

ANALISIS KEBUTUHAN INFORMASI UNTUK PENGEMBANGAN SISTEM INFORMASI KEAMANAN DATA PADA PERUSAHAAN TEKNOLOGI

Meysa Humairoh¹⁾, Dina Mardiaty²⁾

^{1,2)}Sistem dan Teknologi Informasi, Institut Teknologi Bisnis Riau
email: ¹⁾meysahumairoh1311@gmail.com, ²⁾dinamardiaty8@gmail.com

Abstrak

Keamanan data menjadi kebutuhan strategis bagi perusahaan teknologi karena data pelanggan, transaksi, kredensial, antarmuka pemrograman aplikasi, arsip digital, dan *log* sistem terus menghadapi risiko kebocoran, manipulasi, akses tidak sah, serta gangguan layanan. Penelitian ini bertujuan menganalisis kebutuhan informasi untuk pengembangan sistem informasi keamanan data yang adaptif, terukur, dan akuntabel. Penelitian menggunakan pendekatan kualitatif-konseptual melalui studi literatur terarah dan sintesis analitis terhadap penelitian tentang keamanan informasi, manajemen risiko, pengujian kerentanan, pengamanan aplikasi web, pengamanan antarmuka pemrograman aplikasi, enkripsi, *blockchain*, kontrol akses, audit, dan tata kelola keamanan. Analisis dilakukan dengan mengidentifikasi aset data, memetakan risiko, mengategorikan kebutuhan informasi, serta menyusun model konseptual perlindungan data. Hasil penelitian menunjukkan bahwa sistem informasi keamanan data tidak dapat dikembangkan hanya dengan menambahkan fitur teknis secara terpisah. Kebutuhan utama mencakup pemetaan aset data, klasifikasi risiko, pengelolaan hak akses, autentikasi dan otorisasi, enkripsi, audit trail, monitoring, penilaian kerentanan, pengujian penetrasi, serta tata kelola berbasis standar. Temuan ini menegaskan bahwa dimensi teknis seperti kontrol akses berbasis peran, pembatasan permintaan, enkripsi data, *blockchain*, serta validasi input harus dihubungkan dengan dimensi manajerial berupa kebijakan, prosedur, dokumentasi, evaluasi kematangan, dan manajemen risiko. Model yang dihasilkan menempatkan aset data sebagai titik awal analisis, kemudian dilanjutkan dengan identifikasi risiko, pemilihan kontrol keamanan, pemantauan aktivitas, pelaporan insiden, dan rekomendasi mitigasi. Dengan demikian, analisis kebutuhan informasi menjadi fondasi penting bagi perusahaan teknologi dalam merancang sistem informasi keamanan data yang mampu menjaga kerahasiaan, keutuhan, dan ketersediaan informasi sekaligus memperkuat kesiapan organisasi menghadapi ancaman siber modern.

Kata kunci— Analisis Kebutuhan Informasi, Keamanan Data, Manajemen Risiko, Sistem Informasi, Tata Kelola Keamanan.

1. PENDAHULUAN

Perusahaan teknologi beroperasi dalam ekosistem digital yang sangat bergantung pada data, sistem informasi, konektivitas jaringan, layanan berbasis web, komputasi awan, antarmuka pemrograman aplikasi, dan integrasi lintas platform. Dalam kondisi tersebut, data tidak lagi sekadar keluaran administratif, tetapi telah menjadi aset strategis yang menentukan kelangsungan layanan, reputasi organisasi, kepercayaan pengguna, serta daya saing bisnis. Perusahaan teknologi umumnya mengelola data pelanggan, data

transaksi, log aktivitas, arsip internal, basis data aplikasi, kredensial pengguna, informasi layanan, dan data operasional yang bersifat sensitif. Ketika data tersebut tidak dikelola melalui mekanisme keamanan yang memadai, organisasi berhadapan dengan risiko kebocoran, manipulasi, pencurian identitas, gangguan layanan, dan kerugian finansial. Prinsip *confidentiality, integrity, and availability* menjadi landasan penting dalam memastikan bahwa data hanya dapat diakses oleh pihak berwenang, tidak berubah secara tidak sah, dan tetap tersedia ketika dibutuhkan. Oleh sebab itu, pengembangan sistem informasi keamanan data pada perusahaan teknologi memerlukan pemahaman yang lebih sistematis mengenai kebutuhan informasi keamanan, bukan hanya pemilihan perangkat lunak keamanan secara teknis.

Survei literatur terkini menunjukkan bahwa ancaman terhadap sistem informasi terus berkembang seiring meningkatnya adopsi teknologi digital. Evaluasi keamanan berbasis Indeks KAMI menunjukkan bahwa organisasi dapat memiliki kontrol dasar keamanan, tetapi tetap belum matang apabila kebijakan, prosedur, dan dokumentasi belum dikelola secara memadai [1]. Pada konteks aplikasi web, pengujian menggunakan OWASP-ZAP menemukan bahwa sistem masih dapat memiliki berbagai celah keamanan, seperti *Content Security Policy* header yang belum tersedia, kesalahan konfigurasi lintas domain, missing *anti-clickjacking* header, pustaka *JavaScript* rentan, *cookie* tanpa atribut *secure*, dan kebocoran informasi melalui banner halaman [2]. Studi *penetration testing* terhadap sistem berbasis web juga menunjukkan bahwa kerentanan *SQL Injection* masih menjadi ancaman serius karena dapat mengekspos basis data dan memungkinkan akses tidak sah ke informasi sensitif [3]. Sementara itu, pada lingkungan *cloud computing*, risiko keamanan semakin kompleks karena data berada di luar kendali langsung organisasi, bersifat terdistribusi, dan dapat diakses oleh berbagai pihak melalui jaringan internet [4]. Literatur tersebut memperlihatkan bahwa keamanan data harus dipahami sebagai persoalan multidimensi yang mencakup teknologi, tata kelola, risiko, perilaku pengguna, dan kesiapan organisasi.

Masalah penelitian utama yang muncul adalah belum tersedianya model analisis kebutuhan informasi yang secara khusus dapat memandu perusahaan teknologi dalam mengembangkan sistem informasi keamanan data secara terstruktur. Banyak organisasi telah menerapkan sistem digital, tetapi belum selalu memiliki pemetaan yang jelas mengenai jenis data yang perlu dilindungi, tingkat sensitivitas data, aktor pengguna, hak akses, pola ancaman, kontrol keamanan, mekanisme autentikasi, prosedur audit, serta indikator kesiapan keamanan. Akibatnya, solusi keamanan sering kali diterapkan secara parsial, misalnya hanya menambahkan *enkripsi, firewall*, atau autentikasi, tanpa memastikan bahwa kontrol tersebut sesuai dengan risiko aktual dan kebutuhan operasional organisasi. Studi pada sistem informasi enterprise menegaskan bahwa keberhasilan implementasi teknologi tidak hanya ditentukan oleh kualitas sistem, tetapi juga oleh kesiapan organisasi, dukungan manajemen, kompetensi sumber daya manusia, kesesuaian sistem dengan proses bisnis, dan budaya kerja yang adaptif [5]. Dalam perusahaan teknologi, persoalan ini menjadi lebih kritis karena perubahan aplikasi, integrasi layanan, dan pemrosesan data berlangsung cepat.

Solusi umum atas masalah tersebut adalah membangun sistem informasi keamanan data berdasarkan analisis kebutuhan informasi yang komprehensif. Analisis ini perlu dimulai dari identifikasi aset data, klasifikasi risiko, pemetaan pengguna, pengelolaan hak akses, penilaian kerentanan, kontrol teknis, kontrol prosedural, dan kebutuhan pelaporan

keamanan. Kerangka ISO/IEC 27001:2013 memberikan dasar bagi pengelolaan keamanan informasi yang berbasis risiko, terdokumentasi, dan berkelanjutan melalui kebijakan, prosedur, kontrol, serta audit keamanan. ISO 31000:2018 juga relevan karena membantu organisasi mengidentifikasi, menganalisis, mengevaluasi, dan memperlakukan risiko sistem informasi secara sistematis [6]. Di sisi lain, COBIT 2019 dapat digunakan untuk memperkuat tata kelola keamanan data melalui pemantauan akses, audit log, mitigasi risiko, serta pengukuran tingkat kapabilitas proses keamanan [7]. Dengan menggabungkan perspektif tata kelola dan teknis, perusahaan teknologi dapat merancang keamanan data sebagai sistem yang terukur, bukan hanya sebagai reaksi terhadap insiden.

Literatur sebelumnya telah menawarkan beberapa solusi spesifik yang dapat menjadi dasar pengembangan sistem informasi keamanan data. Untuk perlindungan endpoint API, OAuth2 dengan *Laravel Passport* dapat digunakan dalam arsitektur *microservice* untuk mengamankan komunikasi antarlayanan melalui token, otorisasi berbasis *scope*, dan penolakan akses yang tidak sah [8]. Untuk aplikasi berbasis web, *framework Laravel* dapat diperkuat melalui *rate limiting*, *role-based access control*, *Laravel Spatie Permissions*, *hashing Bcrypt*, dan perlindungan terhadap *Cross-Site Request Forgery* [9]. Studi digitalisasi SOP berbasis web juga menunjukkan bahwa *workflow approval* dan *role-based access control* mampu memusatkan pengelolaan dokumen, membatasi akses pengguna, dan meningkatkan efisiensi pencarian dokumen dalam satu platform terintegrasi [10]. Temuan-temuan ini menunjukkan bahwa keamanan data harus mencakup autentikasi, otorisasi, pembatasan permintaan, validasi input, dan pengelolaan peran secara konsisten.

Solusi lain yang juga menonjol adalah enkripsi, blockchain, vulnerability assessment, dan penetration testing. Enkripsi AES terbukti mampu menjaga kerahasiaan dan integritas data rekam medis digital dengan waktu proses yang relatif cepat, sedangkan perancangan sistem pengarsipan berbasis web dengan fitur enkripsi AES menunjukkan tingkat kelayakan 92% dalam mendukung pengelolaan arsip yang aman, cepat, dan terstruktur. Pada konteks data penjualan, algoritma RSA-CRT digunakan untuk mengamankan file transaksi agar tidak mudah disalahgunakan atau dimanipulasi. Teknologi *blockchain* juga dinilai mampu meningkatkan keamanan data melalui desentralisasi dan enkripsi, dengan temuan bahwa skor keamanan meningkat dari 4 sebelum implementasi menjadi 9 setelah implementasi [11]. Selain itu, penggunaan OWASP-ZAP dan *penetration testing* penting untuk mengidentifikasi kelemahan aplikasi web, terutama pada mekanisme autentikasi dan parameter input pengguna. Dalam konteks autentikasi biometrik, pendekatan *Trusted Execution Environment*, *AES-256 encryption*, *liveness detection*, *anti-tamper mechanism*, dan *rate limiting* juga direkomendasikan untuk menjaga integritas serta privasi pengguna [12].

Meskipun literatur tersebut memberikan kontribusi kuat, sebagian besar penelitian masih membahas aspek keamanan secara terpisah. Studi Indeks KAMI menekankan evaluasi kematangan keamanan informasi, tetapi belum merumuskan kebutuhan informasi untuk perusahaan teknologi secara spesifik. Studi OAuth2 lebih berfokus pada keamanan endpoint API dalam arsitektur *microservice*. Studi OWASP-ZAP dan *penetration testing* lebih menekankan identifikasi kerentanan teknis pada aplikasi web [13]. Studi COBIT lebih mengarah pada tata kelola dan peningkatan kapabilitas keamanan [14]. Studi enkripsi AES, RSA, dan blockchain lebih berorientasi pada

perlindungan data dan integritas transaksi [15]. Celah penelitian yang terlihat adalah belum adanya sintesis yang menghubungkan kebutuhan informasi keamanan, tata kelola, manajemen risiko, kontrol teknis, auditabilitas, dan kesiapan organisasi dalam satu model analisis untuk pengembangan sistem informasi keamanan data pada perusahaan teknologi.

Berdasarkan kesenjangan tersebut, penelitian ini bertujuan merumuskan analisis kebutuhan informasi untuk pengembangan sistem informasi keamanan data pada perusahaan teknologi. Kebaruan studi ini terletak pada upaya mengintegrasikan perspektif keamanan informasi berbasis *confidentiality, integrity, and availability*, tata kelola ISO 27001 dan COBIT, manajemen risiko ISO 31000, pengujian kerentanan berbasis OWASP, autentikasi dan otorisasi API, enkripsi data, audit trail, serta kesiapan organisasi ke dalam satu kerangka analitis. Ruang lingkup studi diarahkan pada identifikasi aset data, klasifikasi kebutuhan keamanan, pemetaan pengguna dan hak akses, kebutuhan monitoring, validasi input, enkripsi, manajemen risiko, pengujian kerentanan, dan kebutuhan pelaporan keamanan. Dengan kerangka tersebut, penelitian ini diharapkan dapat memberikan dasar konseptual bagi perusahaan teknologi dalam merancang sistem informasi keamanan data yang adaptif, terukur, akuntabel, dan relevan dengan dinamika ancaman siber modern.

2. METODE PENELITIAN

2.1 Desain Penelitian

Penelitian ini menggunakan pendekatan kualitatif-konseptual dengan desain studi literatur terarah dan sintesis analitis untuk merumuskan kebutuhan informasi dalam pengembangan sistem informasi keamanan data pada perusahaan teknologi. Pendekatan ini dipilih karena fokus penelitian tidak diarahkan pada pengujian statistik antarvariabel, tetapi pada penyusunan kerangka analisis yang mampu menjelaskan jenis informasi keamanan yang perlu diidentifikasi, diklasifikasikan, dikendalikan, dan dimonitor dalam lingkungan organisasi berbasis teknologi. Dalam konteks perusahaan teknologi, keamanan data tidak dapat dipahami hanya sebagai persoalan perangkat lunak atau konfigurasi teknis. Keamanan data harus dilihat sebagai sistem yang menghubungkan aset informasi, pengguna, proses bisnis, risiko, kontrol teknis, tata kelola, dan mekanisme evaluasi berkelanjutan.

Secara metodologis, penelitian ini bersifat eksploratif dan integratif. Sifat eksploratif terlihat dari upaya penelitian untuk menggali kebutuhan informasi keamanan yang muncul dari berbagai bentuk sistem digital, seperti aplikasi web, *endpoint* API, cloud computing, sistem arsip digital, sistem autentikasi, serta layanan berbasis microservice. Sifat integratif tampak dari penggabungan berbagai perspektif literatur, yaitu keamanan informasi berbasis *confidentiality, integrity, and availability*, tata kelola keamanan berbasis ISO/IEC 27001 dan COBIT, manajemen risiko berbasis ISO 31000, *vulnerability assessment, penetration testing*, pengamanan *endpoint* API, enkripsi, *blockchain, role-based access control*, dan *rate limiting*.

2.2 Sumber Data dan Basis Literatur

Sumber data penelitian berasal dari catatan hasil penelitian dan literatur ilmiah yang relevan dengan topik keamanan data dan sistem informasi. Literatur yang digunakan mencakup studi tentang evaluasi keamanan informasi berbasis Indeks KAMI dan

ISO/IEC 27001, keamanan *endpoint* API menggunakan OAuth2, *penetration testing* terhadap SQL Injection, implementasi *blockchain* untuk keamanan data, analisis risiko sistem informasi berbasis ISO 31000, evaluasi autentikasi biometrik, kerentanan *cloud computing*, *vulnerability assessment* menggunakan OWASP-ZAP, penguatan keamanan berbasis Laravel, penerapan COBIT, enkripsi AES, RSA-CRT, dan sistem pengarsipan berbasis web dengan enkripsi.

Pemilihan literatur dilakukan secara purposif berdasarkan tiga pertimbangan.

1. Literatur harus membahas isu keamanan data, sistem informasi, atau kontrol keamanan digital.
2. Literatur harus memberikan temuan empiris atau konseptual yang dapat digunakan untuk menyusun dimensi kebutuhan informasi keamanan.
3. Literatur harus memiliki relevansi dengan karakteristik perusahaan teknologi, terutama yang berhubungan dengan aplikasi web, API, data sensitif, autentikasi, enkripsi, risiko siber, dan tata kelola sistem informasi.

Dengan kriteria tersebut, penelitian sebelumnya digunakan sebagai landasan utama penyusunan metodologi.

2.3 Prosedur Analisis Kebutuhan Informasi

2.3.1 Identifikasi Aset Data dan Risiko Keamanan

Tahap pertama dalam penelitian ini adalah mengidentifikasi aset data yang perlu dilindungi. Aset data dipahami sebagai seluruh informasi digital yang memiliki nilai bagi perusahaan teknologi dan dapat menimbulkan risiko apabila diakses, diubah, dihapus, atau disebarkan secara tidak sah. Identifikasi aset mencakup data pengguna, data transaksi, data operasional, dokumen internal, kredensial akses, endpoint API, basis data aplikasi, file arsip, dan *log* sistem. Tahap ini mengacu pada prinsip keamanan informasi yang menempatkan *confidentiality*, *integrity*, and *availability* sebagai dasar perlindungan informasi.

Setelah aset data diidentifikasi, penelitian memetakan risiko yang mungkin terjadi pada setiap aset. Risiko tersebut meliputi akses tidak sah, manipulasi data, kebocoran informasi, serangan SQL Injection, eksploitasi API, brute force, *spoofing*, kesalahan konfigurasi, penyalahgunaan hak akses, kehilangan dokumen, dan gangguan layanan. SQL Injection dapat mengekspos basis data melalui parameter yang rentan, risiko sistem informasi perlu diidentifikasi, dianalisis, dievaluasi, dan diberi perlakuan berdasarkan pendekatan ISO 31000:2018 [16].

2.3.2 Kategorisasi Kebutuhan Informasi Keamanan

Tahap kedua adalah mengelompokkan kebutuhan informasi keamanan ke dalam beberapa dimensi konseptual. Kategorisasi dilakukan dengan cara menghubungkan jenis data, sumber risiko, kontrol keamanan, dan keluaran informasi yang dibutuhkan oleh organisasi.

Tabel 1 menunjukkan kategori kebutuhan informasi yang digunakan dalam penelitian ini.

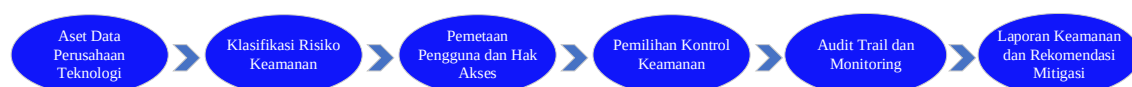
Tabel 1. Kategori Kebutuhan Informasi Keamanan Data Pada Perusahaan Teknologi

Dimensi Kebutuhan Informasi	Fokus Data atau Proses	Tujuan Penggunaan Informasi
Informasi Aset Data	Data Pengguna, Transaksi, API, Arsip, Log, Kredensial	Menentukan Prioritas Perlindungan Data
Informasi Risiko Keamanan	SQL Injection, Brute Force, Spoofing, Malware, Salah Konfigurasi	Mengidentifikasi Ancaman dan Dampaknya
Informasi Akses Pengguna	Role, Permission, Token, Scope, Aktivitas Login	Mengatur Otorisasi dan Mencegah Akses Tidak Sah
Informasi Enkripsi dan Integritas	AES, RSA, Blockchain, Hashing, Digital Signature	Menjaga Kerahasiaan dan Keaslian Data
Informasi Audit dan Monitoring	Audit Trail, Log Aktivitas, Alert, Laporan Insiden	Menelusuri Perubahan dan Mendeteksi Anomali
Informasi Tata Kelola Keamanan	Kebijakan, SOP, COBIT, ISO 27001, ISO 31000	Menilai Kematangan dan Kesiapan Keamanan

Sebagaimana ditampilkan pada Tabel 1, kebutuhan informasi keamanan data bersifat multidimensi. Dimensi akses pengguna dirumuskan berdasarkan studi OAuth2 dan RBAC yang menekankan pentingnya autentikasi, otorisasi, token, scope, dan pembagian peran pengguna [17]. Dimensi enkripsi dan integritas didasarkan pada studi AES, RSA-CRT, dan *blockchain* yang menunjukkan pentingnya perlindungan data melalui penyandian, desentralisasi, dan verifikasi integritas. Dimensi audit dan monitoring merujuk pada temuan COBIT dan sistem pengarsipan terenkripsi yang menekankan *audit log*, *audit trail*, dan kontrol akses sebagai bagian penting dari keamanan data.

2.3.3 Sintesis Model Konseptual

Tahap ketiga adalah menyusun model konseptual analisis kebutuhan informasi. Model ini menghubungkan aset data, risiko keamanan, kontrol teknis, tata kelola, dan keluaran informasi keamanan. Alur konseptual penelitian ditampilkan pada Gambar 1.



Gambar 1. Alur Konseptual Analisis Kebutuhan Informasi untuk Sistem Informasi Keamanan Data

Gambar 1 menunjukkan bahwa analisis kebutuhan informasi keamanan harus dimulai dari pemetaan aset data, bukan langsung dari pemilihan teknologi keamanan. Urutan ini penting karena setiap aset memiliki tingkat sensitivitas, risiko, dan kebutuhan kontrol yang berbeda. Setelah aset dan risiko dipetakan, organisasi menentukan hak akses pengguna, memilih kontrol keamanan yang sesuai, menerapkan audit trail serta monitoring, kemudian menghasilkan laporan keamanan dan rekomendasi mitigasi. Alur ini selaras dengan kerangka ISO 31000 yang menempatkan identifikasi risiko sebagai

dasar perlakuan risiko, serta selaras dengan COBIT yang menekankan pentingnya pemantauan akses, audit log, dan pengukuran kapabilitas keamanan [18].

2.4 Ruang Lingkup Metodologis

Ruang lingkup metodologis penelitian ini dibatasi pada penyusunan model analisis kebutuhan informasi untuk pengembangan sistem informasi keamanan data. Penelitian ini tidak membangun aplikasi final, tidak melakukan penetration testing langsung pada sistem perusahaan tertentu, dan tidak menguji algoritma keamanan secara eksperimental. Hasil penelitian berupa kerangka konseptual yang dapat digunakan sebagai dasar penelitian lanjutan, seperti validasi ahli, studi kasus pada perusahaan teknologi, survei kebutuhan keamanan, atau pengembangan prototipe sistem informasi keamanan data.

Batasan tersebut penting karena analisis kebutuhan informasi merupakan tahap awal dalam siklus pengembangan sistem keamanan. Apabila kebutuhan informasi tidak dipetakan sejak awal, sistem berisiko hanya menjadi kumpulan fitur keamanan yang tidak saling terhubung. Dengan metodologi ini, penelitian diarahkan untuk menyediakan fondasi konseptual yang dapat membantu perusahaan teknologi merancang sistem informasi keamanan data yang adaptif terhadap ancaman, berbasis risiko, terdokumentasi, dapat diaudit, serta relevan dengan kebutuhan tata kelola keamanan modern.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Pemetaan Aset Data dan Kebutuhan Perlindungan

Hasil sintesis literatur menunjukkan bahwa pengembangan sistem informasi keamanan data pada perusahaan teknologi harus diawali dengan pemetaan aset data yang jelas. Aset data tidak hanya berupa basis data utama, tetapi juga mencakup kredensial pengguna, endpoint API, arsip internal, log aktivitas, dokumen transaksi, data pelanggan, konfigurasi server, data operasional *cloud*, serta informasi yang dipertukarkan antarlayanan. Pemetaan ini penting karena setiap aset memiliki tingkat sensitivitas, nilai bisnis, dan potensi risiko yang berbeda. Dalam konteks keamanan informasi, aset data perlu dilindungi berdasarkan prinsip confidentiality, integrity, and availability, yakni kerahasiaan, keutuhan, dan ketersediaan informasi [19]. Dengan cara ini, kebutuhan sistem tidak dimulai dari pemilihan teknologi keamanan, tetapi dari pemahaman terhadap data apa yang paling kritis bagi keberlangsungan layanan perusahaan [20].

Hasil pemetaan juga menunjukkan bahwa aset data pada perusahaan teknologi cenderung tersebar di berbagai lapisan sistem. Pada lapisan aplikasi web, aset utama berkaitan dengan data input pengguna, sesi *login*, *cookie*, pustaka *JavaScript*, konfigurasi keamanan, dan mekanisme pengiriman data. Pada lapisan layanan, aset penting muncul dalam bentuk *endpoint* API, token, *scope* akses, dan komunikasi antarlayanan. Pada lapisan penyimpanan, aset data mencakup basis data transaksi, arsip digital, file terenkripsi, dan cadangan data. Aplikasi web masih dapat memiliki kelemahan pada konfigurasi dasar, seperti tidak adanya *Content Security Policy*, *missing anti-clickjacking header*, *cookie* tanpa *secure flag*, dan *mixed content*. Temuan tersebut memperlihatkan bahwa kebutuhan informasi keamanan harus mencakup data teknis terkait konfigurasi sistem, bukan hanya data pengguna atau data transaksi [21].

3.2 Hasil Identifikasi Risiko Keamanan Data

Hasil analisis menunjukkan bahwa risiko keamanan data pada perusahaan teknologi dapat dikelompokkan ke dalam risiko akses tidak sah, risiko manipulasi data, risiko eksploitasi aplikasi, risiko kelemahan autentikasi, risiko kesalahan konfigurasi, risiko kebocoran informasi, dan risiko ketidaksiapan tata kelola. Risiko tersebut saling berkaitan karena kelemahan pada satu bagian sistem dapat memicu gangguan pada bagian lain. Sebagai contoh, lemahnya validasi input dapat membuka peluang SQL Injection, sedangkan pengelolaan hak akses yang tidak tepat dapat menyebabkan penyalahgunaan data oleh pengguna internal maupun eksternal. Salah satu parameter form login pada sistem berbasis web dapat rentan terhadap SQL Injection, bahkan eksploitasi berhasil mengakses beberapa database, tabel, dan kolom. Temuan ini menjadi bukti bahwa sistem yang tampak berjalan normal tetap dapat menyimpan kerentanan serius apabila pengujian keamanan tidak dilakukan secara sistematis.

Risiko lain yang menonjol adalah risiko pada layanan berbasis API dan *cloud computing*. Komunikasi REST API yang bersifat *stateless* membutuhkan mekanisme autentikasi dan otorisasi yang kuat agar akses terhadap fungsi sistem dapat dikendalikan secara sah. Dalam sistem *microservice*, setiap layanan dapat berdiri sendiri dan berkomunikasi melalui API, sehingga *endpoint* yang tidak terlindungi dapat menjadi pintu masuk serangan. *Cloud computing* memiliki risiko tersendiri karena data disimpan pada lingkungan terdistribusi dan tidak sepenuhnya berada dalam kendali langsung organisasi. Pada lingkungan ini, ancaman dapat muncul melalui akses tidak sah, kelemahan perjanjian keamanan dengan penyedia layanan, penyadapan data, serta risiko gangguan koneksi yang menghambat akses terhadap data.

3.3 Hasil Kategorisasi Kebutuhan Informasi Keamanan

Berdasarkan sintesis penelitian terdahulu, kebutuhan informasi keamanan data dapat dikategorikan ke dalam enam dimensi utama, yaitu informasi aset data, informasi risiko keamanan, informasi akses pengguna, informasi enkripsi dan integritas, informasi audit dan monitoring, serta informasi tata kelola keamanan. Kategori ini memperluas Tabel 1 pada bagian metodologi, karena hasil analisis menunjukkan bahwa setiap dimensi tidak berdiri sendiri, melainkan membentuk hubungan berlapis antara aset, ancaman, kontrol, dan keluaran informasi keamanan. Informasi aset data berfungsi untuk menentukan prioritas perlindungan. Informasi risiko keamanan digunakan untuk mengidentifikasi jenis ancaman dan dampaknya. Informasi akses pengguna digunakan untuk mengatur siapa yang boleh mengakses data, melalui mekanisme apa, dan dalam batas kewenangan apa. Informasi enkripsi dan integritas mendukung perlindungan data selama penyimpanan dan transmisi. Informasi audit dan monitoring diperlukan untuk mendeteksi anomali serta menelusuri perubahan. Informasi tata kelola keamanan dibutuhkan untuk memastikan adanya kebijakan, prosedur, standar, dan evaluasi kematangan.

Tabel 2. Hasil Kategorisasi Kebutuhan Informasi Keamanan Data Pada Perusahaan Teknologi

Dimensi Hasil Analisis	Temuan Utama	Basis Literatur
Aset Data	Data Pengguna, Transaksi, API, Cloud, Arsip, Log, Dan Kredensial Menjadi Objek Utama Perlindungan	Widyarti & Sungkowo (2026); Sakinah, dkk. (2024)
Risiko Keamanan	SQL Injection, Salah Konfigurasi, Brute Force, Spoofing, Akses Tidak Sah, Dan Kebocoran Data Menjadi Ancaman Dominan	Khairul, dkk. (2025); Sihombing, dkk. (2026)
Akses Pengguna	Oauth2, Token, Scope, RBAC, Rate Limiting, Dan Role Permission Diperlukan Untuk Otorisasi	Purba, dkk. (2025); Marya & Febriyani (2025)
Enkripsi Dan Integritas	AES, RSA-CRT, Blockchain, Dan Digital Signature Mendukung Kerahasiaan Serta Keaslian Data	Hakim & Margolang (2025); Purba, dkk (2025); Rohman & Rahmadika (2025)
Audit Dan Monitoring	Audit Trail, Audit Log, Alert, Dan Laporan Insiden Diperlukan Untuk Ketertelusuran	Bangun, dkk. (2026); Ardiyansa, dkk. (2025)
Tata Kelola Keamanan	ISO 27001, ISO 31000, COBIT, Dan Indeks KAMI Diperlukan Untuk Evaluasi Kematangan Dan Risiko	Widyarti & Sungkowo (2026); Nathanael & Nataliani (2025); Bangun, dkk. (2026)

Tabel 2 menunjukkan bahwa kebutuhan informasi keamanan data bersifat multidimensi dan menuntut integrasi antara dimensi teknis dan manajerial. Dimensi teknis terlihat pada kebutuhan *API security*, *vulnerability assessment*, *penetration testing*, *enkripsi*, *rate limiting*, dan RBAC. Dimensi manajerial terlihat pada kebutuhan kebijakan, SOP, audit, dokumentasi, manajemen risiko, dan pengukuran kematangan. Dengan demikian, hasil penelitian ini memperlihatkan bahwa sistem informasi keamanan data harus mampu menggabungkan informasi operasional keamanan dengan informasi tata kelola keamanan.

3.4 Model Hasil Analisis Kebutuhan Informasi Keamanan Data

Berdasarkan seluruh hasil sintesis, penelitian ini menghasilkan model kebutuhan informasi untuk pengembangan sistem informasi keamanan data pada perusahaan teknologi. Model ini menghubungkan aset data, risiko keamanan, pengguna, kontrol akses, enkripsi, pengujian kerentanan, monitoring, tata kelola, dan rekomendasi mitigasi. Sebagaimana ditunjukkan pada Gambar 1 dalam bagian metodologi, alur analisis dimulai

dari aset data perusahaan teknologi, dilanjutkan dengan klasifikasi risiko keamanan, pemetaan pengguna dan hak akses, pemilihan kontrol keamanan, penerapan audit trail dan monitoring, serta penyusunan laporan keamanan dan rekomendasi mitigasi.

Temuan penelitian menunjukkan bahwa pengembangan sistem informasi keamanan data pada perusahaan teknologi perlu dimulai dari pemahaman yang jelas terhadap aset data, bukan langsung dari pemilihan perangkat atau aplikasi keamanan. Posisi ini penting karena perusahaan teknologi mengelola aset digital yang beragam, seperti kredensial pengguna, data pelanggan, data transaksi, log aplikasi, *endpoint* API, arsip internal, konfigurasi server, data berbasis *cloud*, dan catatan komunikasi antarlayanan. Setiap aset memiliki tingkat sensitivitas, eksposur, dan nilai operasional yang berbeda. Oleh karena itu, sistem informasi keamanan harus mampu mengidentifikasi data apa yang perlu dilindungi, di mana data berada, siapa yang dapat mengaksesnya, bagaimana data diproses, dan risiko apa yang dapat muncul apabila kerahasiaan, integritas, atau ketersediaannya terganggu.

Hasil penelitian juga menunjukkan bahwa aset data pada perusahaan teknologi tidak tersimpan dalam satu lapisan tunggal. Data tersebar dalam aplikasi web, API, lingkungan cloud, modul autentikasi, repositori dokumen, dan log pemantauan. Struktur yang terdistribusi ini membuat analisis kebutuhan informasi menjadi lebih kompleks. Sistem berbasis web masih dapat memiliki kelemahan keamanan meskipun secara fungsional berjalan normal, seperti tidak adanya *Content Security Policy header*, kesalahan konfigurasi lintas domain, missing *anti-clickjacking header*, *cookie* yang tidak aman, dan *mixed content*. Artinya, kebutuhan informasi tidak terbatas pada data bisnis atau data pengguna saja. Kebutuhan tersebut juga mencakup data konfigurasi, metadata sistem, security header, catatan akses, dan indikator kerentanan. Bagi perusahaan teknologi, informasi semacam ini menjadi penting karena keamanan sistem tidak hanya bergantung pada fungsi aplikasi, tetapi juga pada kualitas konfigurasi dasar dan tata kelola keamanan.

Diskusi ini perlu dipahami dalam batasan bahwa model yang dikembangkan masih bersifat konseptual dan berbasis literatur. Model ini belum divalidasi melalui pengujian empiris pada perusahaan teknologi tertentu. Penelitian berikutnya dapat melakukan validasi ahli, studi kasus, survei, atau pengembangan prototipe untuk menguji keterterapan model. Penelitian lanjutan juga dapat mengkaji bagaimana ukuran organisasi, ketergantungan pada cloud, arsitektur sistem, tekanan regulasi, dan budaya keamanan memengaruhi implementasi model yang diusulkan. Pengujian empiris akan memberikan dasar yang lebih kuat untuk menyempurnakan dimensi model dan menentukan kebutuhan informasi mana yang paling kritis pada berbagai jenis perusahaan teknologi.

4. KESIMPULAN

Studi ini menunjukkan bahwa pengembangan sistem informasi keamanan data pada perusahaan teknologi perlu dibangun melalui analisis kebutuhan informasi yang terstruktur, bukan hanya melalui penambahan fitur keamanan secara terpisah. Temuan utama memperlihatkan bahwa kebutuhan keamanan data mencakup pemetaan aset data, identifikasi risiko, kontrol akses, autentikasi dan otorisasi, enkripsi, audit trail, vulnerability assessment, penetration testing, monitoring, serta tata kelola keamanan.

Komponen tersebut saling berkaitan karena kelemahan pada satu lapisan sistem dapat memengaruhi kerahasiaan, integritas, dan ketersediaan data secara keseluruhan.

Hasil diskusi menegaskan bahwa perusahaan teknologi membutuhkan pendekatan keamanan yang menyatukan dimensi teknis dan manajerial. Kontrol seperti OAuth2, role-based access control, rate limiting, enkripsi AES atau RSA, *blockchain*, dan pengujian kerentanan perlu didukung oleh tata kelola berbasis standar seperti ISO 27001, ISO 31000, COBIT, dan evaluasi kematangan keamanan. Implikasi praktisnya, model kebutuhan informasi yang diusulkan dapat membantu perusahaan menyusun prioritas perlindungan data, menetapkan kontrol yang sesuai, memantau insiden, dan menghasilkan rekomendasi mitigasi yang dapat ditindaklanjuti.

Kontribusi studi ini terletak pada penyatuan berbagai literatur keamanan yang sebelumnya cenderung terpisah menjadi satu kerangka konseptual kebutuhan informasi keamanan data. Penelitian selanjutnya disarankan melakukan validasi empiris melalui studi kasus, survei pakar, atau pengembangan prototipe agar model ini dapat diuji pada berbagai jenis perusahaan teknologi dengan tingkat kompleksitas sistem yang berbeda.

DAFTAR PUSTAKA

- [1] H. Shabrina and A. Fauzi, “SISTEM INFORMASI DIGITALISASI SOP BERBASIS WEB UNTUK MENINGKATKAN EFISIENSI OPERASIONAL PADA PERUSAHAAN LOGISTIK DI PURWAKARTA,” *Rabit: Jurnal Teknologi dan Sistem Informasi Univrab*, vol. 11, no. 1, pp. 2015–2028, Feb. 2026, doi: 10.36341/rabit.v11i1.7622.
- [2] T. Mary and N. Febriyani, “Peningkatan Keamanan Sistem Informasi Berbasis Laravel 12 dengan Rate Limiting dan Role-Based Access Control (RBAC),” *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 7, no. 3, pp. 473–481, Jul. 2025, doi: 10.47233/jteksis.v7i3.1976.
- [3] J. Kecerdasan Buatan, K. dan Teknologi Informasi, A. Halimi, F. Nur Fajri, and F. Rizal, “Pengembangan Sistem Identifikasi Ancaman Keamanan pada Sistem Penerimaan Mahasiswa Baru dengan Framework Laravel,” *Tahun*, vol. 6, no. 1, 2025, [Online]. Available: <https://ejournal.unuja.ac.id/index.php/core>
- [4] Khairul, A. Abdullah, and S. Sucipto, “Penetration Testing pada Kerentanan Keamanan Sistem PELAKAT Menggunakan SQL Injection,” *Jurnal Nasional Teknologi dan Sistem Informasi*, vol. 11, no. 1, pp. 78–86, May 2025, doi: 10.25077/teknosi.v11i1.2025.78-86.
- [5] A. Oktavian and Z. Imaduddin, “Analisis Keamanan Sistem Informasi RKSchool Depok Menggunakan Metode VAPT,” *Jurnal Teknologi Dan Sistem Informasi Bisnis*, vol. 8, no. 1, pp. 46–54, Jan. 2026, doi: 10.47233/jteksis.v8i1.2363.
- [6] Virki Fardian Nur Rohman and Muhammad Rahmadika, “Analisis Implementasi Teknologi Blockchain pada Sistem Informasi untuk Meningkatkan Keamanan Data Mahasiswa,” *Jurnal Teknik Mesin, Industri, Elektro dan Informatika*, vol. 4, no. 2, pp. 22–31, Mar. 2025, doi: 10.55606/jtmei.v4i2.4888.

- [7] M. Ardiyansa, Efitra, and B. Baharsyah, “Perancangan Sistem Informasi Pengarsipan Data Internal Berbasis Web Dengan Fitur Keamanan Enkripsi Di BPSIP Jambi,” *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)*, vol. 4, no. 2, pp. 677–686, Jul. 2025, doi: 10.62712/juktisi.v4i2.504.
- [8] M. Nathanael and Y. Nataliani, “ANALISIS MANAJEMEN RISIKO SISTEM INFORMASI BERBASIS ISO 31000:2018 PADA PERUSAHAAN LOGISTIK PENGIRIMAN BARANG,” *Jurnal Pendidikan Teknologi Informasi (JUKANTI)*, vol. 8, no. 2, pp. 108–123, Nov. 2025, doi: 10.37792/jukanti.v8i2.1547.
- [9] G. Ramadhan Purba, Rizal, and Y. Afrillia, “KEAMANAN ENDPOINT API MENGGUNAKAN OAUTH2 PADA UNIT LAYANAN TERPADU UNIVERSITAS MALIKUSSALEH,” *Rabit : Jurnal Teknologi dan Sistem Informasi Univrab*, vol. 10, no. 2, pp. 1424–1434, Aug. 2025, doi: 10.36341/rabit.v10i2.6543.
- [10] A. Rahman Hakim, K. Fadhli Margolang, I. Keperawatan, and S. Tinggi Ilmu Kesehatan Columbia Asia, “Nomor 2,” *Volume*, vol. 8, pp. 108–114, 2025, [Online]. Available: <https://ojs.trigunadharma.ac.id/index.php/jsk/index>
- [11] A. Purnomo and R. Hartono, “Analisa Waktu Respon pada Metode Pengukuran Jarak pada Sistem Informasi Geografi,” *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 12, no. 1, pp. 39–46, Feb. 2025, doi: 10.25126/jtiik.2025128690.
- [12] M. Dodi Setyawan, D. Laily Fithri, S. Adiyono, Z. Romadhon, A. Widodo, and P. Setiaji, “Implementasi Customer Relationship Management (CRM) Berbasis Web dalam Meningkatkan Penjualan pada Perusahaan Almazone Penulis Korespondensi.” [Online]. Available: <http://www.jurnal.umk.ac.id/sitech>
- [13] E. N. Nur'allifa, R. R. Judie Putra, and M. Nursalman, “RSA Blind Signature sebagai dasar pengamanan pada sistem e-voting dengan Prinsip Frictionless User : studi desain dan tinjauan keamanan,” *Jurnal Komputer Teknologi Informasi Sistem Informasi (JUKTISI)*, vol. 4, no. 2, pp. 782–793, Jul. 2025, doi: 10.62712/juktisi.v4i2.527.
- [14] H. P. Fitriani, A. Halim Munawar, B. N. Fajar, and F. N. Aima, “Analisis Keamanan dan Ancaman pada Jaringan Komputer di Era Internet of Things (IoT) dalam Bidang Teknologi Sistem Pendidikan,” *Jurnal Nasional Komputasi dan Teknologi Informasi (JNKTI)*, vol. 8, no. 1, p. 2025.
- [15] R. Romayanti Purba and J. Halim, “Volume 8 ; Nomor 1,” *Januari*, 2025, [Online]. Available: <https://ojs.trigunadharma.ac.id/index.php/jsk/index>
- [16] Oktaviana Bangun, Fransisko, Dolly, Sarah, Reski, and Dewi, “Penerapan Framework COBIT dalam Meningkatkan Keamanan Data pada Sistem Informasi Pegadaian Swasta PT Budi Gadai Indonesia,” *LOFIAN: Jurnal Teknologi Informasi dan Komunikasi*, vol. 5, no. 2, pp. 29–37, Feb. 2026, doi: 10.58918/lofian.v5i2.292.

- [17] “1. S1 1. EVALUASI KEAMANAN PENERAPAN SISTEM INFORMASI BERDASARKAN INDEKS KEAMANAN INFORMASI (KAMI) PADA SMK N 1 NANGGULAN”.
- [18] F. Yeovandi, S. Sabariman, and S. E. Prasetyo, “Evaluasi Keamanan Sistem Autentikasi Biometrik pada Smartphone dan Rekomendasi Implementasi Optimal,” *JTIM: Jurnal Teknologi Informasi dan Multimedia*, vol. 7, no. 1, pp. 133–148, Jan. 2025, doi: 10.35746/jtim.v7i1.653.
- [19] A. Sakinah, S. Khofipah, P. Sifrah Tripena, and M. Anjelina Dewi Karoko, “Analisis Kerentanan: Memanfaatkan Kerentanan dan Pengaruh Keamanan Siber pada Cloud Computing Penulis Korespondensi.” [Online]. Available: <http://www.jurnal.umk.ac.id/sitech>
- [20] Saputra, Y., & Irawan, D. (2024). PENERAPAN ALGORITMA GREEDY UNTUK PENYUSUNAN JADWAL KERJA DI INDUSTRI PERHOTELAN. *JURNAL DATA SAINS DAN TEKNOLOGI INFORMASI (DASTIS)*, 2(01), 31–40. <https://doi.org/10.62003/c53fxr97>
- [21] A. P. N. Sihombing, Agung Prabowo, Ibnu Daqiqil Id, and Tisha Melia, “Analisis kerentanan keamanan pada sistem informasi akademik berbasis web menggunakan OWASP-ZAP,” *INFOTECH: Jurnal Informatika & Teknologi*, vol. 7, no. 1, pp. 150–158, Jun. 2026, doi: 10.37373/infotech.v7i1.2277.