Evaluasi Tingkat Keamanan Informasi SIA UIN SUKA Berdasarkan Indeks KAMI (Information Security) 4.0.

Muhammad Haedar Zhafran Hidayatullah [a,1*], Wicaksono Yuli Sulistyo [b,2],

Septia Ayu Pratiwi [b,3]

[a,b]Program Studi PJJ Sistem Informasi Universitas Siber Muhammadiyah, Pakuncen, Wirobrajan, Kota Yogyakarta 55253, Indonesia
[1] haedarzhafran@sibermu.ac.id *; [2] wicaksono@sibermu.ac.id; [3] pratiwi@sibermu.ac.id
* Korespondensi penulis

Submission:23/04/2025, Revision: 25/04/2025, Accepted: 01/05/2025

Abstract

Information is a highly valuable asset for organizations. Therefore, it becomes one of the main targets for exploitation through various attacks. The primary goal of information system security is to maintain three key attributes: confidentiality, integrity, and avaibility. UIN Sunan Kalijaga has work units responsible for managing and providing information. It is necessary to conduct an evaluation of information system security to gain an understanding of the current state of readiness and maturity of information security. The information Security Index, abbreviated as KAMI, is an evaluation tool issued by the Ministry of Communication and Information Technology that functions to analyze the level of information security within an institution. It has been found that the maturity level of information security at UIN Sunan Kalijaga is still relatively low and requires improvements to address the deficiencies found in its information security management system

Keywords: Information Security, Security Maturity Assesment, KAMI Index

Abstrak

Informasi adalah asset organisasi yang sangat berharga. Oleh sebab itu informasi menjadi salah satu objek serangan untuk dieksploitasi. Tujuan utama keamanan sistem informasi adalah menjaga 3 (tiga) atribut yaitu kerahasiaan (*confidentiality)*, keutuhan (*integrity*) dan ketersediaan (*availability*). UIN Sunan Kalijaga memiliki unit kerja yang mempunyai tugas dan kewajiban untuk mengelola dan memberikan informasi. Perlu dilakukan evaluasi keamanan sistem informasi untuk mendapatkan gambaran kondisi kesiapan dan kematangan keamanan informasi. Indeks keamanan informasi disingkat KAMI adalah alat evaluasi yang dirilis oleh Kementrian Komunikasi dan Informasi yang berfungsi untuk menganalisa tingkat keamanan informasi di instansi. Didapati tingkat kematangan keamanan informasi di UIN Sunan Kalijaga masih tergolong rendah dan butuh perbaikan untuk kekurangan yang ditemukan di sistem manajemen keamanan informasi.

Kata kunci: Keamanan Sistem Informasi, Evaluasi Keamanan Sistem, Indeks KAMI

1. Pendahuluan

Di zaman yang modern ini, hampir seluruh data dan informasi kini sangat mudah diakses dan didapatkan [1][2]. Perkembangan teknologi informasi dan komunikasi yang sangat pesat juga mendorong berbagai bidang kehidupan mulai dari instansi, ekonomi hingga pendidikan seperti UIN Sunan Kalijaga yang memanfaatkan perkembangan teknologi informasi dan komunikasi untuk melaksanakan berbagai macam aktifitas yang dilakukan oleh mahasiswa. Seperti pendaftaran, pemilihan mata kuliah, nilai, hingga dosen yang memberi nilai ada pada sistem informasi tersebut yang bernama SIA. Sehingga, informasi dapat dikatakan sebagai aset yang sangat berharga bagi individu yaitu mahasiswa, dosen, sekalipus kampus [3].

Tata kelola teknologi informasi dan komunikasi yang baik dapat memberikan banyak manfaat bagi organisasi pada level eksekutif untuk mencapai tujuan strategis organisasi tersebut. Terkait tata kelola

teknologi informasi dan komunikasi, khususnya pada bidang keamanan informasi, sesuai dengan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 yang dikeluarkan pada tanggal 11 April 2016 tentang Sistem Manajemen Pengamanan Informasi (SMPI) maka UIN Sunan Kalijaga harus melakukan pengamanan terhadap informasi-informasi yang dikelola [4].

Melihat kondisi SIA pada UIN Sunan Kalijaga khususnya pada keamanan informasi, perlu dilakukan evaluasi, mengingat keamanan informasi yang buruk dapat mengganggu kinerja dari tata kelola informasi dan komunikasi apabila informasi yang dimiliki mengalami masalah yang berhubungan dengan karahasiaan, integritas, dan ketersediaan. Evaluasi menggunakan alat bantu yang telah memiliki standar yang dikeluarkan oleh Kementrian Komunikasi dan Informatika berdasarkan peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016. Indeks KAMI dibuat dengan acuan ISO 27001:2018 yang berisi tentang Keamanan Informasi. ISO 27001 adalah suatu bentuk kerangka kerja standar internasional yang berisi tentang standar-standar dalam area keamanan informasi, lingkup penggunaan teknologi dan pengelolaan asset yang membantu organisasi memastikan bahwa keamanan informasi sudah berjalan dengan efektif [5][6].

Indeks KAMI (Keamanan Informasi) 4.0 berfungsi sebagai perangkat lunak untuk memberikan gambaran kondisi tingkat keamanan informasi pada sistem informasi suatu instansi [7].

Indeks KAMI menganalisis keamanan informasi yang mencakup aspek pembenahan, pembangunan dan penerapan. Data yang dihasilkan oleh evaluasi ini akan memberikan gambaran tingkat keamanan informasi yang diterapkan dan kemudian dianalisis sehingga indeks KAMI juga digunakan sebagai pembanding untuk melakukan perbaikan pada sistem informasi UIN Sunan Kalijaga [8].

Proses evaluasi indeks KAMI dilakukan pada enam area meliputi area tata kelola keamanan informasi. Area kedua adalah pengamanan risiko dimana area ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi [9]. Area kerangka kerja pengelolaan keamanan informasi yang akan mengevaluasi kelengkapan dan kesiapan kerangka kerja pengelolaan keamanan informasi dan strategi penerapannya. Area keempat adalah pengelolaan asset informasi yang akan mengevaluasi kelengapan pengamanan asset informasi. Area kelima, teknologi dan keamanan informasi yang mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi keamanan asset informasi [10]. Terdapat satu area baru pada indeks KAMI 4.0 dibandingkan dengan versi sebelumnya yaitu versi 3.1 dengan area suplemen yang mengevalusai aspek pengamanan keterlibatan pihak ketiga sebagai penyedia layanan, Layanan berbasi cloud, dan perlindungan data pribadi [11].

Pada penelitian sebelumnya yang dilakukan oleh Rizki Dewantara pada tahun 2021 yang menerangkan bahwa data indeks keamanan informasi (KAMI) didapatkan melalui pengisian kuisioner mengenai evaluasi manajemen keamanan informasi pada Jaringan UIN Sunan Kalijaga selanjutnya hasil kuesioner baru dibandingkan dengan hasil kuisioner sebelumnya [4]. Berdasarkan tingkat kelengkapan dan kelayakan nilai indeks KAMI yang diuji pada jaringan UIN Sunan Kalijaga masih rendah. Tingkat rendahnya karena beberapa faktor internal. Maka dari itu, dalam penelitian ini akan mengevaluasi kembali tingkat kelayakan dari sistem informasi UIN Sunan Kalijaga dengan parameter indeks KAMI (*Information Security*) 4.0. Penelitian ini dilakukan untuk meningkatkan kredibilitas mahasiswa, dosen dan kampus terkait data pribadi yang ada pada SIA UIN Sunan Kalijaga.

2. Metode Penelitian

Tabel 1. Alur Penelitian

No	Tahapan	Input	Proses	Output
1	Persiapan	Telaah Dokumen Bisnis	Studi Literatur	Identifikasi Masalah
2	Desain Penelitian	Identifitasi Organisasi	Penelitian INDEKS KAMI	Kuisioner/Wawancara, Batasan Masalah
3	Pengumpulan Data dan Analisa Data	Populasi dan Sampel, Analisis Data Kuisioner	Analisis Tingkat Kapabilitas	Nilai Tingkat Kematangan, Saran Rekomendasi
4	Penyusunan Laporan	Saran Rekomendasi	Studi Literatur	Laporan Hasil Penelitian, Kesimpulan, dan Saran

Tahap persiapan dalam penelitian ini adalah peneliti melakukan telaah dokumen bisnis dan studi literature. Dimana peneliti nantinya akan melakukan pencarian dasar-dasar teori dan penemuan dari penelitian yang telah dilakukan sebelumnya. Teori-teori yang terkait dengan permasalahan penelitian indeks KAMI dan

penelitian yang menggunakan indeks KAMI versi lainnya atau penelitian yang menggabungkan beberapa model evaluasi akan dipelajari dan dirangkum secara singkat sesuai dengan kebutuhan penelitian ini. Keluaran yang didapatkan dari tahap persiapan yaitu identifikasi permasalahan TIK yang ada di UIN Sunan Kalijaga [12].

Pada tahapan desain penelitian, peneliti melakukan identifikasi organisasi dan penilaian Indeks KAMI. Identifikasi organisasi berisi tentang visi, misi, struktur organisasi, rencana strategis UIN SUKA tentang TI dan laporan hasil audit. Indeks KAMI adalah perangkat untuk mengevaluasi penerapan tata kelola keamanan informasi yang dilakukan secara berkelanjutan, dan digunakan untuk memberikan gambaran kemajuan hasil penerapan secara berkala. Apabila terjadi perubahan pada infrastruktur atau unit kerja yang ada dalam lingkup awal evaluasi indeks KAMI, pengkajian ulang bermanfaat untuk memastikan kelengkapan dan kematangan bentuk tata kelola yang diterangkan di awal. Keluaran yang didapatkan dari tahap desain penelitian yaitu kuisioner, wawancara dan batasan masalah yang dibutuhkan agar pembahasan mengarah pada tujuan dan tidak meluas [13].

Pada tahap pengumpulan dan analisa data, peneliti menentukan populasi, sampel dan teknik analisis data yang diperlukan. Populasi dalam penelitian ini adalah seluruh pengelola dan pengguna layanan SIA UIN Sunan Kalijaga. Teknik sampling yang digunakan adalah *accidental sampling*, yaitu teknik pengambilan sampel berdasarkan subjek yang tersedia dan bersedia saat penelitian dilakukan. Sebanyak 10 orang informan terlibat dalam penelitian ini. Data yang terkumpul dari setiap responden dipetakan ke dalam domain utama Indeks KAMI yaitu tata kelola, pengelolaan resiko, kerangka kerja, pengelolaan aset, dan aspek teknologi. Setiap domain dinilai berdasarkan skor kelengkapan dan kematangan, kemudian dibandingkan dengan level skala 0-5. Selain itu, analisa juga mencakup interprestasi kesenjangan *(gap analysis)* antara kondisi aktual dan standar ISO/IEC 27001, hasil analisis menghasil pemetaan tingkat kesiapan setiap area keamanan informasi yang diteliti, serta saran dan rekomendasi teknis yang dapat diimplementasikan oleh institusi untuk peningkatan keamanan informasi secara berkelanjutan. [14].

Pada tahap yang terakhir yaitu penyusunan laporan, peneliti memasukan saran rekomendasi dan studi literatur. Keluaran dari tahapan ini yaitu laporan hasil penelitian, kesimpulan dan saran [15].

3. Hasil dan Pembahasan

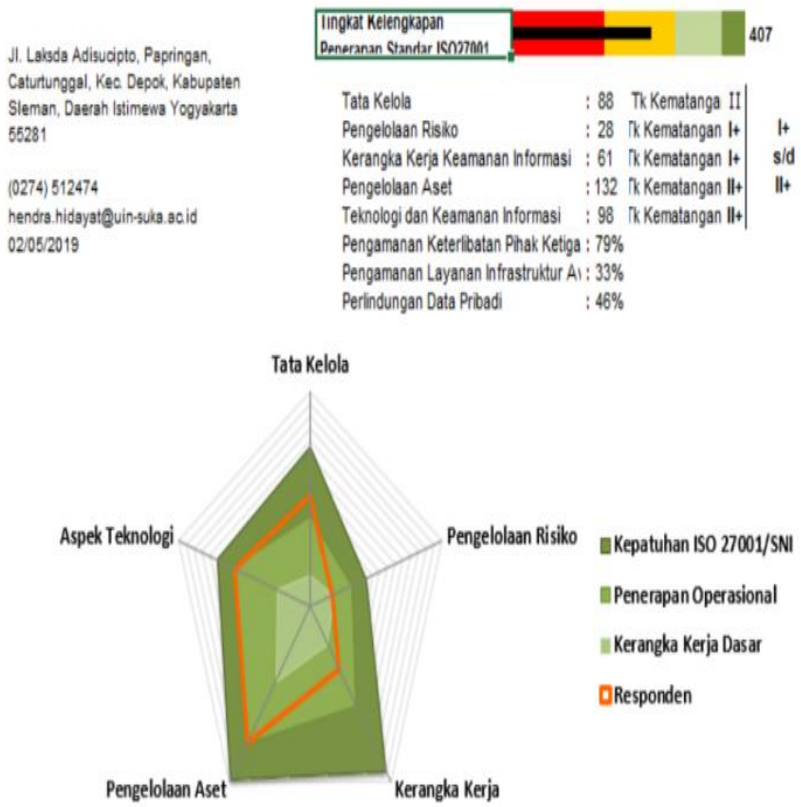
Pada tahap ini pengumpulan data yang menggunakan instrument kuisioner yang diisi oleh responden akan menjadi hasil evaluasi akhir, tingkat kelengkapan dan skor pada target area. Setelah mengisi kuisioner maka perlu dilakukan validasi atau konfirmasi dengan metode checklist terkait bukti. Selain itu, dengan membandingkan ISO/IEC 27001:2013 akan menghasilkan rekomendasi-rekomendasi perbaikan yang diperlukan oleh UIN Sunan Kalijaga. Jika dibandingkan dengan penelitian terdahulu oleh Dewantara dan Sugiantoro (2021), ditemukan bahwa hasil evaluasi indeks KAMI pada UIN Sunan Kalijaga juga menunjukan kematangan informasi yang belum optimal. Namun pada penelitian ini, evaluasi dilakukan lebih komprehensif mencakup enam domain versi terbaru (4.0) yang mencakup area tambahan yaitu Suplemen. Selain itu dilakukan pendekatan triangulasi dengan validasi data melalui metode checklist dan pembandingan dengan SNI ISO/IEC 27001 hal ini memberikan pemetaan lebih rinci terkait aspek mana saja yang mengalami peningkatan maupun stagnasi.

Tabel 2. Skor Area Evaluasi UIN SUKA

Arean	SKor
Tata Kelola Keamanan Informasi	88
Pengelolaan Resiko	28
Kerangka Kerja Keamanan Informasi	61
Pengelolaan Aset	132
Teknologi dan Keamanan Informasi	98

Berdasarkan gambar 1, menunjukan tingkat kategori system eletronik yang digunakan oleh Jaringan UIN Sunan Kalijaga sangat bergantung besar pada penggunaan system elektronik. Sementara dari tingkat kelengkapan penerapan standar ISO 27001 berada pada level "Pemenuhan Kerangka Kerja Dasar" dengan level 407, hal ini menunjukan tingginya ketergantungan instansi terhadap system elektronik. Namun, tidak didukung dengan keamanan informasi yang memadai. Dengan hasil evaluasi akhir ini juga menunjukan bahwa jaringan UIN Sunan Kalijaga masih membutuhkan perbaikan hingga saat ini. Hal ini ditunjukan dari tingkat kelayakan yang rata-rata menduduki level I+ dan II+ sehingga untuk kesiapan sertifikasi masih dikatakan

belum layak sertifikasi keamanan informasi, karena untuk mencapai batas minimum kesiapan sertifikasi keamanan informasi adalah tingkat III.



Gambar 1. Hasil Evaluasi Akhir dan Tingkat Kelengkapan Penerapan Standar ISO27001

Berdasarkan informasi pada Gambar 1 dapat disimpulkan bahwa:

1) Peran/tingkat kepentingan TIK di UIN Sunan Kalijaga berada pada level tinggi (Skor: 88)

2) Sementara dari tingkat kelengkapan penerapan SMKI, UIN Sunan Kalijaga berada pada level "Kurang Layak", area "Merah" yang merupakan jumlah dari seluruh skor rata-rata disetiap area Keamanan yang dievaluasi.

Tingkat kelengkapan penerapan SMKI juga dapat dilihat pada Gambar 1 ~~diatas~~, diagram berwarna merah merupakan kondisi SMKI Univeritas Islam Negri Sunan Kalijaga berdasarkan hasil pengisian kuesioner oleh para informan Dapat dicermati bahwa:

1) Dari kelima area keamanan informasi yang diamati, tampak bahwa Universitas Islam Negeri Sunan Kalijaga telah memiliki aspek Teknologi dan Tata Kelola yang jauh lebih baik dibanding area keamanan lainnya (paling mendekati standar yang ditetapkan dalam proses penerapan).

2) Pada area kerangka kerja mencapai kerangka kerja dasar, kecuali pada area pengelolaan asset dan pengelolaan risiko tampak bajwa Universitas Islam Negeri Sunan Kalijaga tergolong tidak mencapai, kerangka kerja dasar ini sangat perlu diperbaiki untuk meningkatkan pengamanan informasi.

Tingkat kelengkapan SMKI Universitas Islam Negeri Sunan Kalijaga berdasarkan hasil pengumpulan data indeks KAMI menunjukan pada area merah. Pencapaian ini memberikan petunjuk bahwa SMKI yang memerlukan perbaikan pada sejumlah aspek.

Prioritas perbaikan aspek-aspek tersebut berdasrkan diagram radar gambar 1 dan persetase capaian skor informan pada tabel 2 adalah Kerangka Kerja Pengelolaan Keamanan Informasi, Tata Kelola Keamanan Informasi, Pengelolaan Aset Informasi, Teknologi Keamanan Informasi, dan Pengelolaan Risiko Keamanan Informasi.

Skor Kerangka kerja mempunyai nilai 61 dengan tingkat keamanan mencapai I+. Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, UIN SUKA perlu melakukan perbaikan diantaranya:

1) Kebijakan dan prosedur keamanan informasi harus disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya.

2) Kebijakan keamanan informasi harus ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkan.

3) Menyediakan mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan infomasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.

4) Menyediakan mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait.

5) Kebijakan dan prosedur keamanan informasi yang ada harus merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi.

6) Mencantumkan pelaporan insiden, menjaga kerahasiaan, haki, tata tertib penggunaan dan pengamanan asset.

7) Membuat konsekwensi dari pelanggaran kebijakan keamanan informasi yang sudah didefinisikan, dikomunikasikan dan ditegakkan.

8) Membuat prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi.

9) Menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul.

10) Menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul.

11) Menerapkan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya.

12) Melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada.

Skor pengelolaan resiko keamanan informasi dengan nilai 28. Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, UIN SUKA perlu melakukan perbaikan diantaranya:

1) Membuat kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.

2) Membuat kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi.

3) Menetapkan ambang batas tingkat risiko yang dapat diterima.

4) Mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.

5) Menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi).

6) Memantau status penyelesaian langkah mitigasi risiko secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya.

7) Melakukan evaluasi terhadap penyelesaian langkah mitigasi yang sudah diterapkan untuk memastikan konsistensi dan efektifitasnya.

8) Mengkaji ulang secara berkala profil risiko berikut bentuk mitigasinya untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru.

Skor tata kelola dengan nilai 88. Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, UIN SUKA perlu melakukan perbaikan diantaranya:

1) Mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi.

2) Menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi.

3) Pengelola keamanan informasi harus menerapkan dan menjamin kepatuhan pengamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (aparat keamanan).

4) Mendefinisikan dan mengalokasikan tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans).

Skor pengelolaan asset Keamanan Informasi dengan nilai 132. Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, UIN SUKA perlu melakukan perbaikan diantaranya:

1) Membuat Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.

2) Mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya.

3) Menyediakan tingkatan akses yang berbeda dan matrix yang merekam alokasi akses.

4) Menyediakan pengelolaan perubahan terhadap sistem (termasuk perubahan konfigurasi) yang diterapkan secara konsisten.

5) Menyediakan pengelolaan konfigurasi yang diterapkan secara konsisten.

6) Membuat proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi.

7) Mendefinisikan tanggung jawab pengamanan informasi secara individual untuk semua personil.

8) Membuat Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI, Peraturan pengamanan data pribadi.

9) Menetapkan waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data.

10) Membuat Prosedur penghancuran data/aset yang sudah tidak diperlukan

11) Membuat Prosedur kajian penggunaan akses (*user access review)* dan langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku.

12) Menerapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang.

13) Membuat proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik.

14) Membuat peraturan pengamanan perangkat komputasi milik Instansi apabila digunakan di luar lokasi kerja resmi (kantor).

15) Menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai untuk konstruksi ruang penyimpanan perangkat pengolah informasi penting.

16) Membuat proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting.

17) Membuat mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.

18) Membuat peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya (misalnya larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll).

Skor teknologi keamanan informasi dengan nilai 98. Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, UIN SUKA perlu melakukan perbaikan diantaranya:

1) Melindungi dengan lebih dari 1 lapis pengamanan layanan TIK (sistem komputer) yang menggunakan internet.

2) Menganalisis kepatuhan penerapan konfigurasi standar yang ada secara rutin.

3) Menganalisis semua log secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik).

4) Menerapkan standar dalam menggunakan enkripsi.

5) Menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya.

4. Kesimpulan

Berdasarkan hasil evaluasi menggunakan indeks KAMI versi 4.0, tingkat kematangan keamanan informasi di Universitas Islam Negeri Sunan Kalijaga masih tergolong rendah, terutama pada aspek pengelolaan risiko dan area pengelolaan aset. Meskipun demikian aspek teknologi dan tata kelola jauh lebih baik. Saran operasional yang dapat diberikan antara lain penerapan audit keamanan informasi internal secara berkala untuk memantau efektifitas kebijakan, implementasi manajemen risiko serta mitigasi berbasis profil

risiko, dan penyesuaian infrastruktur TIK dengan pendekatan *defense in depth* agar perlindungan berlapis dapat terwujud. Hasil evaluasi tersebut diharapkan mampu meningkatkan kesiapan UIN Sunan Kalijaga dalam memenuhi standar sertifikasi keamanan informasi yang akan datang.

5. Daftar Pustaka

[1] M. Rosidin, W. Y. Sulistyo, K. E. Setyaputri, and J. Supriyanto, "Rancang Bangun Sistem Informasi Pendataan Beasiswa PTMA Berbasis Web Menggunakan Metode Waterfall," *J. Ris. Inform. dan Komput.*, vol. 2, no. 1, pp. 7–11, 2022, doi: 10.53863/juristik.v2i1.474.

[2] W. Y. Sulistyo, P. Widiandana, and M. I. Aulia, "Analisis Multivariat Korelasi Antara Durasi Film , Rating , dan Keuntungan Box Office Di Marvel Cinematic Universe," *Insect Informatics Secur.*, vol. 10, no. 2, pp. 50–56, 2024.

[3] S. Paramita, S. A. Siregar, R. A. Damanik, and M. D. Irawan, "Bulletin of Information Technology (BIT) Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013," *Bull. Inf. Technol.*, vol. 3, no. 4, pp. 374–379, 2022.

[4] R. Dewantara and B. Sugiantoro, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta)," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 8, no. 6, p. 1137, 2021, doi: 10.25126/jtiik.2021863123.

[5] T. Rochmadi and I. Y. Pasa, "Measurement of Risk and Evaluation of Information Security Using The Information Security Index in BKD XYZ Based on ISO 27001/SNI," *CyberSecurity dan Forensik Digit.*, vol. 4, no. 1, pp. 38–43, 2021, doi: 10.14421/csecurity.2021.4.1.2439.

[6] T. Thoyyibah, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO 27001:2013 Pada Pusat Informasi dan Pangkalan Data Perguruan Tinggi X," *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.*, vol. 4, no. 2, p. 72, 2018, doi: 10.24014/coreit.v4i2.6292.

[7] D. I. Khamil, "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Kami 4.2 dan ISO/IEC 27001:2013 (Studi Kasus : Diskominfo Kabupaten Gianyar)," *JATISI (Jurnal Tek. Inform. dan Sist. Informasi)*, vol. 9, no. 3, pp. 1948–1960, 2022, doi: 10.35957/jatisi.v9i3.2310.

[8] G. D. S. Barani, W. H. N. Putra, and B. S. Prakoso, "Analisis Tingkat Kesiapan dan Kematangan Keamanan Informasi menggunakan Indeks Keamanan Informasi (KAMI)(Studi Kasus: Dinas Komunikasi dan Informatika Provinsi Jawa Timur)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 4, no. 9, pp. 3218–3224, 2020, [Online]. Available: http://repository.ub.ac.id/183648/

[9] D. Dwi Prasetyowati, I. Gamayanto, and S. wibowo, "Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang Evaluation of Information Security Management Using KAMI Based on ISO / IEC 27001: 2013: The case of Politeknik Ilmu Pelayaran Semarang," ◼ *65 J. Inf. Syst.*, vol. 4, no. 1, pp. 65–75, 2019.

[10] R. Y. Rahman and M. S. Hasibuan, "Evaluasi Keamanan Informasi Pada Sman 1 Tanggamus Menggunakan Indeks Kami Versi 4.2," *J. Fasilkom*, vol. 13, no. 2, pp. 181–187, 2023.

[11] I. P. S. Syahindra, C. Hetty Primasari, and A. Bagas Pradipta Iriantor, "Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi Xyz Menggunakan Indeks Kami Dan Iso 27005 : 2011," *J. Teknoinfo*, vol. 16, no. 2, p. 165, 2022, doi: 10.33365/jti.v16i2.1246.

[12] G. M. W. Tangka and E. Lompoliu, "Information Technology Governance Using the COBIT 2019 Framework at PT. Pelindo TPK Bitung," *CogITo Smart J.*, vol. 9, no. 2, pp. 355–367, 2023, doi: 10.31154/cogito.v9i2.577.355-367.

[13] A. Nasiri, "Evaluasi Tingkat Kapabilitas Keamanan Sistem Informasi Menggunakan Kerangka Kerja Cobit 2019," *J. Tata Kelola dan Kerangka Kerja Teknol. Inf.*, vol. 9, no. 1, pp. 34–41, 2023.

[14] J. F. Andry *et al.*, "Kebijakan Keamanan Teknologi Informasi Pada Perangkat Keras Di Perusahaan Distributor Sepatu," *J. Pengabdi. dan Kewirausahaan*, vol. 7, no. 2, pp. 118–133, 2023, doi: 10.30813/jpk.v7i2.4775.

[15] C. Fatihin S, "Manajemen Risiko Reputasi Perbankan Syariah," *J. Teknol. dan Manaj. Sist. Ind.*, vol. 3, no. 1, pp. 29–39, 2024, doi: 10.56071/jtmsi.v3i1.481.