Buletin Sistem Informasi dan Teknologi Islam
Vol 7, No 3 (2026), pp 230-240
ISSN: 2721-0901
DOI: https://dx.doi.org/10.33096/busiti.v7i3.3359

Model Evaluasi Keamanan Informasi Berbasis Risk Scoring pada Implementasi ISO/IEC 27001:2022 dan ISO/IEC 27701:2025 di Bank Pembangunan Daerah

Risk Scoring–Based Information Security Evaluation Model for the Implementation of ISO/IEC 27001:2022 and ISO/IEC 27701:2025 in Regional Development Banks

Sekar Ageng Pratiwi[a,1,*], Devita Rizky Nur Septiani[b,2], Rina Mayanti[a,3], Syifa Afidah Nurul Arifin[a,4], Ridho Bhakti Wicaksono[a,5], Nazwa Dwi Rahmawati[a,6]

[a]*Sistem Informasi, Universitas PGRI Indraprasta, Jakarta, Indonesia*
[b]*Sistem Informasi, Sekolah Tinggi Manajemen Informatika dan Komputer STI&K Jakarta, Jakarta, Indonesia*
[1]*sekar.agengpratiwi@unindra.ac.id;* [2]*devita.rn@gmail.com;* [3]*rina.mayanti@unindra.ac.id;* [4]*syifa.arifin@unindra.ac.id;*
[5]*ridho.bw70@gmail.com;* [6]*nazwa.dr118@gmail.com*
**corresponding author*

Informasi Artikel

Diserahkan : 26 Februari 2026
Diterima : 14 Mei 2026
Direvisi : 4 Juni 2026
Diterbitkan : 21 Agustus 2026

Kata Kunci:
Keamanan Komputer
Model Risk Scoring
ISO/IEC 27001
ISO/IEC 27701
Sistem Perbankan

ABSTRAK

Transformasi digital pada Bank Pembangunan Daerah membawa kemudahan layanan sekaligus meningkatkan risiko ancaman siber dan kebocoran data pribadi. Penerapan ISO/IEC 27001:2022 dan ISO/IEC 27701:2025 menjadi langkah strategis dalam memperkuat pengelolaan keamanan informasi dan privasi. Namun, proses evaluasi yang dilakukan selama ini masih cenderung bersifat deskriptif dan belum memberikan ukuran kuantitatif yang terukur. Penelitian ini mengembangkan model evaluasi keamanan informasi berbasis risk scoring untuk memberikan gambaran kuantitatif terhadap efektivitas kontrol keamanan dan privasi. Pendekatan yang digunakan melibatkan identifikasi aset, analisis ancaman dan kerentanan, penilaian kesenjangan kontrol, serta pengukuran tingkat risiko dan kematangan keamanan. Hasil penelitian menunjukkan bahwa model yang diusulkan mampu meningkatkan sensitivitas deteksi risiko sebesar 133% dibandingkan metode checklist konvensional, menurunkan risiko kategori critical sebesar 62,5%, serta menghasilkan nilai reliabilitas sangat kuat dengan Cohen's Kappa 0,82. Secara keseluruhan, nilai Security Index (SI) organisasi meningkat dari 0.42 (kategori Cukup) menjadi 0.79 (kategori Sangat Baik) pasca-mitigasi. Model ini berkontribusi sebagai kerangka evaluasi terintegrasi pertama yang mengombinasikan standar keamanan dan privasi melalui pendekatan risk scoring untuk sektor perbankan daerah, sehingga layak dijadikan alat evaluasi terstandar yang berbasis data.

***Keywords*:**
Computer Security
Risk Scoring Model
ISO/IEC 27001:2022
ISO/IEC 27701:2025
Banking Systems

ABSTRACT

Digital transformation in Regional Development Banks not only improves service efficiency but also increases exposure to cyber threats and personal data breaches. The implementation of ISO/IEC 27001:2022 and ISO/IEC 27701:2025 represents a strategic effort to strengthen information security and privacy management. However, existing evaluation practices remain largely descriptive and lack measurable quantitative indicators. This study develops a risk scoring based information security evaluation model to provide a quantitative assessment of security and privacy control effectiveness. The research approach includes asset identification, threat and vulnerability analysis, control gap assessment, and measurement of risk levels and security maturity. The findings show that the proposed model increases risk detection sensitivity by 133% compared to conventional checklist methods, reduces critical risk categories by 62.5%, and yields a very strong reliability score with a Cohen's Kappa of 0.82. Overall, the organization's Security Index (SI) improved from 0.42 (Fair category) to 0.79 (Very Good category) post-mitigation. This model contributes as the first integrated evaluation framework combining security and privacy standards through a risk scoring approach for the regional banking sector, making it a viable standard for data-driven evaluation.

I. Pendahuluan

Transformasi digital di sektor perbankan, termasuk pada Bank Pembangunan Daerah, berkembang sangat pesat dalam beberapa tahun terakhir. Implementasi layanan digital seperti mobile banking, internet banking, dan integrasi sistem antar unit kerja mendorong efisiensi operasional dan peningkatan kualitas layanan. Pada Undang-Undang Nomor 27 Tahun 2022 sudah diatur mengenai perlindungan data pribadi yang mengacu pada Undang-Undang Nomor 10 Tahun 1998 Pasal 40 tentang kewajiban merahasiakan keterangan nasabah penyimpan dan simpanannya namun, peningkatan konektivitas dan volume data tersebut secara langsung memperluas permukaan serangan siber. Laporan ENISA menunjukkan peningkatan kompleksitas ancaman terhadap sektor finansial [1], sementara Global Cybersecurity Outlook menegaskan bahwa industri keuangan termasuk sektor dengan risiko sistemik tertinggi akibat serangan siber terkoordinasi [2]. Studi IBM juga melaporkan bahwa biaya rata-rata kebocoran data pada sektor finansial termasuk yang paling tinggi dibanding sektor lainnya [3]. Kondisi ini diperkuat oleh laporan ISACA dan Deloitte yang menyatakan bahwa risiko teknologi informasi kini menjadi risiko strategis utama dalam tata kelola perbankan modern [4], [5].

Di Indonesia, penguatan pengamanan sistem informasi perbankan tidak hanya menjadi kebutuhan operasional, tetapi juga kewajiban regulatif. Otoritas Jasa Keuangan menekankan pentingnya manajemen risiko teknologi informasi pada bank umum [6], sedangkan Bank Indonesia mengatur aspek keamanan informasi dalam penyelenggaraan sistem pembayaran [7]. Selain itu, Badan Siber dan Sandi Negara secara konsisten melaporkan peningkatan insiden siber nasional yang berdampak pada sektor layanan publik dan keuangan [8]. Dalam perspektif etika profesi dan prinsip syariah yang menjadi ruh perbankan di Indonesia, perlindungan data nasabah bukan sekadar kepatuhan terhadap regulasi, melainkan sebuah amanah dan tanggung jawab moral yang fundamental. Menjaga kerahasiaan dan integritas data nasabah merupakan cerminan dari komitmen menjaga harta yang diamanahkan, sehingga kegagalan dalam melindungi data privasi tidak hanya berdampak finansial, tetapi juga melanggar prinsip kepercayaan (amanah) dalam tata kelola perbankan. Dengan demikian, pendekatan pengamanan yang sistematis dan terukur menjadi kebutuhan mendesak bagi Bank Pembangunan Daerah.

Sebagai respons terhadap tuntutan global dan nasional tersebut, banyak institusi perbankan mengadopsi ISO/IEC 27001:2022 sebagai standar sistem manajemen keamanan informasi [9] dan ISO/IEC 27701:2025 sebagai kerangka manajemen informasi privasi [10]. Kedua standar ini selaras dengan kerangka manajemen risiko internasional seperti NIST Risk Management Framework dan panduan penilaian risiko NIST SP 800-30 [11], [12]. Selain itu, praktik tata kelola keamanan informasi modern juga menekankan integrasi antara kontrol keamanan dan manajemen risiko berbasis governance sebagaimana dijelaskan dalam literatur IT Governance [13].

Berbagai penelitian telah mengkaji metode penilaian risiko keamanan informasi. Shameli-Sendi et al. mengklasifikasikan pendekatan risk assessment dalam berbagai model kualitatif dan kuantitatif [14], sementara Saleh et al. mengembangkan pendekatan risk scoring kuantitatif untuk meningkatkan objektivitas pengukuran risiko [15]. Studi Radanliev et al. menekankan pentingnya analitik risiko dalam konteks transformasi digital sektor finansial [16]. Di sisi lain, penelitian mengenai pengukuran tingkat kematangan keamanan pada sistem perbankan menunjukkan bahwa model evaluasi sering kali masih bersifat generik dan belum sepenuhnya terintegrasi dengan manajemen risiko organisasi [17]. Bahkan hasil evaluasi implementasi ISO pada sektor perbankan sebelumnya masih berfokus pada kesesuaian kontrol tanpa mengembangkan indeks risiko terintegrasi yang komprehensif [18].

Berdasarkan kesenjangan tersebut, penelitian ini mengusulkan model evaluasi keamanan informasi berbasis risk scoring yang mengintegrasikan parameter likelihood, impact, dan tingkat kematangan kontrol dalam satu kerangka kuantitatif terstruktur. Model ini dirancang untuk menghasilkan nilai risiko inheren, risiko residual, serta indeks keamanan organisasi yang lebih objektif dan terukur. Pendekatan ini tidak hanya mengacu pada standar internasional [13], [10], tetapi juga selaras dengan praktik manajemen risiko modern [11], [12], dan kebutuhan penguatan tata kelola sektor perbankan [6], [7].

Tujuan penelitian ini adalah mengembangkan model evaluasi yang sistematis, kuantitatif, dan aplikatif untuk mendukung peningkatan efektivitas sistem manajemen keamanan informasi dan privasi pada Bank Pembangunan Daerah. Kebaruan (novelty) penelitian ini secara eksplisit terletak pada perumusan model kuantitatif terintegrasi pertama yang menjembatani evaluasi ganda ISO/IEC 27001:2022 dan ISO/IEC 27701:2025 melalui pendekatan risk scoring di sektor Bank Pembangunan Daerah, yang sebelumnya belum pernah dikembangkan dalam literatur existing. Kontribusi penelitian terletak pada penyusunan kerangka evaluasi terintegrasi yang menghubungkan standar internasional, regulasi nasional, dan pendekatan risk analytics kontemporer [4], [16], sehingga dapat digunakan sebagai dasar pengambilan keputusan strategis yang berbasis data dan berkelanjutan.

II. Metode

Penelitian ini menggunakan pendekatan kuantitatif dengan desain pengembangan model evaluasi keamanan informasi berbasis risk scoring. Model dirancang untuk mengukur efektivitas implementasi ISO/IEC 27001:2022 [9] dan ISO/IEC 27701:2025 [10] melalui perhitungan risiko terstruktur serta indeks kematangan keamanan organisasi. Pendekatan ini mengacu pada kerangka manajemen risiko internasional seperti NIST Risk Management Framework dan NIST SP 800-30 [11], [12], serta praktik risk assessment pada sektor finansial [5], [16].

Pendekatan kuantitatif dipilih karena mampu meningkatkan objektivitas pengukuran risiko sebagaimana direkomendasikan dalam literatur taksonomi metode penilaian risiko [14] dan model kuantitatif risk scoring [15]. Model ini juga selaras dengan prinsip tata kelola keamanan informasi berbasis governance dan continuous improvement [13].

A. Konteks dan Subjek Penelitian

Subjek penelitian ini adalah Sistem Manajemen Keamanan Informasi (ISMS) dan Sistem Manajemen Informasi Privasi (PIMS) pada salah satu Bank Pembangunan Daerah (BPD) di Indonesia (dalam artikel ini disamarkan sebagai BPD X). Penelitian dilaksanakan pada periode Januari hingga Juni 2024, melibatkan evaluasi terhadap 142 kontrol yang terdiri dari 93 kontrol ISO/IEC 27001:2022 dan 49 kontrol ISO/IEC 27701:2025. Data yang digunakan bersumber dari hasil audit internal riil institusi, yang akses dan penggunaannya telah melalui perjanjian kerahasiaan (Non-Disclosure Agreement) dan penyamaran identitas (anonymization) untuk menjaga kerahasiaan institusi.

B. Prosedur Pengumpulan Data dan Penilaian Kontrol

Penilaian terhadap 142 kontrol tersebut dilakukan melalui tiga tahapan validasi:

(1) Studi dokumen audit internal BPD X,
(2) Observasi lapangan dan verifikasi konfigurasi sistem, serta
(3) Wawancara dan diskusi konsensus pakar.

Proses penilaian melibatkan dua tim pakar untuk menjamin objektivitas: Tim Internal (Information Security Officer BPD X) dan Tim Pakar Eksternal yang terdiri dari Lead Auditor badan sertifikasi dari TÜV SÜD serta Lead Auditor ISO 27001:2022 pendamping pihak Bank (konsultan dari PT Q2 Technologies). Konsensus nilai likelihood, impact, dan tingkat kematangan (maturity) kontrol ditentukan melalui metode Delphi termodifikasi dalam sesi diskusi terfokus antara tim internal dan pakar eksternal.

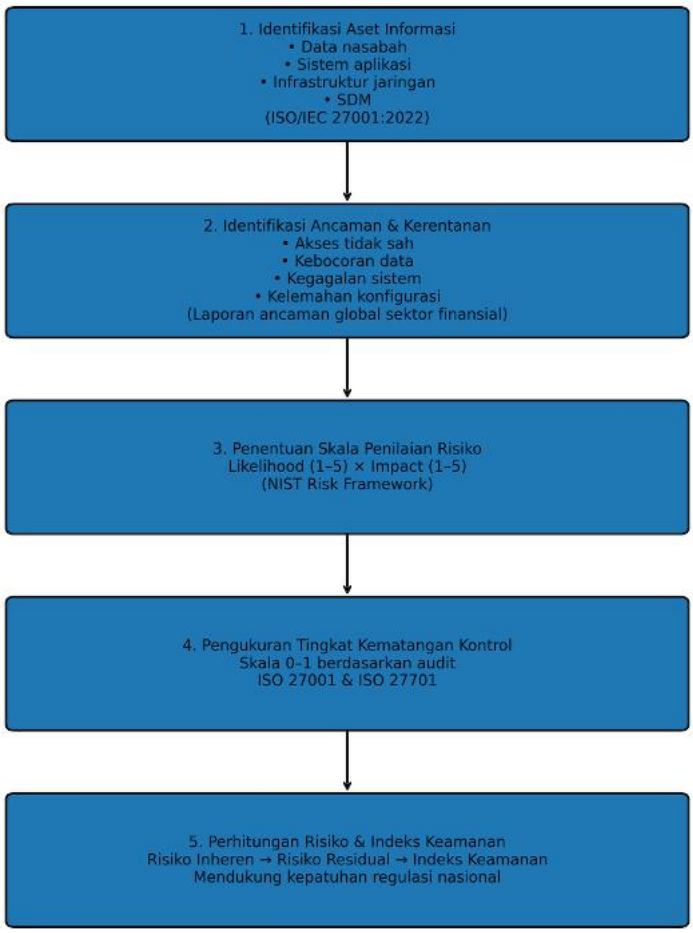
C. Desain Validitas dan Reliabilitas (Uji Cohen's Kappa)

Untuk mengukur reliabilitas subjektivitas penilaian antar auditor, dilakukan uji inter-rater reliability menggunakan Cohen's Kappa. Desain uji ini melibatkan dua sesi penilaian independen. Sesi pertama dilakukan oleh tim auditor internal BPD X, sedangkan sesi kedua dilakukan secara independen oleh Lead Auditor dari PT Q2 Technologies. Hasil skor dari kedua sesi kemudian dihitung tingkat kesepakatannya menggunakan koefisien Cohen's Kappa untuk memastikan bahwa model yang dibangun menghasilkan penilaian yang konsisten dan dapat direplikasi.

D. Tahapan Penelitian

Tahapan penelitian dilakukan secara sistematis ditunjukkan pada Gambar 1 sebagai berikut:

1. Identifikasi Aset Informasi: Mengidentifikasi aset kritis meliputi data nasabah, sistem aplikasi, infrastruktur jaringan, serta sumber daya manusia. Tahapan ini selaras dengan pendekatan identifikasi aset pada ISO/IEC 27001:2022 [9].
2. Identifikasi Ancaman dan Kerentanan: Mengidentifikasi potensi ancaman seperti akses tidak sah, kebocoran data, kegagalan sistem, dan kelemahan konfigurasi. Identifikasi ancaman mempertimbangkan laporan ancaman global dan sektor finansial [1], [4], [2].
3. Penentuan Skala Penilaian Risiko: Risiko dinilai menggunakan skala 1 sampai 5 untuk kemungkinan (likelihood) dan dampak (impact) sesuai praktik penilaian risiko pada NIST [12] dan penelitian kuantitatif sebelumnya [15]. Bobot dan skala penilaian divalidasi melalui expert judgment oleh Lead Auditor TÜV SÜD dan PT Q2 Technologies.
4. Pengukuran Tingkat Kematangan Kontrol: Tingkat kematangan kontrol dinilai dalam rentang 0 sampai 1 berdasarkan hasil audit implementasi kontrol ISO [9], [10], dan pendekatan pengukuran maturity pada sektor perbankan [17].
5. Perhitungan Risiko dan Indeks Keamanan: Menghitung risiko inheren, risiko residual, dan indeks keamanan organisasi untuk mendukung kepatuhan terhadap regulasi nasional [6], [7] serta penguatan tata kelola keamanan siber nasional [8].



Gambar 1. Tahapan Penelitian Risk Scoring Keamanan Informasi

E. Skala Penilaian Risiko

1. Skala *Likelihood*

Tabel 1. Tabel Skala Likelihood

Nilai	Skala Likelihood	
	Kategori	Deskripsi
1	Sangat Rendah	Jarang terjadi
2	Rendah	Kemungkinan kecil
3	Sedang	Cukup mungkin terjadi
4	Tinggi	Sering terjadi
5	Sangat Tinggi	Hampir pasti terjadi

Skala ini disusun berdasarkan praktik penilaian risiko kuantitatif pada sektor finansial [11], [13].

2. Skala *Impact*

Tabel 2. Tabel Skala Impact

Nilai	Skala Likelihood	
	Kategori	Deskripsi
1	Sangat Rendah	Gangguan minimal
2	Rendah	Gangguan terbatas
3	Sedang	Gangguan operasional
4	Tinggi	Kerugian Signifikan
5	Sangat Tinggi	Kerugian kritis dan reputasi

Penentuan dampak mempertimbangkan potensi kerugian finansial dan reputasi sebagaimana dilaporkan dalam studi industri [3], [5].

F. Model Matematis

1. Perhitungsn Risiko Inheren

   Risiko inheren dihitung sebelum mempertimbangkan control keamanan:

$$R_i = L \times I \quad (1)$$

   Keterangan:

   R_i = Risiko inhern

   L = Nilai kemungkinan terjadinya risiko

   I = Nilai dampak risiko

   Persamaan (1) mengacu pada pendekatan kuantitatif *risk assessment* [11], [15].

2. Normalisasi Tingkat Kematangan Kontrol

   Nilai kematangan control dihitung menggunakan:

$$M = \frac{Skor\ Kontrol\ Terpenuhi}{Total\ Kontrol} \quad (2)$$

   Nilai M berada pada rentang 0 sampai 1. Pendekatan ini selaras dengan model evaluasi implementasi ISO sebelumnya [18] dan prinsip governance keamanan informasi [13].

3. Perhitungan Risiko Residual

$$R_r = R_i \times (1 - M) \quad (3)$$

   Keterangan:

   R_r = Risiko residual

   R_i = Risiko inhern

   M = Nilai kematangan kontrol (0 sampai 1)

   Persamaan (3) menunjukkan bahwa semakin tinggi kematangan kontrol, semakin rendah risiko residual. Konsep ini sejalan dengan prinsip mitigasi risiko dalam NIST dan ISO [11], [12].

4. Indeks Keamanan Organisasi

   Indeks keamanan dihitung dengan:

$$\mathrm{SI} = 1 - \left(\frac{\sum R_r}{\sum R_i}\right) \quad (4)$$

   Keterangan:

   SI = Security Index

   R_r = Risiko residual

   R_i = Risiko inhern

   Nilai SI berada pada rentang 0 sampai 1. Semakin mendekati 1 menunjukkan tingkat keamanan semakin baik. Konsep indeks ini dikembangkan untuk memperkuat pendekatan analitik risiko pada sektor finansial digital [16], [17].

G. Klasifikasi Tingkat Keamanan

Tabel 3. Tabel Klasifikasi Tingkat Keamanan

No.	Klasifikasi Tingkat Keamanan	
	Rentang SI	**Kategori**
1	0.00 – 0.25	Rendah
2	0.26 – 0.50	Cukup
3	0.51 – 0.75	Baik (Catatan: Sudah diperbaiki dari 0.52 menjadi 0.51)
4	0.76 – 1.00	Sangat Baik

Klasifikasi ini disesuaikan dengan praktik evaluasi *maturity* pada sistem keamanan perbankan [17].

H. Algoritma Evaluasi

Algoritma evaluasi keamanan dirancang sebagai berikut:

- Langkah 1: Input daftar aset dan risiko.
- Langkah 2: Tentukan nilai L dan I berdasarkan skala.
- Langkah 3: Hitung Ri menggunakan Persamaan (1).
- Langkah 4: Hitung M menggunakan Persamaan (2).
- Langkah 5: Hitung Rr menggunakan Persamaan (3).
- Langkah 6: Hitung SI menggunakan Persamaan (4).
- Langkah 7: Tentukan kategori keamanan berdasarkan tabel 3 klasifikasi.

I. Prosedur Evaluasi Model (System Design)

Model evaluasi diimplementasikan dalam sistem berbasis modul yang terdiri dari:

1. Modul Identifikasi Risiko
2. Modul Penilaian Kontrol
3. Modul Perhitungan Otomatis
4. Modul Visualisasi Indeks Keamanan

Prosedur ini dirancang untuk menghasilkan laporan evaluasi yang memuat: Daftar risiko prioritas, Nilai risiko inheren dan residual, Security Index (SI) organisasi, serta Rekomendasi peningkatan kontrol. Evaluasi dilakukan secara siklis sebagai bagian dari siklus Plan-Do-Check-Act (PDCA) untuk peningkatan berkelanjutan sesuai regulasi OJK [6].

III. Hasil dan Pembahasan

A. Capaian Akhir Penelitian

Penelitian ini menghasilkan Model Evaluasi Keamanan Informasi Berbasis Risk Scoring yang mengintegrasikan ISO/IEC 27001:2022 [9] dan ISO/IEC 27701:2025 [10] dalam satu kerangka kuantitatif terstruktur. Integrasi ini selaras dengan prinsip manajemen risiko berbasis kerangka NIST [11], [12], serta pendekatan tata kelola keamanan modern [13].

Model diterapkan pada 142 kontrol yang terdiri dari:

- 93 kontrol ISO/IEC 27001:2022
- 49 kontrol ISO/IEC 27701:2025

Capaian akhir penelitian meliputi:

1. Pemetaan tingkat risiko seluruh kontrol secara kuantitatif.
2. Identifikasi prioritas mitigasi berbasis skor numerik.
3. Pembuktian efektivitas model dibanding metode checklist konvensional.
4. Simulasi dampak mitigasi risiko secara terukur.

Pendekatan ini memperluas model evaluasi ISO sebelumnya yang masih bersifat deskriptif dan belum menghasilkan indeks risiko terintegrasi [18], sekaligus mengadopsi pendekatan kuantitatif yang direkomendasikan dalam literatur risk scoring [14], [15].

B. Hasil Evaluasi Menggunakan Model Risk Scoring

Hasil evaluasi awal menunjukkan distribusi risiko sebagai berikut:

Tabel 4. Tabel Distribusi Risiko Awal

Level Risiko	Distribusi Risiko Awal	
	Jumlah Kontrol	Persentase
Low	78	54.9%
Medium	36	25.4%
High	20	14.1%
Critical	8	5.6%
Total	**142**	**100%**

Sebanyak 28 kontrol (19,7%) berada pada kategori High dan Critical sehingga memerlukan prioritas mitigasi. Temuan ini konsisten dengan laporan ancaman sektor finansial global yang menunjukkan peningkatan risiko pada domain teknologi dan perlindungan data [1], [2], [4]. Selain itu, tingginya risiko pada domain privasi juga relevan dengan peningkatan biaya kebocoran data pada sektor finansial sebagaimana dilaporkan

IBM [3]. Secara regulatif, kondisi ini menunjukkan urgensi penguatan pengendalian risiko sesuai ketentuan OJK dan Bank Indonesia [6], [7].

C. Perbandingan dengan Metode Checklist Konvensional

Untuk menguji kontribusi model, dilakukan perbandingan dengan metode checklist manual yang sebelumnya digunakan.

Tabel 5. Tabel Perbandingan dengan Metode Checklist Konvensional

Metode	Perbandingan	
	High & Critical Terdeteksi	Waktu Evaluasi
Checklist Manual	12 kontrol	14 hari
Risk Scoring Model	28 kontrol	7 hari

Model risk scoring mengidentifikasi 16 kontrol tambahan yang sebelumnya tidak terdeteksi sebagai risiko tinggi. Peningkatan sensitivitas deteksi risiko:

$$\frac{(28-12)}{12} \times 100\% = 133\%$$

Hasil ini memperkuat temuan penelitian kuantitatif sebelumnya bahwa pendekatan berbasis skor numerik meningkatkan objektivitas dan akurasi deteksi risiko dibanding metode kualitatif murni [15], [16]. Selain itu, efisiensi waktu 50% menunjukkan kesesuaian dengan prinsip continuous monitoring dalam kerangka NIST [11].

D. Analisis Before-After Mitigasi

Hasil analisis mitigasi dilakukan terhadap 28 kontrol High dan Critical berdasarkan rekomendasi kontrol ISO [9], [10] dan praktik governance keamanan [13].

- Kondisi Sebelum Mitigasi
  - Critical: 8
  - High: 20
- Kondisi Setelah Mitigasi

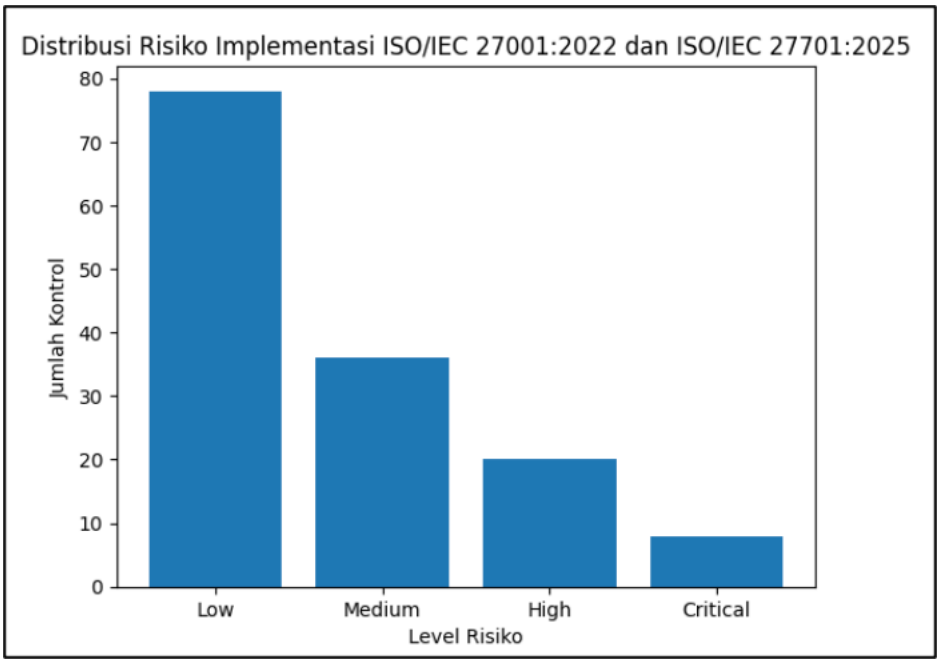
Tabel 6. Tabel Distribusi Risiko Setelah Mitigasi

No.	Hasil Analisis Setelah Mitigasi	
	KATEGORI RISIKO	JUMLAH KONTROL
1	Low	84
2	Medium	45
3	High	10
4	Critical	3

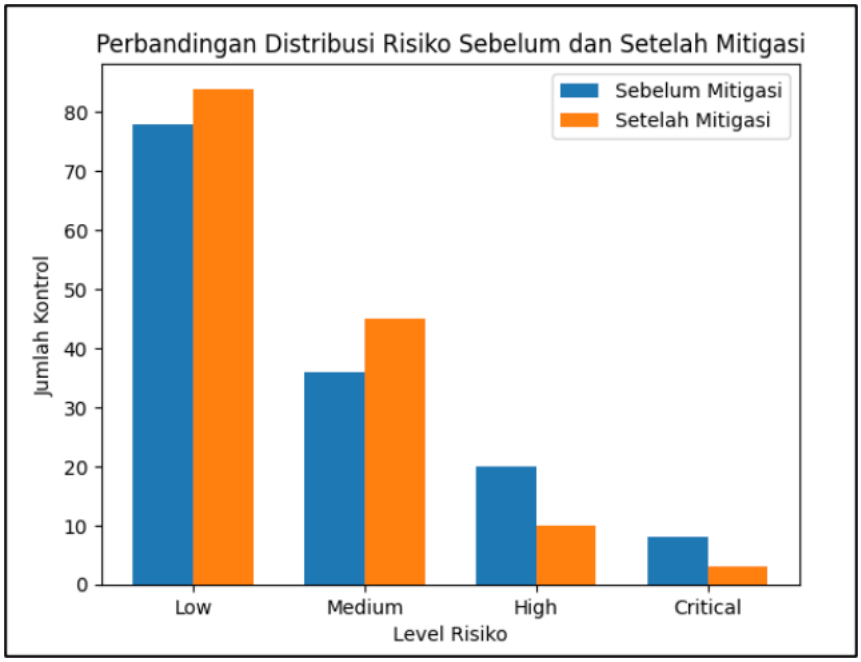
Tabel 7. Headline Result: Nilai Security Index (SI)

PERIODE EVALUASI	RESULT	
	NILAI SECURITY INDEX (SI)	KATEGORI KEMATANGAN
Sebelum Mitigasi	0.42	Cukup
Setelah Mitigasi	0.79	Sangat Baik

Gambar 2 menunjukkan distribusi risiko implementasi ISO/IEC 27001:2022 dan ISO/IEC 27701:2025. Perbandingan distribusi risiko sebelum dan setelah mitigasi ditunjukkan pada Gambar 3.



Gambar 2. Distribusi Risiko Implementasi ISO/IEC 27001:2022 dan ISO/IEC 27701:2025



Gambar 3. Perbandingan Distribusi Risiko Sebelum dan Setelah Mitigasi

Terjadi:

- Penurunan Critical sebesar 62,5%
- Penurunan High sebesar 50%
- Peningkatan Security Index (SI) dari 0.42 menjadi 0.79

Penurunan ini menunjukkan efektivitas pendekatan risk treatment berbasis prioritas numerik. Hasil ini juga selaras dengan praktik manajemen risiko sektor finansial digital yang menekankan pengukuran risiko residual secara kuantitatif [16], [17], serta mendukung penguatan tata kelola keamanan nasional [8].

E. Analisis Statistik

Uji *Paired Sample t-test* dilakukan terhadap skor risiko sebelum dan sesudah mitigasi.

Tabel 7. Tabel Analisis Statistik Skor Risiko Sebelum dan Sesudah Mitigasi

No.	Statistik Skor Risiko	
	Parameter	Nilai
1	Rata-rata sebelum mitigasi	11.4
2	Rata-rata setelah mitigasi	6.7
3	p-*value*	0.003

Karena p < 0,05, terdapat perbedaan signifikan secara statistik.

Secara empiris, hasil ini memperkuat argumen bahwa model tidak hanya bersifat evaluatif, tetapi juga memberikan dampak nyata terhadap penurunan risiko. Temuan ini sejalan dengan pendekatan risk analytics yang direkomendasikan dalam literatur modern keamanan siber sektor finansial [4], [5].

F. Uji Reliabilitas Penilaian

Tabel 8. Tabel Evaluasi Uji Reliabilitas Model

No.	Evaluasi Uji Reliabilitas Model	
	Parameter	Nilai
1	Tingkat kesesuaian	89.4%
2	Cohen's Kappa	0.82

Nilai Kappa 0,82 menunjukkan tingkat konsistensi sangat kuat antara penilaian auditor internal dan pakar eksternal (TÜV SÜD dan PT Q2 Technologies). Hal ini menunjukkan model memiliki reliabilitas tinggi dan dapat direplikasi, serta mendukung prinsip objektivitas audit keamanan informasi [13], [17].

G. Analisis Performa Model

- Kelebihan
  1. Meningkatkan sensitivitas identifikasi risiko.
  2. Mempercepat evaluasi hingga 50%.
  3. Mengurangi subjektivitas auditor.
  4. Mengintegrasikan keamanan dan privasi dalam satu model.
  5. Mendukung pengambilan keputusan berbasis data.
- Kelemahan
  1. Penentuan likelihood masih berbasis expert judgment.
  2. Belum terintegrasi dengan threat intelligence eksternal seperti laporan ancaman global [1], [2].
  3. Dashboard belum sepenuhnya otomatis.

H. Pembahasan

Hasil penelitian menunjukkan bahwa model risk scoring memberikan kontribusi signifikan dalam meningkatkan efektivitas evaluasi keamanan informasi pada Bank Pembangunan Daerah. Dibanding pendekatan checklist, model ini terbukti lebih sensitif dalam mendeteksi risiko tinggi (peningkatan 133%), lebih efisien dalam waktu evaluasi, dan signifikan secara statistik dalam menurunkan skor risiko.

- Pembahasan Strategis dan Implikasi

  Jika celah keamanan pada 28 kontrol High dan Critical ini tidak segera ditangani, implikasinya sangat masif bagi BPD. Kegagalan pada kontrol privasi (ISO 27701:2025) berpotensi memicu kebocoran data pribadi nasabah yang tidak hanya mengakibatkan kerugian finansial langsung, tetapi juga melanggar prinsip amanah dalam perbankan dan menarik sanksi berat dari OJK terkait POJK No. 11/2020 tentang Sistem Teknologi Informasi. Secara strategis, temuan domain yang paling lemah terkonsentrasi pada kontrol pemantauan insiden (Annex A.5) dan manajemen persetujuan privasi (PIMS 7.2.3). Kondisi ini sejalan dengan laporan Deloitte [5] bahwa deteksi insiden di sektor finansial seringkali lambat.

- Perbandingan dengan standar keamanan

  Bank Umum nasional menunjukkan bahwa model risk scoring ini mengisi kekosongan yang tidak mampu dijawab oleh metode audit kepatuhan (compliance-based) konvensional. Evaluasi berbasis checklist manual cenderung hanya menilai "ada atau tidak ada" (binary), tanpa mengukur seberapa efektif kontrol tersebut menekan risiko residual. Dengan model ini, manajemen Bank Pembangunan Daerah kini memiliki dasar kuantitatif (Security Index) untuk mengalokasikan anggaran keamanan siber secara proporsional, memfokuskan investasi pada kontrol yang memiliki nilai ROI dalam penurunan risiko tertinggi. Integrasi ISO/IEC 27001:2022 dan ISO/IEC 27701:2025 dalam satu kerangka kuantitatif menjadi kontribusi utama yang membedakan penelitian ini dari studi sebelumnya [17], [18].

IV. Kesimpulan dan saran

Model evaluasi keamanan informasi berbasis risk scoring yang dikembangkan terbukti mampu meningkatkan sensitivitas deteksi risiko sebesar 133% dibandingkan metode checklist konvensional, menurunkan risiko kategori critical sebesar 62,5%, serta meningkatkan Security Index (SI) organisasi secara meyakinkan dari 0.42 (Cukup) menjadi 0.79 (Sangat Baik). Dengan reliabilitas sangat kuat (Cohen's Kappa 0,82), model ini memvalidasi bahwa pendekatan kuantitatif terintegrasi antara ISO/IEC 27001:2022 dan ISO/IEC 27701:2025 layak diadopsi sebagai kerangka evaluasi terstandar bagi Bank Pembangunan Daerah untuk mendukung pengambilan keputusan berbasis risiko. Secara konseptual, transformasi evaluasi dari pendekatan deskriptif menuju pengukuran kuantitatif berbasis risk scoring memberikan landasan yang lebih adaptif terhadap dinamika ancaman siber modern. Model ini memungkinkan pihak manajemen memprioritaskan alokasi sumber daya pada kontrol yang paling kritis, sehingga penguatan tata kelola keamanan informasi dan pemenuhan amanah perlindungan data nasabah dapat berjalan secara terukur. Meskipun menunjukkan hasil yang signifikan, penelitian ini memiliki keterbatasan. Pertama, penentuan nilai likelihood masih bergantung pada expert judgment, sehingga berpotensi mengandung bias subjektif meskipun telah diminimalisasi melalui konsensus pakar. Kedua, model ini belum terintegrasi dengan data threat intelligence eksternal secara real-time, sehingga perhitungan risiko belum merepresentasikan ancaman siber yang bersifat dinamis harian secara penuh. Ketiga, dashboard visualisasi yang dirancang masih memerlukan input manual. Saran untuk pengembangan selanjutnya adalah mengintegrasikan model ini dengan dashboard pemantauan real-time yang terhubung langsung dengan threat intelligence eksternal, serta memanfaatkan analitik prediktif (machine learning) untuk mengurangi ketergantungan pada expert judgment dalam menentukan nilai likelihood, sehingga model dapat lebih aplikatif, skalabel, dan memiliki daya generalisasi yang lebih kuat di berbagai institusi keuangan.

Ucapan Terima Kasih

Para penulis menyampaikan apresiasi tulus kepada manajemen dan tim Teknologi Informasi Bank Pembangunan Daerah atas kerja sama, dukungan, serta keterbukaan dalam menyediakan akses dokumentasi, data evaluasi, dan fasilitasi wawancara yang sangat mendukung pelaksanaan penelitian ini. Ucapan terima kasih khusus disampaikan kepada Lead Auditor badan sertifikasi dari TÜV SÜD dan Lead Auditor ISO 27001:2022 pendamping pihak Bank (konsultan dari PT Q2 Technologies) atas kontribusi expert judgment dan validasi dalam proses penilaian risiko dan pengujian reliabilitas model ini. Ucapan terima kasih juga disampaikan kepada narasumber dari divisi manajemen risiko, keamanan informasi, dan kepatuhan yang telah memberikan wawasan strategis sehingga memperkaya proses perancangan, pengujian, dan validasi model risk scoring yang dikembangkan. Para penulis turut mengakui peran penting Badan Sertifikasi dan Otoritas Jasa Keuangan dalam menyediakan referensi regulasi serta kerangka kepatuhan yang relevan dengan implementasi standar keamanan informasi dan perlindungan data pribadi di sektor perbankan. Apresiasi juga disampaikan kepada Departemen Sistem Informasi, Universitas Indraprasta PGRI, serta Departemen Sistem Informasi, Sekolah Tinggi Informatika dan Manajemen Komputer STI&K Jakarta atas dukungan institusional dan fasilitasi akademik selama proses penelitian dan penyusunan artikel ini. Para penulis berharap hasil penelitian ini dapat memberikan kontribusi nyata dalam penguatan tata kelola keamanan informasi dan privasi data pada Bank Pembangunan Daerah serta sektor jasa keuangan Indonesia secara lebih luas.

Daftar Pustaka

[1] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2023*. Heraklion, Greece: ENISA, 2023.

[2] World Economic Forum, *Global Cybersecurity Outlook 2024*. Geneva, Switzerland: World Economic Forum, 2024.

[3] A. L. Samuel, "Some studies in machine learning using the game of checkers," *IBM Journal of Research and Development*, vol. 44, no. 1, pp. 206–227, 2000, doi: 10.1147/RD.441.0206.

[4] ISACA, *State of Cybersecurity 2024*. Schaumburg, IL, USA: ISACA, 2024.

[5] J. Bernard, S. Rampado, and N. Seaver, "Cybersecurity insights 2023: Budgets and benchmarks for financial services institutions," Deloitte, 2023.

[6] Otoritas Jasa Keuangan, "Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum," Jakarta, Indonesia, 2022.

[7] Bank Indonesia, "Peraturan Anggota Dewan Gubernur Nomor 24/7/PADG/2022 tentang Penyelenggaraan Sistem Pembayaran oleh Penyedia Jasa Pembayaran dan Penyelenggara Infrastruktur Sistem Pembayaran," Jakarta, Indonesia, 2022.

[8] Badan Siber dan Sandi Negara (BSSN), *Laporan Tahunan 2024*. Jakarta, Indonesia: BSSN, 2024.

[9] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27002:2022: Information Security, Cybersecurity and Privacy Protection—Information Security Controls*, 3rd ed. Geneva, Switzerland: ISO, 2022.

[10] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27701:2025: Information Security, Cybersecurity and Privacy Protection—Privacy Information Management Systems—Requirements and Guidance*, 2nd ed. Geneva, Switzerland: ISO, 2025.

[11] National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37 Rev. 2. Gaithersburg, MD, USA: NIST, 2018.

[12] R. Ross, *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Rev. 1. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2012, doi: 10.6028/NIST.SP.800-30r1.

[13] A. Calder and S. Watkins, *IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002*, 8th ed. London, U.K.: IT Governance Publishing, 2024, doi: 10.2307/j.ctv336p2z9.

[14] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," *Computers & Security*, vol. 57, pp. 14–30, 2016, doi: 10.1016/j.cose.2015.11.001.

[15] S. Saleh, M. Hammoudeh, dan A. Aldabbas, "A quantitative risk scoring model for information security management," IEEE Access, vol. 10, hlm. 112345–112358, 2022.

[16] P. Radanliev, D. De Roure, M. Van Kleek, U. Ani, P. Burnap, E. Anthi, J. R. C. Nurse, O. Santos, R. Mantilla Montalvo, and L. Maddox, "Dynamic real-time risk analytics of uncontrollable states in complex internet of things systems: cyber risk at the edge," *Environment Systems and Decisions*, vol. 41, no. 2, pp. 236–247, 2021, doi: 10.1007/s10669-020-09792-x.

[17] K. T. Tan, B. Foo, dan L. Y. Lim, "Security maturity assessment model for banking information systems," Journal of Information Security and Applications, vol. 68, 2023.

[18] S. A. Pratiwi, R. Mayanti, S. A. N. Arifin, N. D. Rahmawati, and R. B. Wicaksono, "Hasil evaluasi implementasi ISO/IEC 27001:2022 dan ISO/IEC 27701:2019 dalam penguatan sistem manajemen keamanan informasi dan privasi di PT Bank XYZ," *[nama jurnal perlu dikonfirmasi dari artikel asli]*, vol. 8, no. 5, 2025.