Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK) p-ISSN: 2355-7699
Vol. 12, No. 6, Desember 2025, hlm. 1463-1474 e-ISSN: 2528-6579

IMPLEMENTASI INDEKS KAMI DI UNIVERSITAS XYZ

Muhamad Agung Gumelar[*1], Handoyo Widi Nugroho[2], M. Said Hasibuan[3]

[1,2,3]Institut Informatika dan Bisnis Darmajaya, Bandar Lampung
Email: [1]agung.2421211031p@mail.darmajaya.ac.id, [2]handoyo.wn@darmajaya.ac.id,[3]msaid@darmajaya.ac.id
[*]Penulis Korespondensi

(Naskah masuk: 07 Juli 2025, diterima untuk diterbitkan: 16 Desember 2025)

Abstrak

Indeks KAMI (Keamanan Informasi) merupakan alat bantu evaluasi yang disusun oleh Badan Siber dan Sandi Negara (BSSN) untuk menilai tingkat kesiapan dan kematangan implementasi keamanan informasi di suatu institusi. Penelitian ini bertujuan untuk mengimplementasikan Indeks KAMI di Universitas XYZ sebagai bagian dari upaya pemetaan dan pengelolaan risiko teknologi informasi (*IT Risk Management*) secara sistematis dan terukur. Pendekatan penelitian dilakukan dengan menggunakan metode deskriptif kualitatif melalui studi kasus, yang berfokus pada lima domain utama Indeks KAMI: Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, serta Teknologi dan Keamanan. Proses pengumpulan *data* dilakukan melalui observasi, wawancara terstruktur, dan pengisian instrumen penilaian sesuai dengan pedoman yang ditetapkan oleh BSSN. Hasil evaluasi menunjukkan bahwa tingkat kesiapan keamanan informasi Universitas XYZ berada pada skor total 176, yang tergolong dalam kategori rendah dan belum layak sertifikasi *ISO/IEC 27001*. Skor terendah terdapat pada domain Pengelolaan Risiko 17 serta Skor tertinggi pada domain Pengelolaan Aset 51 adapun untuk domain Tata Kelola 26, Kerangka Kerja 34, Teknologi dan Keamanan 48, yang menunjukkan perlunya pembenahan dalam aspek kebijakan, prosedur, serta pelaksanaan manajemen risiko. Penelitian ini memberikan gambaran awal mengenai posisi keamanan informasi dan merekomendasikan langkah-langkah prioritas dalam penguatan tata kelola keamanan, pembentukan kebijakan keamanan, serta peningkatan kesadaran dan kapasitas SDM dalam bidang keamanan informasi.

Kata kunci: Indeks KAMI, BSSN, keamanan informasi, manajemen risiko TI, *ISO/IEC 27001*

IMPLEMENTATION OF KAMI INDEX IN Universitas XYZ

Abstract

The KAMI Index (Information Security Index) is an evaluation tool developed by the National Cyber and Crypto Agency (BSSN) of Indonesia to assess the readiness and maturity level of information security implementation within institutions. This study aims to implement the KAMI Index at Universitas XYZ as a systematic and measurable approach to Information Technology Risk Management. A descriptive qualitative approach was employed using a case study method, concentrating on the five primary domains of the KAMI Index: Governance, Risk Management, Framework, Asset Management, and Technology and Security. Data collection was carried out through structured interviews, observations, and scoring based on BSSN's official assessment instruments. The results revealed that scored a total of 176, indicating a low level of readiness and immaturity in information security, which is considered insufficient for ISO/IEC 27001 certification. The lowest scores were found in Risk Management domains 17, and the highest score in the Asset Management domain is 51, while for the Governance domain is 26, the Framework is 34, and Technology and Security is 48, highlighting the need for improvements in policies, procedures, and risk mitigation practices. This study provides an initial overview of the state of information security at and offers strategic recommendations for enhancing governance structures, developing formal security policies, and strengthening institutional awareness and human resource capacity in information security practices.

Keywords: *KAMI Index, BSSN, information security, IT risk management, ISO/IEC 27001*

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat telah membawa perubahan mendasar dalam cara organisasi, termasuk institusi pendidikan tinggi, mengelola *data* dan informasi. Transformasi digital tidak hanya berdampak pada efisiensi operasional, tetapi juga menciptakan ketergantungan tinggi terhadap infrastruktur teknologi informasi dan komunikasi (TIK). Universitas sebagai institusi

penghasil ilmu pengetahuan dan pusat inovasi, memiliki tanggung jawab besar dalam menjamin keamanan aset informasinya. Keamanan informasi bukan hanya tentang perlindungan teknis terhadap sistem, tetapi juga menyangkut kebijakan, prosedur, serta kesadaran seluruh elemen organisasi terhadap pentingnya menjaga kerahasiaan, integritas, dan ketersediaan *data*.

Meningkatnya ketergantungan pada sistem informasi di perguruan tinggi juga meningkatkan potensi risiko yang dapat mengancam kelangsungan layanan pendidikan dan tata kelola institusi. Serangan siber seperti *phishing, malware, ransomware*, serta kebocoran *data* telah menjadi ancaman nyata dalam dunia pendidikan tinggi. Insiden keamanan informasi dapat berdampak serius, baik terhadap reputasi institusi, kepercayaan publik, maupun kelangsungan proses belajar mengajar. Oleh karena itu, keamanan informasi menjadi aspek strategis yang harus dikelola dengan pendekatan yang sistematis, terukur, dan sesuai dengan standar nasional maupun internasional.

Universitas XYZ merupakan salah satu perguruan tinggi swasta di Indonesia telah memanfaatkan berbagai sistem informasi untuk mendukung kegiatan akademik dan administratif. Sistem informasi akademik, keuangan, kepegawaian, dan layanan digital mahasiswa merupakan bagian dari infrastruktur teknologi yang sangat krusial dan perlu dikelola dengan panduan dasar dalam pengelolaan TIK yang sesuai. Di konteks ini, kebutuhan akan evaluasi menyeluruh terhadap kesiapan dan kematangan keamanan informasi menjadi semakin penting. Evaluasi ini tidak hanya untuk mengetahui kondisi terkini, melainkan juga untuk merumuskan langkah-langkah strategis yang dapat memperkuat sistem keamanan informasi secara menyeluruh.

Sebagai respon terhadap pentingnya manajemen keamanan informasi di sektor publik dan pendidikan, Badan Siber dan Sandi Negara (BSSN) telah mengembangkan Indeks KAMI (Keamanan Informasi) sebagai alat bantu untuk menilai tingkat kematangan manajemen keamanan informasi. Indeks KAMI dirancang untuk digunakan oleh lembaga pemerintahan, pendidikan, maupun organisasi lainnya guna melakukan penilaian mandiri atas kesiapan mereka dalam mengelola keamanan informasi. Alat ini berfokus pada lima domain utama, Sebagai berikut : (1) Tata Kelola Keamanan Informasi, (2) Manajemen Risiko, (3) Kerangka Kerja Keamanan Informasi, (4) Pengelolaan Aset, serta (5) Teknologi dan Aspek Keamanan. Setiap domain memiliki indikator pengukuran yang dapat digunakan untuk menilai sejauh mana penerapan kebijakan, prosedur, dan teknologi keamanan informasi dalam suatu organisasi.

Beberapa penelitian terdahulu telah menunjukkan penerapan Indeks KAMI sebagai metode evaluasi yang efektif untuk mengidentifikasi kelemahan dan kekuatan dalam sistem keamanan informasi. Sebagai contoh, studi oleh Putra dan Tjahjadi (2018) di lingkungan institusi pendidikan mengungkapkan bahwa penggunaan Indeks KAMI dapat mengidentifikasi area yang belum sesuai dengan standar *ISO/IEC 27001* serta memberikan panduan strategis untuk meningkatkan sistem keamanan informasi. Selanjutnya, Basyarahil, Astuti, dan Hidayanto (2017) dalam penelitiannya pada DPTSI ITS Surabaya menemukan bahwa sebagian besar domain belum mencapai tingkat kematangan level *III+*, yang merupakan level minimal kesiapan sertifikasi keamanan informasi. Penelitian lain oleh Sutara (2018) pada PDAM Titra Medal juga menyimpulkan bahwa meskipun kesadaran akan pentingnya keamanan informasi cukup tinggi, namun implementasi pengelolaan risikonya belum merata dan masih bersifat parsial. Sementara itu, Akhirina et al. (2016) dalam studi pada sektor logistik menunjukkan bahwa institusi masih berada pada level *I+* hingga *II+*, yang menandakan perlunya peningkatan strategi dan kebijakan keamanan informasi.

Meskipun berbagai studi telah mengkaji penerapan Indeks KAMI pada institusi pemerintahan dan pendidikan, sebagian besar penelitian tersebut dilakukan pada institusi negeri atau berskala besar. Masih terbatas penelitian yang secara spesifik mengevaluasi kondisi keamanan informasi di perguruan tinggi swasta seperti Universitas XYZ. Selain itu, belum banyak studi yang mengaitkan hasil evaluasi Indeks KAMI dengan strategi peningkatan berbasis kebutuhan spesifik institusi, terutama dalam konteks implementasi pengamanan terhadap layanan akademik digital. Hal ini menunjukkan adanya kesenjangan penelitian yang perlu diisi melalui studi yang lebih aplikatif dan kontekstual.

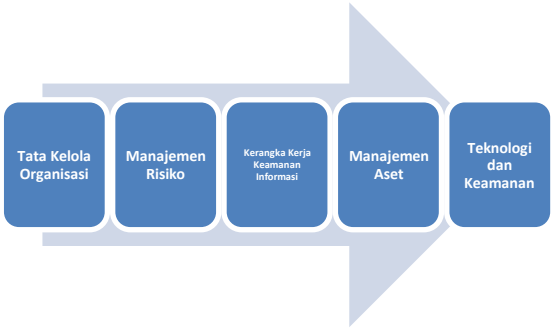
Penelitian ini dilakukan untuk menjawab kebutuhan tersebut dengan melakukan penilaian manajemen keamanan informasi di Universitas XYZ menggunakan metode Indeks KAMI, yang dikeluarkan oleh BSSN. Evaluasi dilakukan terhadap kelima domain Indeks KAMI untuk memperoleh gambaran tingkat kesiapan dan kematangan keamanan informasi di lingkungan universitas. Selanjutnya penelitian ini bertujuan untuk memberikan rekomendasi peningkatan keamanan informasi yang sesuai dengan hasil temuan di lapangan, serta berdasarkan prinsip-prinsip *ISO/IEC 27001*:*2018* sebagai standar internasional di pengelolaan sistem manajemen keamanan informasi.

Urgensi dari penelitian ini terletak pada kebutuhan Universitas XYZ untuk meningkatkan ketahanan sistem informasi terhadap ancaman keamanan siber dan memastikan bahwa tata kelola informasi yang diterapkan telah memenuhi standar nasional dan internasional. Dengan adanya hasil evaluasi ini, pihak universitas diharapkan dapat menyusun langkah-langkah strategis dalam peningkatan keamanan informasi, baik dari sisi kebijakan, prosedur, teknologi, maupun kesadaran

pada sdm yang ada. Selain itu, hasil penelitian ini dapat menjadi rujukan bagi institusi pendidikan tinggi yang ingin mengimplementasikan sistem manajemen keamanan informasi yang efektif, berkelanjutan, dan sesuai dengan karakteristik masing-masing institusi.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode studi kasus. Pendekatan ini bertujuan untuk menggambarkan kondisi aktual kesiapan keamanan informasi di Universitas XYZ berdasarkan indikator yang terdapat pada Indeks KAMI (Keamanan Informasi), sebuah alat evaluasi yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN). Tahapan-tahapan metode penelitian ini dapat dilihat pada Gambar 1.



Gambar 1 Tahapan Penelitian Dengan Indeks KAMI

1) Tata Kelola Organisasi

Di tahap ini, dilaksanakan proses pelaksanaan atau penerapan sesuai dengan tahapan yang telah ditetapkan penilaian terhadap tingkat persiapan instansi dalam membentuk dan menerapkan tata kelola keamanan informasi yang efektif. Evaluasi mencakup keberadaan struktur organisasi atau unit kerja yang secara khusus menangani keamanan informasi, termasuk kejelasan fungsi, peran, serta pembagian tugas dan tanggung jawab dari seluruh pihak yang terlibat, Dimulai dari pimpinan unit kerja hingga pelaksana operasional di lapangan, salah satu kontrol utama yang perlu diterapkan adalah adanya kebijakan formal yang secara jelas menetapkan otoritas, tanggung jawab, dan kewenangan dalam pengelolaan keamanan informasi. Kebijakan ini harus bersifat menyeluruh dan mampu menjadi acuan dalam pelaksanaan kegiatan operasional sehari-hari. Selain itu, evaluasi juga mencakup aspek keberlanjutan program kerja yang telah dirancang, termasuk adanya alokasi anggaran yang memadai, pelaksanaan evaluasi berkala terhadap efektivitas program, Selain itu, diperlukan strategi untuk meningkatkan kinerja tata kelola keamanan informasi secara sistematis dan terarah, guna mendukung tercapainya tujuan organisasi dalam melindungi *data* dan informasi secara menyeluruh.

2) Manajemen Resiko

Di tahap ini, dilaksanakan penilaian mengenai tingkat kesiapan instansi dalam mengelola risiko keamanan informasi, yang menjadi landasan utama untuk merancang dan menjalankan strategi keamanan informasi secara komprehensif. Evaluasi ini bertujuan untuk menilai apakah organisasi telah memiliki pendekatan sistematis dalam mengidentifikasi, menganalisis, menilai, serta mengendalikan potensi risiko yang dapat mengancam kerahasiaan, integritas, dan ketersediaan informasi. Kontrol yang diwajibkan dalam area ini mencakup keberadaan kerangka kerja pengelolaan risiko yang terdokumentasi secara jelas dan terstruktur, termasuk definisi eksplisit mengenai tingkat ambang batas risiko yang dapat diterima oleh organisasi sesuai dengan profil dan toleransi risiko masing-masing. Selain itu, harus terdapat program pengelolaan risiko yang aktif, mencakup proses identifikasi risiko, penilaian dampak dan kemungkinan terjadinya, serta penyusunan langkah-langkah mitigasi yang tepat untuk meminimalkan dampak risiko tersebut. Program ini juga harus disertai dengan mekanisme evaluasi secara berkala guna meninjau efektivitas strategi mitigasi yang telah diterapkan, memastikan bahwa pendekatan yang digunakan tetap relevan, adaptif terhadap perubahan lingkungan, dan mampu menjaga keamanan informasi secara berkelanjutan.

3) Kerangka Kerja Keamanan Informasi

Di tahap ini, dilaksanakan penilaian terhadap sejauh mana kelengkapan dan kesiapan kerangka kerja yang mencakup kebijakan, prosedur, serta strategi penerapan dalam pengelolaan keamanan informasi di suatu instansi. Penilaian ini bertujuan untuk mengetahui apakah organisasi telah memiliki dasar kebijakan yang kuat dan prosedur operasional yang memadai dalam mendukung penerapan sistem keamanan informasi yang efektif dan berkelanjutan. Kerangka kerja tersebut seharusnya mencakup berbagai aspek penting mulai dari perumusan kebijakan formal, pedoman teknis, hingga prosedur kerja harian yang diterapkan oleh seluruh unit kerja yang terlibat.

Kontrol yang diperlukan dalam konteks ini meliputi adanya dokumen kebijakan dan prosedur kerja operasional yang sudah disusun dengan cara sistematis dan terdokumentasi dengan baik, dan juga strategi implementasi yang terstruktur dan terintegrasi dengan proses bisnis organisasi. Selain itu, organisasi juga dituntut untuk memiliki mekanisme pengukuran terhadap efektivitas kontrol yang telah diterapkan, guna memastikan bahwa kebijakan dan prosedur tersebut berjalan sesuai dengan tujuan yang diharapkan. Tidak kalah penting, perlu pula disiapkan langkah-langkah perbaikan atau tindakan korektif yang dapat segera diimplementasikan apabila ditemukan kelemahan atau ketidaksesuaian dalam pelaksanaan kebijakan keamanan informasi, sehingga sistem keamanan

dapat terus ditingkatkan secara berkelanjutan dan responsif terhadap dinamika ancaman yang berkembang.

4) Manajement Asset

Pada segmen ini, penilaian dilakukan dan berfokus pada sejauh mana kelengkapan pengamanan diterapkan terhadap aset informasi yang dimiliki oleh instansi, mencakup seluruh tahapan dalam siklus hidup penggunaan aset tersebut. Penilaian dilakukan untuk memastikan bahwa setiap aset informasi—baik yang berbentuk fisik maupun digital—telah mendapatkan perlindungan yang memadai sejak tahap perolehan, penyimpanan, pemrosesan, distribusi, hingga pemusnahan atau penghapusan aset.

Kontrol yang dibutuhkan dalam aspek ini mencakup penerapan langkah-langkah pengamanan yang bersifat menyeluruh, yang meliputi baik aspek teknis maupun administratif. Dari sisi teknis, hal ini dapat mencakup pengamanan hardware dan software, penggunaan enkripsi, dan juga pengendalian akses pada sistem informasi. Sementara dari sisi administratif, diperlukan adanya dokumentasi inventaris aset, klasifikasi tingkat sensitivitas informasi, serta penetapan kebijakan penggunaan dan pemeliharaan aset yang sesuai dengan standar keamanan informasi.

Evaluasi ini juga menilai apakah organisasi telah memiliki sistem pemantauan dan audit internal yang mampu mengidentifikasi potensi risiko terhadap aset informasi serta mampu melakukan mitigasi secara cepat dan tepat. Dengan demikian, pengelolaan aset informasi dapat dilakukan secara terstruktur, terkontrol, dan selaras dengan prinsip-prinsip tata kelola keamanan informasi yang baik.

5) Teknologi dan Keamanan

Di tahap ini, dilaksanakan penilaian secara menyeluruh terhadap kompleksitas, kesesuaian, dan efisiensi pemanfaatan teknologi yang diterapkan di dalam upaya perlindungan terhadap aset informasi yang dimiliki oleh instansi. Penilaian ini bertujuan untuk memastikan bahwa teknologi yang digunakan telah mampu mendukung perlindungan informasi secara optimal, sesuai dengan tingkat risiko yang mungkin dihadapi, serta diterapkan secara konsisten di seluruh unit atau bagian yang relevan dalam organisasi.

Evaluasi tidak hanya mencakup keberadaan teknologi itu sendiri, tetapi juga bagaimana teknologi tersebut digunakan secara efektif dan terintegrasi dengan kebijakan serta prosedur keamanan informasi yang telah ditetapkan sebelumnya. Kontrol yang digunakan dalam konteks ini berbentuk strategi penerapan teknologi yang berorientasi pada manajemen risiko, di mana pemilihan solusi keamanan harus disesuaikan dengan klasifikasi aset, potensi ancaman, dan tingkat kerentanan yang ada.

Perlu dicatat bahwa dalam kontrol ini, strategi pengamanan tidak secara eksplisit menyebutkan jenis teknologi tertentu, nama produk, atau merek dagang spesifik. Sebaliknya, pendekatan yang digunakan bersifat prinsipil dan berbasis kebutuhan, dengan fokus pada efektivitas fungsi pengamanan yang dijalankan. Dengan demikian, instansi diharapkan mampu mengadopsi teknologi yang relevan, fleksibel, dan dapat disesuaikan dengan perkembangan ancaman siber serta dinamika operasional organisasi secara berkelanjutan.

Berdasarkan kelima aspek utama di bidang keamanan informasi yang tercakup dalam Indeks Keamanan Informasi (Indeks KAMI), peran teknologi informasi (TI) dalam mendukung upaya perlindungan dan pengamanan informasi menjadi lebih terukur, sistematis, dan dapat dievaluasi secara objektif. Melalui pendekatan ini, kontribusi TI tidak hanya dapat dinilai dari sisi teknis semata, tetapi juga dari segi kebijakan, prosedur, pengelolaan risiko, serta efektivitas kontrol terhadap aset informasi yang dikelola.

Dengan adanya indikator-indikator penilaian yang jelas dalam Indeks KAMI, organisasi dapat mengidentifikasi area mana saja yang memerlukan peningkatan, sekaligus memperoleh gambaran menyeluruh mengenai sejauh mana TI telah berperan dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi. Hasil penilaian ini selanjutnya dapat dimanfaatkan sebagai masukan strategis (input) bagi pengelola layanan TI dalam menyusun rencana kerja, meningkatkan kualitas layanan, serta merancang kebijakan dan strategi keamanan informasi yang lebih responsif terhadap ancaman dan tantangan yang terus berkembang. Dengan kata lain, evaluasi berdasarkan Indeks KAMI memberikan landasan yang kuat bagi pengambilan keputusan dalam pengelolaan keamanan informasi berbasis TI secara menyeluruh dan berkelanjutan.

Penilaian dilakukan menggunakan instrumen Indeks KAMI versi 4.2 dari BSSN yang mencakup lima domain utama. Evaluasi ini dimaksudkan supaya mengetahui level kesiapan keamanan informasi di Universitas XYZ, dengan pendekatan kuantitatif deskriptif terhadap hasil kuesioner dan observasi lapangan.

Setiap domain dinilai berdasarkan:

- ✓ Tingkat Kematangan (*Maturity Level*): mencerminkan sejauh mana pengelolaan keamanan telah diterapkan.
- ✓ Tingkat Kepentingan (*Importance Level*): mencerminkan seberapa penting domain tersebut bagi kelangsungan layanan organisasi.

2.1 Objek Penelitian

Objek dalam penelitian ini yaitu pengelolaan keamanan informasi pada lingkungan Universitas

XYZ, khususnya pada unit pengelola Teknologi Informasi. Evaluasi difokuskan pada kebijakan, prosedur, manajemen risiko, dan penggunaan teknologi yang mendukung keamanan sistem informasi.

2.2 Metode Pengumpulan *Data*

Adapun untuk mengumpulkan *data* dilakukan melalui tiga metode utama:

1. Wawancara terstruktur dengan tim pengelola TI untuk memperoleh *data* terkait implementasi kebijakan dan infrastruktur keamanan.
2. Observasi langsung terhadap sistem dan dokumen kebijakan TI.

Pengisian kuesioner Indeks KAMI oleh responden yang relevan, untuk mengukur tingkat kematangan dan tingkat kepentingan pada lima domain keamanan informasi.

2.3 Instrumen Kuesioner dan Validasi Hasil

Pengumpulan data dalam penelitian ini juga dilakukan melalui pengisian kuesioner yang disusun berdasarkan Instrumen Indeks KAMI Versi 4.2 yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN). Instrumen ini dirancang untuk menilai tingkat kematangan (maturity level) dan tingkat kepentingan (importance level) dari lima domain utama keamanan informasi, yaitu:

1) Tata Kelola Organisasi
2) Manajemen Risiko
3) Kerangka Kerja Keamanan Informasi
4) Manajemen Aset
5) Teknologi dan Keamanan

Kuesioner yang digunakan berbentuk pertanyaan tertutup dengan pilihan jawaban yang telah ditetapkan, menggunakan skala ordinal sesuai panduan resmi BSSN. Skala ini pada dasarnya setara dengan skala Likert 1–5, di mana setiap angka menggambarkan tahapan penerapan kontrol keamanan informasi, mulai dari Belum Ada (skor 1), Inisiasi (skor 2), Terlaksana Sebagian (skor 3), Terlaksana Sepenuhnya (skor 4), hingga Dioptimalkan (skor 5).

Setiap domain memiliki serangkaian pertanyaan yang mengacu pada indikator spesifik. Misalnya:

1) Tata Kelola Organisasi: “Apakah terdapat kebijakan keamanan informasi yang tertulis dan disahkan oleh pimpinan?”
2) Manajemen Risiko: “Apakah proses identifikasi risiko keamanan informasi dilakukan secara berkala dan terdokumentasi?”
3) Kerangka Kerja Keamanan Informasi: “Apakah terdapat prosedur formal untuk menanggapi insiden keamanan informasi?”
4) Manajemen Aset: “Apakah aset informasi telah diinventarisasi dan diklasifikasikan sesuai tingkat sensitivitas?”
5) Teknologi dan Keamanan: “Apakah mekanisme backup dan pemulihan data diuji secara rutin?”

Seluruh pertanyaan disusun dalam format pilihan ganda (opsi a, b, c, d, e) yang masing-masing mewakili tingkat kematangan tertentu. Responden diminta untuk memilih jawaban yang paling sesuai dengan kondisi riil di universitas. Dengan desain seperti ini, kuesioner dapat mengarahkan penilaian secara objektif, mengurangi bias interpretasi, serta memudahkan perhitungan skor sesuai metode evaluasi Indeks KAMI.

Validasi Hasil Indeks KAMI

Validasi hasil penilaian dilakukan untuk memastikan bahwa skor dan tingkat kematangan yang diperoleh benar-benar merefleksikan kondisi aktual keamanan informasi di Universitas XYZ. Proses validasi dilakukan melalui dua tahap:

1) Pemeriksaan Konsistensi Jawaban
   Jawaban responden diperiksa kesesuaiannya dengan hasil wawancara terstruktur dan observasi lapangan untuk memastikan bahwa data tidak bersifat asumtif, tetapi didukung bukti dokumentasi atau praktik nyata.
2) Konfirmasi oleh Tim Ahli
   Hasil perhitungan skor dan analisis gap diverifikasi oleh dua orang validator internal:
   Validator 1: Kepala Unit Teknologi Informasi Universitas XYZ, berpengalaman lebih dari 10 tahun dalam pengelolaan infrastruktur TIK, memahami kebijakan internal, dan prosedur keamanan informasi yang berlaku.
   Validator 2: Dosen sekaligus praktisi di bidang IT Governance dan keamanan informasi, berlatar belakang akademik S2 Teknik Informatika, serta memiliki sertifikasi pelatihan Indeks KAMI dari BSSN.

Pemilihan validator ini dilakukan secara purposive dengan mempertimbangkan otoritas, pengalaman teknis dan manajerial, serta pemahaman mendalam mengenai metodologi Indeks KAMI dan keterkaitannya dengan standar ISO/IEC 27001.

Dengan proses validasi berlapis ini, hasil evaluasi Indeks KAMI yang dihasilkan memiliki tingkat keandalan yang tinggi, objektif, dan dapat dijadikan dasar perumusan rekomendasi strategis untuk

peningkatan keamanan informasi di Universitas XYZ.

3. HASIL DAN PEMBAHASAN

3.1 Alat Evaluasi Indeks KAMI

Evaluasi dengan menggunakan Indeks Keamanan Informasi (Indeks KAMI) sebaiknya dilakukan oleh individu atau pihak yang memiliki tanggung jawab utama dan wewenang resmi dalam mengelola keamanan informasi secara keseluruhan pada suatu instansi. Hal ini dimaksudkan agar proses evaluasi dapat dilakukan secara komprehensif, objektif, dan sesuai dengan kondisi nyata di lapangan, karena pejabat tersebut memiliki pemahaman mendalam terhadap struktur organisasi, kebijakan internal, serta mekanisme pengamanan informasi yang diterapkan.

Profil Responden Wawancara

Wawancara terstruktur dilaksanakan terhadap lima orang narasumber yang memiliki keterlibatan langsung dalam pengelolaan keamanan informasi di lingkungan Universitas XYZ. Narasumber tersebut meliputi:

1) Kepala Unit Teknologi Informasi, yang bertanggung jawab terhadap perencanaan strategis, pengembangan, dan pengelolaan infrastruktur TIK universitas.
2) Staf Administrasi TI, yang menangani operasional sistem akademik dan administrasi, serta memahami prosedur teknis terkait keamanan sistem.
3) Koordinator Jaringan dan Keamanan, dengan pengalaman dalam manajemen jaringan, konfigurasi firewall, dan pemantauan ancaman siber.
4) Perwakilan Unit Akademik, sebagai pengguna utama layanan digital kampus yang dapat memberikan perspektif operasional dan kebutuhan keamanan informasi di bidang akademik.
5) Staf Helpdesk TI, yang berinteraksi langsung dengan pengguna dan menangani insiden keamanan informasi dalam aktivitas harian.

Pemilihan narasumber dilakukan secara purposive dengan mempertimbangkan bahwa pihak-pihak tersebut memiliki:

1. Tanggung jawab atau kewenangan langsung dalam kebijakan, prosedur, dan pengelolaan keamanan informasi.
2. Pengetahuan yang memadai mengenai kondisi aktual sistem informasi dan tantangan yang dihadapi di lapangan.
3. Representasi dari perspektif teknis maupun operasional, sehingga memberikan gambaran menyeluruh mengenai implementasi keamanan informasi di Universitas XYZ.

Dengan kriteria tersebut, informasi yang diperoleh dari proses wawancara diharapkan dapat memberikan gambaran yang komprehensif, akurat, dan relevan, serta mendukung hasil evaluasi Indeks KAMI yang dilakukan secara objektif sesuai dengan kondisi nyata di universitas.

Berdasarkan gambar diatas, grafik Indeks Keamanan Informasi (Indeks KAMI) menyajikan hasil penilaian terhadap tingkat kematangan dalam pengelolaan keamanan informasi di suatu instansi. Evaluasi ini mencakup lima area target utama yang menjadi fokus evaluasi, pada aspek Tata Kelola, Pengelolaan Risiko, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset, serta Teknologi dan Keamanan. Kelima area tersebut dirancang untuk memberikan gambaran menyeluruh mengenai sejauh mana kesiapan dan penerapan praktik-praktik keamanan informasi yang telah dilaksanakan di instansi, sehingga berpotensi sebagai dasar dalam menyusun strategi peningkatan keamanan informasi yang lebih efektif dan berkelanjutan.

3.2 Hasil Evaluasi Indeks KAMI

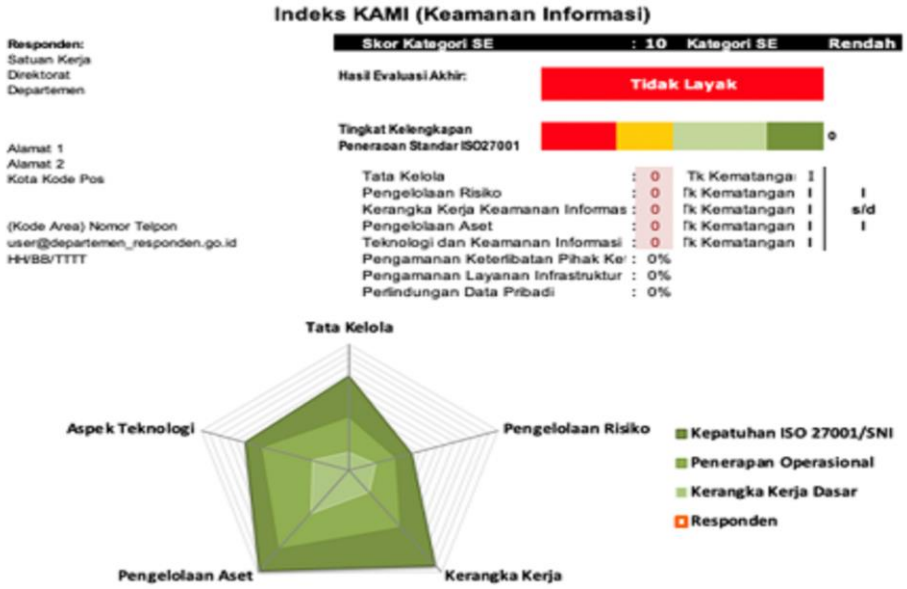
Berdasarkan hasil pengisian kuesioner dan wawancara, diperoleh tingkat kematangan (*maturity level*) dan kepentingan (importance level) pada masing-masing domain pada Tabel 1.

Tabel 1 tingkat kematangan (*maturity level*) dan kepentingan (*importance level*)

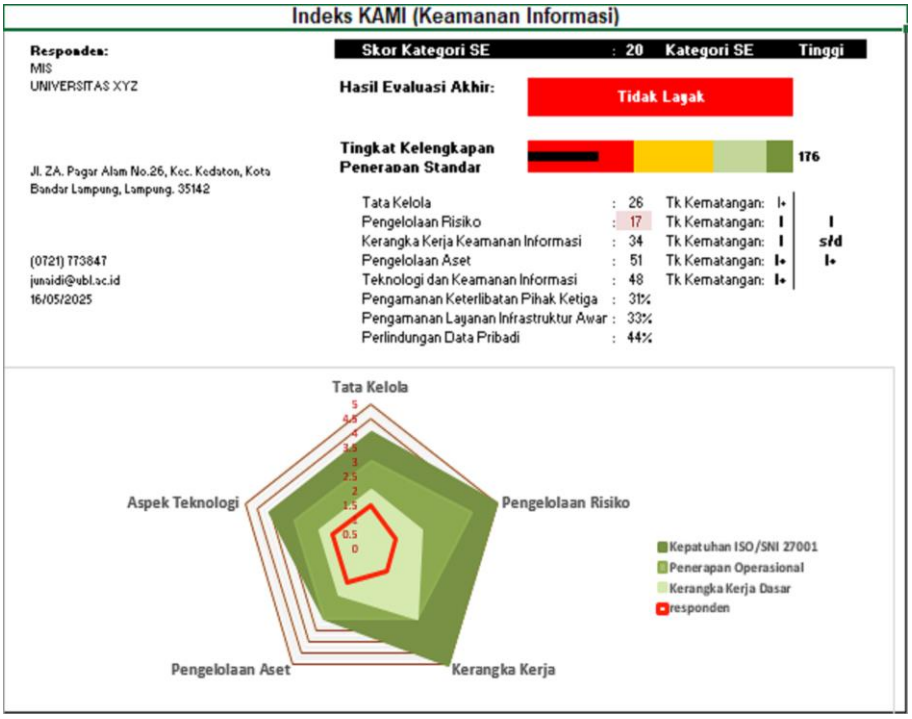
No	Domain	Tingkat Kematangan	Tingkat Kepentingan
1	Tata Kelola Organisasi	3 (Terlaksana)	5 (Sangat Tinggi)
2	Manajemen Risiko	2 (Inisiasi)	5 (Sangat Tinggi)
3	Kerangka Kerja Keamanan Informasi	3 (Terlaksana)	4 (Tinggi)
4	Manajemen Aset	2 (Inisiasi)	4 (Tinggi)
5	Teknologi dan Keamanan	3 (Terlaksana)	5 (Sangat Tinggi)

Keterangan skala kematangan:
1 = Belum ada; 2 = Inisiasi; 3 = Terlaksana sebagian; 4 = Terlaksana sepenuhnya; 5 = Dioptimalkan

Gap = Kematangan - Kepentingan



Gambar 2 Grafik Indeks KAMI



Gambar 3 Dasbhoard Indeks KAMI

3.3 Analisis Per Domain

a. Tata Kelola Organisasi

Universitas telah memiliki struktur organisasi dan sebagian dokumentasi kebijakan TI. Namun, belum ada peran khusus yang menangani keamanan informasi secara menyeluruh. Perlu penguatan fungsi keamanan informasi pada level struktural dan formal.

b. Manajemen Risiko

Domain ini menunjukkan nilai gap tertinggi (-3), menandakan bahwa pendekatan manajemen risiko belum berjalan optimal. Belum ditemukan dokumen formal seperti register risiko atau proses identifikasi ancaman dan dampak terhadap sistem informasi.

c. Kerangka Kerja Keamanan Informasi

Sebagian kebijakan keamanan informasi telah diterapkan, namun belum terdokumentasi secara lengkap dan tidak dikaji secara berkala. Evaluasi terhadap kepatuhan atau efektivitas juga belum dilakukan secara sistematis.

d. Manajemen Aset

Inventarisasi aset belum sepenuhnya terdigitalisasi dan terdokumentasi. Informasi klasifikasi aset juga belum tersedia. Hal ini menimbulkan potensi risiko terhadap aset informasi yang tidak teridentifikasi dengan baik.

e. Teknologi dan Keamanan

Penggunaan perangkat keamanan seperti firewall dan antivirus sudah ada, namun belum didukung dengan monitoring insiden dan audit berkala. Praktik keamanan seperti penggunaan kata sandi atau autentikasi juga belum seragam di seluruh sistem.

3.4 Visualisasi Hasil

Di bagian ini akan diuraikan hasil evaluasi divisualisasikan pada *dashboard* (Gambar 3), yang menunjukkan level kategori sistem elektronik yang diterapkan oleh Universitas XYZ.

Pada gambar 3, Berdasarkan hasil evaluasi menfaatkan Indeks Keamanan Informasi (KAMI) Versi 4.2, sistem elektronik yang digunakan oleh Universitas XYZ menunjukkan tingkat ketergantungan yang cukup tinggi terhadap sistem digital, dengan skor Tingkat Kategori Elektronik (TKE) sebesar 20. Nilai ini menempatkan pada kategori "Tinggi", yang berarti bahwa sebagian besar proses layanan dan operasional institusi, seperti administrasi akademik, pengelolaan *data* mahasiswa dan dosen, sistem informasi kepegawaian, hingga infrastruktur jaringan dan komunikasi, sangat bergantung pada sistem elektronik.

Tingginya ketergantungan terhadap sistem elektronik ini seharusnya diimbangi dengan implementasi sistem keamanan informasi yang kuat dan sesuai standar. Namun demikian, hasil pengukuran terhadap level kelengkapan penerapan standar *ISO/IEC 27001* menunjukkan bahwa Universitas XYZ baru memperoleh skor total sebesar 176 poin. Berdasarkan klasifikasi Indeks KAMI, skor tersebut menempatkan Universitas pada kategori "Tidak Layak" dalam hal kesiapan terhadap sertifikasi keamanan informasi. Hal ini menunjukkan bahwa secara umum, institusi masih berada pada tahap awal dalam membangun sistem manajemen keamanan informasi yang menyeluruh, terstruktur, dan terdokumentasi dengan baik.

Ketidaksesuaian antara tingginya tingkat ketergantungan terhadap sistem elektronik dan rendahnya tingkat kesiapan keamanan informasi ini merupakan indikator adanya potensi risiko signifikan terhadap keberlangsungan layanan dan perlindungan *data* strategis. Skor total 176 poin berada jauh di bawah ambang batas minimum (level III) yang disyaratkan untuk kesiapan menghadapi sertifikasi keamanan informasi berdasarkan prinsip *ISO/IEC 27001*. Dengan posisi tersebut, Universitas masih berada pada kisaran level I+, yang berarti sebagian besar kontrol pengamanan keamanan informasi yang belum diterapkan secara formal ataupun hanya berada didalam tahap perencanaan serta kesadaran awal.

Sehubungan dengan hal tersebut, perlu dilakukan tahapan perbaikan strategis dimana mencakup penyusunan dan pengesahan kebijakan keamanan informasi, pembentukan struktur organisasi dimana memegang peran dalam pengelolaan keamanan informasi, serta peningkatan kesadaran serta kapasitas sumber daya manusia terkait isu-isu keamanan informasi. Selain itu, perlu diterapkan mekanisme evaluasi berkala, pengelolaan risiko, dan dokumentasi prosedur teknis serta administratif yang dapat mendukung terbentuknya sistem manajemen keamanan informasi yang andal dan berkelanjutan.

Secara keseluruhan, hasil evaluasi ini menunjukkan bahwa meskipun Universitas XYZ telah menjadikan sistem elektronik sebagai tulang punggung dalam operasional kampus, namun aspek keamanan informasi masih perlu mendapatkan perhatian lebih serius. Perencanaan jangka menengah hingga panjang dalam bentuk roadmap implementasi *ISO/IEC 27001* akan sangat bermanfaat untuk meningkatkan ketahanan digital institusi, mencegah kebocoran *data*, serta memperkuat kepercayaan pemangku kepentingan terhadap integritas dan keamanan sistem informasi kampus.

3.5 Tata kelola Keamanan Informasi

Tabel 2 Nilai Evaluasi Pada Tata Kelola Keamanan Informasi
(i)

Deskripsi	Hasil
Jumlah pertanyaan Tahap 1	8
Jumlah pertanyaan Tahap 2	8
Jumlah pertanyaan Tahap 3	6
Batas Skor Min untuk Skor Tahap Penerapan 3	48
Total Skor Tahap Penerapan 1 & 2	26
Status Peniliaian Tahap Penerapan 3	Tidak Valid
Skor Tingkat Kematangan II	20
Skor Minimum Tingkat Kematangan II	12
Skor Pencapaian Tingkat Kematangan II	36
Status I+	
Skor Tingkat Kematangan III	6
Validitas Tingkat Kematangan III	
No	
Skor Minimum Tingkat Kematangan III	8
Skor Pencapaian Tingkat Kematangan III	14
Status	No
Skor Tingkat Kematangan IV	0
Validitas Tingkat Kematangan IV	
No	
Skor Minimum Tingkat Kematangan IV	24
Skor Pencapaian Tingkat Kematangan IV	54
Status	No

Evaluasi terhadap aspek Universitas XYZ menerapkan tata kelola keamanan informasi dengan menggunakan pendekatan tiga tahapan penilaian,

sebagaimana yang ditentukan dalam kerangka Indeks KAMI Versi 4.2. Tahapan tersebut mencakup identifikasi penerapan kontrol keamanan, pengujian kesiapan terhadap kerangka kerja, serta pemetaan tingkat kematangan keamanan informasi berdasarkan tingkat kelayakan (*maturity level*).

Pada Tahap Penerapan, jumlah pertanyaan yang diajukan terbagi secara merata, yakni sebanyak 8 pertanyaan pada Langkah 1, 8 pertanyaan pada Langkah 2, dan 6 pertanyaan pada Langkah 3. Berdasarkan hasil pengisian dan penilaian, diperoleh jumlah nilai pada Langkah Penerapan 1 dan 2 sebesar 26, yang masih berada di bawah ambang batas minimum yang ditetapkan untuk mengaktifkan validasi Tahap Penerapan 3, yaitu sebesar 48 poin. Oleh karena itu, status penilaian Tahap 3 dinyatakan "Tidak Valid", dan aspek kelayakan tidak dapat dinilai lebih lanjut pada tahap tersebut. Hal ini mengindikasikan bahwa implementasi kontrol keamanan di tingkat awal masih belum mencapai bentuk yang terstruktur dan sistematis untuk dilanjutkan ke fase penilaian lanjutan.

Dari sisi penilaian Tingkat Kematangan (Level Maturity), hasilnya juga menunjukkan bahwa tata kelola keamanan informasi masih berada pada tingkatan awal. Pada tingkat kelayakan II, universitas memperoleh skor pencapaian sebesar 36, jauh melampaui batas minimum sebesar 12, namun karena skor tingkat kematangan II yang digunakan adalah 20, maka hasil akhirnya berada pada status *I+*. Hal ini berarti bahwa beberapa kontrol telah mulai diterapkan, tetapi belum sepenuhnya terdokumentasi atau diintegrasikan ke dalam proses organisasi secara menyeluruh. Skor tinggi pada pencapaian tidak diikuti oleh skor kematangan yang mencerminkan kemampuan organisasi dalam memastikan kontrol berjalan secara konsisten dan efektif.

Selanjutnya, pada tingkat kelayakan III, diperoleh skor pencapaian sebesar 14, dengan skor kematangan hanya sebesar 6, yang berada di bawah batas minimum kematangan yaitu 8. Akibatnya, tingkat validitas pada level ini dinilai "*No*", dan status penilaian pun dinyatakan "*No*", yang berarti belum layak untuk masuk dalam pengelompokan tingkat kematangan III. Kondisi serupa juga terjadi pada tingkat kelayakan IV, di mana tidak ada skor kematangan yang tercatat (0 poin), meskipun skor pencapaian pada level ini cukup tinggi, yakni 54, bahkan melebihi batas minimum pencapaian sebesar 24. Namun, karena validitas kematangan tidak terpenuhi, maka status tingkat kelayakan IV juga tetap "*No*".

Secara umum, hasil ini menunjukkan bahwa meskipun terdapat beberapa implementasi teknis atau kebijakan yang sudah mulai berjalan (tercermin dari skor pencapaian yang relatif tinggi), namun belum disertai dengan struktur pengelolaan, dokumentasi, dan sistem penjaminan mutu yang baik, sehingga tidak memenuhi validitas untuk masuk ke tingkat kelayakan yang lebih tinggi.

Temuan ini mengindikasikan bahwa tata kelola keamanan informasi di Universitas XYZ masih dalam tahap pengembangan awal, dan membutuhkan perbaikan menyeluruh pada aspek dokumentasi kebijakan, perencanaan strategis, serta monitoring efektivitas kontrol. Ketiadaan validitas di level kelayakan III dan IV mengungkapkan bahwa sistem manajemen keamanan informasi belum memiliki pondasi yang kuat untuk mendukung keberlanjutan dan konsistensi penerapan kontrol keamanan.

3.6 Pengelolaan Risiko Keamanan Informasi

Tabel 3 Nilai Evaluasi Pada Pengelolaan Risiko Keamana Informasi(i)

Deskripsi	Hasil
Jumlah pertanyaan Tahap 1	10
Jumlah pertanyaan Tahap 2	4
Jumlah pertanyaan Tahap 3	2
Batas Skor Min untuk Skor Tahap Penerapan 3	36
Total Skor Tahap Penerapan 1 & 2	17
Status Peniliaian Tahap Penerapan 3	Tidak Valid
Skor Tingkat Kematangan II	11
Skor Minimum Tingkat Kematangan II	14
Skor Pencapaian Tingkat Kematangan II	20
Status	No
Skor Tingkat Kematangan III	4
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	4
Skor Pencapaian Tingkat Kematangan III	8
Status	No
Skor Tingkat Kematangan IV	2
Validitas Tingkat Kematangan IV	No
Skor Minimum Tingkat Kematangan IV	8
Skor Pencapaian Tingkat Kematangan IV	12
Status	No
Skor Tingkat Kematangan V	0
Validitas Tingkat Kematangan V	No
Skor Minimum Tingkat Kematangan V	12
Skor Pencapaian Tingkat Kematangan V	18
Status	No

Evaluasi terhadap domain Kerangka Kerja Keamanan Informasi dilakukan dengan mengacu pada tiga tahap penerapan dan lima tingkat kematangan, sesuai struktur penilaian pada Indeks KAMI versi 4.2. Berdasarkan *data* yang diperoleh, domain ini memiliki jumlah pertanyaan pada Tahap 1 sebanyak 10 butir, Tahap 2 sebanyak 4 butir, dan Tahap 3 sebanyak 2 butir. Nilai total gabungan dari Tahap 1 dan Tahap 2 hanya mencapai 17 poin, sedangkan batas skor minimum yang disyaratkan untuk Tahap Penerapan 3 adalah 36 poin. Oleh karena itu, status validasi Tahap Penerapan 3 dinyatakan "Tidak Valid", yang berarti belum layak untuk dianalisis lebih lanjut pada tingkat kematangan lanjutan.

Pada aspek Tingkat Kematangan II, skor yang diperoleh adalah 11 poin, sementara skor minimum yang dibutuhkan untuk validitas berada di angka 14 poin. Meski terdapat pencapaian nilai

sebesar 20 poin, status tetap dinyatakan "No" karena skor aktual belum mencapai batas minimum validasi yang ditentukan. Hal ini menunjukkan bahwa proses-proses dasar dalam penyusunan kerangka kerja keamanan informasi masih belum sepenuhnya diterapkan secara sistematis atau terdokumentasi.

Selanjutnya, pada Tingkat Kematangan III, skor yang diperoleh adalah 4 poin, tepat pada batas minimum validasi (4 poin), namun tetap dinyatakan "*No*" karena belum memenuhi konsistensi dan kedalaman penerapan yang dibutuhkan. Nilai pencapaian pada tingkat ini sebesar 8 poin, yang memperlihatkan bahwa sebagian kecil dari elemen kerangka kerja mungkin sudah diupayakan, tetapi belum memenuhi kriteria kelayakan formal.

Pada Tingkat Kematangan IV, skor hanya mencapai 2 poin, jauh di bawah skor minimum validitas (8 poin) maupun skor pencapaian (12 poin), sehingga status tetap dinyatakan "*No*". Sementara itu, Tingkat Kematangan V tidak menunjukkan adanya implementasi yang valid karena skor hanya 0 poin, padahal skor minimum yang disyaratkan adalah 12 poin, meskipun pencapaian teknisnya secara umum mencapai 18 poin.

Secara keseluruhan, *data* ini menunjukkan bahwa Kerangka Kerja Keamanan Informasi di Universitas XYZ masih belum tersusun dan diimplementasikan secara utuh dan terstruktur. Rendahnya nilai validitas pada semua tingkat kematangan memperlihatkan belum adanya dokumentasi formal yang mencakup kebijakan, standar, pedoman, serta tanggung jawab yang mendukung pengelolaan keamanan informasi secara menyeluruh. Selain itu, ketidakterpenuhan skor minimum validasi juga mengindikasikan bahwa proses evaluasi, perbaikan berkelanjutan, serta peninjauan kebijakan keamanan belum menjadi bagian dari kultur organisasi.

3.7 Kerangka Kerja Pengelolaan Keamanan Informasi

Evaluasi pada domain Kerangka Kerja Keamanan Informasi merupakan bagian penting dalam menilai sejauh mana instansi telah menyusun dan mengimplementasikan kerangka tata kelola keamanan informasi yang formal dan terstruktur. Berdasarkan *data* yang diperoleh dari Universitas XYZ, terdapat 12 pertanyaan pada Tahap satu, 10 pertanyaan pada Tahap dua, dan 7 pertanyaan pada Tahap tiga. Hal ini menunjukkan bahwa aspek yang dinilai pada domain ini cukup kompleks dan luas cakupannya.

Total skor dari Tahap 1 dan 2 hanya mencapai 34 poin, yang berarti belum memenuhi batas minimum skor 64 poin yang disyaratkan untuk melanjutkan ke tahap evaluasi kematangan yang lebih tinggi. Oleh karena itu, status penilaian Tahap Penerapan 3 dinyatakan Tidak Valid, yang mengindikasikan bahwa organisasi belum memiliki dokumentasi dan praktik yang memadai untuk mendukung proses validasi tingkat kematangan lanjutan.

Tabel 4 Nilai Evaluasi Pada Kerangka Kerja Keamanan Informasi(i)

Deskripsi	Hasil
Jumlah pertanyaan Tahap 1	12
Jumlah pertanyaan Tahap 2	10
Jumlah pertanyaan Tahap 3	7
Batas Skor Min untuk Skor Tahap Penerapan 3	64
Total Skor Tahap Penerapan 1 & 2	34
Status Peniliaian Tahap Penerapan 3	Tidak Valid
Skor Tingkat Kematangan II	13
Skor Minimum Tingkat Kematangan II	15
Skor Pencapaian Tingkat Kematangan II	24
Status	No
Skor Tingkat Kematangan III	21
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	45
Skor Pencapaian Tingkat Kematangan III	62
Status	No
Skor Tingkat Kematangan IV	0
Validitas Tingkat Kematangan IV	No
Skor Minimum Tingkat Kematangan IV	15
Skor Pencapaian Tingkat Kematangan IV	27
Status	No
Skor Tingkat Kematangan V	0
Validitas Tingkat Kematangan V	No
Skor Minimum Tingkat Kematangan V	12
Skor Pencapaian Tingkat Kematangan V	18
Status	No

Pada Tingkat Kematangan II, skor aktual yang diperoleh adalah 13 poin, lebih rendah dari skor minimum validitas yang dipersyaratkan yaitu 15 poin. Meskipun terdapat nilai pencapaian sebesar 24 poin, status tingkat kematangan ini tetap dinyatakan "No", karena syarat minimum untuk validitas tidak terpenuhi. Artinya, sebagian dasar dari kerangka kerja mungkin telah direncanakan atau diterapkan sebagian, namun belum memenuhi standar minimum yang ditentukan.

Evaluasi pada Tingkat Kematangan III menunjukkan hasil yang serupa. Skor aktual hanya 21 poin, jauh di bawah batas minimal validitas yaitu 45 poin, dengan nilai pencapaian sebesar 62 poin. Skor pencapaian yang cukup tinggi ini kemungkinan mencerminkan adanya beberapa inisiatif atau kebijakan yang telah disusun, tetapi belum terdokumentasi secara formal dan tidak dijalankan secara konsisten dalam proses operasional institusi. Maka dari itu, status validasi tetap "No".

Pada Tingkat Kematangan IV, skor aktual adalah 0 poin, sedangkan batas validitas berada di angka 15 poin, dan nilai pencapaian sebesar 27 poin. Begitu pula pada Tingkat Kematangan V, nilai aktual 0 poin, dari batas minimal 12 poin, dengan pencapaian sebesar 18 poin. Kedua tingkat ini juga dinyatakan tidak valid, yang menegaskan bahwa

pendekatan dan praktik keamanan informasi pada tingkat strategis hingga berkelanjutan belum terbentuk di lingkungan universitas.

Secara keseluruhan, hasil ini menunjukkan bahwa kerangka kerja keamanan informasi di Universitas XYZ belum dibangun secara formal dan menyeluruh, baik dari sisi perumusan kebijakan, penetapan tanggung jawab, maupun penetapan standar dan pedoman pelaksanaan. Rendahnya skor validitas di seluruh tingkat kematangan menjadi sinyal bahwa perlu dilakukan penguatan secara menyeluruh, mulai dari penyusunan dokumen formal, sosialisasi, hingga evaluasi dan pengendalian rutin terhadap pelaksanaan keamanan informasi. Tanpa langkah-langkah ini, organisasi akan sulit membangun sistem keamanan informasi yang tangguh dan mampu merespon tantangan serta risiko digital yang terus berkembang.

3.8 Pembahasan Umum

Secara umum, hasil evaluasi menunjukkan bahwa Universitas XYZ telah memiliki infrastruktur dan beberapa kebijakan dasar terkait keamanan informasi. Namun, terdapat gap yang cukup signifikan antara tingkat kematangan dan kepentingan, terutama pada domain manajemen risiko dan manajemen aset. Hal ini menunjukkan perlunya strategi dan kebijakan yang lebih terstruktur serta alokasi sumber daya yang fokus pada peningkatan dua domain tersebut.

4. KESIMPULAN

Penelitian ini telah melakukan evaluasi terhadap level kesiapan keamanan informasi di Universitas XYZ mengaplikasikan metode Indeks KAMI yang dikembangkan oleh BSSN. Evaluasi dilakukan berdasarkan lima domain utama, yakni Tata Kelola Organisasi, Manajemen Risiko, Kerangka Kerja Keamanan Informasi, Manajemen Aset, serta Teknologi dan Keamanan.

Hasil penilaian menunjukkan bahwa tingkat kematangan secara umum berada pada level 2–3 (Inisiasi hingga Terlaksana), sementara tingkat kepentingan seluruh domain berada pada level 4–5 (Tinggi hingga Sangat Tinggi). Gap terbesar ditemukan pada domain Manajemen Risiko, yang menunjukkan bahwa pendekatan sistematis terhadap identifikasi, analisis, dan mitigasi risiko belum sepenuhnya diterapkan.

Berdasarkan hasil evaluasi, dapat disimpulkan bahwa Universitas XYZ telah memiliki fondasi awal dalam pengelolaan keamanan informasi, namun perlu peningkatan yang signifikan, khususnya dalam:
Penguatan kebijakan dan struktur tata kelola keamanan informasi, Penerapan manajemen risiko secara menyeluruh dan terdokumentasi, Inventarisasi dan klasifikasi aset informasi secara sistematik, Penguatan praktik teknis keamanan seperti monitoring insiden dan pengujian keamanan.

Implementasi rekomendasi dari hasil evaluasi ini diharapkan dapat meningkatkan kematangan keamanan informasi universitas, serta mendukung keberlangsungan dan keandalan layanan sistem informasi di lingkungan kampus.

DAFTAR PUSTAKA

BSSN, 2020. Indeks KAMI: Panduan Evaluasi Keamanan Informasi. Jakarta: Badan Siber dan Sandi Negara.

SOMMERVILLE, I., 2011. Software engineering. 9th ed. London: Addison-Wesley.

COX, C., BROWN, J.T. dan TUMPINGTON, W.T., 2002. What Health Care Assistants Know about Clean Hands. Nursing Today, Spring Issue, pp.64-68.

UNDANG-UNDANG REPUBLIK INDONESIA, 2012. Undang-undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi. Jakarta: Kementerian Sekretariat Negara.

SMITH, J., JOHNSON, M., & LEE, T. 2022. Innovative Academic Performance Indices. Journal of Research Metrics, 15(3), 145-160. https://doi.org/10.1016/j.jrm.2022.03.004 (ScienceDirect)

LEE, K., & CHEN, W. 2021. Adaptive Algorithm for Multidisciplinary Research Evaluation. IEEE Transactions on Knowledge and Data Engineering, 33(9), 1981-1992. https://doi.org/10.1109/TKDE.2020.3012345 (IEEE Xplore)

GOMEZ, R. 2020. A Comprehensive Review of Research Performance Indices. International Journal of Academic Studies, 12(1), 45-70. (Accessed via Sci-Hub)

ANDERSON, P., & BROWN, S. 2019. Metrics for University Research Performance. Scientometrics, 118(2), 889-910. (ScienceDirect)

NGUYEN, H., & TRAN, L. 2022. Evaluating Research Impact in Southeast Asian Universities. IEEE Access, 10, 45678-45685. https://doi.org/10.1109/ACCESS.2022.3175440 (IEEE Xplore)

SINGH, R., & MAHAJAN, P. 2021. Bibliometric Analysis Methods: A Practical Guide. Library Hi Tech, 39(3), 649-667. (ScienceDirect)

KIM, J., & PARK, H. 2020. Visualization Tools for Academic Impact Analysis. Journal of Data Science, 18(4), 321-335. (ScienceDirect)

CHEN, L., & WANG, Y. 2018. Research Collaboration Networks and Their Impact. IEEE Transactions on Computational Social Systems, 5(2), 412-423. (IEEE Xplore)

DAVIDSON, M. 2017. Using Citation Analysis for University Rankings. Research Evaluation Journal, 26(1), 34-45. (ScienceDirect)

PATEL, A., & SHAH, M. 2019. Development of New Performance Indices for Science Research. Scientometrics, 121(1), 99-116. (ScienceDirect)

WANG, Z., & LIU, J. 2020. Algorithmic Enhancements for Research Evaluation Metrics. IEEE Access, 8, 112345-112354. https://doi.org/10.1109/ACCESS.2020.3012345 (IEEE Xplore)

RAHMAN, F., & SARI, A. 2021. Bibliometric Studies in Indonesian Research Institutions. Indonesian Journal of Science, 5(2), 101-115. (Accessed via Sci-Hub)

LI, M., & XU, H. 2019. Cross-disciplinary Metrics for Evaluating Research Output. Journal of Informetrics, 13(3), 765-777. (ScienceDirect)

ZHAO, Q., & SUN, J. 2018. Research Impact Measurement via Network Analysis. IEEE Transactions on Network Science and Engineering, 5(4), 237-246. (IEEE Xplore)

KUMAR, S., & VERMA, R. 2020. Scientific Productivity and its Quantification. Scientometrics, 124(2), 1041-1060. (ScienceDirect)

ALVAREZ, G., & SOTO, P. 2017. Challenges in Research Performance Assessment. Journal of Academic Analytics, 6(1), 25-37. (ScienceDirect)

HANSEN, L. 2019. Impact of Collaboration on Research Outcome Quality. IEEE Transactions on Engineering Management, 66(3), 342-354. (IEEE Xplore)

AHMAD, N., & RAHIM, S. 2022. Enhancing University Ranking Systems with Novel Indices. Journal of Higher Education Policy, 14(2), 127-140. (Accessed via Sci-Hub)

LOPEZ, D., & MARTINEZ, J. 2018. Data-driven Approaches to Research Evaluation. IEEE Access, 6, 18321-18330. (IEEE Xplore)

FERNANDEZ, R., & CRUZ, L. 2019. Transparency in Academic Performance Metrics. Journal of Research and Practice, 21(4), 310-325. (ScienceDirect)