The Indonesian Journal of Computer Science
www.ijcs.net
Volume 13, Issue 4, August 2024
https://doi.org/10.33022/ijcs.v13i4.4167

Audit Keamanan Informasi Pemasok Pada Perusahaan Penyelenggara Sistem Pembayaran XYZ

Farroh Sakinah[1], Rizal Fathoni Aji[2]
farroh.sakinah@ui.ac.id[1], rizal@cs.ui.ac.id[2]
[1,2] Universitas Indonesia

Informasi Artikel

Diterima : 21 Jun 2024
Direvisi : 4 Jul 2024
Disetujui : 25 Jul 2024

Kata Kunci

Audit Keamanan Informasi, Pemasok, COBIT, ISO/IEC 27001:2022, Indeks KAMI 5.0

Abstrak

Hubungan kerja sama yang terjalin antara perusahaan dengan pemasok merupakan salah satu perwujudan strategi sumber daya perusahaan untuk tetap produktif dan kompetitif. Namun, Pemasok juga berperan menimbulkan risiko keamanan informasi seperti ancaman keamanan siber dan perlindungan data. Dalam rangka menjamin keamanan aset informasi perusahaan, PT XYZ menerapkan sistem manajemen keamanan informasi dengan mengimplementasikan ISO/IEC 27001:2022 di seluruh aset informasi perusahaan baik yang dikelola secara mandiri oleh internal maupun dikelola oleh pihak eksternal (pemasok). Oleh karena itu, penelitian ini bertujuan untuk melakukan pengukuran tingkat kritikalitas pemasok terhadap keamanan informasi perusahaan dengan pendekatan manajemen risiko aset teknologi informasi. Pemasok yang termasuk sebagai pemasok kritikal akan di evaluasi penerapan kontrol keamanan informasinya melalui proses pemantauan yang sistematis seperti audit dan uji tuntas. Hasil penelitian ini menunjukkan bahwa dua pemasok di PT XYZ dengan tingkat kritikalitas tinggi perlu untuk diaudit dan tiga pemasok dengan tingkat kritikalitas sedang perlu untuk melakukan uji tuntas.

Keywords

Information Security Audit, Supplier, COBIT, ISO/IEC 27001:2022, KAMI's Index 5.0

Abstract

The relationship between companies and suppliers is one of the manifestations of the company's resource strategy to remain productive and competitive. However, suppliers also create information security risks, such as cybersecurity threats and data protection. To ensure the security of the company's information assets, PT XYZ implements an information security management system based on ISO / IEC 27001: 2022 for all company information assets, both managed by internal and external parties (suppliers). Therefore, this research aims to measure suppliers' criticality level with an information technology asset risk management approach. The company will evaluate the critical suppliers's information security control implementation through systematic monitoring processes such as audits and due diligence. The results of this study indicate that two suppliers at PT XYZ with a high level of criticality need to be audited, and three suppliers with a medium level of criticality need to conduct due diligence.

A. Pendahuluan

Pemasok adalah pihak di luar perusahaan baik individu maupun organisasi yang berhubungan atau bekerja bersama-sama dengan perusahaan [1]. Tanpa dukungan dari pemasok, terdapat kesenjangan pengetahuan dan/atau sumber daya khusus yang perlu diupayakan oleh perusahaan baik dengan meningkatkan biaya atau menurunkan pendapatan. Pendekatan ini tidak layak secara finansial jangka panjang sehingga perusahaan (terlepas dari ukuran dan industrinya) mempercayai pemasok untuk memenuhi kebutuhan bisnis tersebut [2]. Hal ini secara progresif menyebabkan perusahaan menghadapi risiko yang secara sadar diterima dengan manajemen risiko yang memadai, namun ada pula yang diabaikan. Hampir dari sebagian perusahaan (46%) menyadari dampak finansial dari kegagalan pemasok setidaknya meningkat dua kali lipat selama lima tahun terakhir, mencakup denda, biaya kompensasi langsung, dan hilangnya pendapatan. Hanya 20% perusahaan dapat secara efektif memantau keseluruhan pemasok sampai dengan sub-kontraktor kritikal. Kurangnya perhatian ini disebabkan oleh sejumlah faktor seperti kurangnya pengetahuan tentang sub-kontraktor berikut risiko yang ditimbulkan, serta kurangnya kapasitas (waktu, orang, dan anggaran) perusahaan untuk menjalankan pemantauan[3].

Ketika kerjasama terjalin, pelaksanaan kontrol keamanan sesuai kebijakan keamanan informasi yang berlaku di perusahaan tidak berarti dipindahkan kepada pemasok. Perusahaan tetap berkewajiban untuk memastikan langkah penanganan insiden keamanan informasi dijalankan oleh pemasok [4]. Untuk dapat menjalankan pemantauan, perusahaan diharapkan memiliki fungsi independen yang berwenang menjalankan audit [5]. Seorang auditor dalam fungsi audit memiliki keahlian untuk menilai dan menganalisis praktik yang dipersyaratkan dibandingkan dengan praktik yang dijalankan pemasok baik pada tahap pemilihan, maupun tahap proses kerja sama. Hasil dari pelaksanaan audit akhirnya memberi keyakinan bahwa perusahaan berinteraksi dengan pemasok yang tepat dan dengan cara yang benar [2].

Bank Indonesia selaku regulator mendorong penyelenggara sistem pembayaran berhati-hati dalam menjalankan layanannya dengan memperhatikan kesiapan dukungan dari sumber daya internal maupun eksternal [6]. Salah satu cara paling efektif untuk mencapai tujuan ini adalah melalui audit keamanan informasi. Audit keamanan informasi dapat membantu perusahaan menilai efektivitas pengendaliannya dan mengidentifikasi potensi risiko dan area kerentanan [7]. PT XYZ merupakan salah satu perusahaan penyelenggara sistem pembayaran di Indonesia dengan produk dan layanan pembayaran yang dapat diakses secara global dan *real-time*. PT XYZ berkomitmen menjamin tingkat keamanan, integritas dan pemantauan yang tinggi untuk semua jenis transaksi yang dioperasikan. PT XYZ senantiasa menyadari bahwa suatu sistem yang handal sekalipun tidak terlepas dari potensi ancaman yang dapat dilakukan oleh pihak internal maupun eksternal. Oleh sebab itu PT XYZ berencana untuk melakukan kegiatan evaluasi kontrol keamanan informasi secara berkala untuk memenuhi regulasi [6], [8] dan meningkatkan keamanan perusahaan [9].

Ketika perusahaan tumbuh lebih besar dan menjadi lebih bergantung pada pemasok, maka perlu untuk membangun program audit pemasok yang efektif, minimal dijalankan pada pemasok yang bernilai kritikal bagi perusahaan [10].

Penilaian risiko dalam penetapan prioritas pelaksaan audit pemasok dilakukan untuk memastikan audit yang dijalankan telah memperhatikan ruang lingkup, waktu, dan sumber daya yang tersedia. Pendekatan berbasis risiko dapat menjadi dasaran dalam menentukan ambang batas risiko dan menerapkan kontrol yang perlu dikonfirmasi dalam proses audit[11].

Keberhasilan pelaksanaan audit terletak pada perencanaan audit. Penting bagi auditor untuk merencanakan daftar kontrol yang ingin ditinjau (*audit checklist*) untuk membantu auditor menilai secara memadai, tepat waktu dan memberikan rasa percaya diri untuk menghindari bias[12]. Karena audit bersifat dinamis dan tidak seharusnya dikendalikan oleh daftar periksa statis [13], *audit checklist* bersifat fleksibel, dapat disesuaikan dengan faktor risiko dan kriteria yang relevan pada setiap penugasan audit.

Beberapa penelitian terdahulu seperti Heikkila [14], Depczynski [15] dan Zammani [16] melakukan penelitian yang berkaitan dengan skala dan atribut yang dapat dipertimbangkan dalam penentuan prioritas pemantauan pemasok dengan menggunakan berbagai konsep seperti keamanan informasi yaitu c*onfidentiality, integrity* dan *availability* (CIA) dari ISO/IEC 27001 dan persyaratan spesifik dari industri dan regulasi yang berlaku. Selain itu, Al-Karaki [17] memberikan pandangan untuk melakukan penelitian dengan memadukan alat ukur kesiapan penerapan keamanan informasi yang sudah ada dan berlaku nasional. Adapun Kramarz [18] memberikan pandangan untuk melibatkan kerjasama yang erat antar unit kerja terkait di perusahaan untuk memastikan penilaian risiko yang efektif. Berdasarkan penelitian-penelitian tersebut dan diskusi dengan narasumber *subject matter expert* di PT XYZ, faktor kritikalitas pemasok akan dikombinasikan dengan kriteria yang paling sesuai dengan kebutuhan organisasi pada studi kasus penelitian.

Oleh karena itu, penelitian ini bertujuan untuk menyusun kertas kerja audit keamanan informasi pemasok sebagai *tools* penetapan kritikalitas berikut penyusunan daftar periksa audit dan uji tuntas pemasok di PT XYZ. Diharapkan hasil penelitian ini dapat digunakan sebagai panduan perusahaan dalam menjalankan audit dan uji tuntas pemasok sehingga mampu mendeteksi dan/atau mencegah terjadinya insiden yang mungkin disebabkan oleh pemasok.

B. Kajian Literatur

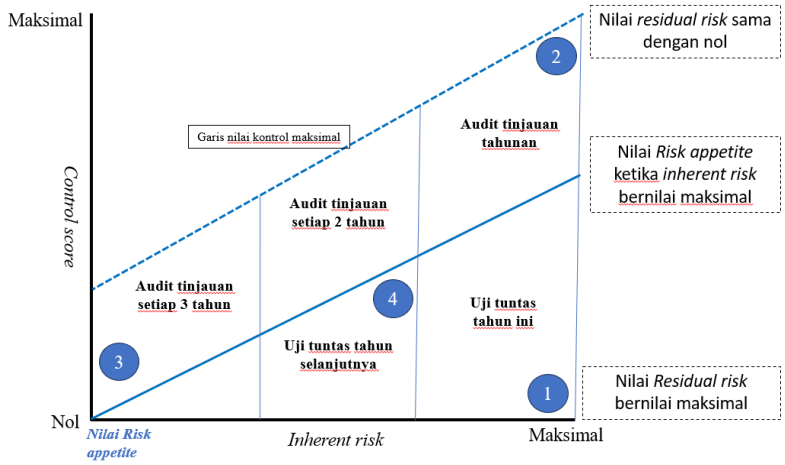
Sistem Manajemen Keamanan Informasi

The International Organization for Standardization (ISO) menerbitkan standar internasional untuk penerapan tata kelola keamanan informasi ISO/IEC 27001 yang dikenal dengan *Information Security Management System* (ISMS). Pada tahun 2022, ISO menerbitkan persyaratan terbaru yang penerapannya dapat disesuaikan dengan profil risiko keamanan informasi masing-masing organisasi. Persyaratan yang ditetapkan dalam ISO/IEC 27001 bersifat umum untuk dapat diterapkan di semua tipe organisasi. Dengan meningkatnya kejahatan siber dan ancaman keamanan informasi baru yang terus bermunculan, ISO/IEC 27001:2022 dapat membantu untuk mengelola risiko, memperkuat ketahanan siber, dan meningkatkan keunggulan operasional organisasi [4].

Audit Internal Berbasis Risiko

Audit internal berbasis risiko adalah metodologi yang digunakan unit audit internal untuk memberikan jaminan bahwa risiko organisasi dikelola sesuai dengan selera risiko (*risk appetite*). Pada sebagian organisasi besar biasanya telah tersedia kerangka kerja manajemen risiko yang telah disesuaikan dan ditetapkan karena organisasi dipengaruhi oleh peraturan dan regulasi. RBIA mengarahkan sumber daya audit internal yang terbatas untuk menprioritaskan pemeriksaan risiko yang merupakan ancaman serius bagi organisasi [11]

Penetapan frekuensi pelaksanaan audit dan uji tuntas (Gambar 1) dapat disusun prioritasnya, misalnya, prioritas pelaksanaan audit dengan *control score* tertinggi dan uji tuntas dengan *control score* terendah. Garis tebal mewakili *risk appetite* (persamaan garisnya adalah nilai risiko pengendalian sama dengan nilai risiko bawaan dikurangi nilai selera risiko).



Gambar 1. Penetapan Frekuensi Audit dan Uji Tuntas [11]

COBIT

Panduan standar praktik manajemen teknologi informasi bernama COBIT (*Control Objective for Information Technologies*) diterbitkan oleh ISACA untuk dapat diterapkan di berbagai macam bentuk perusahaan [19]. Selain dikenal sebagai kerangka kerja untuk mengimplementasikan tata kelola TI perusahaan, COBIT juga memberikan dukungan untuk melaksanakan penugasan jaminan/audit TI. Panduan "COBIT 5 *For Assurance*" dimana kata *assurance* atau jaminan berarti bahwa, berdasarkan hubungan akuntabilitas antara dua pihak atau lebih, seorang profesional audit TI dapat dilibatkan untuk mengeluarkan pernyataan dalam bentuk komunikasi tertulis yang menyatakan kesimpulan mengenai jaminan kepada pihak manajemen yang bertanggung jawab (*auditee*) [20].

Untuk mengoptimalkan kemampuan IT yang tersedia dalam mendukung strategi dan roadmap IT perusahaan, meminimalkan risiko terkait dengan vendor yang tidak berkinerja baik atau tidak patuh, dan memastikan harga yang kompetitif, pengelolaan produk dan layanan terkait IT yang disediakan oleh semua jenis vendor masuk dalam *management objectives* COBIT *Align, Plan and Organize* (APO) 10 *Manage vendors* yang terbagi dalam 5 proses pengelolaan[21].

Indeks KAMI 5.0

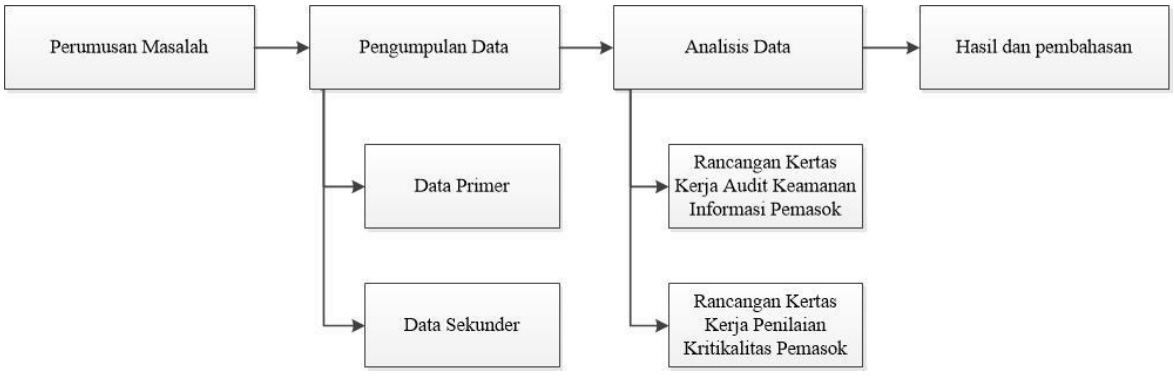
Indeks KAMI merupakan instrumen untuk menganalisis kualitas kelengkapan dan kematangan penerapan keamanan informasi suatu organisasi berdasarkan kriteria SNI ISO/IEC 27001. Indeks KAMI tidak ditujukan untuk menganalisis kelayakan model keamanan yang ada, namun sebagai alat untuk menggambarkan kesiapan (kelengkapan dan kematangan) kerangka keamanan informasi saat ini [22]. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2022. Hasil evaluasi dapat digunakan sebagai pembanding dalam rangka menyusun langkah dan penetapan prioritas perbaikan [23].

Perkembangan teknologi yang pesat dan pola bisnis yang dinamis menyebabkan munculnya risiko keamanan informasi baru seperti keterlibatan pihak ketiga dalam rantai pasok layanan suatu organisasi. Untuk menilai kesiapan perusahaan dalam mengelola risiko di area baru ini, Indeks KAMI revisi 5.0 menyediakan modul suplemen yang berisikan daftar evaluasi kesiapan pengamanan dasar bagi organisasi yang terpapar risiko terkait area tersebut. Hasil penilaian evaluasi kesiapan pengamanan keterlibatan pihak ketiga disampaikan dalam bentuk persentase (%) terhadap sasaran pencapaian [23].

C. Metode Penelitian

Tahapan penelitian (Gambar 2) dirincikan sebagai berikut:

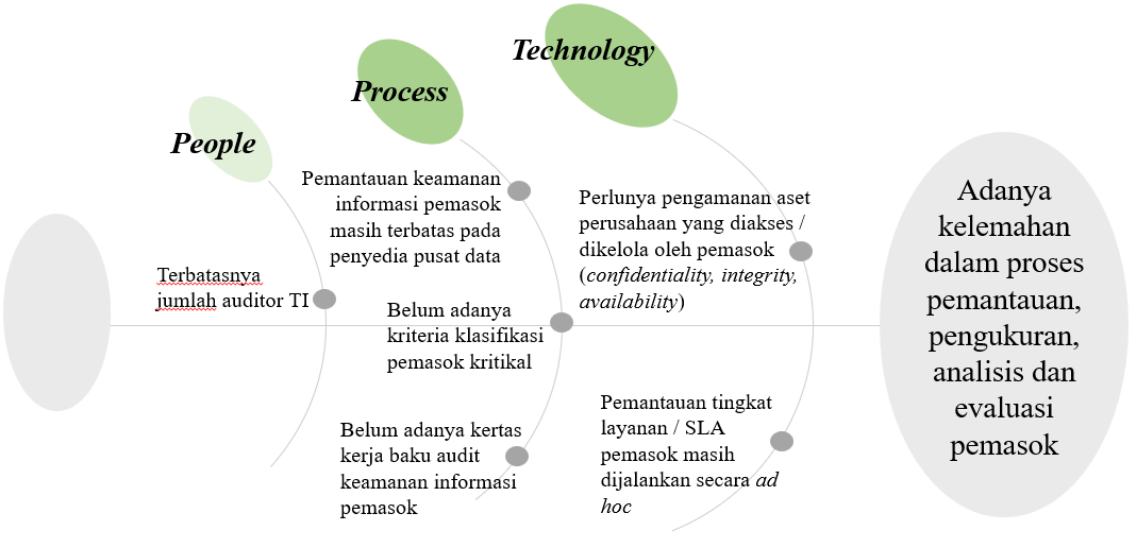
1) Perumusan masalah: permasalahan utama dari hasil analisa *gap* antara ekspektasi dan realita di PT XYZ menggunakan diagram *fishbone* pada tiga domain yaitu *people, process*, dan *technology* [24].
2) Pengumpulan data: Data yang digunakan dan dikumpulkan pada penelitian ini berupa data primer yaitu hasil pelaksanaan wawancara dengan narasumber dan observasi langsung pada perusahaan studi kasus penelitian dan data sekunder berupa pengetahuan teoritis yang diperoleh dari dokumen pendukung sesuai topik penelitian.
3) Analisis data: data yang terkumpul dari tahapan 2 kemudian diolah dan dianalisis untuk ditarik kesimpulan dan menyusun tahap 4 penelitian.
4) Hasil dan pembahasan: memuat hasil penelitian dan pembahasan, serta implementasi dari rancangan kertas kerja audit yang dikembangkan.



Gambar 2. Alur Tahap Penelitian

Perumusan Masalah

Permasalah utama dari pelaksanaan audit keamanan informasi pemasok di PT XYZ dengan pendekatan diagram *fishbone* (Gambar 3) adalah adanya kelemahan dalam proses pemantauan, pengukuran, analisis dan evaluasi pemasok.



Gambar 3. Diagram *Fishbone* Perumusan Masalah

Pengumpulan Data

Data primer untuk merancang kertas kerja penilaian kritikalitas pemasok didapatkan dari hasil wawancara pada narasumber. Pemilihan narasumber berdasarkan keahlian, sertifikasi dan pengalaman kerja di perusahaan tempat penelitian (Tabel 1).

Tabel 1. Daftar Narasumber Penelitian

No	Jabatan	Keahlian	Sertifikasi	Pengalaman
1	Kepala unit audit internal	Auditor keuangan	CA, CPA	Lebih dari 10 tahun
2	Kepala unit kepatuhan	Kepatuhan, tata kelola, keamanan informasi, mutu, audit dan manajemen risiko	*Lead auditor* ISO 27001, 9001, 22301, CISA, CISM.	Lebih dari 20 tahun
3	Kepala unit keamanan TI	Infrastruktur TI, keamanan TI, Pengembangan TI	CISM	Lebih dari 15 tahun
4	Kepala unit pengadaan	Manajemen proyek, layanan pelanggan	*Agile project management*	Lebih dari 15 tahun
5	Kepala unit infrastruktur TI	Infrastruktur TI	*IT Capacity planning Expert, CCNA-CISCO*	Lebih dari 10 tahun
6	Kepala unit manajemen risiko	Proses bisnis, manajemen risiko, keamanan informasi, mutu	ISO 31000:2018, *Lead auditor* ISO 27001 dan 9001	Lebih dari 10 tahun
7	Kepala biro layanan umum	Infrastruktur TI, kepatuhan, tata kelola, keamanan informasi dan manajemen risiko	*Lead auditor* ISO 27001	Lebih dari 25 tahun

Pengumpulan data dilakukan dengan metode wawancara mendalam (*in-depth interview*) untuk mengungkap detail terkait perspektif narasumber tentang suatu subjek atau konsep. Rancangan pertanyaan wawancara telah disiapkan namun narasumber diberi kesempatan untuk berbicara secara bebas tentang peristiwa, perilaku dan keyakinannya terkait area topik penelitian (Tabel 2).

Tabel 2. Pertanyaan Wawancara - Identifikasi Kontrol Keamanan dan Risiko

No.	Pertanyaan	Referensi	
1	Bagaimana strategi perusahaan dalam mencari pemasok terkait TI? Berapa jumlah pemasok TI yang teridentifikasi dapat mempengaruhi kerahasiaan, integritas dan ketersediaan informasi perusahaan saat ini? Sebutkan.	ISO/IEC 27001:2022	• *Clause 4. Context of the organization* • *Annex 5.19 Information security in supplier relationships*
		COBIT	• *APO10.01 Identify and evaluate vendor relationships and contracts*
2	Bagaimana PT XYZ mendefinisikan tugas dan tanggung jawab keamanan informasi pemasok?	ISO/IEC 27001:2022	• *Clause 4.3 Determining the scope of the information security management system* • *Annex 5.20 Addressing information security within supplier agreements*
		COBIT	• *APO10.03 Manage vendor relationships and contracts*
3	Bagaimana proses pemilihan dan evaluasi pemasok? Apakah terdapat penetapan klasifikasi pemasok berdasarkan risiko? Adakah kriteria khusus untuk dapat menjadi pemasok tersebut?	ISO/IEC 27001:2022	• *Annex 5.19 Information security in supplier relationships*
		COBIT	• *APO10.02 Select vendors*
4	Bagaimana prosedur penilaian risiko keamanan informasi terkait penggunaan informasi dan aset oleh pemasok? Apakah turut mempertimbangkan risiko personil pemasok?	ISO/IEC 27001:2022	• *Clause 6.1.2 Information security risk assessment*
		COBIT	• *APO10.04 Manage vendor risk*
5	faktor apa saja yang dipertimbangkan dalam menilai kritikalitas pemasok?	ISO/IEC 27001:2022	• *Clause 8.2 Information security risk assessment*
		COBIT	• *APO10.04 Manage vendor risk*
6	Apakah penanganan insiden dan bencana keadaan darurat telah disepakati dengan pihak pemasok?	ISO/IEC 27001:2022	• *Annex 5.20 Addressing information security within supplier agreements*
		COBIT	• *APO10.03 Manage vendor relationships and contracts*
7	Adakah program *awareness* terkait kebijakan topik khusus keamanan informasi pemasok?	ISO/IEC 27001:2022	• *Clause 7.3 Awareness* • *Annex 6.3 Information security awareness, education and training*
		COBIT	• *APO10.03 Manage vendor relationships and contracts*
8	Apakah perusahaan telah menetapkan kriteria evaluasi pemasok dengan cara yang konsisten?	ISO/IEC 27001:2022	• *Annex 5.19 Information security in supplier relationships*
		COBIT	• *APO10.05 Monitor vendor performance and compliance*

Data sekunder didapati dari hasil analisa data yang akan digunakan untuk menyusun kerangka teoritis dan menjawab pertanyaan penelitian (Tabel 3).

Tabel 3. Daftar Dokumen Internal Perusahaan Penelitian

No	Jenis Dokumen	Keterangan	Sumber
1	Tata kelola audit internal	Untuk mendapatkan data mengenai tata kelola audit.	• Prosedur Umum Internal Audit • Prosedur Audit Pemasok • *Audit Program* Perusahaan
2	Laporan audit keamanan informasi	Untuk mendapatkan format c*hecklist* audit berikut penyajian data hasil audit di perusahaan.	• Laporan Audit Keamanan Informasi
3	Kebijakan manajemen risiko TI	Untuk mendapatkan informasi terkait alur proses manajemen risiko TI di perusahaan	• Kebijakan Manajemen Risiko • IT *Risk Register*
4	Formulir penilaian pemasok	Untuk mendapatkan gambaran awal kriteria yang dipertimbangkan dalam pemilihan dan evaluasi pemasok di perusahaan	• Formulir penilaian pemilihan pemasok • Formulir evaluasi pemasok
5	Struktur organisasi perusahaan	Menentukan tanggung jawab dari setiap unit kerja dalam pengelolaan keamanan informasi.	• Struktur organisasi • Surat pemberitahuan pelaksanaan audit pemasok

Analisis Data

Analisis data penelitian dan pembahasan dengan narasumber dilakukan untuk menyelesaikan permasalahan penelitian dengan menyusun kertas kerja *checklist* audit dan penilaian kritikalitas pemasok. Perhitungan tingkat kritikalitas pemasok menggunakan standar penilaian risiko keamanan informasi [25] yang dimodifikasi sesuai dengan skala yang telah ditentukan perusahaan studi kasus penelitian [26].

Kertas kerja audit keamanan informasi pemasok disusun dengan merujuk kontrol pengamanan yang menggunakan istilah *supplier* pada ISO/IEC 27001:2022 [4], [27]. Kontrol pengamanan pemasok tersebut kemudian dipetakan dengan pendekatan *assurance engagement* COBIT 5 Tahap B dengan *audit process goal* merujuk pada *management objectives – APO10 manage vendors* yang berfokus untuk mengoptimalkan kemampuan, meminimalkan risiko terkait dengan pemasok yang tidak berkinerja baik atau tidak patuh, serta memastikan perusahaan mendapatkan harga yang kompetitif [21]. Untuk mengukur kesiapan penerapan keamanan informasi pemasok, penelitian ini merujuk pada Indeks KAMI 5.0 sebagai aplikasi evaluasi untuk menganalisis tingkat kematangan program keamanan informasi yang berlaku umum di Indonesia, terutama pada Bagian VIII-suplemen pengamanan keterlibatan pihak ketiga penyedia layanan. Bagian VIII-suplemen terdiri dari tujuh kategori yang dapat diukur dalam empat tingkat status pengamanan [23].

Pengolahan Data

Hasil dari identifikasi kontrol keamanan informasi dan proses pelaksanaan kegiatan *assurance* dari ketiga standar dan *framework* tersebut dipetakan untuk dapat digunakan sebagai rujukan daftar periksa audit keamanan informasi yang diilustrasikan pada Tabel 4.

Tabel 4. Perancangan Daftar Periksa Audit Keamanan Informasi Pemasok

ISO 27001:2022	COBIT 5 – *Assurance for Engagement*	Indeks KAMI 5.0
Klausul 4-10	B-1 *Audit Subject Review*	Suplemen VIII
5 *Organizational Control* • *5.5 Contact with authorities* • *5.8 Information security in project management* • *5.19 Information security in supplier relationship* • *5.20 Addressing information security within supplier agreements* • *5.21 Managing information security in the ICT supply chain* • *5.22 Monitoring, review and change management of supplier services* • *5.31 Legal, statutory, regulatory and contractual requirements*	B-2 *Audit Process Goal* • *APO10.01 Identify and evaluate supplier relationships and contracts* • *APO10.02 Select vendors* • *APO10.03 Manage vendor relationships and contracts* • *APO10.04 Manage vendor risk* • *APO10.05 Monitor vendor performance and compliance*	• Manajemen risiko dan pengelolaan keamanan pihak ketiga • Pengelolaan sub-kontraktor/alih daya pihak ketiga • Pengelolaan layanan dan keamanan pihak ketiga • Pengelolaan perubahan layanan dan kebijakan pihak ketiga • Penanganan aset • Pengelolaan insiden oleh pihak ketiga • Rencana kelangsungan layanan pihak ketiga
6 People Control • *6.1 Screening* • *6.2 Terms and conditions of employment* • *6.3 Information security awareness, education and training* • *6.5 Responsibilities after termination or change of employment* • *6.6 Confidentiality or non-disclosure agreements*	B-3 *Principles, Policies and Framework* B-4 *Organisational Structure in Scope* B-5 *Culture, Ethics and Behaviours*	Kriteria penilaian Indeks KAMI, yaitu: • Diterapkan secara menyeluruh • Dalam penerapan/penerapan sebagian • Dalam perencanaan • Tidak dilakukan
7 Physical Control • *7.2 Physical entry* • *7.10 Storage Media* • *7.13 Equipment maintenance*	B-6 *Information item in Scope*	
8 Technological Control • *8.7 Protection against malware* • *8.8 Management of technical vulnerabilities* • *8.10 Information deletion* • *8.19 Installation of software on operational systems* • *8.24 Use of cryptography* • *8.25 Secure development life cycle* • *8.27 Secure system architecture and engineering principles* • *8.29 Security testing in development and acceptance* • *8.30 Outsourced development*	B-7 *Services, Infrastructure and Applications* B-8 *People, Skills and Competencies*	

Penyusunan Kertas Kerja Audit

Penyusunan kertas kerja audit berupa daftar periksa/*checklist* audit dan kertas kerja penilaian kritikalitas pemasok didasarkan dari hasil pengolahan data dan analisis yang telah dilakukan dan divalidasi oleh *subject matter expert* di perusahaan tempat penelitian.

D. Hasil dan Pembahasan

Kertas Kerja Penilaian Kritikalitas Pemasok

Berdasarkan hasil wawancara dengan narasumber untuk mengidentifikasi kontrol keamanan dan risiko pemasok, maka didapatkan faktor-faktor pertimbangan dalam menentukan kriteria kritikalitas pemasok ditunjukkan pada Tabel 5.

Tabel 5. Identifikasi Awal Faktor Kritikalitas Pemasok

No	Narasumber	Identifikasi Faktor Kritikalitas
1	Kepala unit kepatuhan	1. Ketergantungan PT XYZ terhadap produk/layanan pihak ketiga 2. Sifat dari layanan yang diberikan pihak ketiga (*primer, sekunder, tersier*) 3. Harga, tetapi bukan yang utama 4. Pengalaman kerjasama (kejadian/insiden)
2	Kepala unit keamanan TI	1. Dampak produk/layanan pihak ketiga terhadap operasional PT XYZ 2. Interupsi ke sisi bisnis ketika terjadi gangguan/insiden 3. Dukungan produk/layanan pihak ketiga pada layanan kritikal PT XYZ 4. Strategi jangka panjang PT XYZ
3	Kepala biro layanan umum	1. Pertukaran informasi rahasia PT XYZ 2. Keahlian sumber daya pihak ketiga 3. Sertifikasi yang dimiliki oleh pihak ketiga 4. Pengalaman kerjasama (kejadian/insiden)
4	Kepala unit infrastruktur TI	1. Dukungan produk/layanan pihak ketiga terhadap operasional PT XYZ 2. *Effort* untuk perubahan produk/layanan pihak ketiga

Berdasarkan hasil identifikasi awal faktor kritikalitas pemasok, didapatkan 4 (empat) kriteria kemungkinan atau kecenderungan terjadinya risiko dari pemasok yang berdampak ke perusahaan. Penjabaran dampak risiko untuk setiap kategori yang teridentifikasi diuraikan dalam beberapa kategori pada Tabel 6.

Tabel 6. Kategorisasi Faktor Kritikalitas Pemasok

No	Klasifikasi	Faktor Kritikalitas
1	Dampak produk dan layanan	1. Ketergantungan perusahaan terhadap produk/layanan pemasok berikut upaya untuk perubahannya 2. Dampak dukungan pemasok terhadap operasional perusahaan 3. Pertukaran informasi rahasia perusahaan
2	Sifat produk dan layanan	1. Sifat dari layanan yang diberikan pemasok (primer, sekunder, tersier) 2. Interupsi ke sisi bisnis ketika terjadi gangguan/insiden 3. Dukungan produk/layanan terhadap strategi perusahaan
3	Pengalaman kerjasama	1. Penanganan kejadian/insiden 2. Koordinasi
4	Kesiapan Sumber Daya	1. Keterampilan sumber daya pemasok 2. Kompetensi yang dimiliki oleh sumber daya pemasok
5	Harga	1. Nilai investasi

Berdasarkan hasil analisa kemudian dilanjutkan ke proses validasi kepada *subject matter expert* melalui proses wawancara lanjutan. Pembobotan untuk masing-masing kriteria penilaian kritikalitas juga ditetapkan sesuai dengan risk appetite perusahaan tempat penelitian. Penjabaran faktor kritikalitas pemasok setelah validasi diuraikan pada Tabel 7.

Tabel 7. Faktor Kritikalitas Pemasok Setelah Validasi

No	Klasifikasi	Bobot	Faktor Kritikalitas
1	Dampak produk dan layanan	25%	1. Ketergantungan terhadap produk pemasok 2. Dampak gangguan layanan pemasok ke operasional perusahaan 3. Pertukaran informasi rahasia perusahaan
2	Sifat produk dan layanan	20%	1. Sifat layanan pemasok (primer, sekunder, tersier) 2. Interupsi ke sisi bisnis ketika terjadi gangguan/insiden 3. Dukungan produk/layanan terhadap strategi perusahaan
3	Pengalaman kerjasama	10%	1. Kejadian insiden 2. Koordinasi
4	Kesiapan Sumber Daya	15%	Kualitas SDM
5	Harga	30%	Nilai investasi

Kriteria dampak dari terjadinya risiko pada pemasok kritikal perusahaan ditetapkan dengan pendekatan harga atau biaya investasi ke masing-masing pemasok. Penetapan nilai merujuk pada kebijakan perusahaan tempat penelitian yang dijabarkan pada Tabel 8.

Tabel 8. Kriteria Pengukuran Dampak

Kriteria	Rendah	Sedang	Tinggi
Harga	Nilai pengadaan < 500 Juta Rupiah per tahun	Nilai pengadaan ≥ 500 Juta Rupiah per tahun	Nilai pengadaan ≥ 7 Milyar Rupiah per tahun

Kriteria kemungkinan dari terjadinya risiko pada pemasok kritikal perusahaan ditetapkan dengan pendekatan empat faktor kritikalitas pemasok setelah validasi yang telah dijabarkan pada Tabel 7. Penetapan klasifikasi kemungkinan dibagi menjadi tiga tingkatan yang dijabarkan pada Tabel 9 sampai dengan Tabel 12.

Tabel 9. Kriteria Penilaian Kemungkinan - Dampak dan Layanan Pemasok

Kriteria	Rendah	Sedang	Tinggi
Ketergantungan produk	Tersedianya produk/layanan pengganti sejenis	• Tersedianya produk/layanan pengganti sejenis. • Upaya perubahan membutuhkan sedikit modifikasi (≤1 tahun)	• Produk/layanan pengganti sejenis langka • Upaya perubahan membutuhkan banyak usaha (>1 tahun)
Dampak gangguan layanan pemasok	• Operasional sedikit terganggu (<30 menit)	• Operasional terganggu (30 menit – 2 jam) • memerlukan upaya yang mengganggu kinerja untuk mengembalikannya.	• Operasional terpuruk (>2 jam) • Memerlukan upaya dan sumber daya yang besar untuk mengembalikannya.
Pertukaran informasi rahasia	Tidak adanya pertukaran informasi rahasia	Adanya pertukaran informasi rahasia (di luar data pribadi)	Adanya pertukaran informasi rahasia dan informasi PDP (pelindungan data pribadi)

Tabel 10. Kriteria Penilaian Kemungkinan - Sifat Produk dan Layanan Pemasok

Kriteria	Rendah	Sedang	Tinggi
Sifat produk atau layanan	**Tersier** pemenuhannya tidak mendesak, dan dapat digantikan.	**Sekunder** pemenuhannya tidak mendesak.	**Primer** pemenuhannya mendesak dan tidak bisa ditunda.
Interupsi bisnis	Gangguan/insiden di sisi pemasok tidak mempengaruhi SLA perusahaan	Gangguan/insiden di sisi pemasok mempengaruhi SLA perusahaan	Gangguan/insiden di sisi pemasok mempengaruhi SLA dan pencapaian bisnis perusahaan
Dukungan ke Strategi Perusahaan	Produk, teknologi dan layanan non-strategis perusahaan	Produk, teknologi dan layanan strategis jangka pendek perusahaan	Produk, teknologi dan layanan strategis jangka panjang perusahaan

Tabel 11. Kriteria Penilaian Kemungkinan - Pengalaman Kerjasama

Kriteria	Rendah	Sedang	Tinggi
Insiden	Insiden terjadi tidak lebih dari 1 kali dalam 2 tahun	Insiden terjadi antara setiap 2 bulan s/d satu tahun sekali	Insiden terjadi setiap hari atau bulan
Koordinasi	Respon terhadap permintaan / pertanyaan rata-rata <15 menit	Respon terhadap permintaan atau pertanyaan rata-rata 15-30 menit	Respon terhadap permintaan atau pertanyaan rata-rata >30 menit

Tabel 12. Kriteria Penilaian Kemungkinan - Kualitas SDM Pemasok

Kriteria	Rendah	Sedang	Tinggi
Kualitas SDM	• Tidak berdampak pada kualitas operasional/ produksi perusahaan • SDM Kompeten, memiliki sertifikasi yang sesuai dengan persyaratan dan kebutuhan pekerjaan	• Tidak berdampak langsung terhadap kualitas operasional/ produksi perusahaan • Lebih dari 50% SDM memiliki sertifikasi yang sesuai dengan persyaratan dan kebutuhan pekerjaan	• Berdampak langsung terhadap kualitas operasional/produksi perusahaan • Lebih dari 50% SDM belum memiliki sertifikasi yang sesuai dengan persyaratan dan kebutuhan pekerjaan

Penilaian kritikalitas dilakukan dengan metodologi kajian risiko PT XYZ yang merujuk pada standar ISO/IEC 27001 dan Peraturan Bank Indonesia terkait penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum. Hasil penilaian dampak dan kemungkinan yang telah diidentifikasi pada Tabel 8 sampai dengan Tabel 12 akan menjadi suatu nilai risiko inheren yang dikelompokkan menjadi parameter pada Gambar 4.

	Tinggi 2.21-3,00	Sedang 1.61-2.20	Rendah 1.00-1.60
Tinggi	Tinggi	Tinggi	Sedang
Sedang	Tinggi	Sedang	Rendah
Rendah	Sedang	Rendah	Rendah

Gambar 4. Kriteria Nilai Risiko Inheren

Penilaian dan Validasi

Berdasarkan nilai risiko inheren yang ditetapkan pada Gambar 4, kemudian dilakukan evaluasi risiko untuk menentukan prioritas dan langkah penanganan risiko. Tabel 15 menampilkan kriteria penerimaan risiko inheren sesuai dengan nilai risiko yang telah divalidasi oleh *subject matter expert* PT XYZ.

Tabel 13. Penerimaan Risiko Kritikalitas Pemasok

Nilai Risiko	Mitigasi
Rendah	Secara langsung diterima oleh perusahaan
Sedang	Dilakukan langkah mitigasi berupa penyampaian pengisian uji tuntas / *due diligence* keamanan informasi
Tinggi	Dilakukan langkah mitigasi berupa pelaksanaan audit keamanan informasi

Merujuk pada kriteria kritikalitas pemasok yang telah diidentifikasi dan diverifikasi, kemudian dilakukan penilaian risiko terhadap pemasok pada Tabel 14 kepada 7 *sampling* pemasok di PT XYZ. Penilaian dilakukan oleh manajemen setingkat kepala pada unit kerja pengguna.

Tabel 14. Penilaian Risiko Pemasok PT XYZ

No	Pemasok	Pekerjaan	Dampak	Sifat	SDM	Kerjasama	Harga	Nilai
1	PT A	*Data Center* dan jaringan produksi	3	3	1	2	3	2.60
2	PT B	Perangkat operasional	3	2	2	1	3	2.45
3	PT C	PAM	2	2	1	1	2	1.75
4	PT D	DLP	1	1	1	1	1	1.00
5	PT E	*Penetration Testing*	2	2	1	1	2	1.75
6	PT F	*Anti-malware*	3	2	1	1	2	2.00
7	PT G	*Firewall analyzer*	1	1	2	1	1	1.15

Berdasarkan hasil penilaian risiko (Tabel 14), selanjutnya dilakukan evaluasi risiko untuk menentukan perlakuan risiko kepada pemasok (Tabel 15). Didapatkan 2 (dua) perusahaan pemasok dengan nilai risiko inheren tinggi perlu dilakukan audit oleh auditor PT XYZ dan 3 (tiga) perusahaan pemasok yang perlu untuk dikirimkan kuesioner uji tuntas / due diligence dengan pengisian penilaian mandiri.

Tabel 15. Hasil Evaluasi Penilaian Kritikalitas Pemasok

No	Pemasok	Pekerjaan	Nilai	Perlakuan Risiko	
1	PT A	*Data Center* dan jaringan produksi	2.60	Mitigasi	Audit Keamanan Informasi
2	PT B	Perangkat operasional	2.45	Mitigasi	Audit Keamanan Informasi
3	PT F	*Anti-malware*	2.00	Mitigasi	*Due Diligence*
4	PT E	*Penetration Testing*	1.75	Mitigasi	*Due Diligence*
5	PT C	Privileged Access Management (PAM)	1.75	Mitigasi	*Due Diligence*
6	PT G	*Firewall analyzer*	1.15	Terima	Terima
7	PT D	Data Lost Prevention (DLP)	1.00	Terima	Terima

E. Simpulan

Pengukuran kritikalitas pemasok disusun berdasarkan faktor risiko yang ingin diminimalkan oleh perusahaan baik risiko teknikal maupun risiko kehilangan nilai dari biaya/investasi yang telah dikeluarkan. Berdasarkan hasil penilaian kritikalitas, perusahaan dapat menetapkan langkah pemantauan risiko yang melekat di pemasok. Perusahaan dapat mengandalkan proses dan laporan hasil audit untuk memastikan perusahaan telah bekerjasama dengan pemasok yang tepat dan sesuai dengan *best practice.*

Audit keamanan informasi pemasok merupakan proses sistematis untuk memperoleh dan mengevaluasi bukti secara objektif mengenai pemenuhan perjanjian kerjasama antara pemasok dengan perusahaan terutama terkait penerapan kontrol keamanan informasi secara konsisten dan memenuhi persyaratan yang ditetapkan. Kertas kerja periksa audit (*checklist*) pada perusahaan dapat disusun dengan mengacu kepada ISO/IEC 27001:2022, COBIT 5 dan Indeks KAMI 5.0.

F. Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada perusahaan tempat penelitian yang telah memberikan ijin dan dukungan sehingga penelitian ini dapat terlaksana.

G. Referensi

[1] ISO/IEC, ISO 27000:2018 Information security management systems Overview and vocabulary. 2018. Accessed: Feb. 05, 2024. [Online]. Available: https://www.iso.org/standard/73906.html

[2] ISACA, “Audit-Oversight-for-Onboarding-Vendors_res_eng_0220,” 2020, Accessed: Feb. 05, 2024. [Online]. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoDYEA0

[3] Deloitte, “Be responsible and effective Strike a balance Extended enterprise risk management (EERM) Third-party risk management (TPRM) global survey 2020,” 2020. Accessed: Feb. 05, 2024. [Online]. Available: https://www2.deloitte.com/us/en/pages/risk/articles/extended-enterprise-risk-management-report.html

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

[5] ISO, “ISO 19011,” Guideline for Auditing Management. 2018.

[6] Central Bank of Indonesia, “Peraturan Bank Indonesia No 23/6/PBI/2021 tentang Penyedia Jasa Pembayaran,” 1 07 2021. [Online]. Available: https://www.bi.go.id/id/publikasi/peraturan/Pages/PBI_230621.aspx.

[7] D. Owens, “Managing Data Privacy and Information Security With IT Audits,” ISACA, May 23, 2023. Accessed: Feb. 07, 2024. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2023/managing-data-privacy-and-information-security-with-it-audits

[8] Central Bank of Indonesia, “Peraturan Bank Indonesia Nomor 22/23/PBI/2020 Tahun 2020 tentang Sistem Pembayaran,” 29 12 2020. [Online]. Available:

https://www.bi.go.id/id/publikasi/peraturan/Pages/PBI_222320.aspx, 2020.
[9] J. Kassing, "Five Controls to Consider When Auditing a Vendor Management Program," ISACA, Jan. 23, 2024. Accessed: Feb. 07, 2024. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2024/five-controls-to-consider-when-auditing-a-vendor-management-program
[10] D. Podeswik, "The Pitfalls of Supply Chain Risk Management," ISACA, vol. 3, May 2022.
[11] D. Griffiths, "Risk Based Internal Auditing Three views on implementation," 2006. [Online]. Available: www.internalaudit.biz
[12] C. Anand, "Preparing Your First Supplier Audit Plan," ISACA, Jul. 07, 2022. Accessed: Feb. 07, 2024. [Online]. Available: https://www.isaca.org/resources/news-and-trends/industry-news/2022/preparing-your-first-supplier-audit-plan
[13] O. A. Abuazza, A. Labib, and B. M. Savage, "Development of an auditing framework by integrating ISO 9001 principles within auditing," International Journal of Quality and Reliability Management, vol. 37, no. 2, pp. 328–353, Jan. 2020, doi: 10.1108/IJQRM-02-2019-0048.
[14] E. Heikkila, R. Tiusanen, and E. Oz, "Towards requirements for third-party assessments in the Specific Operations Risk Assessment process," in 2023 International Conference on Unmanned Aircraft Systems, ICUAS 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 207–212. doi: 10.1109/ICUAS57906.2023.10155905.
[15] R.Depczynski, "MCDA based approach to supplier evaluation - Steel industry enterprise case study," in Procedia Computer Science, Elsevier B.V., 2021, pp. 5081–5092. doi: 10.1016/j.procs.2021.09.286.
[16] M. Zammani, R. Razali, and D. Singh, "Factors Contributing to the Success of Information Security Management Implementation," 2019. [Online]. Available: www.ijacsa.thesai.org
[17] J. N. Al-Karaki, A. Gawanmeh, and S. El-Yassami, "GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 6, pp. 3079–3095, Jun. 2022, doi: 10.1016/j.jksuci.2020.09.011.
[18] K. Kramarz and J. Korpysa, "The evolution of the concept of risk management in IT+ organizations," in Procedia Computer Science, Elsevier B.V., 2023, pp. 4843–4849. doi: 10.1016/j.procs.2023.10.484.
[19] ISACA. (2020b). COBIT® 2019 Framework : Introduction and Methodology (2020th ed.). ISACA.
[20] S. De Haes and W. Van Grembergen, "COBIT as a Framework for IT Assurance," in Management for Professionals, vol. Part F319, Springer Nature, 2015, pp. 129–149. doi: 10.1007/978-3-319-14547-1_6.
[21] ISACA, "WAPO10-Manage-Suppliers-Audit-Assurance-Program_icq_Eng_0814," 2014. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoDAEA0

[22] Wulansari, T. T., & Novandi, D. (2022). Evaluation of Information Security Management Using the KAMI Index Framework. 2022 International Conference of Science and Information Technology in Smart Administration, ICSINTESA 2022, 173–177. https://doi.org/10.1109/ICSINTESA56431.2022.10041714
[23] BSSN. (2023). Indeks KAMI Versi 5.0.-16 Agustus 2023_Protected. 5.0. Available: https://www.bssn.go.id/indeks-kami/
[24] M. Prodan, A. Prodan, and A. A. Purcarea, "Three New Dimensions to People, Process, Technology Improvement Model," in Advances in Intelligent Systems and Computing, Springer Verlag, 2015, pp. 481–490. doi: 10.1007/978-3-319-16486-1_47.
[25] ISO/IEC, ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management. 2018. Accessed: Feb. 13, 2023. [Online]. Available: https://www.iso.org/standard/75281.html
[26] PT XYZ, Prosedur Metodologi Kajian Risiko PT XYZ, 2.1. 2016.
[27] ISO/IEC, ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. https://www.iso.org/, 2022.