Vol. 6, No. 2, Agustus 2025, hal. 206-213

Jurnal Computer Science and Information Technology (CoSciTech)

p-ISSN: 2723-567X
e-ISSN: 2723-5661

http://ejurnal.umri.ac.id/index.php/coscitech/index

PENILAIAN RESIKO KEAMANAN APLIKASI WEB MENGGUNAKAN STANDAR ISO/IEC 27005 : 20022 PADA LAYANAN ORGANISASI

Nungky Awang Chandra[*1], Mohamad Yusuf[2]
Email: [1]nungky_awang@mercubuana.ac.id, [2]mhd.yusuf@mercubuana.ac.id

[1]Program Studi Teknik Informati, Fakultas Ilmu Komputer, Universitas Mercu Buana
[2]Program Studi Teknik Informati, Fakultas Ilmu Komputer, Universitas Mercu Buana

Diterima: 10 Agustus 2025 | Direvisi: 28 Agustus 2025 | Disetujui: 3 September 2025

Abstrak

Permasalahan akan resiko kerentanan dan ancaman keamanan informasi semakin meningkat, sehingga diperlukan kemampuan dalam menganalisa situasi resiko ancaman dan kerentanan keamanan Informasi yang akan datang khususnya untuk layanan aplikasi sebuah organisasi masyarakat. Penelitian tentang penerapan analisa resiko keamanan informasi berdasarkan kerangka ISO/IEC 27005 : 2022 pada aplikasi layanan sebuah organisasi. ISO/IEC 27005 : 2022 merupakan standar internasional yang digunakan untuk petunjuk penerapan proses analisa resiko keamanan informasi yang paling efektif dibandingkan kerangka metode penilaian resiko keamanan informasi lainnya. Hasil dari penilaian adalah mengukur tingkat resiko keamanan informasi dari sebuah aplikasi layanan organisasi sehingga dapat digunakan sebagai bahan perbaikan dalam melakukan tindakan pencegahan dan pengendalian keamanan informasi agar celah kerentanan dan ancaman serangan keamanan informasi bisa dikurangi. Adapun hasil penelitian ini dapat mengambarkan nilai risiko pada aplikasi layanan organisasi dengan 3 kategori bernilai risiko tinggi yaitu pada *data transaksi finansial* (nilai risiko 20), *database pelanggan* (nilai risiko 16), dan *konfigurasi server* (nilai risiko 15). Dan nilai risiko sedang terdapat pada *API publik* (nilai risiko 12) dan *data laporan internal* (nilai risiko 6).

Kata kunci: *Resiko; Keamanan; ISO 27005; Aset Informasi; Aplikasi*

ISO/IEC 27005:2022 STANDARD FOR WEBSITE SECURITY RISK ASSESSMENT IN ORGANIZATIONAL SERVICES

The problem of information security vulnerability and threat risks is increasing, so it is necessary to be able to analyze the risk situation of future information security threats and vulnerabilities, especially for the application services of a community organization. Research on the application of information security risk analysis based on the ISO/IEC 27005:2022 framework in an organization's service applications. ISO/IEC 27005:2022 is an international standard used for guidelines on the implementation of the most effective information security risk analysis process compared to other information security risk assessment method frameworks. The results of the assessment are to measure the level of information security risk of an organization's service application so that it can be used as a basis for improvement in carrying out information security prevention and control measures so that vulnerability gaps and threats of information security attacks can be reduced.Tempatkan abstrak berbahasa Inggris pada bagian ini. Gunakan font Times New Roman 10pt, italic.

Keywords: *Risk, Security, ISO 27005, Information Asset, Application*

1. PENDAHULUAN

Perkembangan ancaman di dunia siber dan meningkatnya kompleksitas infrastruktur jaringan komputer telah menyebabkan keamanan informasi menjadi perhatian utama dalam berbagai sektor, mulai dari pemerintahan hingga layanan digital. Meskipun banyak penelitian telah dilakukan dalam bidang ini, tantangan dalam mengelola risiko terhadap **kerahasiaan (confidentiality)**, **integritas (integrity)**, dan **ketersediaan (availability)** informasi masih menjadi isu kritis (Chandra et al., 2022; Akinrolabu et al., 2019).

Penilaian risiko keamanan informasi merupakan proses penting untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko terhadap aset informasi penting dalam organisasi. Tujuan utama dari penilaian risiko ini adalah untuk menetapkan kontrol yang efektif demi mengurangi risiko ke tingkat yang dapat diterima. Pendekatan penilaian risiko dapat dilakukan secara **kuantitatif**, **semi-kuantitatif**, atau **kualitatif**, tergantung pada tujuan dan konteks organisasi (ISO 31010, 2009; ISO 27005, 2022).

ISO/IEC 27005:2022 merupakan salah satu standar internasional yang memberikan panduan teknis dan metodologis untuk manajemen risiko keamanan informasi, serta dapat digunakan secara terintegrasi dengan ISO/IEC 27001:2013. Dalam standar ini, penilaian risiko dibagi menjadi tiga tingkatan: **rendah**, **sedang**, dan **tinggi**, tergantung pada tingkat kompleksitas dan sumber daya organisasi (ISO 27005, 2022). Proses manajemen risiko dalam standar ini meliputi identifikasi risiko, analisis risiko, evaluasi risiko, penanganan risiko, monitoring, komunikasi, dan konsultasi.

Komponen utama dari sistem manajemen keamanan informasi (SMKI) adalah **Information Security Risk Assessment (ISRA)**, yang berperan dalam mendukung organisasi mengidentifikasi aset utama dan menilai tingkat risiko secara komprehensif. Menurut Shamala et al. (2015), ISRA dapat dilakukan melalui pendekatan **formal** yang mengukur kemungkinan dan dampak dari potensi ancaman, atau melalui pendekatan **temporal**, yang melibatkan pengujian sistem secara langsung untuk menghasilkan nilai risiko (Wangen et al., 2018).

Selain ISO/IEC 27005, terdapat pula berbagai metodologi lain untuk pelaksanaan ISRA, seperti:

- **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- **FAIR** (Factor Analysis of Information Risk)
- **CRAMM** (CCTA Risk Analysis and Management Method)
- **NIST SP 800-30** dari NIST (Computer Security Division, 2022)

(Studi-studi seperti oleh Shameli-Sendi et al., 2016; Griogoriadis et al., 2022; Aksu et al., 2017 juga memberikan kontribusi penting dalam pengembangan pendekatan dan model risiko informasi secara kuantitatif dan adaptif.) Penelitian ini mengadopsi pendekatan berdasarkan **ISO/IEC 27005:2022** dalam melakukan penilaian risiko keamanan informasi pada aplikasi layanan milik suatu organisasi. Aplikasi tersebut digunakan untuk mendukung operasional penting yang berkaitan dengan pelayanan masyarakat. Dengan demikian, perlindungan terhadap aset informasi dan evaluasi risiko menjadi sangat penting.

Kontribusi Penelitian

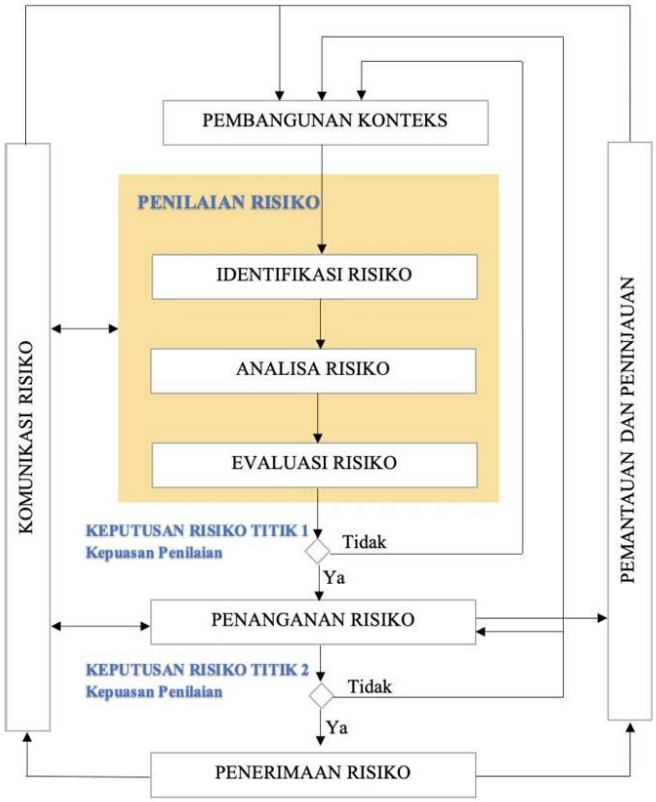
1. Memberikan gambaran implementasi penilaian risiko keamanan informasi berdasarkan kerangka kerja ISO/IEC 27005:2022.
2. Mengembangkan pendekatan evaluasi risiko dengan mengintegrasikan berbagai teknik untuk menghasilkan hasil yang **lebih akurat dan relevan dengan kebutuhan organisasi** (Chandra et al., 2022).Pendahuluan tidak lebih dari 1.500 kata

State of the art dari penelitian ini adalah penilaian resiko keamanan informasi dengan metode ISO/IEC 27005 : 2022. Metode ISO/IEC 27005 : 20022 merupakan metode penilaian resiko keamanan informasi terbaru yang dipublikasi tahun 2022. Kerangka ISO/IEC 27005 : 2022 merupakan kerangka penilaian keamanan informasi yang tahapannya metodenya berbeda dengan beberapa metode penilaian resiko lainnyaa seperti pada penelitian sebelumnya menggunakan metode FMEA dengan judul *Information Security Risk Assessment Using Situational Awareness Frameworks and Application Tools (Risk, MDPI, Nungky et al. 2022).*

2. METODE PENELITIAN

2.1. Tahapan Penelitian

Metode penelitian ini mengacu kepada standard ISO 27005 : 2022 yaitu yaitu merupa deskriptif kualitatif dengan pendekatan studi kasus pada salah satu aplikasi layanan sebuah organisasi. Dapat ditunjukan pada gambar 1. Dibawah ini.



Gambar 2.1. Penilaian Risiko Keamanan Informasi ISO 27005 : 2022

Adapun tahapan penelitian ini sebagai berikut :

1. **Membangun Konteks Organisasi**
   - Mengidentifikasi lingkungan operasional aplikasi layanan.
   - Menentukan aset informasi yang bernilai, seperti data pengguna, kredensial, dan konfigurasi sistem.
   - Mengidentifikasi pemangku kepentingan dan tujuan keamanan informasi.
2. **Identifikasi Risiko**
   - Mengidentifikasi potensi ancaman seperti malware, phishing, dan akses tidak sah.
   - Menentukan kerentanan yang ada dalam sistem aplikasi seperti kesalahan konfigurasi, celah keamanan pada kode, atau kurangnya pembaruan sistem.
   - Mengembangkan skenario risiko yang realistis berdasarkan kombinasi antara ancaman dan kerentanan.
3. **Analisa Risiko**
   - Menilai kemungkinan terjadinya setiap risiko.
   - Menilai dampak potensial terhadap organisasi jika risiko tersebut terjadi.
   - Menggunakan pendekatan kualitatif dengan klasifikasi tinggi, sedang, dan rendah.
4. **Evaluasi Risiko**
   - Membandingkan tingkat risiko terhadap kriteria yang ditetapkan.
   - Menentukan risiko yang dapat diterima dan yang perlu ditangani.
5. **Penanganan dan Penerimaan Risiko**
   - Menentukan tindakan mitigasi, seperti penerapan kontrol akses, enkripsi data, atau peningkatan pelatihan keamanan.
   - Memilih strategi penanganan risiko yang sesuai: menghindari, mengurangi, mentransfer, atau menerima risiko.
6. **Pemantauan dan Tinjauan**
   - Melakukan pemantauan berkala terhadap efektivitas tindakan mitigasi.

- Melakukan peninjauan ulang terhadap risiko yang mungkin berubah akibat perkembangan teknologi atau proses bisnis.

7. **Komunikasi dan Konsultasi Risiko**
   - Melibatkan semua pemangku kepentingan dalam proses penilaian risiko.
   - Mendokumentasikan semua aktivitas untuk keperluan audit dan peningkatan berkelanjutan.

2.2. Teknik Pengumpulan Data

Penelitian ini menggunakan teknik:

1. **Wawancara** dengan pengembang dan administrator aplikasi.
2. **Observasi** langsung terhadap penggunaan dan operasional aplikasi.
3. **Studi dokumen** terhadap SOP, log keamanan, dan dokumentasi sistem.
4. **Kuesioner** (jika diperlukan) untuk mendapatkan persepsi pengguna terhadap risiko.

2.3. Teknik Analisis Risiko

Menganalisis risiko yang teridentifikasi mencakup penilaian dampak risiko terhadap aset dan kemungkinan terjadinya risiko yang teridentifikasi. Dampak di sini diperiksa berdasarkan kerahasiaan, integritas, dan ketersediaan informasi. Misalnya, jika server mati dan informasi di dalamnya tidak dapat diakses, ketersediaannya akan terpengaruh. Demikian pula, jika ada akses tidak sah ke informasi yang tersimpan, kerahasiaan akan terganggu. Ada berbagai skala yang dapat dipilih untuk menentukan dampak dan kemungkinan, dan organisasilah yang menentukan pilihannya. Skalanya bisa tinggi-sedang-rendah, 0 – 10/0 – 5, dan seterusnya. Keputusan harus didokumentasikan dalam metodologi penilaian risiko. Berdasarkan NIST SP-800-30 dan ISO 27005 : 2022, tingkat risiko dapat ditentukan menggunakan rumus berikut:

$$Risiko = Dampak\ x\ Kemungkinan\ atau\ Risiko = Dampak + Kemungkinan$$

3. HASIL DAN PEMBAHASAN

Setelah dilakukan pengumpulan data dengan fokus pada penentuan ruanglingkup aplikasi layanan. Dalam konteks aplikasi layanan, setiap aset informasi memiliki tingkat kepentingan yang berbeda jika dilihat dari tiga aspek utama keamanan informasi, yaitu kerahasiaan (Confidentiality), integritas (Integrity), dan ketersediaan (Availability).

Pertama, aspek kerahasiaan berkaitan dengan perlindungan informasi agar tidak diakses atau diungkapkan oleh pihak yang tidak berwenang. Aset yang memiliki tingkat kerahasiaan tinggi biasanya berisi data sensitif, seperti **database pelanggan** yang memuat nama, alamat, email, nomor telepon, hingga identitas resmi. Kebocoran terhadap informasi ini tidak hanya melanggar privasi pengguna, tetapi juga dapat menimbulkan risiko hukum dan kerugian reputasi bagi organisasi. Contoh lainnya adalah **data medis pasien** pada aplikasi layanan kesehatan, yang dilindungi ketat oleh regulasi seperti GDPR atau UU Perlindungan Data Pribadi.

Kedua, aspek integritas mengacu pada keakuratan dan keutuhan informasi, sehingga data tetap valid dan tidak dimodifikasi tanpa otorisasi. Aset yang memiliki integritas tinggi meliputi **data transaksi finansial** pada aplikasi e-commerce, di mana perubahan sekecil apapun pada jumlah atau nilai transaksi dapat mengakibatkan kerugian finansial. Begitu pula dengan **data hasil laboratorium** pada sistem rumah sakit, yang jika diubah dapat mempengaruhi diagnosis dan tindakan medis. Selain itu, **konfigurasi server aplikasi** juga termasuk aset dengan integritas tinggi, karena perubahan yang tidak sah dapat menciptakan celah keamanan atau mengganggu operasional sistem.

Ketiga, aspek ketersediaan berkaitan dengan memastikan informasi dan sistem dapat diakses oleh pihak berwenang kapan pun dibutuhkan. Aset dengan ketersediaan tinggi mencakup **server aplikasi layanan publik**, seperti sistem e-banking atau e-learning, yang harus beroperasi 24/7 untuk memenuhi kebutuhan pengguna. **Data real-time** pada sistem pemantauan lalu lintas juga membutuhkan ketersediaan tinggi, karena downtime dapat menyebabkan gangguan koordinasi dan keselamatan. Demikian pula, **sistem tiket online** pada saat penjualan besar membutuhkan ketersediaan maksimal, karena gangguan layanan dapat menyebabkan kerugian bisnis dan hilangnya kepercayaan pelanggan.

Dengan memahami nilai setiap aset berdasarkan ketiga aspek CIA ini, organisasi dapat menentukan prioritas perlindungan dan alokasi sumber daya keamanan informasi. Misalnya, **data transaksi finansial** sering kali memiliki nilai tinggi pada ketiga aspek sekaligus, sehingga memerlukan perlindungan menyeluruh, mulai dari enkripsi, kontrol akses, hingga mekanisme failover untuk menjamin ketersediaannya. Sebaliknya, **API publik** mungkin memiliki tingkat kerahasiaan rendah tetapi memerlukan integritas dan ketersediaan tinggi, sehingga strategi pengamanannya akan lebih difokuskan pada pencegahan modifikasi data dan mitigasi

serangan DoS/DDoS. Adapun contoh perhitungan prioritas nilai asset dalam penelitian aplikasi layanan disebuah organsisasi sebagai berikut :

Tabel 2.1. Penilaian Aset Aplikasi Layanan Organisasi berdasarkan Kerahasiaan (C), Integritas (I), dan Ketersediaan (A)

Aset Informasi	C	I	A
Database pelanggan	Tinggi (5)	Sedang (3)	Sedang (3)
Data transaksi finansial	Tinggi (5)	Tinggi (5)	Tinggi (5)
API publik	Rendah (2)	Tinggi (5)	Tinggi (5)
Konfigurasi server	Sedang (3)	Tinggi (5)	Tinggi (5)
Data laporan internal	Sedang (3)	Tinggi (5)	Rendah (2)

Nilai Skor Antara 1–5, dengan klasifikasi tingkat prioritas rendah (1–2), sedang (3), tinggi (4–5).

Adapun dari penelitian ini dalam menentukan nilai prioritas aset informasi aplikasi layanan dengan membobotkan faktor kerahasiaan, integritas dan ketersediaan, sebagai berikut:

- Kerahasiaan (C) = 40% (0.40)
- Integritas (**I**) = 35% (0.35)
- Ketersediaan (**A**) = 25% (0.25)

Sehingga kita tetapkan rumus penilaian prioritas aset informasi aplikasi layanan sebagai berikut :

$$Prioritas\ Aset = (C \times 0.40) + (I \times 0.35) + (A \times 0.25)$$

Sehingga hasil penilaian prioritas aset informasi aplikasi dapat ditunjukan pada tabel 2.2. sebagai berikut :

Tabel 2.2. Hasil Penilaian Prioritas Aset Aplikasi Layanan Organisasi berdasarkan Kerahasiaan (C), Integritas (I), dan Ketersediaan (A)

Aset Informasi	C	I	A	Perhitungan	Nilai Prioritas	Status
Database pelanggan	5	3	3	(5×0.40) + (3×0.35) + (3×0.25)	3.85	Prioritas Tinggi
Data transaksi finansial	5	5	5	(5×0.40) + (5×0.35) + (5×0.25)	5.00	Prioritas Sangat Tinggi
API publik	2	5	5	(2×0.40) + (5×0.35) + (5×0.25)	3.85	Prioritas Tinggi
Konfigurasi server	3	5	5	(3×0.40) + (5×0.35) + (5×0.25)	4.30	Prioritas Tinggi
Data laporan internal	3	5	2	(3×0.40) + (5×0.35) + (2×0.25)	3.35	Prioritas Sedang

Dengan hasil interpretasi sebagai berikut :

- Aset dengan nilai **≥ 4** harus segera diberi perlindungan maksimal (kontrol teknis, kebijakan, monitoring).
- Nilai **3–3.99** tetap penting, tetapi bisa diprioritaskan setelah aset yang nilainya lebih tinggi.
- Nilai **< 3** memiliki prioritas rendah, tetapi tetap harus dijaga agar tidak menjadi titik lemah sistem

Berdasarkan hasil nilai prioritas aset pada aplikasi layanan organisasi, maka hasil perhitungan analisis penilaian aset dapat ditunjukan pada tabel 2.3. sebagai berikut :

Tabel 2.3. Hasil Penilaian Risiko Keamanan Informasi Berdasarkan ISO 27005 : 2022

No	Aset Informasi	Prioritas Aset (CIA)	Kerentanan (Vulnerability)	Ancaman (Threat)	Kemungkinan (1–5)	Dampak (1–5)	Nilai Risiko (Likelihood × Impact)	Level Risiko
1	Data transaksi finansial	5.00	Validasi input tidak ketat, enkripsi lemah	Manipulasi transaksi, pencurian data	4	5	20	**Tinggi**

2	Konfigurasi server	4.30	Patch keamanan tidak rutin, tidak ada hardening	Serangan malware, akses ilegal	3	5	15	**Tinggi**
3	Database pelanggan	3.85	Password default, kontrol akses lemah	Kebocoran data pribadi	4	4	16	**Tinggi**
4	API publik	3.85	Tidak ada rate limiting, otentikasi lemah	DDoS, brute force	3	4	12	Sedang
5	Data laporan internal	3.35	Tidak ada integritas checksum	Modifikasi tanpa izin	2	3	6	Sedang

Nilai kemungkinan, dampak dan nilai risiko dalam tabel berdasarkan deskripsi sebagai berikut :

- **Likelihood (Kemungkinan)** dengan nilai antara :
  1 = Sangat jarang terjadi serangan sampai dengan nilai 5 = Sangat sering terjadi
- **Impact (Dampak)** dengan nilai antara :
  1 = Tidak signifikan terhadap dampak layanan sampai dengan nilai 5 = Kritis berpengaruh pada reputasi layanan
- **Tingkat Risiko**:

Tabel 2.4. Kategori Tingkat Risiko

Range Nilai Risiko	Ketegori Tingkat Risiko	Status Tindakan
1-5	Rendah	Diterima dengan Monitoring
6-10	Sedang	Diterima dengan Mitigasi
11-15	Tinggi	Tidak Dapat Diterima
16-25	Sangat Tinggi	Tidak Dapat Diterima

Dari hasil penilian risiko dan tingkat risiko yang dapat diterima maka kita dapat evaluasi tingkat risiko bahwa data transaksi finansial, konfogurasi server, dan database pelanggan merupakan risiko yang tidak dapat diterima. Untuk API Publik dan data Laporan internal nilai risikos sedang artinya risiko dapat diterima dengan mitigasi pengendalian tertentu. Tindakan pengendalian risiko dapat ditunjukan pada tabel 2.5. berikut :

Tabel 2.5. Pengendalian Risiko Keamanan Informasi pada Aplikasi Layanan

No	Aset Informasi	Nilai Risiko	Level Risiko	Tindakan Pengendalian Risiko (Risk Treatment)
1	Data transaksi finansial	20	Tinggi	- Terapkan enkripsi kuat (AES-256) untuk data transaksi
				- Gunakan **Multi-Factor Authentication (MFA)** untuk semua akses sistem pembayaran
				- Implementasi **fraud detection system** real-time
				- Audit log transaksi secara berkala dan deteksi anomali
2	Konfigurasi server	15	Tinggi	- Lakukan patch & update keamanan rutin
				- Terapkan **server hardening** (nonaktifkan port/layanan yang tidak digunakan)
				- Gunakan **IDS/IPS** untuk memantau aktivitas mencurigakan
				- Batasi akses admin hanya untuk personel tertentu dengan MFA
3	Database pelanggan	16	Tinggi	- Enkripsi data sensitif di database (at rest & in transit)
				- Terapkan **role-based access control (RBAC)**
				- Ganti default password dan gunakan kebijakan password kuat
				- Implementasikan **Database Activity Monitoring (DAM)**
4	API publik	12	Sedang	- Terapkan **rate limiting** dan throttling request
				- Gunakan autentikasi berbasis token/JWT
				- Implementasikan **Web Application Firewall (WAF)** khusus API
				- Monitoring log API untuk mendeteksi percobaan serangan
5		6	Sedang	- Gunakan checksum/hash (SHA-256) untuk menjaga integritas file

	Data laporan internal			- Simpan file di repositori terproteksi dengan version control
				- Lakukan backup terjadwal ke media terenkripsi
				- Batasi akses hanya untuk unit terkait

Dari tindakan pengendalian risiko ini akan dikomunikasikan,dikonsultasikan, dimonitoring dan ditinjau sejauh mana efektitas implementasi dari pengendalian risiko.

4. KESIMPULAN

Berdasarkan proses penilaian risiko keamanan informasi yang dilakukan, langkah awal dimulai dari identifikasi dan penentuan prioritas aset informasi menggunakan pendekatan CIA (Confidentiality, Integrity, Availability). Hasil analisis menunjukkan bahwa data transaksi finansial memiliki prioritas tertinggi karena memerlukan tingkat kerahasiaan, integritas, dan ketersediaan yang sama-sama tinggi (skor prioritas 5,00). Aset lain yang juga masuk kategori prioritas tinggi adalah konfigurasi server, database pelanggan, dan API publik, sedangkan data laporan internal memiliki prioritas sedang.

Tahap selanjutnya adalah penilaian risiko dengan mempertimbangkan faktor kerentanan (vulnerability), ancaman (threat), kemungkinan (likelihood), dan dampak (impact). Perhitungan nilai risiko menunjukkan bahwa:

- Risiko tinggi ditemukan pada *data transaksi finansial* (nilai risiko 20), *database pelanggan* (nilai risiko 16), dan *konfigurasi server* (nilai risiko 15).
- Risiko sedang terdapat pada *API publik* (nilai risiko 12) dan *data laporan internal* (nilai risiko 6).

Temuan ini menegaskan bahwa risiko tinggi umumnya terjadi pada aset yang memiliki prioritas tinggi, terutama yang mengandung data sensitif atau mendukung layanan inti aplikasi.

Sebagai tindak lanjut, strategi pengendalian risiko (risk treatment) difokuskan pada penerapan langkah mitigasi yang bersifat pencegahan, deteksi, dan respons cepat. Untuk risiko tinggi, tindakan yang direkomendasikan mencakup penerapan enkripsi kuat (AES-256) baik pada data *at rest* maupun *in transit*, penggunaan *Multi-Factor Authentication* (MFA), *server hardening*, pembaruan keamanan berkala, kontrol akses berbasis peran (*RBAC*), serta pemantauan aktivitas melalui *Intrusion Detection/Prevention System* (IDS/IPS) dan *Database Activity Monitoring*. Sementara itu, untuk risiko sedang, pengendalian difokuskan pada penerapan *rate limiting* pada API, penggunaan autentikasi token, proteksi integritas file dengan checksum/hash, backup terjadwal, serta pembatasan akses berdasarkan kebutuhan.

Secara keseluruhan, hasil penilaian risiko ini memberikan gambaran jelas mengenai hubungan antara prioritas aset dan tingkat risiko, serta mengarahkan organisasi untuk memfokuskan sumber daya pada pengamanan aset yang paling kritis. Implementasi pengendalian yang tepat akan membantu mengurangi kemungkinan terjadinya insiden keamanan informasi, meminimalkan dampak yang ditimbulkan, dan memastikan kelangsungan layanan aplikasi secara aman dan andal.

Ucapan Terimakasih

Terimakasih kepada Fakultas Ilmu Komputer dan Pusat Penelitian Univeritas Mercubuana yang telah mendanai penelitian ini.

DAFTAR PUSTAKA

[1] ISO/IEC, "International Standard ISO/IEC 27005: 2022," International Organization for Standardization, London, 2022.
[2] Z. Liao, S. Nazir, H. U. Khan, and M. Shafiq, “Assessing security of software components for internet of things: A systematic review and future directions,” Security and Communication Networks”, vol. 2021, pp. 1–22, 2021.
[3] I. M. Putra and K. Mutijarsa, “Designing information security risk management on Bali Regional Police Command Center based on ISO 27005. 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT), 2021.
[4] NIST, “NIST SP 800-30 Revision 1: Guide for conducting risk assessments,” National Institute of Standards and Technology, Gaithersburg, 2012.
[5] H. D. Hadmanto, R. F. Aji, and J. P. Nurahman, “Penilaian risiko keamanan informasi aplikasi online travel agent: Studi kasus PT.XYS,” Jurnal Restikom: Riset Teknik Informatika dan Komputer, vol. 3, no. 2, pp. 60–69, 2021.
[6] M. Albalawi, “Website defacement detection and monitoring methods: A review,” Electronics, vol. 11, no. 3573, 2022.
[7] I. P. S. Syahindra, C. H. Primasari, and A. B. P. Irianto, “Evaluasi risiko keamanan informasi DISKOMINFO Provinsi XYZ menggunakan Indeks KAMI dan ISO 27005:2011,” Jurnal Teknoinfo, vol. 16, no. 2, pp. 165–182, Jul. 2022.
[8] M. Hendayun, H. P. Utomo, and D. P. Nababan, “Pengujian dan penilaian kerentanan e-learning Universitas Langlangbuana menggunakan metode STRIDE dan DREAD,” Jurnal Teknologi Informasi, vol. 2, no. 2, pp. 2–6, 2021.
[9] K. N. Isnaini and S. A. Solikhatin, “Information security analysis on physical security in university X using maturity model,” Jurnal Informatika, vol. 14, no. 2, pp. 76–83, 2020.
[10] K. N. Isnaini and D. Suhartono, “Evaluation of basic principles of information security at university using COBIT 5,” Matrik: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 21, no. 2, pp. 317–326, 2022.

[11] J. Jonny, A. Ambarwati, and C. Darujati, "Penilaian risiko data sistem informasi manajemen puskesmas dan aset menggunakan ISO 27005," Sistemasi, vol. 10, no. 1, pp. 1–8, 2021.
[12] A. C. Laksono and Y. Prayudi, "Threat modeling menggunakan pendekatan STRIDE dan DREAD untuk mengetahui risiko dan mitigasi keamanan pada sistem informasi akademik," JUSTINDO, vol. 6, no. 1, pp. 9–20, 2021.
[13] R. Ramadhintia and R. Bisma, "Analisis manajemen risiko aplikasi ujian online dengan metode OCTAVE Allegro pada lembaga pendidikan," Jurnal Sistem dan Teknologi Informasi, vol. 6, no. 2, 2021.
[14] R. A. Wijaya and K. Karmilasari, "Pengukuran kualitas website Pengurus Cabang NU Depok menggunakan software metric," Jurnal Sisfokom: Sistem Informasi dan Komputer, vol. 10, no. 3, pp. 438–443, 2021.
[15] N. A. Chandra, K. Ramli, and A. A. P. Ratna, "Information security risk assessment using situational awareness frameworks and application tools," Risks, vol. 10, no. 165, 2022. [Online]. Available: https://doi.org/10.3390/risks10080165
[16] E. Handoyo and I. E. Nigrum, "Penilaian risiko keamanan siber kampus menggunakan framework cybersecurity NIST 1.1," Jurnal CoSciTech (Computer Science and Information Technology), vol. 4, no. 3, pp. 677–685, 2024.
[17] K. N. Ramdhani, Y. M. Sari, R. M. Nafi', A. G. F. Zahid, R. Fajariansyah, and F. Y. Arini, "Etika Web Developer dalam Pendistribusian Pop-Up Ads pada Website," Jurnal Computer Science and Information Technology (CoSciTech), vol. 5, no. 3, pp. 775–781, Dec. 2024.
[18] M. Albalawi, "Website defacement detection and monitoring methods: A review," Electronics, vol. 11, no. 3573, 2022.
[19] I. M. Putra and K. Mutijarsa, "Designing information security risk management on Bali Regional Police Command Center based on ISO 27005," in Proc. 2021 3rd East Indonesia Conf. on Computer and Information Technology (EIConCIT), 2021.
[20] I. P. S. Syahindra, C. H. Primasari, and A. B. P. Irianto, "Evaluasi risiko keamanan informasi DISKOMINFO Provinsi XYZ menggunakan Indeks KAMI dan ISO 27005:2011," Jurnal Teknoinfo, vol. 16, no. 2, pp. 165–182, Jul. 2022.
[21] N. A. Chandra, K. Ramli, and A. A. P. Ratna, "Information security risk assessment using situational awareness frameworks and application tools," Risks, vol. 10, no. 165, 2022. [Online]. Available: https://doi.org/10.3390/risks10080165
[22] H. D. Hadmanto, R. F. Aji, and J. P. Nurahman, "Penilaian risiko keamanan informasi aplikasi online travel agent: Studi kasus PT. XYS," Jurnal Restikom, vol. 3, no. 2, pp. 60–69, 2021.
[23] K. N. Isnaini and D. Suhartono, "Evaluation of basic principles of information security at university using COBIT 5," Matrik: Jurnal Manajemen, Teknik Informatika dan Rekayasa Komputer, vol. 21, no. 2, pp. 317–326, 2022.
[24] A. C. Laksono and Y. Prayudi, "Threat modeling menggunakan pendekatan STRIDE dan DREAD untuk mengetahui risiko dan mitigasi keamanan pada sistem informasi akademik," JUSTINDO, vol. 6, no. 1, pp. 9–20, 2021.
[25] R. Ramadhintia and R. Bisma, "Analisis manajemen risiko aplikasi ujian online dengan metode OCTAVE Allegro pada lembaga pendidikan," Jurnal Sistem dan Teknologi Informasi, vol. 6, no. 2, 2021.
[26] G. H. Pradana and D. Hartono, "Implementation of threat modeling using STRIDE framework in smart home system," Jurnal CoSciTech, vol. 3, no. 2, pp. 85–91, 2021.
[27] R. Nugraha and R. A. Permadi, "Risk assessment on e-learning application using ISO 27005," Jurnal CoSciTech, vol. 4, no. 1, pp. 45–52, 2022.