Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI
Volume 7, Nomor 1, Tahun 2024, Hal 328-332
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

# Evaluasi Keamanan Sistem Informasi dalam Lingkungan Bisnis Digital

**Muhammad Alim[1*], Ibnu Rasyid Munthe[2], Angga Putra Juledi[3]**

[1,2,3]Manajemen Informatika, Unversitas Labuhan Batu, Rantauprapat, Indonesia
Email Penulis Korespondensi: [1]storehallo421@gmail.com

**Abstrak**– Evaluasi keamanan sistem informasi dalam lingkungan bisnis digital menjadi semakin penting seiring dengan peran yang semakin dominan dari teknologi informasi dalam operasi bisnis. Penelitian ini bertujuan untuk mengevaluasi keamanan sistem informasi dalam konteks bisnis digital, dengan fokus pada identifikasi kerentanan dan risiko yang mungkin timbul serta pengembangan strategi mitigasi yang efektif. Metode penelitian yang digunakan meliputi analisis risiko, audit keamanan, dan pengujian penetrasi. Data yang dikumpulkan mencakup informasi tentang sistem informasi yang digunakan, kerentanan yang terdeteksi, dan hasil pengujian keamanan. Hasil penelitian menunjukkan bahwa meskipun banyak perusahaan telah mengimplementasikan langkah-langkah keamanan, masih ada kerentanan yang dapat dieksploitasi oleh penyerang. Dari analisis risiko dan pengujian penetrasi, beberapa kerentanan kritis telah diidentifikasi yang dapat mengancam keamanan sistem informasi dan data bisnis. Sebagai hasil dari evaluasi ini, disarankan untuk mengadopsi pendekatan yang holistik dalam mengelola keamanan sistem informasi, termasuk implementasi tindakan pengamanan tambahan, pelatihan karyawan tentang praktik keamanan IT yang baik, dan pemantauan yang terus-menerus terhadap lingkungan bisnis digital. Dengan menerapkan strategi mitigasi yang tepat, diharapkan perusahaan dapat mengurangi risiko keamanan dan melindungi aset informasi mereka dalam lingkungan bisnis digital yang semakin kompleks dan rentan terhadap serangan cyber.

**Kata Kunci:** Keamanan Sistem Informasi, Bisnis Digital, Evaluasi Keamanan, Risiko Keamanan, Strategi Mitigasi

**Abstract**– Evaluation of information systems security in the digital business environment is becoming increasingly important along with the increasingly dominant role of information technology in business operations. This study aims to evaluate information system security in the context of digital business, focusing on identifying vulnerabilities and risks that may arise as well as developing effective mitigation strategies. Research methods used include risk analysis, security audits, and penetration testing. The data collected includes information about the information systems used, vulnerabilities detected, and security test results. The results showed that although many companies have implemented security measures, there are still vulnerabilities that attackers can exploit. From risk analysis and penetration testing, several critical vulnerabilities have been identified that could threaten the security of information systems and business data. As a result of this evaluation, it is recommended to adopt a holistic approach in managing information system security, including the implementation of additional security measures, employee training on good IT security practices, and continuous monitoring of the digital business environment. By implementing appropriate mitigation strategies, it is expected that companies can reduce security risks and protect their information assets in an increasingly complex and vulnerable digital business environment to cyber attacks.

**Keywords:** Information Systems Security, Digital Business, Security Evaluation, Security Risk, Mitigation Strategy

## 1. PENDAHULUAN

Dalam era digital yang berkembang pesat saat ini, teknologi informasi telah menjadi tulang punggung dari berbagai aspek bisnis. Bisnis digital menawarkan fleksibilitas, efisiensi, dan aksesibilitas yang tak tertandingi, namun juga membawa risiko keamanan yang signifikan. Keamanan sistem informasi dalam lingkungan bisnis digital menjadi semakin penting karena serangan cyber yang semakin canggih dan sering terjadi..[4].

Penelitian ini bertujuan untuk mengevaluasi keamanan sistem informasi dalam konteks bisnis digital. Evaluasi ini bertujuan untuk mengidentifikasi kerentanan potensial yang mungkin dimanfaatkan oleh penyerang serta untuk mengembangkan strategi mitigasi yang efektif untuk melindungi aset informasi perusahaan.

Dalam pendahuluan ini, kami akan membahas latar belakang masalah, signifikansi penelitian, dan tujuan penelitian. Selain itu, kami juga akan menjelaskan metodologi yang akan digunakan dalam evaluasi keamanan sistem informasi dalam lingkungan bisnis digital. Dengan memahami dan mengatasi tantangan keamanan yang dihadapi oleh bisnis digital, diharapkan perusahaan dapat melindungi diri dari serangan cyber dan menjaga kelangsungan bisnis mereka dalam era digital yang semakin kompleks.[6],[7].

Dalam pendahuluan ini, kami akan membahas latar belakang masalah, signifikansi penelitian, dan tujuan penelitian. Selain itu, kami juga akan menjelaskan metodologi yang akan digunakan dalam evaluasi keamanan sistem informasi dalam lingkungan bisnis digital. Dengan memahami dan mengatasi tantangan keamanan yang dihadapi oleh bisnis digital, diharapkan perusahaan dapat melindungi diri dari serangan cyber dan menjaga kelangsungan bisnis mereka dalam era digital yang semakin kompleks. Pada tahap selanjutnya, penelitian ini akan membahas analisis mendalam tentang risiko keamanan yang dihadapi oleh bisnis digital, mengidentifikasi strategi mitigasi yang tepat, dan


Submitted: **07/03/2024**; Accepted: **14/03/2024**; Published: **31/03/2024**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI
Volume 7, Nomor 1, Tahun 2024, Hal 328-332
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

menyajikan kesimpulan dan rekomendasi untuk perbaikan keamanan sistem informasi. Dengan demikian, diharapkan penelitian ini akan memberikan wawasan yang berharga bagi para praktisi keamanan informasi dan pemangku kepentingan bisnis dalam upaya mereka untuk melindungi aset dan operasi mereka dari serangan cyber yang semakin kompleks. Selain itu, kami juga akan menjelaskan metodologi yang akan digunakan dalam evaluasi keamanan sistem informasi dalam lingkungan bisnis digital. Metodologi ini akan mencakup langkah-langkah analisis risiko, audit keamanan, dan pengujian penetrasi yang akan dilakukan untuk mengidentifikasi kerentanan dan merancang strategi mitigasi yang efektif. Dengan memahami dan mengatasi tantangan keamanan yang dihadapi oleh bisnis digital, diharapkan perusahaan dapat melindungi diri dari serangan cyber dan menjaga kelangsungan bisnis mereka dalam era digital yang semakin kompleks. Selanjutnya, penelitian ini akan membahas analisis mendalam tentang risiko keamanan, strategi mitigasi yang tepat, dan menyajikan kesimpulan serta rekomendasi untuk perbaikan keamanan sistem informasi.

## 2. METODOLOGI PENELITIAN

### 2.1 Analisis Risiko

Tahap awal penelitian ini akan melibatkan analisis risiko keamanan sistem informasi dalam lingkungan bisnis digital. Langkah ini akan mencakup identifikasi potensi ancaman, kerentanan, dan dampak yang mungkin timbul akibat serangan cyber. Analisis risiko akan membantu dalam pemahaman mendalam tentang ancaman yang dihadapi oleh sistem informasi perusahaan.

### 2.2 Audit Keamanan

Selanjutnya, akan dilakukan audit keamanan sistem informasi untuk mengevaluasi kepatuhan sistem terhadap standar keamanan yang berlaku dan praktik terbaik industri. Audit ini akan melibatkan pemeriksaan langsung terhadap konfigurasi sistem, pengaturan keamanan, dan kebijakan yang ada.

### 2.3 Pengujian Penetrasi

Tahap terakhir dari metodologi penelitian ini adalah pengujian penetrasi, di mana akan dilakukan serangkaian uji coba untuk mengidentifikasi kerentanan sistem yang dapat dimanfaatkan oleh penyerang. Pengujian ini akan mencakup skenario serangan yang realistis untuk mengevaluasi efektivitas sistem dalam menghadapi ancaman.

### 2.4 Analisis Hasil

Setelah pengumpulan data dari langkah-langkah sebelumnya, akan dilakukan analisis mendalam terhadap temuan dan hasil evaluasi. Hal ini akan mencakup identifikasi kerentanan yang paling kritis, rekomendasi untuk tindakan perbaikan, dan pemetaan strategi mitigasi yang tepat.

Dengan menerapkan metodologi ini, diharapkan penelitian ini dapat memberikan pemahaman yang lebih baik tentang keamanan sistem informasi dalam bisnis digital serta memberikan panduan yang bermanfaat bagi perusahaan untuk meningkatkan pertahanan mereka terhadap serangan cyber.

Penelitian mengadopsi pendekatan penelitian deskriptif kuantitatif mempertimbangkan bagaimana pendekatan ini tidak melihat, tidak berupaya menemukan, dan tidak membandingkan dua variabel untuk melihat sebab dan akibat dari suatu fenomena (Yusuf, 2017). Pendekatan kualitatif juga dilakukan guna menggali faktor penyebab buruknya sistem manajemen informasi yang diterapkan. Responden penelitian terdiri dari dua orang dengan latar belakang pekerjaan dari divisi Sub Koordinator Pengembangan Sistem Informasi yang bertanggung jawab atas keamanan informasi pada Sistem Elektronik di Dinas XYZ

## 3. HASIL DAN PEMBAHASAN

### 3.1 Analisa Data

Analisis data dilakukan melalui dua tahapan, yaitu tahap pengklasifikasian kategori Sistem Elektronik dan tahap pengukuran tingkat kesiapan SMKI pada enam area yang lainnya. Penggolongan kategori Sistem Elektronik dibedakan menjadi tiga kategori dengan rentang skor seperti pada Tabel 1. Kategori Sistem Elektronik:

**Tabel 1.** Kategori Sistem Elektronik

| Kategori Sistem Elektronik | Skor |
|---|---|
| Rendah | 10-15 |
| Tinggi | 16-34 |
| Strategis | 35-50 |


Submitted: **07/03/2024**; Accepted: **14/03/2024**; Published: **31/03/2024**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI
Volume 7, Nomor 1, Tahun 2024, Hal 328-332
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

Penilaian tingkat kesiapan dan kelengkapan penerapan Sistem Manajemen Keamanan Informasi pada area Tata Kelola Keamanan Informasi hingga area Teknologi dan Keamanan Informasi terbagi menjadi tiga tahap penerapan, yaitu:
Penerapan tahap 1: kerangka kerja dasar keamanan informasi
Penerapan tahap 2: efektivitas dan konsistensi dari penerapan keamanan informasi
Penerapan tahap 3: kemampuan meningkatkan kinerja keamanan informasi

Status penilaian pada area Tata Kelola Keamanan Informasi hingga area Suplemen terbagi menjadi empat kategori sebagai berikut:

**Tabel 2.** Skor Penerapan sesuai Kategori Pengamanan

| Status Pengamanan | Kategori Pengamanan | | |
|---|---|---|---|
| | 1 | 2 | 3 |
| Tidak Dilakukan | 0 | 0 | 0 |
| Dalam Perencanaan | 1 | 2 | 3 |
| Dalam Penerapan atau Diterapkan Sebagian | 2 | 4 | 6 |
| Diterapkan secara Menyeluruh | 3 | 6 | 9 |

Pertanyaan pada penerapan tahap 3 dapat diisi ketika pertanyaan pada penerapan tahap 1 dan 2 sudah terisi dengan minimal status "Diterapkan sebagian". Selain itu, penilaian terhadap area Suplemen dapat dilakukan apabila organisasi mengalami permasalahan terkait pengelolaan data pribadi, seperti akses ilegal dan sebagainya. Sesudah semua area keamanan dinilai, output akhir yang diperoleh berupa total skor status kesiapan dengan rentang pada Tabel 3. Skor Akhir dan Status Kesiapan:

**Tabel 3.** Skor Akhir dan Status Kesiapan

| KATEGORI SISTEM ELEKTRONIK | | | | |
|---|---|---|---|---|
| **Rendah** | | **Skor Akhir** | | **Status Kesiapan** |
| 10 | 15 | 0 | 174 | Tidak Layak |
| | | 175 | 312 | Perlu Perbaikan |
| | | 313 | 535 | Cukup |
| | | 536 | 645 | Baik |
| **Tinggi** | | **Skor Akhir** | | **Status Kesiapan** |
| 16 | 34 | 0 | 272 | Tidak Layak |
| | | 273 | 455 | Perlu Perbaikan |
| | | 456 | 583 | Cukup |
| | | 584 | 645 | Baik |
| **Strategis** | | **Skor Akhir** | | **Status Kesiapan** |
| 35 | 50 | 0 | 333 | Tidak Layak |
| | | 334 | 535 | Perlu Perbaikan |
| | | 536 | 609 | Cukup |
| | | 610 | 645 | Baik |

Pembahasan :

A. Kategori Sistem Elektronik

Dinas XYZ Provinsi Jawa Tengah merupakan salah satu Penyelenggara Sistem Elektronik (PSE) yang ditujukan untuk kepentingan pelayanan publik dan sebagai Penyelenggara Sistem Elektronik (PSE), Dinas XYZ harus menerapkan manajemen pengamanan informasi berdasarkan asas risiko sesuai dengan peraturan Sistem Manajemen Keamanan Informasi (SMKI) yang berlaku. Berdasarkan hasil penilaian diperoleh skor 26 berada di kategori "Tinggi". Hasil ini berarti instansi memiliki ketergantungan tinggi terhadap Sistem Elektronik. Sesuai dengan Permen Kominfo RI No.4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi Pasal 4 ayat (3) menyebutkan bahwa "Sistem Elektronik Tinggi merupakan Sistem Elektronik yang berdampak terbatas pada kepentingan sektor dan/atau daerah tertentu", dan dan pasal 10 ayat (1) bahwa "Penyelenggara Sistem Elektronik strategis dan Penyelenggara Sistem Elektronik tinggi wajib memiliki Sertifikat Sistem Manajemen Keamanan Informasi". Jadi, sebagai penyelenggara Sistem Elektronik tinggi, Dinas XYZ wajib menerapkan standar SNI ISO/IEC 27001 untuk dapat melaksanakan sertifikasi SMKI.

B. Tata Kelola Keamanan Informasi

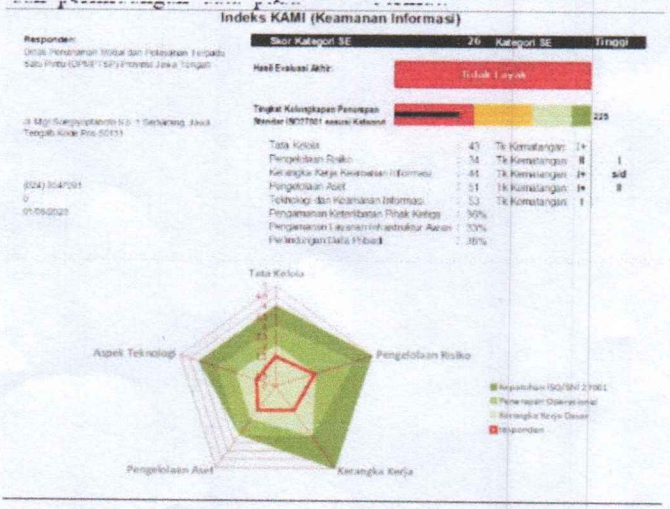
Tata kelola keamanan informasi berhubungan dengan prosedur untuk memastikan penggunaan teknologi informasi sesuai dengan tujuan organisasi (Riswaya et al., 2020). Organisasi yang menggunakan teknologi informasi harus menerapkan dan memperhatikan dengan serius. Penilaian terhadap tingkat kesiapan dan kematangan SMKI pada area


Submitted: **07/03/2024**; Accepted: **14/03/2024**; Published: **31/03/2024**

Jurnal Ilmu Komputer dan Sistem Informasi (JIKOMSI
Volume 7, Nomor 1, Tahun 2024, Hal 328-332
ISSN 2723- 6129 (media online)
Link Jurnal : https://ejournal.sisfokomtek.org/index.php/jikom

Tata Kelola Keamanan Informasi ditujukan guna mengevaluasi bentuk tata kelola keamanan informasi beserta fungsi, tugas, dan tanggung jawab pengelola keamanan informasi. Penilaian pada area ini dilakukan dengan 22 pertanyaan yang terbagi menjadi 3 tahap penerapan. Berdasarkan hasil penilaian, keamanan informasi pada area Tata Kelola Keamanan Informasi yang telah diimplementasikan oleh Dinas XYZ Provinsi Jawa Tengah berada pada tahap 1 dan 2. Hal ini disebabkan karena total skor penerapan tahap 1 dan 2 kurang dari batas skor minimal tahap penerapan 3, sehingga penerapan keamanan informasi pada area Tata Kelola Keamanan Informasi masih belum mengupayakan tindakan peningkatan keamanan informasi. Skor penerapan tahap 1, 2 dan 3 diperoleh skor 43. Pengelolaan Risiko Keamanan Penilaian tingkat kematangan area Tata Kelola Keamanan Informasi diperoleh skor tingkat kematangan II sebesar 33, sedangkan ditetapkan skor minimum tingkat kematangan II adalah 12 dan skor pencapaian tingkat kematangan II 36. Hal ini berarti skor tingkat kematangan II kurang dari skor pencapaian tingkat kematangan II, sehingga diperoleh level kematangan I+ dengan skor ambang batas 43,2 (80% dari total skor kematangan II). Untuk naik di tingkat kematangan III, maka harus memperoleh validitas tingkat kematangan II "Yes" dan skor kematangan II lebih dari skor ambang batas kematangan II. Berdasarkan analisa, skor kematangan tingkat II kurang dari skor ambang batas kematangan tingkat II, sehingga diperoleh validitas "No" untuk kematangan III dan level kematangan tetap berada pada level I+.

Terdapat beberapa kendala yang dialami sehingga banyak syarat yang tidak dapat dipenuhi seperti instansi sulit mengintegrasikan persyaratan keamanan informasi karena masih menggunakan kerangka kerja lama yang sudah digunakan sejak dahulu sehingga diperlukan perombakan, kemudian untuk koordinasi pengelolaan aset baik internal maupun eksternal belum memiliki panduan khusus dan hanya dilakukan seadanya, yang terakhir yakni belum adanya program khusus untuk mematuhi tujuan dan sasaran kepatuhan keamanan informasi.




**Gambar 1.** Hasil Penilaian Indeks KAMI v.4.2

## 4. KESIMPULAN

Dalam penelitian ini, kami berhasil menerapkan algoritma pohon keputusan C4.5 untuk deteksi serangan dalam jaringan komputer. Melalui penggunaan dataset yang mencakup berbagai jenis serangan dan aktivitas jaringan, kami berhasil membangun model deteksi serangan yang efektif dan dapat diandalkan. Hasil evaluasi menunjukkan bahwa model deteksi serangan yang dikembangkan menggunakan algoritma C4.5 mampu mengklasifikasikan aktivitas jaringan dengan tingkat akurasi yang memuaskan. Model ini mampu mengenali pola-pola yang terkait dengan serangan dan secara efektif membedakannya dari aktivitas jaringan normal. Selain itu, kami juga berhasil mengidentifikasi faktor-faktor yang paling berpengaruh dalam deteksi serangan, sehingga memberikan wawasan yang berharga bagi praktisi keamanan jaringan dalam mengembangkan strategi deteksi yang lebih efektif. Kesimpulannya, penelitian ini memberikan kontribusi yang signifikan dalam pengembangan sistem deteksi serangan yang lebih canggih dan dapat diandalkan dalam konteks jaringan komputer. Dengan memanfaatkan kekuatan algoritma pohon keputusan C4.5, kami berharap dapat membantu meningkatkan keamanan jaringan komputer dan melindungi infrastruktur informasi dari ancaman serangan cyber yang semakin kompleks..

## 5. REFERENCES

[1] B. G. Ginting and F. A. Sianturi, "Sistem Pendukung Keputusan Pemberian Bantuan Kepada Keluarga Kurang Mampu Menggunakan Metode AHP," *J Nas Komputasi Dan Teknol Inf*, vol. 4, no. 1, 2021.

[2] F. Sahputra and F. A. Sianturi, "Decision Support System Selection of Best Employee At PT. Intiberkah Sinar Sejahtera Using Simple Additive weighting Method," *J. Comput. Netw. Archit. High Perform. Comput.*, vol. 2, no. 1, pp. 1–6, 2020.


Submitted: **07/03/2024**; Accepted: **14/03/2024**; Published: **31/03/2024**

[3] A. Afrisawati and S. Sahren, "ANALISIS PERBANDINGAN MENGGUNAKAN METODE MOORA DAN WASPAS PEMILIHAN BIBIT SAPI POTONG TERBAIK," *JURTEKSI J. Teknol. Dan Sist. Inf.*, vol. 6, no. 3, pp. 269–276, Aug. 2020, doi: 10.33330/jurteksi.v6i3.827.

[4] Y. U. Alsabri, A. Zakir, and D. Irwan, "Penerapan Customer Relationship Management Pada Sistem Informasi Klinik Kecantikan Berbasis Website (Studi Kasus: Ms Glow Aesthetic Clinic)," vol. 4, 2022.

[5] F. M. Matondang and F. A. Sianturi, "Decision Support System for Determination of Nutrition in Pulmonary Tuberculosis Patients using Multi-Objective Optimization Method On The Basic Of Analysis (MOORA)," *Login J. Teknol. Komput.*, vol. 14, no. 2, pp. 198–204, 2020.

[6] W. Wati and F. A. Sianturi, "Implementasi Metode Topsis Dalam Merekomendasikan Pestisida Terbaik Pada Tanaman Padi Di Desa Rumbia," *J. Sains Dan Teknol.*, vol. 3, no. 2, pp. 31–35, 2022.

[7] F. A. Sianturi and M. Sitorus, "Kombinasi Metodesimpleadditiveweighting (Saw) Denganalgoritma Nearest Neighbor Untuk Rekruitmen Karyawan," *J. Mantik Penusa*, vol. 3, no. 2, Des, 2019.

[8] R. I. Batubara and Y. Siregar, "Sistem Pendukung Keputusan Karyawan Honorer Terbaik di Dinas Perkebunan Medan Dengan Metode Gada," *J. Media Inform.*, vol. 3, no. 2, pp. 104–111, Jun. 2022, doi: 10.55338/jumin.v3i2.279.

[9] F. Laia and F. A. Sianturi, "Sistem Pendukung Keputusan Penilaian Kinerja Pegawai Terbaik dengan Metode Simple Additive Waighting (SAW)," *RESOLUSI Rekayasa Tek. Inform. Dan Inf.*, vol. 1, no. 3, pp. 195–200, 2021.

[10] A. Arisman and F. A. Sianturi, "Sistem Pendukung Keputusan Penerimaan Siswa Baru Menggunakan Metode Moora (Multi-Objective Optimization On The Basis Of Ratio Analysis)," *J. Ilmu Komput. Dan Sist. Inf. JIKOMSI*, vol. 3, no. 1.1, pp. 73–83, 2020.


Submitted: **07/03/2024**; Accepted: **14/03/2024**; Published: **31/03/2024**