information Security Employees X Bank in Bandung Indonesia", *Journal of Informatics, Control Systems, and Computers*, vol. 10, no. 1, pp. 19-26, Mei 2016.

[6] H. F. Tipton and M. Krause. *Information Security Management Handbook*, London: CRC Press, 2010.

[7] R. Sarno dan I. Iffano. *Sistem Manajemen Keamanan Informasi*, Surabaya: ITS Press, 2009.

[8] Budi, Rahardjo. *Keamanan Sistem Informasi Berbasis Internet*. Bandung: PT. Insan Indonesia, 2005.

[9] A. Deswadi dan B. Hudaya, "Audit Pengembangan Perangkat Lunak Menggunakan Metode Capability Maturity Model Integration Level 3", *Jurnal Informatika*, vol. 7, no. 2, pp. 148-155, September 2020.

[10] F. Febrianto, dan D. I. Sensuse, "Evaluasi Keamanan Informasi Menggunakan ISO/IEC 27002: Studi Kasus Pada STMIK Tunas Bangsa Banjarnegara". *Jurnal Infokom,* vol. 13, no. 2, pp. 21-26, 2017.

[11] Y. C. N. Bless, G. M. A. Sasmita, dan A. A. K. A. Cahyawan, "Audit Keamanan SIMAK Berdasarkan ISO 27002 (Studi Kasus: FE UNUD)", *Menara Penelitian Akademika Teknologi Informasi*, vol. 2, no. 2, pp. 162-166, 2014.

[12] W. Apriandari, dan A. Sasongko, "Analisis Sistem Keamanan Informasi Menggunakan ISO/IEC 27001:2013 Pada Pemerintahan Daerah Kota Sukabumi (Studi Kasus: Di Diskominfo Kota Sukabumi)". *Jurnal Ilmiah Santika,* vol. 8, no. 1, pp. 715-729, 2018.

[13] A. P. Galih, "Keamanan Informasi (Information Security) Pada Aplikasi Perpustakaan iPusnas". *Jurnal Almaktabah,* vol. 5, no. 1, pp. 9-17, 2020.

[14] Kurniawan, E., *Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE-CMM*. Tesis: Universitas Islam Indonesia, 2018.

[15] A. Herman dan A. Darmawan, "Audit Keamanan Informasi Menggunakan ISO 27002 Pada Data Center PT. Gigipatra Multimedia". *Jurnal TIM Darmajaya,* vol. 1, no. 2, pp. 175-191, 2015.

[16] R. Fauzi, "Implementasi Awal Sistem Manajemen Keamanan Informasi pada UKM Menggunakan Kontrol ISO/ICE 27002". *Jurnal Teknologi Rekayasa,* vol. 3, no. 2, pp. 145-156, 2018.

[17] R. D. P. Suhanda dan D. Pratami, "RACI Matrix Design for Managing Stakeholders in Project Case Study of PT. XYZ". *International Journal Of Innovation In Enterprise System,* vol. 5, no. 2, pp. 122-133, 2021.

[18] Y. Y. Asmy dan L. P. Hasugian, "Penilaian Maturity Level Perangkat Lunak Menggunakan CMMI-Dev 1.3 pada Aplikasi Manans MINT". *Jurnal Manajemen Informatika,* vol. 11, no. 2, pp. 158-173, 2021.

[19] N. M. N. Putri, I. G. J. E. Putra, dan I. G. P. K. Juliharta, "Analisis Tata Kelola dan Audit Sistem Informasi pada Rumah Sakit Umum XYZ Menggunakan Kerangka Kerja COBIT 5". Jutisi: *Jurnal Ilmiah Teknik Informatika dan Sistem Informasi,* vol. 9, no. 1, pp. 137-150, 2020.

[20] T. Kristanto, dkk., "Analisis Keamanan Manajemen Informasi Menggunakan Standar ISO 27001:2005 Pada Staff IT Support Di Instansi XYZ". *Jurnal Informatika dan Sains*, vol. 2, no. 2, pp. 30-33, 2019.

[21] Erfina, E. Utami, dan A. Sunyoto, “Evaluasi Tingkat Kematangan Keamanan Informasi Pada Sistem Informasi Manajemen Universitas Cokroaminoto Palopo”. *Jurnal Ilmiah d’Computare,* vol. 8, no. 2, pp. 48-55, 2018.
[22] Rosmiati dan I. Riadi, “Analisis Keamanan Informasi Berdasarkan Kebutuhan Teknikal Dan Operasional Mengkombinasikan Standar ISO 27001:2005 Dengan Maturity Level (Studi Kasus Kantor Biro Teknologi Informasi PT. XYZ)” *in Seminar Nasional Teknologi Informasi Dan Multimedia 2016*, Yogyakarta, 1-6, 6-7 Februari 2016.