Jurnal Borneo Informatika & Teknik Komputer **p-ISSN:** 2808-8190
Vol. 4, No. 2, 2024. Hlm 13—21 **e-ISSN:** 2808-6600

ANALISIS KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) VERSI 5.0

Fariz Firmansyah[1], Aryo Nugroho[2]

[1,2] Univeristas Narotama, Surabaya, Jawa Timur, 60117, Indonesia

e-mail: *[1]farizfirmansyah09@gmail.com, [2]aryo.nugroho@narotama.ac.id

Diterima	Direvisi	Disetujui
10-08-2024	07-09-2024	01-11-2024

Abstract: *In this research, the KAMI Index version 5.0 will be used to measure and report the level of information security at the Surabaya City General Election Commission (KPU) office. Data is vital in the digital era, but so is the risk of data breaches. Indonesia alone has experienced 347 cyber incidents in 2023, most of which were caused by a lack of data protection. The aim of the KAMI index, which is based on the SNI ISO/IEC 27001 standard, is to information security measures that have the potential to hinder data dissemination. This research was conducted to comprehensively assess the information security situation at the Surabaya City KPU using the latest KAMI index version 5.0 and provides recommendations to improve security. As a result of the evaluation, the electronic system received a score of 21 (high category), information security governance received a score of 93 (maturity level II+), and risk management received a score of 41 (maturity level II). And the information security framework was evaluated with a score of: 87 (maturity level II); Asset Management received a score of 149 (maturity level I+); Technology and Information Security received a score of 135 (maturity level II). Personal data protection received a score of 72 (maturity level II). According to this study, although the Surabaya City KPU has substantial experience in information security, it is still necessary to comply with ISO/ISO compliance and/or IEC standards to achieve greater SNI compliance. This means that further improvements are needed in terms of data protection. against the SNI ISO/IEC 27001:2022 standard.*

Keywords: information security, information security management system, SNI ISO/IEC:27001; WE Index 5.0, excel

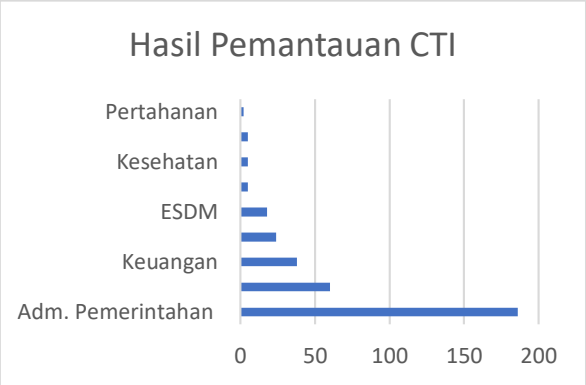
Abstrak: Dalam penelitian ini, Indeks KAMI versi 5.0 digunakan untuk mengukur dan melaporkan tingkat keamanan informasi di kantor Komisi Pemilihan Umum (KPU) Kota Surabaya. Data sangatlah penting diera digital, namun demikian juga dengan risiko pelanggaran data. Indonesia sendiri, telah mengalami 347 insiden siber pada tahun 2023, sebagian besar disebabkan kurangnya perlindungan data. indeks KAMI yang didasarkan standar SNI ISO/IEC 27001 menilai langkah keamanan informasi yang berpotensi menghambat data. Penelitian ini dilakukan untuk menilai secara komprehensif situasi keamanan informasi diKPU Kota Surabaya dengan menggunakan indeks KAMI versi 5.0 memberikan rekomendasi meningkatkan keamanan. Hasil evaluasi, sistem elektronik memperoleh skor 21poin (kategori tinggi), tatakelola keamanan informasi memperoleh skor 93 (tingkat kematangan level II+), dan manajemen risiko memperoleh skor 41 (tingkat kematangan level II). Kerangka keamanan informasi memperoleh skor: 87 (tingkat kematangan level II); Manajemen Aset memperoleh skor 149 (tingkat kematangan level I+); Keamanan Teknologi Informasi memperoleh skor 135 (tingkat kematangan level II). Perlindungan data pribadi memperoleh skor 72 (tingkat kematangan level II). Menurut studi, meskipun KPU Kota Surabaya memiliki pengalaman substansial dalam keamanan informasi, masih perlu untuk mematuhi kepatuhan ISO dan standar IEC untuk mencapai kepatuhan SNI yang lebih besar. Artinya, perlu perbaikan lebih lanjut dalam hal data perlindungan terhadap standar SNI ISO/IEC 27001:2022.

Kata Kunci: keamanan informasi, sistem manajemen keamanan informasi, SNI ISO/IEC:27001; Indeks KAMI 5.0, excel

I. PENDAHULUAN

Kemajuan dalam teknologi informasi dan komunikasi terjadi dengan cepat, dengan banyak sektor, baik pemerintah maupun swasta, merangkul potensi untuk meningkatkan efisiensi, efektivitas, dan produktivitas dalam pekerjaan sehari-hari. (Dewi dkk., 2020). Perusahaan, misalnya, dapat memanfaatkan kemajuan teknologi ini untuk mengelola data dengan lebih efisien, yang pada gilirannya, data tersebut dapat digunakan sebagai dasar yang kuat dan akurat untuk pengambilan keputusan strategis yang lebih tepat(Wicaksana dkk., 2022). Dengan demikian, data ini dianggap sebagai salah satu aset paling berharga yang dimiliki oleh perusahaan, yang keberadaannya harus dijaga, dikelola, dan dilindungi dengan sebaik-baiknya (Ulfah dkk., 2021).

Namun demikian, di tengah kemajuan teknologi yang begitu pesat, ancaman terhadap keamanan data dan informasi juga semakin meningkat. Menurut laporan Lanskap Keamanan Siber Tahun 2023, terdapat 347 dugaan insiden siber yang dilaporkan(TIM Redaksi BSSN, 2023). Insiden-insiden tersebut mencakup berbagai bentuk ancaman, termasuk kebocoran data, serangan ransomware, defacement situs web, indikasi serangan Distributed Denial of Service (DDoS), serta berbagai bentuk pemantauan proaktif terhadap dugaan insiden siber yang dipublikasikan. Insiden-insiden ini tidak hanya menyerang sektor swasta, tetapi juga berbagai sektor yang terdampak, menunjukkan bahwa ancaman keamanan siber adalah masalah yang serius dan harus dihadapi dengan strategi yang tepat(Setiawan & Najicha, 2022).



Gambar 1. Hasil Pemantauan CTI

(Sumber : BSSN ini dilihat di alamat https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf)

Kerentanan dalam sistem teknologi informasi sering kali terjadi karena sistem tersebut tidak dilengkapi dengan langkah-langkah keamanan yang memadai(Handoyo, 2020). Untuk menjaga keamanan informasi, terdapat tiga aspek utama yang harus dievaluasi secara menyeluruh, yaitu kerahasiaan, keutuhan, dan ketersediaan informasi (Nurul dkk., 2022). Evaluasi terhadap ketiga aspek ini sangat penting untuk membantu perusahaan mengidentifikasi dan mengelola risiko keamanan informasi yang mungkin terjadi(Adawiyyah dkk., 2023). Evaluasi ini harus dilakukan dengan mengacu pada standar internasional dan nasional yang telah diakui (Jelita dkk., 2024).

Salah satu alat ukur yang digunakan untuk menilai tingkat keamanan informasi suatu organisasi adalah Indeks Keamanan Informasi (Indeks KAMI), yang didasarkan pada standar internasional SNI ISO/IEC 27001(Maryanto dkk., 2022). Indeks KAMI ini mengkaji berbagai aspek penting seperti kebijakan keamanan informasi, manajemen risiko, perlindungan data, serta tingkat kesadaran keamanan di kalangan pengguna. Dengan menggunakan Indeks KAMI(Ramadhani dkk., 2020), organisasi dapat memperoleh pemahaman yang komprehensif tentang keadaan keamanan data mereka dan dapat melakukan evaluasi serta perbaikan yang

diperlukan untuk meningkatkan keamanan informasi secara keseluruhan(Dewantara & Sugiantoro, 2021).

Salah satu contoh organisasi yang telah mengimplementasikan teknologi informasi dalam aktivitas sehari-hari mereka adalah Komisi Pemilihan Umum (KPU) Kota Surabaya. KPU Kota Surabaya adalah lembaga negara di Indonesia yang bertanggung jawab untuk menyelenggarakan pemilihan umum (pemilu) di tingkat daerah. Namun KPU Kota Surabaya saat ini belum memiliki sertifikasi audit berdasarkan SNI/ISO 27001: 2022, yang termasuk standar nasional sistem manajemen keamanan informasi. (Sundari & Wella, 2021). Penelitian ini memilih untuk menggunakan Indeks KAMI sebagai alat bantu dalam mengevaluasi tingkat kematangan dan keamanan teknologi informasi di KPU Kota Surabaya(Deva & Jayadi, 2022). Diharapkan bahwa melalui penelitian ini, KPU Kota Surabaya dapat memperoleh wawasan yang lebih mendalam mengenai kondisi keamanan informasi mereka, serta dapat meningkatkan kesadaran dan kapasitas mereka dalam mengelola keamanan informasi(Syahindra dkk., 2022). Dengan demikian, penelitian ini tidak hanya bertujuan untuk membantu KPU Kota Surabaya dalam meningkatkan keamanan informasi, tetapi juga berkontribusi pada pengembangan praktik terbaik dalam manajemen keamanan informasi yang dapat diterapkan oleh berbagai organisasi di seluruh Indonesia. Penelitian ini juga menyoroti pentingnya penerapan standar internasional dalam manajemen keamanan informasi untuk menghadapi berbagai ancaman siber yang semakin kompleks danberagam(Jauhary dkk., 2022).

II. METODE PENELITIAN

1. Objek Penelitian

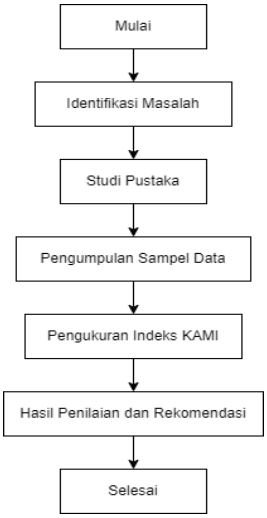
Objek penelitian ini adalah kantor Panitia Pemilihan Umum (KPU) Kota Surabaya, dan tujuan utamanya adalah melakukan penilaian secara komprehensif terhadap tingkat keamanan informasi yang ada dengan menggunakan metode pengukuran yang dikenal dengan Indeks KAMI.

2. Jenis Penelitian

Dalam investigasi jenis ini, peneliti melakukan wawancara mendalam dengan informan kunci, mengamati partisipan di lapangan, dan meninjau dokumen terkait guna mengidentifikasi karakteristik kejadian dan menyelidikinya secara menyeluruh. Data yang diperoleh kemudian diteliti untuk meningkatkan pemahaman kita tentang kejadian tersebut.

3. Alur Penelitian

Alur penelitian seperti yang ditunjukkan pada Gambar 2.



Gambar 2. Alur Penelitian

Mengidentifikasi Masalah

Pada tahap pertama penelitian ini, peneliti mengidentifikasi suatu masalah untuk mengetahui keadaan perusahaan saat ini dan permasalahan yang dihadapi. Pada tahap ini, dilakukan wawancara. Dengan mewawancarai Kasubag dan karyawan perusahaan. Dari wawancara tersebut dilakukan untuk menentukan masalah, tujuan, dan data pendukung untuk menjawab pertanyaan penelitian.

Studi Pustaka

Studi pustaka sangat diperlukan untuk mempelajari dan mengkaji penelitian-penelitian terdahulu yang berkaitan dengan subjek yang relevan dengan topik penelitian ini. Topik lebih lanjut yang dipertimbangkan mencakup berbagai aspek keamanan informasi, dengan fokus pada penerapan dan kepatuhan terhadap standar SNI/ISO/IEC 27001: 2022. Selain itu, penelitian ini juga mengeksplorasi evaluasi Keamanan Informasi menggunakan metode Indeks Keamanan Informasi (KAMI), serta memanfaatkan berbagai referensi dan literatur lainnya yang mendukung analisis dan pembahasan yang mendalam serta komprehensif.

Pengumpulan Sampel Data

Pada tahap ini, data dan informasi dikumpulkan sesuai dengan rumusan dan batasan masalah. Wawancara dengan Kasubag dan karyawan perusahaan digunakan untuk mengumpulkan data ini. Tahap ini diawali dengan analisis untuk membuat daftar pertanyaan terkait Indeks KAMI 5.0. Selain itu, ada dokumen tambahan yang membahas kelengkapan ujian tingkat terkait indeks KAMI 5.0. Peneliti kemudian melakukan wawancara dan mengkaji dokumen untuk memperoleh data dan informasi. Informasi dan data yang dikumpulkan akan disesuaikan dengan indikator dan standar Indeks KAMI 5.0. Hasil pencocokan ini akan menentukan tingkat kesiapan organisasi untuk melindungi informasinya.

Pengukuran Indeks KAMI

Selama fase pengumpulan data, semua informasi dan data yang relevan dikumpulkan untuk penilaian delapan bidang keamanan informasi yaitu sistem elektronik, tat kelola, rincian data pribadi; mengelola aset, manajemen risiko, kerangka keamanan informasi; perlindungan teknologi dan informasi (IPS) informasi suplemen keamanan yang dikumpulkan secara sistematis.Data tersebut akan dievaluasi secara mendalam berdasarkan standar yang ditetapkan oleh Indeks Keamanan Informasi (KAMI) versi 5.0. Tujuan dari penilaian ini adalah untuk memastikan bahwa setiap aspek keamanan informasi dinilai dengan cermat dan akurat sesuai dengan kriteria Indeks KAMI 5.0. Selama tahap ini, data akan dikumpulkan dan kemudian digunakan untuk menanggapi pertanyaan dalam Kerangka Evaluasi Indeks KAMI 5.0, sehingga menghasilkan pemahaman yang komprehensif dan mendetail tentang kondisi keamanan informasi di lingkungan penelitian.

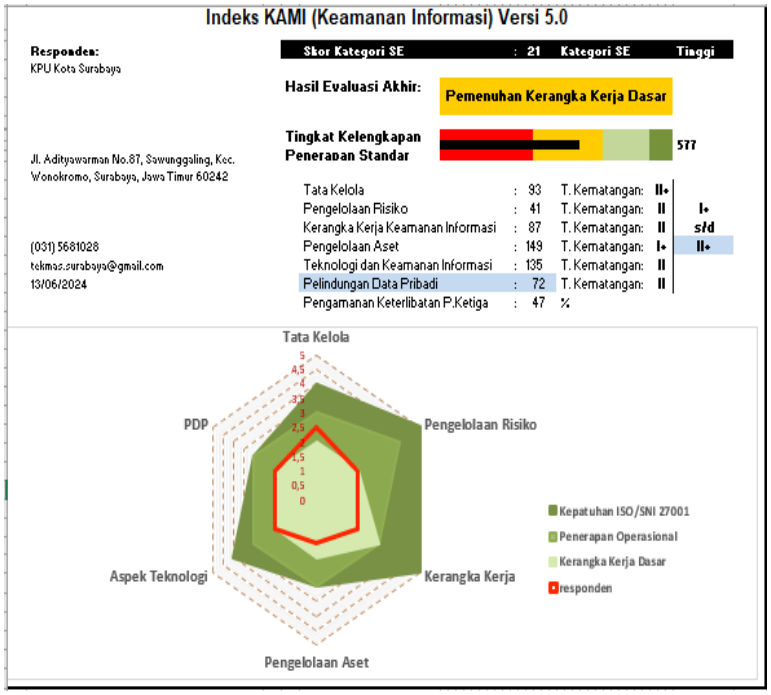
Hasil Penilaian dan Rekomendasi

Selanjutnya, hasil penilaian setiap area yang dilakukan pada tahap sebelumnya akan digabungkan. Hasil penjumlahan ditampilkan dalam dashboard yang menunjukkan skor kategori sistem elektronik, hasil evaluasi akhir, dan tingkat kelengkapan standar. ISO 27001 Selain itu, dashboard menampilkan tingkat kematangan setiap area, serta Radar Chart yang mencakup enam area utama dan informasi perusahaan. Rekomendasi dibuat berdasarkan dashboard yang sudah diperoleh. Rekomendasi ISO/IEC 27001:2022 dimaksudkan untuk digunakan sebagai alat evaluasi untuk meningkatkan keamanan data bisnis.

III. HASIL DAN PEMBAHASAN

Pada bab ini, kita akan menggunakan indeks KAMI untuk memvalidasi hasil evaluasi. Penilaian ini mencakup sistem elektronik, tata kelola, data pribadi, pengelolaan aset, manajemen risiko, kerangka keamanan informasi, teknologi dan keamanan informasi, serta pelengkapnya. Selain itu, rekomendasi dibuat berdasarkan hasil evaluasi. Indeks KAMI digunakan untuk

menentukan data dan informasi yang diambil.Penilaian Penilaian ini membuat dashboard serupa dengan yang ditunjukkan pada Gambar 3.



Gambar 3. Radar Dashboard Indeks KAMI 5.0

1. Penilaian Sistem Elektronik

Terdapat 10 soal khusus untuk kategori penilaian sistem elektronik dengan masing-masing pertanyaan memiliki 3 pilihan untuk setiap soal. Pertanyaan-pertanyaan ini dirancang untuk menyelidiki penggunaan sistem elektronik oleh perusahaan dan mengukur ketergantungan perusahaan terhadap teknologi informasi.Berdasarkan hasil yang ditunjukkan pada Gambar 2, sistem elektronik pada kategori ini mempunyai penilaian sebesar 21 poin yang sudah termasuk kedalam kategori tinggi.

2. Penilaian Tata Kelola

Tujuan dari pelaksanaan penilaian tata kelola keamanan informasi adalah untuk mengevaluasi kesiapan dan efektivitas sistem informasi dalam suatu organisasi. Nilai 93 diberikan untuk tata kelola keamanan informasi perusahaan, yang menunjukkan bahwa tata kelola tersebut telah mencapai kematangan Level II+. Proses dan layanan manajemen bisnis perusahaan yang sukses tercermin dalam level ini, yang juga menunjukkan peningkatan signifikan dalam penerapan kebijakan dan prosedur keamanan informasi yang efektif.

3. Penilaian Pengelolaan Risiko

Tujuan evaluasi manajemen risiko adalah untuk mengevaluasi kemampuan organisasi dalam menangani risiko yang terkait dengan keamanan data. Penilaian tersebut menghasilkan tingkat kematangan Level II sebesar 41 untuk manajemen risiko. Hal ini terlihat pada grafik radar Gambar 2 pada dashboard Indeks KAMI. Hal ini menunjukkan bahwa perusahaan tersebut patuh terhadap standar SNI/ISO 27001:2022. Skor ini menunjukkan bahwa kebijakan dan prosedur yang diterapkan oleh organisasi untuk mengidentifikasi, menilai & mengendalikan risiko keamanan informasi berjalan dengan baik.

4. Penilaian Kerangka Kerja Keamanan Informasi

Penilaian dilakukan untuk kerangka kerja keamanan informasi, yang bertujuan untuk menilai kesiapan dan efektivitas mekanisme perlindungan organisasi. Evaluasi menunjukkan bahwa kerangka

keamanan informasi perusahaan mencapai kematangan Level II dengan skor 87. Peringkat tersebut terlihat pada grafik radar pada dashboard Indeks KAMI pada Gambar 2 yang menunjukkan kepatuhan perusahaan terhadap standar SNI/ISO/IEC 27001: 2022. Peringkat ini mencerminkan bahwa perusahaan telah mengembangkan dan menerapkan kerangka keamanan informasi yang cukup canggih yang mencakup kebijakan, prosedur, dan pengendalian yang dirancang untuk melindungi aset informasi dari berbagai ancaman dan risiko keamanan yang dilakukan.

5 Penilaian Pengelolaan Aset

Penilaian manajemen aset dilakukan untuk menentukan efektivitas dan tingkat organisasi untuk kerangka kerja keamanan data perusahaan. Berdasarkan penilaian memiliki peringkat manajemen aset sebesar 149 dan tingkat jatuh tempo I+. Penilaian tersebut terlihat pada grafik radar pada dashboard Indeks KAMI pada Gambar 2 yang menunjukkan tingkat kepatuhan suatu perusahaan terhadap standar SNI/ISO/IEC 27001: 2022. Peringkat ini mencerminkan bahwa perusahaan memiliki kerangka manajemen aset yang terus berkembang, termasuk informasi identifikasi aset, inventaris, dan perlindungan yang memadai, namun masih kurang dalam prosedur dan penerapan kontrol keamanan yang lebih komprehensif.

6. Penilaian Teknologi dan Keamanan Informasi

Evaluasi keamanan informasi dan teknologi digunakan untuk mendeteksi potensi ancaman terhadap perlindungan data yang disebabkan oleh penggunaan teknologi dalam suatu organisasi. Berdasarkan hasil penilaian tersebut, Manajemen Teknologi dan Keamanan Informasi memperoleh skor sebesar 135 yang menunjukkan tingkat kematangan level II. Visualisasi hasil tersebut dapat dilihat pada grafik dashboard radar dashboard Indeks KAMI pada Gambar 2. Hal ini menunjukkan tingkat kepatuhan perusahaan terhadap standar SNI/ISO/IEC 27001: 2022. Peringkat ini mencerminkan bahwa perusahaan telah menerapkan berbagai teknologi dan pengendalian keamanan informasi yang tepat, dan memiliki mekanisme untuk mengidentifikasi, menilai, dan mengatasi ancaman keamanan yang timbul dari penggunaan teknologi tersebut. Meskipun perusahaan telah mencapai level yang cukup matang, namun masih terdapat ruang untuk perbaikan dalam hal optimalisasi dan integrasi teknologi keamanan informasi.

7. Penilaian Perlindungan Data Pribadi

Penilaian perlindungan data pribadi bertujuan untuk mengidentifikasi area di mana kontrol keamanan perlu ditingkatkan untuk menjamin keamanan data pribadi.. Berdasarkan hasil penilaian tersebut, aspek pengelolaan aset memperoleh skor 72 yang menunjukkan kematangan Level II. Rating tersebut ditampilkan dalam bentuk grafik radar pada dashboard Indeks KAMI seperti terlihat pada Gambar 2. Tingkat kematangan ini menunjukkan bahwa standar SNI/ISO/IEC 27001: 2022 saat ini telah terpenuhi, namun masih ada perbaikan lebih lanjut dan perlu dicapai tingkat yang lebih tinggi.

8. Penilaian Suplemen

Tujuan dari evaluasi suplemen ini adalah untuk mengukur tingkat, kecukupan, dan efisiensi yang dicapai oleh langkah-langkah keamanan yang digunakan dalam memprediksi berbagai risiko yang terkait dengan operasi bisnis dan layanan manajemen yang melibatkan pelaku eksternal.. Hasil evaluasi ini menunjukkan skor yang dicapai sebesar 47%. Peringkat ini mencerminkan kekurangan yang signifikan dalam penerapan mekanisme keamanan dan manajemen risiko yang tepat ketika berinteraksi dengan pihak ketiga eksternal untuk memastikan perlindungan data dan operasi bisnis yang lebih aman dan andal. Peringkat ini menyoroti perlunya perbaikan dan kontrol keamanan yang lebih ketat.

.

Tabel 1. Penilaian Suplemen

Jawaban	**Jumlah**
Tidak Dlakukan	7
Dalam Penerapan / Diterapkan sebagian	4
Diterapkan Secara Menyeluruh	12
Diterapkan Secara Menyeluruh	3
Total Skor	**47%**

9. Rekomendaasi Perbaikan

Setelah evaluasi selesai, saran perbaikan diberikan untuk persyaratan yang belum terpenuhi. Rekomendasi ini didasarkan pada Manajemen ISO/IEC 27001: 2022. Diharapkan dapat membantu KPU Kota Surabaya untuk dapat meningkatkan manajemen keamanan informasi dan diharapkan juga bahwa saran akan meningkatkan status penerapan untuk syarat yang belum terpenuhi. Kontrol keamanan informasi tersebut dapat berupa kontrol teknis, administratif, atau organisasional. Oleh karena itu, rekomendasi yang disarankan sebagai berikut.

NO	Kondisi yang Perlu Diperbaiki	Rekomendasi Perbaikan Berdasarkan dengan Standar ISO/IEC 27001:2022
1	Perusahaan belum memberikan pernyataan resmi apa pun terkait pembagian tugas.	A 5.2 *Information Security Roles and Duties Responsibilities* Perusahaan harus menetapkan peran dan tanggung jawab yang jelas untuk memastikan bahwa semua individu menyadari tugas mereka, jika tidak dilakukan.
2	Kebijakan transfer data perusahaan tidak ada.	A 5.14 *Information Transfer* Kebijakan transfer data harus ditetapkan oleh perusahaan untuk menjamin transmisi yang aman, yang mencakup kontrol dan pelacakan data serta informasi kontak.
3	Tidak ada kebijakan yang ditetapkan untuk melindungi data cloud komersial yang dikelola oleh perusahaan.	A 5.23 *Users of cloud-based information services are protected by security measures.* Perusahaan harus memiliki prosedur untuk menggunakan layanan cloud.Langkah-langkah ini setidaknya harus mencakup penerapan prosedur untuk memperoleh, menggunakan, mengelola, menonaktifkan layanan cloud, menilai risiko keamanan informasi, dan memantau serta mengendalikan layanan cloud.Rephrase
4	Insiden keamanan informasi tidak ditangani oleh prosedur perusahaan mana pun.	A 5.24 *Preparation and planning for information security incident management.*

		Untuk meminimalkan kerugian operasional, perusahaan harus menerapkan langkah-langkah manajemen insiden keamanan informasi. Menyertakan peran dan tanggung jawab, kebijakan manajemen insiden, dan kebijakan pelaporan dalam prosedur ini sangatlah penting.
5	Dokumentasi operasional resmi tidak tersedia dari perusahaan itu sendiri	A 5.37 *Documented Operating Procedures* Perusahaan keamanan informasi harus mendokumentasikan operasi dan proses mereka. Melakukan proses operasional seperti pencadangan data, penghapusan media (penutupan media yang hilang), dan pembaruan perangkat lunak memerlukan dokumentasi.
6	Tidak ada sistem pelaporan insiden keamanan informasi di dalam perusahaan	A 6.8 *Information Security Event Reporting* Perusahaan keamanan informasi harus mendokumentasikan operasi dan proses mereka. Melakukan proses operasional seperti pencadangan data, penghapusan media (penutupan media yang hilang), dan pembaruan perangkat lunak memerlukan dokumentasi.

IV. KESIMPULAN

Berdasarkan hasil evaluasi dengan menggunakan indeks KAMI 5.0, tingkat respon keselamatan adalah 577, yang merupakan tingkat yang "memenuhi kerangka dasar". Hal ini dikarenakan salah satu bidang yaitu "Pengelolaan Manajemen Aset" perlu ditingkatkan guna meningkatkan level bidang penilaian dan menjadikan bidang perbaikan tersebut sesuai dengan standar SNI/ISO/IEC 27001: 2022. Meskipun demikian, dalam area penilaian yang lain seperti tata kelola, manajemen risiko, kerangka kerja keamanan informasi, dan teknologi serta perlindungan informasi data pribadi, tingkat kerangka kerja dasar masih di level kerangka kerja dasar.

V. UCAPAN TERIMAKASIH

Berbagai pihak berkontribusi pada keberhasilan penelitian ini. Saya berterima kasih kepada sekretariat dan karyawan KPU Kota Surabaya karena telah memberikan izin saya untuk melakukan penelitian ini selama proses penilaian evaluasi keamanan informasi dengan menggunakan Indeks KAMI 5.0 ini. Saya juga berterima kasih kepada Universitas Narotama karena telah memberikan izin kepada penulis untuk melakukan penelitian ini. Saya juga ingin mengucapkan terima kasih kepada Bapak Dr. Aryo Nugroho S.T., S.kom., M.T., dosen pembimbing saya, termasuk teman-teman saya yang membantu saya dalam menyelesaikan penelitian ini.

REFRENSI

Adawiyyah, R., Fauzi, A., Indriyanah, A., Safitri, A., Nabila, E. P., Maidani, M., & A, S. N. I. (2023). Pengaruh Keamanan Informasi dan Perkembangan Teknologi di Era Revolusi 4.0 Terhadap Kinerja Perusahaan (Literature Review Manajemen Kinerja). *Jurnal Ilmu Multidisplin*, *2*(1), 50–57. https://doi.org/10.38035/jim.v2i1.238

Deva, B. S., & Jayadi, R. (2022). Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro. *Jurnal Teknologi Dan Informasi*, *12*(2), 106–117. https://doi.org/10.34010/jati.v12i2.6829

.

Dewantara, R., & Sugiantoro, B. (2021). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta). *Jurnal Teknologi Informasi dan Ilmu Komputer*, *8*(6), Article 6. https://doi.org/10.25126/jtiik.2021863123

Dewi, S., Listyowati, D., & Napitupulu, B. E. (2020). SEKTOR INFORMAL DAN KEMAJUAN TEKNOLOGI INFORMASI DI INDONESIA. *JURNAL MITRA MANAJEMEN*, *11*(1), Article 1. https://doi.org/10.35968/jmm.v11i1.391

Handoyo, E. (2020). Analisis Tingkat Keamanan Informasi: Studi Komparasi Framework Cobit 5 Subdomain Manage Security Services (DSS05) dan NIST Sp 800 – 55. *Jurnal CoSciTech (Computer Science and Information Technology)*, *1*(2), Article 2. https://doi.org/10.37859/coscitech.v1i2.2199

Jauhary, H., Pratiwi2, G. E., Salim, A. Z., & Fitroh, F. (2022). Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi: Literatur Review. *Media Jurnal Informatika*, *14*(1), Article 1. https://doi.org/10.35194/mji.v14i1.1581

Jelita, L. D. A., Azam, M. N. A., & Nugroho, A. (2024). Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022. *Jurnal Saintekom : Sains, Teknologi, Komputer Dan Manajemen*, *14*(1), Article 1. https://doi.org/10.33020/saintekom.v14i1.623

Maryanto, A. L., Azam, M. N. A., & Nugroho, A. (2022). EVALUASI MANAJEMEN KEAMANAN INFORMASI PADA PERUSAHAAN PEMULA BERBASIS TEKNOLOGI MENGGUNAKAN INDEKS KAMI. *Jurnal Simantec*, *11*(1), Article 1. https://doi.org/10.21107/simantec.v11i1.14099

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). FAKTOR-FAKTOR YANG MEMPENGARUHI KEAMANAN SISTEM INFORMASI: KEAMANAN INFORMASI, TEKNOLOGI INFORMASI DAN NETWORK (LITERATURE REVIEW SIM). *Jurnal Ekonomi Manajemen Sistem Informasi*, *3*(5), 564–573. https://doi.org/10.31933/jemsi.v3i5.992

Ramadhani, N. D., Putra, W. H. N., & Herlambang, A. D. (2020). Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Malang menggunakan Indeks KAMI (Keamanan Informasi). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, *4*(5), Article 5.

Setiawan, H. B., & Najicha, F. U. (2022). *PERLINDUNGAN DATA PRIBADI WARGA NEGARA INDONESIA TERKAIT DENGAN KEBOCORAN DATA*. *6*(1).

Sundari, P., & Wella, W. (2021). SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR). *Ultima InfoSys : Jurnal Ilmu Sistem Informasi*, *12*(1), 35–42. https://doi.org/10.31937/si.v12i1.1701

Syahindra, I. P. S., Primasari, C. H., & Iriantor, A. B. P. (2022). EVALUASI RISIKO KEAMANAN INFORMASI DISKOMINFO PROVINSI XYZ MENGGUNAKAN INDEKS KAMI DAN ISO 27005: 2011. *Jurnal Teknoinfo*, *16*(2), Article 2. https://doi.org/10.33365/jti.v16i2.1246

TIM Redaksi BSSN. (2023). *LANSKAP KEAMANAN SIBER INDONESIA 2023*.

Ulfah, A. N., Lizarti, N., Anam, M. K., Sudyana, D., & Asnal, H. (2021). Pelatihan Secure Computer User Untuk Meningkatkan Kesadaran Siswa Terhadap Keamanan Data dan Informasi. *J-PEMAS - Jurnal Pengabdian Masyarakat*, *2*(1), Article 1.

Wicaksana, S. H., Saedudin, R. R., & Fathinuddin, M. (2022). Perancangan Infrastruktur Teknologi Informasi Adaptif Dengan Metode Ppdioo Untuk Mendukung Implementasi Sistem Informasi Manajemen Puskesmas Studi Kasus: Puskesmas Jatilawang. *eProceedings of Engineering*, *9*(2), Article 2. https://openlibrarypublications.telkomuniversity.ac.id/index.php/engineering/article/view/17641