BRAHMANA: Jurnal Penerapan Kecerdasan Buatan
Terakreditasi Nomor 204/E/KPT/2022 | Vol. 6, No. 1, Desember (2024), pp. 10-15

Penilaian Keamanan Informasi Menggunakan Pendekatan Indeks Keamanan Informasi 4.0 dan *Vulnerability Asessment*

I Gede Putu Krisna Juliharta[1], Ayu Pradnyandari Dananjaya Erawan[2]*
[1,2]Universitas Primakara, Denpasar, Bali
Email: krisna@primakara.ac.id[1], ayu13pradnyandari@gmail.com[2]

Abstract

In the era of rapidly evolving information technology, information security has become increasingly crucial. Threats to data and information are becoming more diverse and complex, making information security preparedness the key to protecting an organization's critical assets. XYZ City, with its commitment to optimizing the use of information technology, recognizes the importance of information security. Therefore, the Information and Communication Technology Office (Diskominfo) of XYZ City conducted an assessment using the Information Security Index (KAMI) to measure, analyze, and improve the maturity of information security in its organization. The results of the KAMI assessment indicate that XYZ City has achieved a good evaluation result. While there are some areas that show good performance, such as Risk Management and Technology and Information Security, there are still areas that need to be strengthened.

***Keywords**: Information Security Index, Information System Security, Vulnerability Assessment*

Abstrak

Di era teknologi informasi yang terus berkembang pesat, keamanan informasi menjadi semakin krusial. Ancaman terhadap data dan informasi semakin beragam dan kompleks, sehingga kesiapan keamanan informasi menjadi kunci untuk melindungi aset penting organisasi. Kota XYZ, dengan komitmennya untuk memanfaatkan teknologi informasi secara optimal, menyadari pentingnya keamanan informasi. Oleh karena itu, Dinas Komunikasi dan Informatika (Diskominfo) Kota XYZ melakukan penilaian menggunakan Indeks Keamanan Informasi (KAMI) untuk mengukur, menganalisis, dan meningkatkan kematangan keamanan informasi di organisasinya. Hasil penilaian KAMI menunjukkan bahwa Kota XYZ telah mencapai hasil evaluasi yang Cukup Baik. Meskipun hasil KAMI menunjukkan klaim yang cukup baik secara subjektif, penilaian objektif melalui Vulnerability Assessment mengidentifikasi area yang perlu ditangani dan menjadi perhatian utama.

***Kata kunci**: Indeks KAMI, Keamanan Sistem Informasi, Vulnerability Assessment*

1. Pendahuluan

Di era digital yang kian dinamis, teknologi informasi telah menjelma menjadi pilar fundamental bagi kemajuan organisasi. Namun, di balik kecanggihan teknologi, terbentang pula potensi ancaman yang kian besar terhadap keamanan informasi. Hal ini menjadikan keamanan informasi sebagai aspek krusial dalam melindungi aset data dan informasi organisasi.

Indeks Keamanan Informasi (KAMI) hadir sebagai alat ukur penting untuk menilai tingkat kematangan keamanan informasi organisasi. Penilaian KAMI menggabungkan dua pendekatan utama: subjektif dan objektif. Pendekatan subjektif dilakukan dengan mengevaluasi kesiapan organisasi dalam menerapkan standar keamanan informasi, sedangkan pendekatan objektif dilakukan melalui *Vulnerability Assessment* untuk mengidentifikasi celah keamanan yang berpotensi dieksploitasi [1].

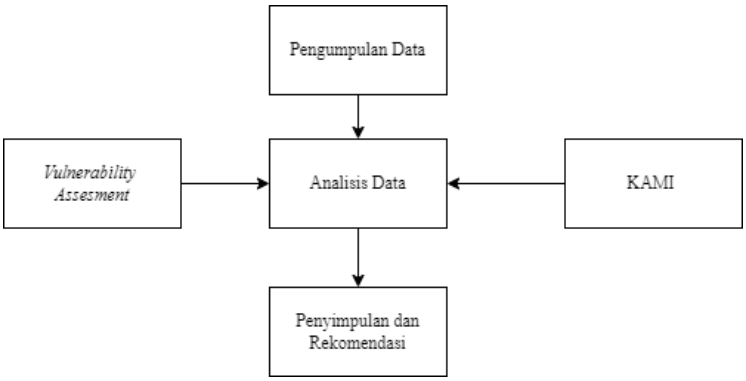
Studi kasus Dinas Kominfo dan Statistik Kota XYZ menawarkan wawasan menarik terkait temuan penilaian KAMI dan implikasinya terhadap postur keamanan informasi.

ISSN: 2715-9906

Meskipun penilaian KAMI menunjukkan tingkat kematangan V pada kerangka kerja keamanan sistem informasi dan IV pada teknologi dan keamanan informasi, hasil *Vulnerability Testing* justru mengungkapkan bahwa aspek manajemen keamanan informasi masih belum memenuhi standar yang diharapkan.

2. Metodologi Penelitian

Penelitian ini bertujuan untuk menyelidiki postur keamanan informasi di Dinas Kominfo dan Statistik Kota XYZ dengan menganalisis temuan dan rekomendasi dalam dua dokumen resmi: Hasil *Security Assessment* dan *Penetration Testing*, kemudian laporan penilaian keamanan sistem informasi Kota XYZ. Dinas Kominfo dan Statistik Kota XYZ memanfaatkan dua *tools* penting: Indeks Keamanan Informasi (KAMI) 4.2 dan *Vulnerability Assessment* (VA). KAMI 4.2 berperan sebagai alat ukur subjektif untuk menilai tingkat kematangan keamanan informasi organisasi, sedangkan VA berperan sebagai alat ukur objektif untuk mengidentifikasi celah keamanan yang berpotensi dieksploitasi.



Gambar 1. Diagram Rancangan Penelitian

Metodologi penelitian yang digunakan melibatkan tiga langkah utama:

a. Pengumpulan Data:
   1. Mengumpulkan dokumen-dokumen resmi terkait.
   2. Membaca dan memahami secara menyeluruh isi dokumen.
   3. Mengidentifikasi temuan dan rekomendasi yang relevan dengan keamanan informasi.

b. Analisis Data:
   1. Melakukan analisis kualitatif terhadap temuan dan rekomendasi.
   2. Mengategorikan temuan dan rekomendasi berdasarkan jenis, tingkat keparahan, dan dampaknya.
   3. Mengidentifikasi pola dan tren dalam temuan dan rekomendasi.
   4. Menginterpretasikan temuan dan rekomendasi dalam konteks postur keamanan informasi di Dinas Kominfo dan Statistik Kota XYZ.

c. Penyimpulan dan Rekomendasi:
   1. Merumuskan kesimpulan berdasarkan hasil analisis data.
   2. Menyusun rekomendasi untuk meningkatkan keamanan informasi di Dinas Kominfo dan Statistik Kota XYZ.

Teknik pengumpulan data yang digunakan adalah analisis dokumen. Teknik analisis data yang digunakan adalah analisis konten dan analisis tematis. Jadwal penelitian diprediksi membutuhkan waktu 4 minggu, dengan 1 minggu untuk pengumpulan data, 2 minggu untuk analisis data, dan 1 minggu untuk penyusunan laporan penelitian.

Etika penelitian ditegakkan dengan menjaga kerahasiaan data, melaporkan temuan dan rekomendasi secara objektif, serta menghormati privasi dan hak-hak individu. Hasil penelitian diharapkan dapat menghasilkan laporan yang berisi analisis temuan dan rekomendasi, gambaran postur keamanan informasi, identifikasi celah keamanan, dan

rekomendasi untuk meningkatkan keamanan informasi secara keseluruhan di Dinas Kominfo dan Statistik Kota XYZ.

Manfaat penelitian ini diharapkan dapat membantu Dinas Kominfo dan Statistik Kota XYZ dalam meningkatkan keamanan informasi, menjadi acuan bagi organisasi lain, dan bermanfaat bagi penelitian terkait keamanan informasi di sektor pemerintahan.

2.1. Indeks KAMI (Keamanan Informasi)

Indeks KAMI hadir sebagai alat penting untuk menilai kematangan sistem keamanan informasi pada organisasi. Alat ini tidak untuk menganalisis kelayakan atau efektivitas pengamanan yang ada, melainkan untuk memberikan gambaran menyeluruh tentang kesiapan kerangka kerja keamanan informasi kepada pimpinan organisasi [2]. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2013.

Indeks KAMI dirancang dengan fleksibilitas tinggi, memungkinkan penggunaannya oleh organisasi dari berbagai skala, ukuran, dan tingkat ketergantungan pada teknologi informasi dan komunikasi (TIK). Hal ini menjadikan Indeks KAMI sebagai alat yang ideal untuk menilai kesiapan keamanan informasi di berbagai jenis organisasi. Proses evaluasi dengan Indeks KAMI menghasilkan gambaran menyeluruh tentang kesiapan kerangka kerja keamanan informasi organisasi, baik dari segi kelengkapan maupun kematangan [3]. Data ini dapat dijadikan sebagai tolak ukur untuk melacak kemajuan dan mengukur efektivitas program keamanan informasi. Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan kepada pihak yang terkait (*stakeholders*) [4].

2.2. Vulnerability Assesment

Vulnerability Assessment (VA) bagaikan pemindai canggih yang membantu organisasi dalam mendeteksi celah keamanan informasi (*vulnerability*) dalam sistem, jaringan, atau aplikasi mereka [1]. VA bekerja dengan mengidentifikasi, mengkategorikan, dan memprioritaskan vulnerability yang berpotensi dieksploitasi oleh penyerang untuk mengakses, mengubah, atau bahkan menghancurkan data berharga.

Proses VA memanfaatkan berbagai teknik, seperti pemindai *vulnerability*, penilaian keamanan manual, dan simulasi serangan siber (*penetration testing*), untuk memastikan deteksi *vulnerability* yang menyeluruh.

3. Hasil dan Pembahasan

3.1. Hasil Pengukuran Penelitian Indeks KAMI pada DISKOMINFO Kota XYZ

DISKOMINFO Kota XYZ memanfaatkan metode Indeks KAMI untuk mengevaluasi tingkat keamanan informasinya. Proses evaluasi ini dilakukan melalui beberapa tahapan, dengan serangkaian pertanyaan yang diajukan di setiap area evaluasi. Area-area yang dievaluasi meliputi, kategori sistem elektronik yang digunakan oleh instansi, manajemen tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja pengelolaan keamanan informasi, pengendalian aset informasi, teknologi dan keamanan informasi. Setelah mengkategorikan peran sistem elektronik dalam organisasi, DISKOMINFO Kota XYZ melanjutkan proses evaluasi dengan menyeluruh di berbagai area terkait. Berdasarkan hasil analisis menggunakan Indeks Keamanan Informasi, diperoleh dua informasi penting:

1. Peran Sistem Elektronik: Kategori sistem elektronik di DISKOMINFO Kota XYZ memiliki peran penting, dengan skor Indeks KAMI 37 yang menunjukkan tingkat Strategis.

2. Tingkat Kematangan Divisi Keamanan Informasi: Data mengenai tingkat kematangan tiap divisi keamanan informasi di DISKOMINFO Kota XYZ juga tersedia.

Tabel 1. Hasil Penilaian Tingkat Keperluan Kategori SE

Divisi I: Divisi ini menyampaikan tingkatan kedudukan serta kebutuhan TIK (Kategori SE) pada organisasi		**Nilai DISKOMINFO Kota XYZ**
Nilai	Tingkat	**37**
10 – 15	[Rendah]	
16 – 34	[Tinggi]	
35 – 50	**[Strategis]**	**Strategis**

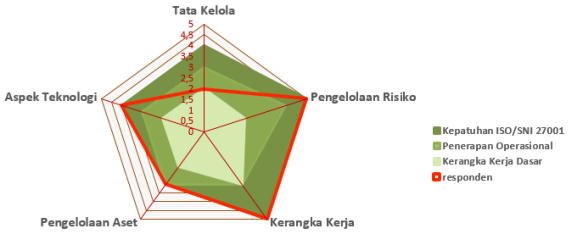
Nilai skor 37 pada Indeks KAMI menunjukkan bahwa sistem elektronik di DISKOMINFO Kota XYZ memegang peran vital dalam mendukung operasional dan pencapaian tujuan organisasi.

Sementara pada divisi II, III, IV, V, serta VI dipakai untuk mengukur tingkat kematangan keamanan informasi pada DISKOMINFO Kota XYZ. Hasil pengukuran dapat dilihat pada tabel 2.

Tabel 2. Hasil Tingkat Kematangan Indeks KAMI

Indeks Keamanan Informasi	**Nilai DISKOMINFO Kota XYZ**	**Tingkat Kematangan**
Divisi II: Manajemen Tata Kelola Keamanan Informasi	84	II
Divisi III: Pengelolaan Risiko Keamanan Informasi	72	V
Divisi IV: Kerangka Kerja Pengelolaan Keamanan Informasi.	159	V
Divisi V: Pengelolaan Aset Informasi	168	III
Divisi VI: Teknologi serta Keamanan Informasi	120	IV
Total Skor (II+III+IV+ V+VI)	**603**	**II s/d V**

Tabel 2 menunjukkan hasil penilaian divisi II, III, IV, V, VI dengan tingkat kematangan keamanan informasi pada DISKOMINFO Kota XYZ ada pada tingkatan (level) II sampai dengan V yaitu Cukup Baik.



Gambar 2. Diagram Radar Indeks KAMI pada DISKOMINFO Kota XYZ

3.2. Hasil *Vulnerability Assesment*

Penilaian keamanan informasi ini mengidentifikasi beberapa kerentanan signifikan pada situs web dan server *website* Sistem Informasi Administrasi dan Layanan Publik Desa/Kelurahan Kota XYZ. Kerentanan ini dikategorikan berdasarkan tingkat keparahannya:

Tabel 3. Kategori Kerentanan yang teridentifikasi

Risk Level	**Number Of Alert**
High	0
Medium	**4**
Low	0
Info	0

Meskipun KAMI secara subjektif menyatakan bahwa manajemen risiko telah diterapkan secara menyeluruh, hasil vulnerability assessment menunjukkan temuan yang bertolak belakang. Hal ini menimbulkan pertanyaan mengenai efektivitas implementasi manajemen risiko di KAMI. Berikut adalah kerentanan yang ditemukan:

1. Perpustakaan JavaScript Rentan (*Medium Priority*)
   Versi 1.3 jQuery memiliki kerentanan yang memungkinkan serangan terhadap situs web/aplikasi yang menggunakannya dan kerentanan terkait dengan cara jQuery mengelola input pengguna.
2. Daftar Direktori Terbuka (*Medium Priority*)
   Server web tidak membatasi akses ke daftar direktori dan file di dalamnya. Pengguna/penyerang dapat menjelajahi struktur direktori dan mengakses *file* yang tidak seharusnya.
3. *Reflected XSS* (*Medium Priority*)
   Pada fitur login dengan CAPTCHA, terdapat risiko:
   a. Injeksi Script
   b. Pengalihan dan Phishing
   c. Injeksi Malware
   d. Manipulasi tampilan web
4. *Directory Traversal* (*Medium Priority*)
   Penyerang dapat mengakses *file*/direktori yang tidak terotorisasi melalui input pengguna yang tidak divalidasi. Dalam kasus ini, penyerang mengakses file /etc/passwd yang berisi informasi pengguna sistem.

Kemudian pada hasil OWASP *Scan* yang didapatkan pada sisi server, ditemukan 14 kerentanan termasuk *critical, high*, dan *medium*. Versi PHP dan DNS server perlu di-*update* untuk mencegah celah keamanan. Berikut adalah rincian kerentanan sisi server:

a. *Reflected XSS* (*Medium Priority*)
   Fitur *Search* pada situs web, meskipun tampaknya sederhana, dapat menjadi celah keamanan yang dimanfaatkan untuk melancarkan serangan Reflected XSS. Serangan ini menyuntikkan skrip berbahaya ke halaman web, memungkinkan penjahat siber untuk mencuri data sensitif, mengambil alih akun, menyebarkan malware, dan bahkan melumpuhkan server web [5].
b. SQLi - MYSQL (*Medium Priority*):
   Skrip SQLi Injection pada fitur *Search*. Skrip menyebabkan error sintaks MySQL, bukan akses database/kebocoran data. Meskipun tidak langsung meretas database, kesalahan SQL Injection pada fitur Search dapat menimbulkan konsekuensi serius. Gangguan fungsionalitas aplikasi, pesan *error* yang membingungkan, dan potensi eksploitasi lebih lanjut oleh penyerang adalah beberapa bahaya yang harus diwaspadai [6]. Serangan ini dapat merusak reputasi organisasi dan berakibat pada kerugian finansial.

3.3. Rekomendasi

Terdapat ketidakcocokan antara hasil *Vulnerability Assessment* (VA) yang menunjukkan tingkat kerentanan medium dan klaim KAMI tentang penerapan Divisi III, IV, dan VI terkait pengelolaan risiko keamanan informasi dengan tingkat kematangan yang cukup memuaskan. Anomali ini menimbulkan keraguan tentang efektivitas manajemen risiko KAMI dan berpotensi mengakibatkan kerugian finansial dan reputasi. Perbedaan ini bisa disebabkan oleh subjektivitas penilaian KAMI yang didasarkan pada kebijakan dan prosedur internal, sedangkan VA menggunakan metode pengujian dan alat ukur yang objektif.

Untuk mengatasi anomali ini, KAMI perlu melakukan audit berkala dengan *tools penetration testing*, meninjau kembali proses manajemen risiko, dan memperkuat komunikasi serta transparansi. Dengan langkah-langkah ini, KAMI dapat memastikan

efektivitas manajemen risiko, meningkatkan postur keamanan informasi, dan meminimalkan risiko kerugian.

Penting untuk melakukan investigasi lebih lanjut dan memantau serta meningkatkan proses manajemen risiko secara berkelanjutan untuk memastikan keamanan informasi yang optimal.

4. Kesimpulan

Studi kasus Dinas Kominfo dan Statistik Kota XYZ menunjukkan bahwa sinergi antara penilaian KAMI dan *Vulnerability Assessment* (VA) sangatlah penting dalam menghadirkan gambaran menyeluruh tentang postur keamanan informasi. Mengatasi kesenjangan antara penilaian subjektif dan objektif merupakan langkah krusial dalam membangun strategi keamanan informasi yang kokoh dan melindungi aset data dan informasi organisas.

Penilaian KAMI memberikan pemahaman menyeluruh tentang kesiapan organisasi dalam menerapkan standar keamanan informasi, mengidentifikasi area yang perlu diperkuat, dan mengukur tingkat kematangan keamanan informasi organisasi. Di sisi lain, *Vulnerability Assessment* mendeteksi celah keamanan yang berpotensi dieksploitasi oleh penyerang, memberikan gambaran objektif tentang kerentanan yang ada pada sistem, jaringan, dan aplikasi. Dengan menerapkan keduanya, organisasi dapat membangun strategi keamanan informasi yang kokoh dan melindungi aset data dan informasi dari berbagai ancaman.

Daftar Pustaka

[1] I. G. P. K. Juliharta, I. K. Suwidiana and I. P. C. Taruna, “Vulnerability Assessment Sistem Manajemen Keamanan Informasi Studi Kasus Sistem Sidarling dan Jagabaya Kota Denpasar”. Jurnal Teknologi Informasi Dan Komputer, vol. 8, no.4, (2022).

[2] M. F. Husin, F. H. Wowor and D. S. Karouw, “Implementasi Indeks KAMI di Universitas Sam Ratulangi”, EJournal Teknik Informatika, vol. 12, no. 1, (2017).

[3] S. F. Rahayu, D. Prawira, and I Rusi, “Pengukuran Tingkat Keamanan Informasi Menggunakan Metode Indeks Kami (Studi Kasus: Dinas Komunikasi Dan Informatika Kota Pontianak)”. Coding : Jurnal Komputer dan Aplikasi, vol. 9, no. 3, (2021).

[4] BSSN, “Indeks KAMI”, (2018).

[5] S. Suroto and A. Asman, “Ancaman Terhadap Keamanan Informasi oleh Serangan *Cross-Site Scripting* (Xss) dan Metode Pencegahannya”, Zona Komputer: Program Studi Sistem Informasi Universitas Batam, vol 11, no.1, (2021).

[6] BSSN, “Mengenal *SQL Injection* dan Cara Mencegahnya”, (2018).