Jurnal Ilmu Komputer Agri-Informatika

Tersedia secara daring di:
https://jurnal.ipb.ac.id/index.php/jika

Volume 12 Nomor 1 halaman 38–49
eISSN: 2654-9735, pISSN: 2089-6026

Analisis Keamanan Informasi pada Sistem Komputerisasi Terpadu Menggunakan Metode Indeks KAMI dan Octave Allegro

Information Security Analysis on the Integrated Computerized System using KAMI Index and OCTAVE Allegro Method

NUZUL RAKHMAT ROMADHONI[1], MUHAMMAD SAID HASIBUAN[1]*, KURNIA MULUDI[1]

Abstrak

Transformasi digital meningkatkan pelayanan publik melalui teknologi, seperti Sistem Komputerisasi Terpadu di Kementerian XYZ, yang memproses data secara terpadu. Namun, ancaman keamanan data menjadi perhatian utama. Upaya mitigasi melibatkan Indeks KAMI untuk evaluasi keamanan berbasis ISO 27001 dan metode OCTAVE Allegro untuk identifikasi risiko aset informasi, sehingga mendukung pengelolaan data yang aman dan andal. Penelitian ini dimulai dengan identifikasi masalah keamanan informasi, dilanjutkan tinjauan pustaka terkait teori, standar, dan metode seperti Indeks KAMI dan Octave Allegro. Data dikumpulkan melalui observasi, wawancara, dan kuesioner, lalu dianalisis menggunakan kedua metode tersebut. Berdasarkan penilaian Indeks KAMI menunjukkan skor 570 dengan predikat "Cukup Baik". Sedangkan dalam penilaian Octave Allegro menghasilkan 4 dari 5 area risiko memiliki kategori *mitigate or transfer* dan 1 area lainya berkategori *defer*. Risiko seperti pencurian perangkat dapat ditangani kantor kabupaten, sementara risiko besar seperti peretasan atau kegagalan *backup* ditransfer ke kantor pusat untuk mitigasi lebih lanjut. Analisis keamanan informasi dengan Indeks KAMI dan Octave Allegro menunjukkan bahwa kantor kabupaten memiliki pencapaian baik dalam kepatuhan ISO 27001, namun pengelolaan risiko masih bergantung pada kantor pusat. Octave Allegro lebih efektif dalam mengidentifikasi dan menangani risiko, sehingga cocok digunakan untuk instansi dengan kewenangan yang terbatas.

Kata Kunci**:** Indeks KAMI, ISO 27001, Keamanan Informasi, Octave Allegro, Pengelolaan Risiko, Tranformasi Digital

Abstract

Digital transformation improves public services through technology, such as the Integrated Computerized System at the XYZ Ministry, which ensures comprehensive data processing. However, data security threats remain a critical concern. Mitigation efforts include using the KAMI Index for security evaluation based on ISO 27001 and the OCTAVE Allegro method for identifying information asset risks, supporting secure and reliable data management. This study identifies information security issues, reviews relevant theories and methods, and collects data through observations, interviews, and questionnaires. The KAMI Index assessment scored 570 with a "Fairly Good" rating. OCTAVE Allegro identified 7 out of 8 risk areas as "mitigate or transfer", while 1 area was categorized as "defer". Risks like device theft can be managed at the district level, whereas major risks such as hacking or backup failures are transferred to the central office for further handling. The analysis shows that the district office performs well in ISO 27001 compliance but remains dependent on the central office for risk management. OCTAVE Allegro proves more effective in identifying and addressing risks, making it ideal for organizations with limited authority.

Keywords: Digital Transformation, Information Security, ISO 27001, KAMI Index, Octave Allegro, Risk Management

PENDAHULUAN

Transformasi digital merupakan salah satu langkah yang dilakukan oleh pemerintah dalam meningkatkan pelayanan publik kepada masyarakat. Upaya tersebut telah membawa

[1] Institut Informatika dan Bisnis Darmajaya Bandar Lampung
* Penulis Korespondensi : Telp/Faks : +62818461051; Surel : msaid@darmajaya.ac.id

perubahan signifikan dalam pengelolaan data dan layanan di berbagai sektor. Salah satu contoh pelaksanaan implementasi teknologi informasi pada sektor publik adalah penerapan Sistem Komputerisasi Terpadu yang digunakan oleh Kementerian XYZ. Sistem dirancang untuk memberikan kemudahan kepada pengelola dalam memproses administrasi layanan secara terpadu, mulai dari pendaftaran, pendataan, hingga pengelolaan visa dan akomodasi. Seiring dengan meningkatnya pengelolaan data dan informasi melalui teknologi tersebut, maka ancaman terhadap keamanan data menjadi masalah untuk segera dicegah dan ditangani secepatnya (Savitri *et al*., 2024).

Berdasarkan informasi dari Lanskap Keamanan Siber Indonesia pada tahun 2022 bahwa telah terjadi sejumlah 311 insiden kebocoran data. Hal tersebut adalah suatu yang rentan terjadi pada era tranformasi digital (Jelita *et al*., 2024). Keamanan informasi memiliki tiga faktor utama, terdiri dari kerahasiaan, integritas, dan ketersediaan data. Faktor tersebut menjadi sangat penting dalam Sistem Komputerisasi Terpadu yang telah diterapkan di seluruh kantor provinsi, kabupaten, dan kota untuk mengolah, menyimpan, dan mengelola data pribadi masyarakat.

Pemerintah melalui Kementerian Komunikasi dan Informatika telah berupaya untuk meningkatkan keamanan informasi dengan membuat alat ukur sebagai kerangka kerja pengamanan informasi, yaitu Index Keamanan Informasi atau biasa disebut indeks KAMI. (Anas *et al*., 2021) Metode tersebut digunakan oleh seluruh instansi pemerintah untuk melakukan evaluasi kesiapan keamanan informasi yang mengacu pada standar ISO/IEC 27001 (Yusuf I dan Said H, 2024; Wasilah *et al*., 2024) maupun juga dilakukan pada lembaga swasta dari berbagai bidang yang menggunakan teknologi informasi, seperti dunia kesehatan, keuangan, perbankan, dan pendidikan (Gerardo dan Fajar, 2022).

Pendekatan lain yang juga dapat diterapkan dalam melakukan evaluasi keamanan informasi adalah Metode OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability* Evaluation) Allegro. Metode yang digunakan untuk mengidentifikasi risiko terhadap aset informasi yang dimiliki oleh organisasi atau instansi dengan menilai ancaman yang memiliki potensi berpengaruh terhadap keamanan informasi. Metode Octave Allegro memiliki depan tahapan yang dimulai dari identifikasi aset hingga analisis risiko dana pemilihan langkah mitigasi (Riadi dan Sukri, 2021).

Berikut penelitian yang pernah dilakukan untuk melakukan evaluasi keamanan informasi, antara lain penelitian yang dilakukan oleh Razikin dan Soewito pada sebuah perusahaan ritel publik menggunakan pengembangan model sistem pendukung keputusan keamanan siber menggunakan metode Octave Allegro dan ISO/IEC 27001. Hasil yang diperoleh secara signifikan model berhasil meningkatkan efektivitas mitigasi ancaman keamanan informasi dengan nilai kepatuhan terhadap ISO/IEC 27001 dari rata-rata skor 36,27 menjadi 82,37 dan mengurangi tingkat kekritisan ancaman dari 8,75 menjadi 4,00 (Razikin dan Soewito, 2022).

Penelitian dari Rizki Dewantara dan Bambang Sugiantoro adalah mengenai evaluasi manajemen keamanan informasi menggunakan indeks KAMI pada jaringan UIN Sunan Kalijaga Jogjakarta. Evaluasi dengan menggunakan metode tersebut menghasilkan peningkatan pada aspek tata kelola, pengelolaan aset dan teknologi. Namun, tingkat kelayakan keamanan informasi masih berada pada level I+ sampai dengan II+, sehingga tingkat keamanan informasi pada jaringan masih belum layak dan menuntut perbaikan. (Dewantara dan Sugiantoro, 2021)

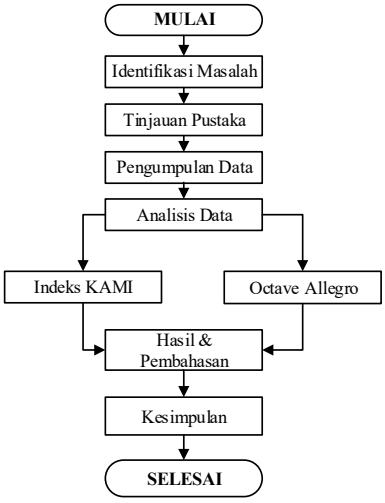
Penelitian selanjutnya yaitu oleh Biswas *et al.*, juga memperlihatkan keberhasilan penerapan sistem pendukung keputusan berbasis analisis risiko di perusahaan ritel publik. Dengan metode Octave Allegro dan ISO/IEC 27001, peningkatan kemampuan organisasi dalam mengelola keamanan informasi, penurunan tingkat ancaman dan peningkatan kepatuhan terhadap standar keamanan tercapai.(Biswas *et al*., 2024)

Sistem Komputerisasi Terpadu pada Kementerian XYZ memiliki risiko keamanan, maka langkah yang perlu dilakukan antara lain upaya memberikan perlindungan data dan informasi terhadap ancaman siber. Bentuk evaluasinya adalah dengan melakukan evaluasi keamanan informasi melalui tahapan identifikasi risiko yang akan terjadi hingga tahapan penanganannya.

Metode evaluasi yang akan digunakan dalam penelitian ini adalah indeks KAMI dan Octave Allegro. Oleh sebab itu penelitian ini selanjutnya bertujuan untuk menganalisis tingkat keamanan Sistem Komputerisasi Terpadu untuk memberikan gambaran kesiapan keamanan informasi dan upaya perbaikan sistem selanjutnya.

METODE

Berikut adalah tahapan penelitian yang dilakukan guna memudahkan penelitian sehingga dapat berjalan dengan baik dan sistematis. Tahapan tersebut disajikan pada Gambar 1.



Gambar 1 Tahapan Penelitian

Identifikasi Masalah

Tahapan awal penelitian hal yang dilakukan adalah mengidentifikasi masalah keamanan sistem informasi yang kemungkinan berpotensi terjadi. Permasalahan tersebut seperti adanya ancaman keamanan, kerentanan sistem, atau ketidaksesuaian dengan standar keamanan informasi yang berlaku.

Tinjauan Pustaka

Tinjauan pustaka dilakukan terhadap teori dan standar keamanan informasi seperti kerangka kerja analisis seperti Indeks KAMI dan Octave Allegro (Irsheid *et al*., 2022) serta menelusuri penelitian terdahulu yang relevan (Aziz *et al*., 2024).

Pengumpulan Data

Penelitian ini mengumpulkan data melalui observasi, wawancara, dan kuesioner. Observasi dilakukan untuk memahami penggunaan Sistem Komputerisasi Terpadu di kantor kabupaten Kementerian XYZ. Wawancara melibatkan tiga pegawai, yaitu kepala unit pelaksana, operator, dan pranata komputer, guna menggali informasi terkait kebijakan, prosedur keamanan, serta persepsi terhadap risiko dan kendala sistem. Subjek dalam penelitian adalah pegawai yang secara langsung terlibat dalam pengelolaan dan penggunaan Sistem Komputerisasi Terpadu pada Kantor Kementerian XYZ tingkat kabupaten di Provinsi Lampung.

Sedangkan untuk kuesioner disusun berdasarkan indikator-indikator yang tercantum dalam *template* resmi indeks KAMI versi 4.2 berupa *file* Microsoft Excel dapat diunduh pada website resmi Badan Siber dan Sandi Negara (BSSN). Sedangkan *template* kuesioner di tahapan dalam metode Octave Allegro bersumber dari (Caralli *et al*., 2007). Adapun rincian jumlah pertanyaan dan responden dapat dilihat pada Tabel 1. Setiap jawaban kuesioner diberikan skor yang nantinya dikonsolidasi untuk menghasilkan angka. Adapun skor yang dimaksud sebagaimana Tabel 2.

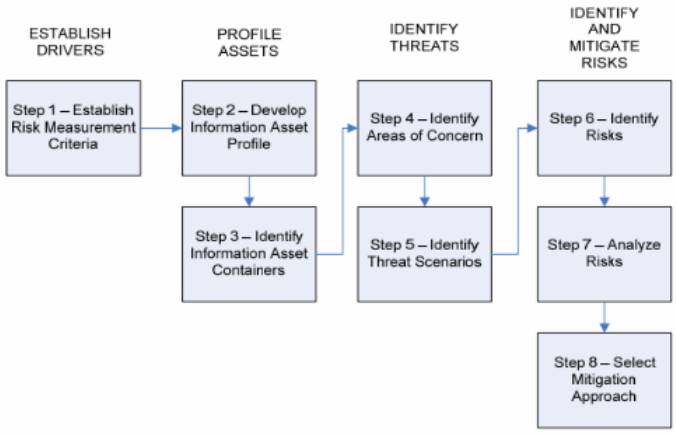
Sedangkan untuk penerapan metode Octave Allegro menggunakan tahapan sesuai dengan Gambar 2 yaitu melalui wawancara yang difokuskan pada delapan area utama seperti identifikasi aset informasi, skenario ancaman, kondisi sistem kritis, dan pendekatan mitigasi risiko.

Tabel 1 Jumlah Pertanyaan dalam Kuesioner Indeks KAMI 4.2

Kuesioner	Jumlah	Responden
Kategori Sistem Elektronik	10	Kepala Unit Pelaksana
Tata Kelola	22	Kepala Unit Pelaksana
Pengelolaan Risiko	16	Pranata Komputer
Kerangka Kerja Keamanan Informasi	29	Pranata Komputer
Pengelolaan Aset	38	Operator
Teknologi dan Keamanan Informasi	26	Operator
Suplemen	53	Kepala Unit Pelaksana
TOTAL	**194**	

Tabel 2 Skor Jawaban Kuesioner

Jawaban Kuesioner	Kategori Pengamanan		
Status 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



Gambar 2 Tahapan Metode Octave Allegro (Gerardo dan Fajar, 2022)

Berdasarkan Gambar 2 pada *template* kuesioner telah disediakan petunjuk dan pertanyaan yang berfungsi untuk melakukan pengumpulan data dan pertanyaan yang disusun disesuaikan dengan sistem yang akan di analisis. Validasi isi dilakukan dengan mengacu pada *template* resmi dari website BSSN serta literatur akademik terkait indeks KAMI dan Octave Allegro.

Analisis Data

Berdasarkan pengumpulan data yang telah dilakukan sebelumnya kemudian dianalisis menggunakan metode yang telah ditetapkan yaitu Indeks KAMI digunakan untuk mengevaluasi tingkat kesiapan keamanan informasi dan Octave Allegro digunakan untuk mengidentifikasi, menilai dan mengelola risiko keamanan informasi (Gutandjala *et al*., 2019).

Metode Indeks KAMI dan Octave Allegro

Analisis keamanan informasi menggunakan indeks KAMI menghasilkan skor yang menunjukkan seberapa siap Kantor Kementerian XYZ dalam menghadapi ancaman keamanan informasi (Hartomo, 2023), dan Octave Allegro untuk menampilkan prioritas risiko berdasarkan dampak ancaman terhadap aset informasi organisasi (Irsheid *et al*., 2022; Hom *et al*., 2020; Abdullah *et al*., 2020).

Hasil dan Pembahasan

Hasil analisis menggunakan kedua pendekatan di atas dilakukan perbandingan kemudian dibahas untuk mengidentifikasi kelemahan keamanan dan memberikan rekomendasi perbaikan serta melihat area yang memerlukan perhatian lebih untuk meningkatkan keamanan sistem.

Kesimpulan

Tahap akhir dalam penelitian yaitu pengambilan kesimpulan untuk merangkum temuan terkait peningkatan keamanan Sistem Komputerisasi Terpadu di Kantor Kementerian XYZ.

HASIL DAN PEMBAHASAN

Pada bagian ini disajikan hasil analisis keamanan informasi menggunakan indeks KAMI dan Octave Allegro. Penilaian dilakukan secara kuantitatif dan visual dengan menyajikan hasil dalam bentuk tabel dan gambar. Pembahasan menggunakan indeks KAMI, terdiri dari 7 langkah penilaian antara lain, kategori sistem elektronik, tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan aset, aspek teknologi, dan suplemen.

Sedangkan pada Octave Allegro memiliki 8 langkah, yang meliputi menetapkan kriteria pengukuran risiko, mengembangkan profil aset informasi, mengidentifikasi wadah aset informasi, mengidentifikasi kondisi dan situasi sistem kritis, mengidentifikasi skenario ancaman, mengidentifikasi risiko, menganalisis risiko, dan menentukan pendekatan mitigasi risiko.

Indeks KAMI

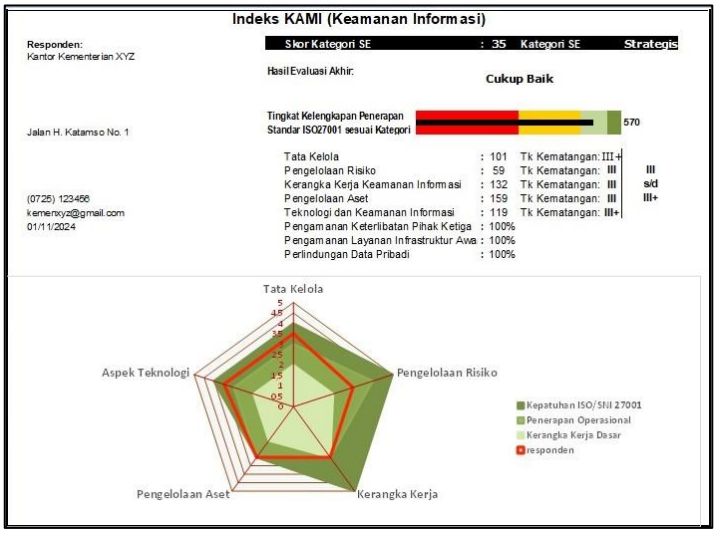
Berdasarkan hasil data dan informasi yang diperoleh dari responden kemudian diolah menggunakan *template* penilaian indeks KAMI versi 4.2 dengan hasil penilaian seperti disajikan dalam Tabel 3 dan tampilan *dashboard* sebagaimana ditunjukkan pada Gambar 3.

Tabel 3 Tabel Penilaian menggunakan indeks KAMI

Area	Skor	Tingkat Kematangan/Predikat
Kategori Sistem Elektronik	35	Strategis
Tata Kelola	101	III+
Pengelolaan Risiko	59	III
Kerangka Kerja	132	III
Pengelolaan Aset	159	III
Teknologi	119	III+
Suplemen	100%	Layak
Total Skor	570	Cukup Baik

Hasil dari tingkat kematangan/predikat diperoleh dari seluruh kuesioner yang telah terisi dengan skor setiap area, predikat kategori sistem elektronik, dan predikat total skor akan tampil secara otomatis. Selain skor, hasil lainnya adalah gambaran visual kekuatan dan kelemahan pada tiap area keamanan informasi seperti disajikan dalam Gambar 3. Adapun tingkat kematangan pada setiap kategori berbeda-beda sebagaimana ketentuan *template* dari BSSN.

Dashboard indeks KAMI menunjukkan skor kesiapan keamanan informasi di Kantor Kementerian XYZ dalam bentuk bagan radar. Sistem elektronik dinilai strategis dengan skor 35, menandakan perannya yang krusial dalam operasional layanan. Evaluasi menunjukkan tata kelola (101) dan kerangka kerja (132) pada tingkat kematangan III+, mencerminkan kepatuhan terhadap ISO 27001, meski masih bergantung pada kebijakan kantor pusat. Pengelolaan risiko (59), aset (159), dan teknologi (119) juga berada pada level III, dengan peran penting kantor pusat dan kesiapan kantor kabupaten dalam sarana dan SDM. Aspek suplemen seperti keamanan pihak ketiga dan perlindungan data pribadi mendapat skor 100%, sepenuhnya ditangani kantor pusat.



Gambar 3 *Dashboard* Penilaian Indeks KAMI
(Sumber : *Template* Kuesioner versi 4.2 oleh BSSN)

Hasil penilaian Indeks KAMI menunjukkan skor 570 dengan predikat "Cukup Baik" dan kepatuhan tinggi terhadap ISO 27001. Namun, aspek pengelolaan risiko masih lemah dan membutuhkan perbaikan, khususnya yang dapat ditangani oleh kantor kabupaten. Kelemahan ini mencerminkan ketergantungan pada kantor pusat, meskipun kantor kabupaten dapat berkontribusi melalui sarana, SDM, dan pemeliharaan teknologi.

Octave Allegro

Sebagaimana pengumpulan data dan informasi yang telah dilakukan pada penilaian menggunakan Indeks KAMI. Hal tersebut juga bersumber dari responden yang sama, namun pada penilaian ini dilakukan menggunakan Octave Allegro (Caralli *et al*., 2007). Berikut adalah langkah-langkah penilaiannya.

Menetapkan Kriteria Pengukuran Risiko

Langkah awal yang perlu dilakukan adalah mengidentifikasi risiko dan menetapkan pengukuran risiko pada area yang paling tinggi berdampak hingga yang paling rendah. Berikut daftar identifikasi risiko, *impact area*, dan skala prioritas *impact area* disajikan pada Tabel 4, Tabel 5, dan Tabel 6.

Tabel 4 Daftar Identifikasi Risiko

Kategori Risiko	Risiko	Penyebab	Dampak
Faktor alam	Cuaca : hujan, petir, badai	Bencana alam	Koneksi jaringan terganggu
Manusia	*Human error*	Kelalaian, kecapekan, kurang konsentrasi	Kesalahan entri data, kerugian bagi instansi dan masyarakat
Sistem	*Server down*	*High traffic, maintanance*	Sistem tidak dapat diakses
	Gagal *update*	*Server down*	Data tidak tersimpan
	Koneksi jaringan buruk	Cuaca	Sistem sulit/tidak dapat diakses
Infrastruktur	*Overheat*	Penggunaan perangkat dalam waktu yang lama	Perangkat panas, responbilitas sistem terganggu
	Kerusakan *hardware*	Arus listrik tidak stabil	Kerugian materil instansi
	Listrik padam	*Maintanance*, faktor alam	Operasional terganggu/ terhenti
Keamanan data	Kebocoran data	Akses tidak sah atau peretasan	Kehilangan data, penyalahgunaan data
	Penyalahgunaan hak akses	Penyebaran hak akses tanpa izin	Data penting dapat diakses pihak tidak berwenang

Kategori risiko ditentukan berdasarkan aset penting instansi, seperti data jemaah, akun pengguna, data keuangan, dan cadangan. Risiko diklasifikasikan dari sumber ancaman internal

(misalnya kesalahan pengguna), eksternal (peretasan), dan lingkungan (listrik padam, cuaca ekstrem), lalu disusun skenario dan dampaknya mengacu pada referensi (Caralli *et al*., 2007) dari Carnegie Mellon University, penelitian oleh (Riadi dan Sukri, 2021) dan (Gutandjala *et al*., 2019). Setiap risiko dikaitkan dengan tiga area dampak utama yaitu reputasi, keamanan, dan produktivitas, seperti disajikan dalam Tabel 5.

Tabel 5 *Impact Area*

Area Terdampak	Tingkat Dampak		
	Rendah / *Low*	**Sedang / *Medium***	**Tinggi / *High***
Reputasi	Reputasi sedikit terpengaruh sehingga diperlukan upaya untuk perbaikan	Reputasi terkena dampak buruk sehingga perlu dilakukan upaya perbaikan dengan mengeluarkan biaya	Penurunan reputasi yang besar bahkan rusak yang menyebabkan hampir tidak dapat diperbaiki
Keamanan	Terjadi adanya peristiwa menyangkut keamanan yang berdampak ringan, seperti gangguan server sementara sehingga pengguna tidak dapat mengakses sistem	Terjadi adanya peristiwa menyangkut keamanan yang cukup serius yaitu kebocoran data sehingga perlu dilakukan tindakan untuk meminimalisir dampak yang mungkin terjadi	Terjadi adanya peristiwa menyangkut keamanan yang serius hingga mengakibatkan sistem tidak dapat diakses, kehilangan data, dan dampak finansial.
Produktivitas	Adanya hambatan kegiatan operasional pengguna saat mengakses dan menggunakan sistem	Adanya pengaruh yang cukup signifikan yang mengakibatkan lambatnya operasional	Adanya kerugian serius yang ditimbulkan pada kegiatan operasional sehingga sistem tidak dapat diakses/ digunakan

Penilaian dampak risiko dilakukan untuk menentukan tingkat pengaruh terhadap area terdampak. Dampak dibagi menjadi tiga: rendah (*low*) yang mudah ditangani**,** sedang (*medium*) yang mengganggu operasional dan butuh pemulihan, serta tinggi (*high*) yang bersifat signifikan dan dapat merusak reputasi atau menyebabkan kerugian besar. Setiap area terdampak diberi skor menggunakan skala prioritas sebagaimana ditampilkan pada Tabel 6.

Tabel 6 Skala Prioritas *Impact Area*

Prioritas	*Impact Area*
3	Reputasi
2	Keamanan
1	Produktivitas

Penetapan prioritas didasarkan pada tingkat kepentingan dan kerentanan tiap area terhadap operasional instansi. Reputasi diberi bobot tertinggi (3) karena dampaknya jangka panjang, keamanan diberi bobot sedang (2) karena masih bisa dikendalikan secara teknis, dan produktivitas terendah (1) karena gangguan operasional bersifat sementara dan mudah dipulihkan.

Mengembangkan Profil Aset Informasi

Hal yang perlu dilakukan pada tahap ini adalah mengidentifikasi dan menginventaris sekumpulan aset informasi yang penting pada sistem. Berikut profil aset informasi disajikan pada Tabel 7. Aset informasi pada Tabel 7 dipilih karena kebocorannya dapat mengganggu layanan operasional. Untuk menjaganya, diperlukan kebijakan keamanan informasi, autentikasi kuat, enkripsi data, dan pelatihan keamanan bagi pengguna.

Tabel 7 Profil Aset Informasi

Aset Informasi	Deskripsi Aset	Pengguna
Data jemaah	Informasi data pribadi, kesehatan, dan administratif jemaah	Operator, Pegawai Unit Pelaksana, Kepala Unit Pelaksana
Data keberangkatan dan pemulangan	Informasi jadwal dan logistik jemaah	Operator, Pegawai Unit Pelaksana, Kepala Unit Pelaksana, Maskapai Penerbangan

Aset Informasi	Deskripsi Aset	Pengguna
Data keuangan jemaah	Data pembayaran, pelunasan, dan alokasi dana	Operator, Pegawai Unit Pelaksana, Kepala Unit Pelaksana, Auditor Internal
Data akun dan hak akses	Informasi *username* dan *password* pengguna	Admin sistem/Pranata Komputer
Data *log* aktivitas sistem	Catatan akses dan aktivitas pengguna dalam sistem	Admin sistem/Pranata Komputer
Data *backup*	Salinan data penting (data jemaah, keuangan, dan log aktivitas)	Admin sistem/Pranata Komputer

Mengidentifikasi Wadah Aset Informasi

Tahap ini dilakukan identifikasi terhadap wadah atau tempat di mana aset informasi diproses dan disimpan, baik dari pihak internal maupun pihak eksternal yang terdiri dari *software, hardware*, ataupun hal teknis lainnya sebagaimana dapat dilihat pada Tabel 8.

Tabel 8 Wadah Aset Informasi

Kontainer Aset Informasi : Internal	
Deskripsi	Pemilik
Module : Database layanan Sistem Komputerisasi Terpadu yang digunakan oleh pegawai yang telah diberikan tugas dan tanggung jawab dalam penggunaannya dari tingkat pusat, provinsi, dan kabupaten	Direktorat Pusat
Server : Perangkat keras yang digunakan untuk penyimpanan sistem/aplikasi dan database	
Jaringan Internet Internal : *Local Area Network* (LAN) beserta perangkat jariangan pendukung lainnya.	Kantor Kabupaten
Komputer : Perangkat keras yang digunakan oleh pengguna untuk melakukan akses ke Sistem Komputerisasi Terpadu beserta sistem operasi server didalamnya.	
Aplikasi : Sistem Komputerisasi Terpadu	Direktorat Pusat Instansi pada tingkat provinsi dan kabupaten/kota hanya diberikan Hak Guna Pakai.
Kontainer Aset Informasi : Eksternal	
Deskripsi	Pemilik
Jaringan Internet Utama menggunakan vendor pihak ketiga	Indihome

Mengidentifikasi Kondisi dan Situasi Sistem Kritis

Kondisi dan situasi item kritis adalah terjadinya kondisi dalam operasional layanan yang mempengaruhi aset informasi instansi. Pada tahap ini instansi mengidentifikasi kondisi dan situasi sistem kritis berdasarkan informasi yang telah disajikan pada Tabel 8. Adapun hasil identifikasi kondisi dan situasi sistem kritis seperti dalam Tabel 9.

Tabel 9 Kondisi Sistem Kritis

No	*Area of Concern*
1	Kesalahan penanganan pada sistem database saat pemeliharaan/*maintanance*
2	*Server down* menyebabkan sistem tidak dapat diakses dan mengganggu kegiatan operasional layanan
3	Kerusakan pada sarana layanan seperti perangkat keras sistem
4	Kebocoran data dan penyalahgunaan hak akses yang menyebabkan perubahan atau hilangnya data yang tidak semestinya.

Mengidentifikasi Skenario Ancaman

Pada tahap ini instansi membuat skenario ancaman yang dapat mempengaruhi aset infomasi secara detail berdasarkan Tabel 9 dengan mengidentifikasi aktor, *means*, motif, dan *outcome* serta probabilitas terjadinya skenario ancaman tersebut. Informasi yang diperoleh kemudian dituangkan ke dalam Tabel 10.

Tabel 10 Identifikasi Skenario Ancaman

No	*Area of Concern*	*Threat of Scenarios*	
1	Kesalahan penanganan pada sistem database saat pemeliharaan/*maintanance*	*Actor*	Admin database, teknisi IT, pegawai pemeliharaan
		Means	Akses ke sistem database melalui perangkat lunak (DBMS), akses langsung ke server, atau *remote access*.
		Motives	Mengoptimalkan performa sistem, memperbaiki masalah yang muncul, memperbaharui sistem, atau kurangnya pelatihan yang cukup terhadap penanganan sistem.
		Outcome	Potensi kehilangan data, kerusakan data, *downtime* sistem.
		Probabilitas	*High Risk*
2	*Server down* menyebabkan sistem tidak dapat diakses dan mengganggu kegiatan operasional layanan	*Actor*	Admin server, teknisi jaringan, penyedia layanan/*cloud,* pihak eksternal yang tidak berwenang (peretas)
		Means	Gangguan perangkat keras dan perangkat lunak, serangan *hacker*, kesalahan konfigurasi hingga pemadaman listrik
		Motives	Menjaga stabilitas layanan atau keamanan sistem, namun juga dapat disebabkan oleh serangan peretas sehingga mengganggu layanan operasional atau menyebabkan kerugian finansial
		Outcome	Sistem tidak dapat diakses oleh pengguna, terhentinya layanan operasional, kehilangan data sementara dan potensi kerugian finansial bahkan reputasi
		Probabilitas	*High Risk*
3	Kerusakan pada sarana layanan seperti perangkat keras sistem	*Actor*	Teknisi IT, operator, faktor lingkungan seperti kelembaban, panas, debu, cacat perangkat dari toko
		Means	Kerusakan komponen perangkat keras, kerusakan fisik, keausan disebabkan usia perangkat, atau kurangnya pemeliharan.
		Motives	Adanya ketidaksengajaan dalam penggunaan sehari-hari, keausan alami, pemeliharaan tidak dilakukan secara berkala, atau penggunaan yang tidak sesuai prosedur.
		Outcome	Gangguan terhadap layanan seperti pelayanan yang menjadi lamban, *downtime* sistem, potensi kehilangan data, biaya perbaikan hingga penggantian perangkat keras.
		Probabilitas	*Medium Risk*
4	Kebocoran data dan penyalahgunaan hak akses yang menyebabkan perubahan atau hilangnya data yang tidak semestinya.	*Actor*	Operator, pihak eksternal yang tidak berwenang seperti peretas atau bahkan mantan pegawai
		Means	Akses langsung ke sistem, penggunaan yang tidak sah, pencurian data
		Motives	Menyalahgunakan wewenang demi keuntungan pribadi, merusak citra instansi, ketidakpuasan/sakit hati pegawai, atau kurangnya pemahaman terhadap pentingnya keamanan data.
		Outcome	Kebocoran data, perubahan data yang tidak semestinya, hilangnya data, kerugian finansial, kerusakan reputasi, dan potensi sanksi hukum baik pidana maupun perdata.
		Probabilitas	*High Risk*

Mengidentifikasi Risiko

Pada tahap ini aktivitas yang dilakukan adalah menentukan dampak atau konsekuensi dari skenario ancaman sebagaimana dijelaskan sebelumnya. Hasil identifikasi risiko terhadap keamanan informasi ditampilkan pada Tabel 11.

Tabel 11 Identifikasi Risiko

Risiko	Konsekuensi
Akses Tidak Sah Terhadap Data Jemaah	Data pribadi jamaah haji dapat diakses oleh pihak yang tidak berwenang sehingga menyebabkan pelanggaran privasi
Kegagalan Sistem Saat Pendaftaran	Pengguna tidak dapat mengakses atau memasukan data jamaah sehingga menyebabkan keterlambatan proses pendaftaran
Peretasan dari Pihak Eksternal	Sistem dapat mengalami serangan dari peretas yang berpotensi merusak atau mengganggu operasi sistem
Kegagalan Backup Data	Kehilangan data penting jika terjadi kerusakan sistem atau bencana, yang berdampak pada kelangsungan layanan.
Pencurian Perangkat Keras	Data penting yang tersimpan dalam perangkat keras dapat dicuri dan diakses oleh pihak yang tidak berwenang.

Menganalisis Risiko

Berdasarkan identifikasi yang telah dilakukan terhadap risiko yang kemungkinan terjadi, selanjutnya dilakukan analisis risiko dengan mengukur seberapa jauh dampak yang ditimbulkan dari ancaman sebagaimana pada Tabel 11 untuk dilakukan perhitungan skor berdasarkan *impact area* pada Tabel 6 dalam menentukan mitigasi yang lebih dahulu.

Nilai dari setiap *impact area* sebagaimana disajikan pada Tabel 12 yang kemudian dilakukan analisis risiko terhadap *area on concern* dapat dilihat pada Tabel 13.

Tabel 12 Skor *Impact Area*

Impact Area	*Priority*	*Low (1)*	*Medium (2)*	*High(3)*
Reputasi	3	3	6	9
Keamanan	2	2	4	6
Produktivitas	1	1	2	3

Nilai skor impact area diperoleh dari pengalian bobot skala prioritas di Tabel 6 dengan nilai tingkat dampak setiap area (*low, medium,* dan *high)*. Pendekatan ini mengacu pada kerangka Octave Allegro yang menekankan penyesuaian terhadap konteks organisasi dalam menentukan nilai strategis dari setiap impact area.

Tabel 13 Analisis Risiko

Area of Concern	*Risk*			
Akses tidak sah terhadap data jemaah	*Consequences*	Data pribadi jamaah haji dapat diakses oleh pihak yang tidak berwenang sehingga menyebabkan pelanggaran privasi		
	Severity	*Impact Area*	*Value*	*Score*
		Reputasi	High	9
		Keamanan	High	6
		Produktivitas	Medium	2
			Relative Risk Score	17
Kegagalan sistem saat pendaftaran	*Consequences*	Pengguna tidak dapat mengakses atau memasukan data jamaah sehingga menyebabkan keterlambatan proses pendaftaran		
	Severity	*Impact Area*	*Value*	*Score*
		Reputasi	Medium	6
		Keamanan	Low	2
		Produktivitas	High	3
			Relative Risk Score	11
Peretasan dari Eksternal	*Consequences*	Sistem dapat mengalami serangan dari peretas yang berpotensi merusak datau atau mengganggu operasi sistem		
	Severity	*Impact Area*	*Value*	*Score*
		Reputasi	High	9
		Keamanan	High	6
		Produktivitas	High	3
			Relative Risk Score	18
Kegagalan Backup Data	*Consequences*	Kehilangan data penting jika terjadi kerusakan sistem atau bencana, yang berdampak pada kelangsungan layanan.		
	Severity	*Impact Area*	*Value*	*Score*
		Reputasi	High	9
		Keamanan	High	6
		Produktivitas	High	3
			Relative Risk Score	18
Pencurian Perangkat Keras	*Consequences*	Data penting yang tersimpan dalam perangkat keras dapat dicuri dan diakses oleh pihak yang tidak berwenang.		
	Severity	*Impact Area*	*Value*	*Score*
		Reputasi	High	9
		Keamanan	High	6
		Produktivitas	Medium	2
			Relative Risk Score	17

Menentukan Pendekatan Mitigasi Risiko

Setiap risiko yang telah dianalisis dan diperoleh skor *risk relative matrix* menggunakan penilaian pada Tabel 13 kemudian ditentukan pendekatan mitigasi risiko berdasarkan tabel *risk relative matrix score*, seperti ditunjukkan pada Tabel 14.

Tabel 14 *Risk Relative Matrix Score*

Risk Score	POOL	Mitigation Approach
0-6	3	Accept
7-12	2	Defer
13-18	1	Mitigate or Transfer

Tabel 14 menyajikan informasi *risk relative matrix score,* setiap baris dalam tabel mencerminkan interval skor yang menjadi dasar untuk menentukan strategi mitigasi yang tepat terhadap risiko keamanan informasi. Berikut penjelasan pada setiap kolom dalam Tabel 14.

1. *Risk* Score : merupakan total skor dampak risiko dari tiga area utama, dihitung dari nilai dampak dikalikan bobot prioritas.
2. *POOL* : mengkategorikan tingkat risiko, yaitu nilai 1 untuk risiko tinggi, nilai 2 untuk risiko sedang, dan nilai 3 untuk risiko rendah.
3. *Mitigation Approach* : strategi penanganan risiko terbagi menjadi tiga, antara lain.
   a. *Accept* dengan skor 0-6 adalah risiko rendah, cukup dengan dipantau.
   b. *Defer* dengan skor 7-12 adalah risiko sedang, penanganan bisa ditunda.
   c. *Mitigate or Transfer* dengan skor 13-18 adalah risiko tinggi, perlu dilakukan mitigasi langsung atau dialihkan ke kantor pusat.

Adapun hasil penentuan pendekatan mitigasi risiko ditunjukkan pada Tabel 15.

Tabel 15 Tabel Penilaian menggunakan Metode Octave Allegro

Areas of Concern	***Reputasi***	***Keamanan***	***Produktivitas***	***Risk Relative Matrix***	***Mitigation Approach***
Akses Tidak Sah Terhadap Data Jemaah	9 *(High)*	6 *(High)*	2 (*Medium)*	17	*Mitigate or Transfer*
Kegagalan Sistem Saat Pendaftaran	6 (*Medium)*	2 (*Low)*	3 (*High)*	11	*Defer*
Peretasan dari Eksternal	9 (*High)*	6 (*High)*	3 (*High)*	18	*Mitigate or Transfer*
Kegagalan Backup Data	9 (*High)*	6 (*High)*	3 (*High)*	18	*Mitigate or Transfer*
Pencurian Perangkat Keras	9 (*High*)	6 (*High)*	2 (*Medium)*	17	*Mitigate or Transfer*

Berdasarkan Tabel 15, sebagian besar risiko berada pada kategori *mitigate or transfer*. Risiko seperti pencurian perangkat dapat ditangani oleh kantor kabupaten. Sementara itu, risiko besar seperti akses tidak sah, peretasan, dan kegagalan *backup* perlu ditransfer ke kantor pusat. Kegagalan sistem saat pendaftaran dapat ditangani sendiri jika penyebabnya bersifat lokal; jika sistem *error*, perlu koordinasi dengan kantor pusat. Adapun rekomendasi yang diberikan kepada Kantor Kementerian XYZ adalah penguatan pengelolaan risiko pada kantor kabupaten, kolaborasi dan koordinasi dengan kantor pusat secara berkala, dan peningkatan infrastruktur teknologi.

SIMPULAN

Berdasarkan analisis keamanan informasi menggunakan Indeks KAMI dan Octave Allegro dapat diambil kesimpulan bahwa Penggunaan Indeks KAMI pada kantor kabupaten menunjukkan kepatuhan tinggi terhadap ISO 27001, namun terbatas dalam kewenangan, terutama pada aspek pengelolaan risiko yang masih bergantung pada kantor pusat. Sebaliknya, metode Octave Allegro lebih efektif dalam mengidentifikasi dan mengelola risiko, dengan 4 dari 5 risiko berada pada kategori *mitigate or transfer*. Metode ini dinilai cocok diterapkan pada

instansi yang masih bergantung pada otoritas pusat karena mampu menyesuaikan penanganan risiko sesuai kapasitas lokal.

DAFTAR PUSTAKA

Abdullah K, Isnainiyah IN, Faried MI. 2020. Risk Management Analysis on Organizational Website Using Octave Allegro Method. In: Proceedings - 2nd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2020. Institute of Electrical and Electronics Engineers Inc., pp. 201–206.

Anas AS, Utami IGASDG, Maulachela AB, Juliansyah A. 2021. KAMI index as an evaluation of academic information system security at XYZ university. Matrix : Jurnal Manajemen Teknologi dan Informatika 11, 55–62.

Aziz RA, Ikhsanudin A, Hasibuan MS. 2024. Governance Evaluation Electronic Security System (ESS) (Case Study: ABC Central Bank). Sinkron 8, 713–726.

Caralli RA, Stevens JF, Young LR, Wilson WR. 2007. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Carnegie Mellon University.

Dewantara R, Sugiantoro B. 2021. Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Pada Jaringan (Studi Kasus : UIN Sunan Kalijaga Yogjakarta). Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) 8, 1137–1149.

Gerardo V, Fajar AN. 2022. Academic IS Risk Management using OCTAVE Allegro in Educational Institution. Journal of Information Systems and Informatics 4.

Gutandjala II, Gui A, Maryam S, Mariani V. 2019. Information System Risk Assessment And Management (Study Case at XYZ University). In: IEEE. IEEE, Jakarta & Bali, pp. 602–607.

Hartomo A. 2023. Perencanaan Strategis Sistem Informasi Dan Sistem Manajemen Keamanan Informasi Berbasis ISO/IEC 27001:2013 Menggunakan Ward & Peppard Pada Perusahaan Transshipment. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) 10, 141–152.

Hom J, Anong B, Rii KB, Choi LK, Zelina K. 2020. The Octave Allegro Method in Risk Management Assessment of Educational Institutions. Aptisi Transactions on Technopreneurship (ATT) 2, 167–179.

Irsheid A, Murad A, Alnajdawi M, Qusef A. 2022. Information security risk management models for cloud hosted systems: A comparative study. In: Procedia Computer Science. Elsevier B.V., pp. 205–217.

Jelita LDA, Al Azam MN, Nugroho A. 2024. Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/EIC 27001:2022. Jurnal SAINTEKOM 14, 84–94.

Razikin K, Soewito B. 2022. Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. Egyptian Informatics Journal 23, 383–404.

Riadi I, Sukri M. 2021. Risk Management Analysis on Administration System using OCTAVE Allegro Framework Risk Management Analysison Administration System using OCTAVE Allegro Framework. Int J Comput Appl 174, 975–8887.

Savitri R, Firmansyah, Dworo, Hasibuan MS. 2024. Information Security Measurement using INDEX KAMI at Metro City. Journal of Applied Data Sciences 5, 33–45.

Wasilah, Kurniawan, Hasibuan MS, Firmansyah. 2024. Evaluation of Information Security Level at The South Lampung Communications and Information Service Using the Kami 4.3 Index. Jurnal Ilmu Komputer & Agri-Informatika 11, 13–8.

Yusuf IS, Said HM. 2024. Evaluation of Information Security at The Raden Inten II Lampung Meterological Statiun Using The Index KAMI 12, 1668–1678.