JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1948-1959

EVALUASI KEAMANAN SISTEM INFORMASI PADA PUSAT KEGIATAN BELAJAR MASYARAKAT ADI JAYA MENGGUNAKAN INDEKS KAMI 4.2

Vika Felika*[1)], Damayanti[2)]
1. Universitas Teknokrat Indonesia
2. Universitas Teknokrat Indonesia

Article Info
Kata Kunci: Keamanan Informasi; Indeks KAMI; Evaluasi; PKBM Adi Jaya

Keywords:
Information Security; KAMI Index; Evaluation; PKBM Adi Jaya

Article history:
Received 29 September 2024
Revised 13 Oktober 2024
Accepted 4 November 2024
Available online 4 December 2024

DOI :
https://doi.org/10.29100/jipi.v9i4.5580

* Corresponding author.
Vika Felika
E-mail address:
felikavika@gmail.com

ABSTRAK
Evaluasi keamanan sistem informasi menjadi krusial bagi organisasi dan perusahaan guna mendeteksi dini potensi kebocoran informasi dan gangguan pada sistem. Penelitian ini dilakukan pada Pusat Kegiatan Belajar Masyarakat Adi Jaya dengan tujuan menilai tingkat kesiapan keamanan informasi berdasarkan standar ISO/IEC 27001:2013 menggunakan alat bantu Indeks KAMI Versi 4.2. Metode pengumpulan data melibatkan observasi langsung pada objek penelitian dan wawancara dengan tim IT yang bertanggung jawab terhadap sistem informasi. Hasil evaluasi menunjukkan bahwa PKBM Adi Jaya mendapatkan nilai 20 point pada level kebutuhan perangkat elektronik dan telah berhasil memenuhi kerangka kerja dasar dalam menjaga keamanan informasi, meskipun masih berada dalam rentang Level I hingga Level II. Total skor akhir mencapai 201, menandakan efektivitas upaya dalam mengelola dan melindungi aset informasi. Namun, untuk mencapai kualifikasi sesuai dengan standar ISO/IEC 27001:2013, diperlukan langkah-langkah penting yang dapat dilakukan antara lain menyusun *roadmap* keamanan informasi secara jelas, memperbarui daftar aset dan manajemen risiko secara berkala, menyusun dan melengkapi SOP untuk setiap proses pengelolaan, serta memprioritaskan perbaikan pada keamanan sistem informasi yang sudah ada.

ABSTRACT
Security information system evaluation becomes crucial for organizations and companies to early detect potential information leaks and disruptions in the system. This research was conducted at the Community Learning Activity Center Adi Jaya with the aim of assessing the level of information security readiness based on ISO/IEC 27001:2013 standards using the KAMI Index Version 4.2 tool. Data collection methods involved direct observation of the research object and interviews with the IT team responsible for the information system. The evaluation results showed that PKBM Adi Jaya scored 20 points at the electronic device requirement level and had successfully met the basic framework in maintaining information security, although still within the range of Level I to Level II. The total final score reached 201, indicating the effectiveness of efforts in managing and protecting information assets. However, to qualify according to ISO/IEC 27001:2013 standards, important steps need to be taken, including developing a clear information security roadmap, updating asset lists and risk management periodically, drafting and completing SOPs for each management process, and prioritizing improvements to existing information system security.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1948-1959

I. PENDAHULUAN

SEIRING dengan pesatnya kemajuan teknologi informasi, risiko yang terkait dengan penggunaannya juga meningkat. Terutama dalam konteks pendidikan, penggunaan teknologi informasi dalam pendidikan dapat memberikan manfaat signifikan dalam hal efisiensi dan produktivitas. Namun, penting untuk diakui bahwa penggunaan teknologi informasi juga membawa risiko keamanan yang perlu diperhatikan. Oleh karena itu, tata kelola yang terstruktur dalam menerapkan teknologi menjadi keharusan bagi suatu instansi atau organisasi karena penting untuk memiliki tingkat keamanan yang baik dalam sistem informasi [1][2]. Keamanan sistem informasi mencakup berbagai aspek, seperti kerahasiaan data, integritas, dan ketersediaan sumber daya informasi [3]. Hal ini dianggap sebagai suatu aset berharga yang perlu dijaga dengan baik oleh instansi atau organisasi, mengingat kerugian yang mungkin terjadi akibat hilangnya data, bocornya informasi, atau kegagalan sistem, yang bisa berdampak kompleks secara finansial maupun operasional, sehingga investasi dalam keamanan sistem informasi merupakan langkah penting untuk mencegah dampak yang kompleks dan merugikan bagi perusahaan atau organisasi.

Penilaian terhadap keamanan sistem informasi adalah sebuah metode yang efektif untuk mengurangi ancaman atau risiko dari penyalahgunaan sistem oleh pihak yang tidak berhak. Salah satu pedoman yang digunakan dalam proses evaluasi perlindungan tersebut adalah Indeks KAMI yang mengikuti standar ISO/IEC 27001:2013 [4][5]. Indeks KAMI merupakan alat yang digunakan untuk menganalisis dan menilai tingkat kesiapan sistem informasi dalam berbagai entitas seperti lembaga, instansi pemerintahan, dan organisasi, sesuai dengan standar yang telah diatur dalam SNI ISO/IEC 27001:2013 [6][7]. Indeks KAMI menggambarkan tingkat kehati-hatian dalam memilih kerangka kerja keamanan informasi yang sesuai, yang dapat diterapkan di berbagai konteks sehingga memungkinkan untuk melakukan evaluasi yang komprehensif terhadap berbagai aspek keamanan informasi [8][9].

Indeks KAMI memiliki tiga fokus utama dalam proses penilaian. Pertama, itu melibatkan pengelompokan bagian-bagian dari sistem elektronik yang digunakan oleh sebuah perusahaan, instansi pemerintahan, atau organisasi. Kedua, evaluasi terhadap area-area seperti manajemen keamanan informasi, manajemen risiko keamanan informasi, *Framework* keamanan informasi, manajemen aset informasi, teknologi informasi dan keamanan, serta integritas pengamanan informasi. Yang ketiga, penilaian terhadap faktor-faktor yang berpotensi memengaruhi keamanan informasi, seperti campur tangan pihak lain, layanan infrastruktur *Cloud Computing*, dan perlindungan data pribadi [10].

Standar ISO/IEC 27001 adalah panduan standarisasi keamanan informasi yang dikeluarkan oleh International Organization for Standardization dan Electronics Engineering Committee (ISO/IEC) [11][12][13]. Standar ini bertujuan untuk membantu organisasi, perusahaan, dan instansi pemerintahan dalam menjaga keamanan informasi mereka. ISO/IEC 27001 menetapkan persyaratan yang harus dipenuhi untuk memastikan, menerapkan, memonitor, mengawasi, dan menyimpan Sistem Manajemen Keamanan Informasi (ISMS). Standar tersebut berdiri sendiri dalam konteks teknologi informasi, mengadopsi pendekatan manajemen berbasis risiko, dan dibuat untuk menetapkan kontrol keamanan yang dapat melindungi aset informasi dengan efektif [14].

Terdapat beberapa penelitian terdahulu yang relevan dengan penelitian ini yaitu penelitian dengan judul "Evaluasi Keamanan Informasi Pada Sman 1 Tanggamus Menggunakan Indeks Kami Versi 4.2". Tujuan dari penelitian ini adalah untuk mengevaluasi tingkat kesiapan keamanan informasi di institusi pendidikan negeri menggunakan Indeks KAMI 4.2. Hasil penelitian menunjukkan bahwa tingkat integritas mencapai skor 245 dan hasil evaluasi akhir dinilai Tidak Layak. Berdasarkan hasil tersebut, rekomendasi diberikan untuk melakukan perbaikan pada keamanan informasi guna meningkatkan kelayakan sistem [15].

Selain itu, terdapat penelitian lain yang relevan yaitu penelitian dengan judul "Evaluasi Manajemen Keamanan Informasi Pada Perusahaan Pemula Berbasis Teknologi Menggunakan Indeks Kami" Tujuan dari penelitian ini adalah untuk mengevaluasi sejauh mana tingkat kesiapan dan kelengkapan pengelolaan keamanan informasi di perusahaan toko *online* dan distributor parfum dan pakaian. Hasil penelitian menunjukkan bahwa dari tiga area pengamanan informasi yang diteliti, tingkat kematangan secara keseluruhan dinilai sebagai "Tidak Layak" dengan tingkat kesiapan pada level I hingga I+, yang menunjukkan bahwa perusahaan masih berada dalam tahap awal penerapan manajemen keamanan informasi [16].

PKBM (Pusat Kegiatan Belajar Masyarakat) Adi Jaya merupakan lembaga pendidikan non-formal di bandar lampung yang berdiri sejak tahun 2020 dengan menyediakan layanan pendidikan bagi masyarakat yang tidak dapat mengakses pendidikan formal atau memiliki keterbatasan dalam mengaksesnya. Lembaga pendidikan non-formal

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1948-1959

ini memberikan berbagai program pendidikan, seperti Program Paket A, B, atau C untuk menyelesaikan pendidikan dasar dan menengah, kursus-kursus pelatihan, dan program-program pendidikan lainnya yang disesuaikan dengan kebutuhan masyarakat setempat [17][18]. PKBM Adi Jaya berada dalam tahap pengembangan yang memerlukan evaluasi tingkat keamanan informasi untuk memastikan bahwa proses pengembangan dapat berjalan dengan baik dan aman.

Evaluasi keamanan informasi di PKBM Adi Jaya sangat penting dilakukan untuk memastikan bahwa data dan informasi sensitif terlindungi dari ancaman dan kebocoran. Evaluasi ini juga membantu lembaga dalam mematuhi standar keamanan yang ditetapkan, meningkatkan efisiensi operasional, dan membangun budaya keamanan di seluruh organisasi. Hasil penelitian ini diharapkan memberikan dampak positif bagi PKBM Adi Jaya dengan meningkatkan kepercayaan dari masyarakat, melindungi lembaga dari ancaman siber, dan memastikan kelancaran operasional. Selain itu, penelitian ini juga dapat menjadi model bagi lembaga pendidikan lainnya di wilayah tersebut untuk meningkatkan standar keamanan informasi mereka.

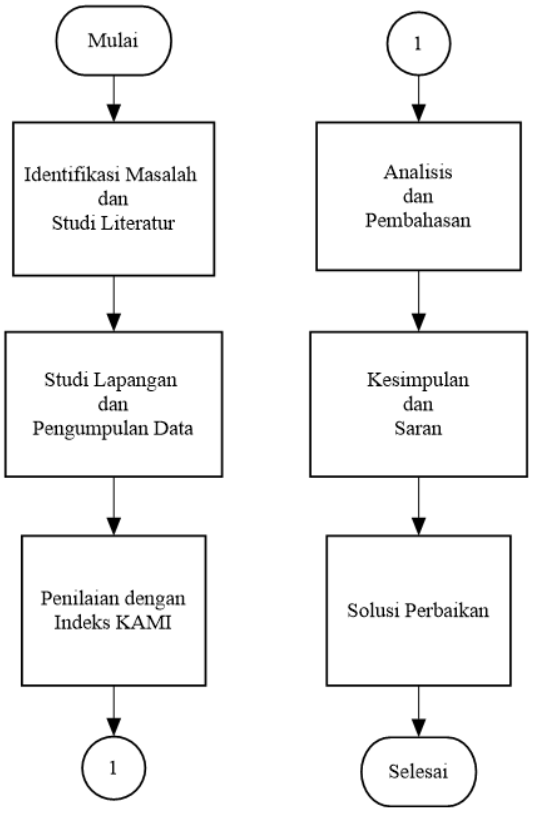
Berdasarkan pemaparan latar belakang masalah dan hasil penelitian terdahulu yang relevan, maka diperoleh pemahaman yang penting tentang pentingnya tata kelola keamanan informasi, terutama dalam konteks pendidikan dan perusahaan. Melalui penelitian ini, tujuan utamanya adalah untuk mengevaluasi keamanan sistem informasi di PKBM Adi Jaya menggunakan Indeks KAMI 4.2. Dengan demikian, penelitian ini diharapkan dapat memberikan wawasan yang berharga tentang tingkat keamanan sistem informasi di lembaga pendidikan non-formal ini serta memberikan rekomendasi untuk perbaikan jika diperlukan. Dengan demikian, penelitian ini memiliki tujuan yang sangat relevan dan penting dalam memastikan keamanan informasi yang optimal di PKBM Adi Jaya.

II. METODE PENELITIAN

Dalam tahap metode penelitian, akan diuraikan tentang pendekatan yang digunakan, lokasi penelitian, subjek penelitian, serta instrumen dan prosedur yang diterapkan untuk mengevaluasi tingkat keamanan sistem informasi di PKBM Adi Jaya menggunakan Indeks KAMI 4.2.

A. Tahapan Penelitian

Tahapan penelitian terdiri dari beberapa langkah penting yang harus dilakukan untuk mencapai tujuan penelitian. Adapun tahap-tahap dari penelitian ini dapat dilihat pada Gambar 1 sebagai berikut.



Gambar 1. Tahap Penelitian

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1948-1959

Dalam penelitian ini, tahapan penelitian meliputi:

1. Identifikasi Masalah dan Studi Literatur: Tahap awal melibatkan identifikasi masalah keamanan sistem informasi di PKBM Adi Jaya serta tinjauan literatur untuk memahami konsep dan teori terkait.
2. Studi Lapangan dan Pengumpulan Data: Dilakukan pengumpulan data melalui studi lapangan untuk mendapatkan informasi tentang kondisi keamanan sistem informasi di PKBM Adi Jaya.
3. Penilaian Indeks KAMI: Menggunakan Indeks KAMI 4.2 untuk mengevaluasi tingkat keamanan sistem informasi di PKBM Adi Jaya berdasarkan pada standar yang ditetapkan.
4. Analisis dan Pembahasan: Data yang terkumpul dianalisis dan dibahas untuk memahami temuan serta implikasinya terhadap keamanan sistem informasi di PKBM Adi Jaya.
5. Solusi Perbaikan: Berdasarkan hasil analisis, disusun solusi perbaikan yang dapat meningkatkan tingkat keamanan sistem informasi di PKBM Adi Jaya.
6. Kesimpulan dan Saran: Menyajikan kesimpulan dari penelitian serta memberikan saran untuk langkah selanjutnya yang dapat diambil untuk memperbaiki keamanan sistem informasi di PKBM Adi Jaya.

B. Lokasi dan Subjek Penelitian

Subjek penelitian ini adalah Pusat Kegiatan Belajar Masyarakat (PKBM) Adi Jaya, sebuah lembaga pendidikan nonformal yang berlokasi di Jl. Raya Pon-Pes dsn Sidodadi, Talang Sepuh, Kecamatan Talang Padang, Kabupaten Tanggamus, Lampung, dengan kode pos 35377. Lokasi ini dipilih sebagai fokus utama penelitian karena PKBM Adi Jaya merupakan lembaga pendidikan yang relevan untuk mengevaluasi tingkat kesiapan keamanan informasi.

C. Teknik Pengumpulan Data

Proses pengumpulan data dalam penelitian ini didasarkan pada pendekatan kuantitatif, yaitu :

1. Metode Observasi

Melakukan observasi lapangan terhadap kegiatan dan proses yang terjadi di PKBM Adi Jaya untuk memperoleh pemahaman tentang praktik keamanan informasi yang sedang berlangsung. Berikut adalah rincian tentang bagaimana observasi dilakukan dapat dilihat pada tabel 1.

TABEL I
METODE OBSERVASI

Lingkup Observasi	Pengamatan langsung terhadap perangkat keras dan perangkat lunak yang digunakan dalam operasional sehari-hari.
	Meninjau bagaimana kebijakan keamanan diterapkan, seperti prosedur login, penggunaan password, dan mekanisme backup data.
	Mengamati aktivitas pengguna, baik staf maupun peserta didik, dalam menggunakan sistem informasi dan bagaimana mereka mematuhi protokol keamanan.
Metode Pelaksanaan	Melakukan kunjungan langsung ke lokasi untuk melihat secara fisik kondisi perangkat dan infrastruktur teknologi yang digunakan.
	Mencatat temuan-temuan yang relevan, dan mengumpulkan dokumen terkait seperti kebijakan keamanan informasi dan SOP (Standar Operasional Prosedur).
Apa yang diamati	Apakah kebijakan keamanan yang telah ditetapkan dijalankan dengan baik oleh semua pihak.
	Identifikasi potensi kerentanan dalam sistem yang bisa dieksploitasi oleh pihak yang tidak berwenang.
	Menilai sejauh mana langkah-langkah pengamanan yang ada mampu melindungi data dan sistem dari ancaman eksternal dan internal.

2. Metode Wawancara

Wawancara dilakukan dengan interaksi atau dialog dengan pakar teknologi informasi yang memegang tanggung

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1948-1959

jawab atas penggunaan fasilitas elektronik serta pimpinan PKBM yang membuat keputusan strategis terkait kebijakan keamanan informasi di PKBM Adi Jaya dengan mengikuti arahan yang sesuai dengan instrumen yang tertera dalam Indeks KAMI versi 4.2 untuk menggali informasi mendalam. Wawancara dilakukan secara terstruktur dengan menggunakan daftar pertanyaan yang telah disiapkan sebelumnya untuk memastikan setiap wawancara mencakup topik yang sama. Selain itu, wawancara mendalam juga dilakukan dengan menyesuaikan pertanyaan sesuai dengan jawaban responden guna menggali informasi yang lebih spesifik dan detail. Topik yang dibahas mencakup pemahaman dan implementasi kebijakan keamanan informasi, tantangan dan masalah yang dihadapi, serta persepsi tentang efektivitas sistem keamanan informasi yang ada dan saran untuk perbaikan.

D. Metode Analisis Data

Langkah awal sebelum memulai tahap evaluasi adalah dengan mengelompokkan data elektronik. Tujuan dari pengelompokan ini adalah untuk mengklasifikasikan dan mengorganisir data elektronik ke dalam bentuk tertentu. Langkah ini dilakukan agar data mudah dianalisis dan digunakan untuk menarik kesimpulan. Setelah hasil kesimpulan diperoleh, selanjutnya data tersebut dipelajari dan dianalisis lebih lanjut untuk merumuskan rekomendasi perbaikan yang diperlukan. Kaitannya, ada hubungan yang terbentuk antara bagian-bagian dari sistem elektronik dengan tingkat kematangan keamanan informasi, yang diukur menggunakan indeks KAMI yang telah ditentukan sebelumnya.

TABEL 2
PENGELOMPOKAN KATEGORI SISTEM ELEKTRONIK

Rendah	Skor Akhir	Status Kesiapan
10 - 15	0 - 174	Tidak layak
	175 - 312	Pemenuhan kerangka kerja dasar
	313 - 535	Cukup baik
	536 - 645	Baik
Tinggi	Skor Akhir	Skor Akhir
16 - 34	0 - 272	Tidak layak
	273 - 455	Pemenuhan kerangka kerja dasar
	456 - 583	Cukup baik
	586 - 645	Baik
Strategis	Skor Akhir	Skor Akhir
35 - 50	0 - 333	Tidak layak
	334 - 535	Pemenuhan kerangka kerja dasar
	536 - 609	Cukup baik
	610 - 645	Baik

Indeks KAMI versi 4.2 memiliki lima kategori atau tingkatan level kematangan keamanan informasi untuk menentukan status keamanan suatu entitas sebagai berikut:

1. Level I - Keadaan awal
2. Level II - Implementasi kerangka kerja dasar
3. Level III - Terdefinisi serta selaras
4. Level IV - Dikelola dan terhitung
5. Level V – Ideal

Mengacu pada tingkat kematangan yang telah disebutkan di atas, terdapat empat kategori tambahan yang ditambahkan ke level kematangan untuk memberikan penjelasan yang lebih rinci, yaitu level I+, II+, III+, dan IV+. Standar ISO/IEC 27001:2013 menetapkan bahwa tingkat kematangan keamanan informasi minimal yang diperlukan adalah level III+. Evaluasi dengan indeks KAMI versi 4.2 menghasilkan tingkat kesiapan keamanan informasi seperti pada gambar 2 sebagai berikut:

Gambar 2. Tingkat kesiapan keamanan informasi

Untuk mencapai skor dalam evaluasi tingkat kesiapan keamanan informasi yang mengikuti Indeks KAMI Versi 4.2, langkahnya adalah dengan mendistribusikan pertanyaan kepada responden yang terbagi menjadi tujuh kelompok aspek, yaitu:

1. Aspek Kategori Sistem Elektronik: Melakukan evaluasi seberapa besar reliansi terhadap sistem elektronik.
2. Aspek Pengelolaan Keamanan Informasi: Evaluasi kesiapan pengelolaan keamanan informasi bersama dengan fungsi, tugas, dan tanggung jawab yang terkait.
3. Aspek Pengelolaan Risiko Keamanan Informasi: Menekankan proses penilaian tingkat kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
4. Aspek Kerangka Kerja Pengelolaan Keamanan Informasi: Menekankan penilaian terhadap kesiapan penggunaan kerangka kerja, termasuk kebijakan, prosedur, dan strategi dalam penerapannya.
5. Aspek Pengelolaan Aset Keamanan Informasi.
6. Aspek Teknologi Informasi: Menyoroti integritas, kestabilan, dan kesuksesan dalam menerapkan teknologi untuk menjaga keamanan informasi.
7. Aspek Suplemen: Memiliki tujuan untuk mengawasi kemunculan ancaman baru terhadap keamanan informasi dari pihak ketiga.

Setiap aspek memiliki poin tersendiri tergantung pada tingkat kematangannya. Berikut adalah skor level kematangan berdasarkan status penerapannya.

TABEL 3
SKOR TINGKAT KEMATANGAN

Status	Level Kematangan		
	1	2	3
Tidak dilakukan	0	0	0
Dalam perencanaan	1	2	3
Dalam penerapan atau sebagian	2	4	6
Diterapkan secara menyeluruh	3	6	9

Penyelesaian soal Kategori 3 akan menghasilkan skor jika semua pertanyaan dalam Kategori 1 dan Kategori 2 dalam aplikasi dapat dijawab minimal atau diterapkan sebagian. Peningkatan ketergantungan lembaga, instansi pemerintahan, atau perusahaan terhadap peran sistem elektronik dapat mengakibatkan pertumbuhan berbagai bentuk implementasi keamanan informasi.

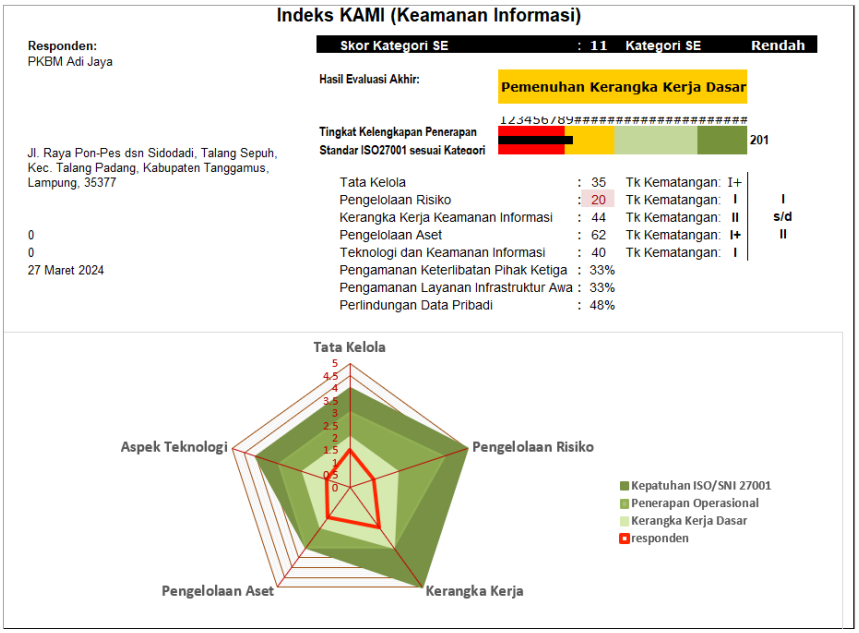
E. Konsep ISO/IEC 27001:2013 dan Implementasi dalam Evaluasi Keamanan Informasi

ISO/IEC 27001:2013 merupakan standar internasional yang menyediakan persyaratan untuk Sistem Manajemen Keamanan Informasi (SMKI) [19][20]. Standar ini membantu organisasi mengelola dan melindungi aset informasi melalui serangkaian kontrol keamanan yang sesuai. Dalam penelitian ini, konsep-konsep utama ISO/IEC 27001:2013 diterapkan pada Indeks KAMI untuk mengevaluasi keamanan informasi di PKBM Adi Jaya. Konteks organisasi dipahami melalui wawancara dengan pemangku kepentingan untuk mengidentifikasi kebutuhan dan ekspektasi keamanan informasi. Komitmen kepemimpinan dinilai melalui wawancara dengan pimpinan PKBM untuk menilai implementasi dan pemahaman kebijakan keamanan informasi. Perencanaan mencakup analisis risiko dan identifikasi kontrol yang ada dan diperlukan, sementara dukungan dievaluasi melalui penilaian sumber daya, kompetensi, dan komunikasi internal. Observasi operasi sehari-hari memastikan kontrol keamanan diterapkan dengan efektif, dan evaluasi kinerja dilakukan menggunakan Indeks KAMI untuk menilai kematangan dan efektivitas kontrol keamanan.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1948-1959

III. HASIL DAN PEMBAHASAN

Berdasarkan penilaian tingkat kematangan keamanan informasi di PKBM Adi Jaya, hasilnya dapat diklasifikasikan ke dalam tujuh kelompok yang telah disesuaikan dengan Indeks KAMI versi 4.2. Berikut adalah ringkasan evaluasi keamanan informasi dapat dilihat pada gambar di bawah ini:



Gambar 3. Dashboard Indeks KAMI

A. Kategori Sistem Elektronik

Berdasarkan hasil penilaian, skor tertinggi yang diperoleh pada evaluasi efektivitas sistem elektronik di PKBM Adi Jaya adalah 11. Skor ini didapat dari 10 pertanyaan yang masing-masing memiliki nilai maksimal 50 poin. Dalam kategori ini, hanya kegagalan dalam sistem elektronik yang dievaluasi, sehingga perhatian lebih diperlukan pada identifikasi dan penanganan kegagalan sistem tersebut. Konsekuensinya, kegagalan dalam sistem elektronik dapat mengakibatkan gangguan dalam operasional PKBM Adi Jaya, terutama dalam pengelolaan dan akses informasi yang vital. Hal ini dapat menghambat efisiensi dan produktivitas organisasi serta memengaruhi pelayanan yang diberikan kepada masyarakat. Oleh karena itu, diperlukan tindakan preventif dan perbaikan yang cepat dan efisien untuk mengatasi kegagalan dalam sistem elektronik guna memastikan kelancaran dan keamanan operasional PKBM Adi Jaya..

B. Tata Kelola Keamanan Informasi

Langkah berikutnya dari proses evaluasi adalah mengevaluasi tingkat kesiapan dalam pengelolaan keamanan informasi dan tugas sera tanggung jawab fungsi pengelola. Ini mencakup evaluasi terhadap manajemen keamanan informasi yang berpotensi memengaruhi kualitas informasi yang dihasilkan oleh PKBM Adi Jaya. Adapun hasil penilaian aspek ini dapat dilihat pada tabel 4 sebagai berikut:

TABEL 4
HASIL PENILAIAN TATA KELOLA KEAMANAN INFORMASI

Status	Level Kematangan						
	1	Skor	2	Skor	3	Skor	Total
Tidak Dilakukan	0	0	0	0	0	0	0
Dalam Perencanaan	1	6	2	10	3	0	16
Dalam Penerapan atau Sebagian	2	2	4	8	6	0	10
Dietrapkan Secara Menyeluruh	3	3	6	6	9	0	9
Total Nilai Evaluasi Keamanan Informasi							35

Pada bagian tata kelola manajemen keamanan informasi, nilai skor yang diperoleh adalah 35 poin, menempatkan kategori ini pada pada tingkat kematangan II dengan level status kesiapan I+. Hal ini menunjukkan bahwa tata kelola keamanan informasi di PKBM Adi Jaya memerlukan perbaikan. Penyebabnya adalah kurangnya pelaksanaan

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1948-1959

fungsi pengelolaan sistem informasi di area ini, serta kekurangan dokumen pendukung yang memvalidasi bahwa beberapa fungsi telah dilakukan di PKBM Adi Jaya. Oleh karena itu, diperlukan perbaikan dalam pengelolaan sistem informasi yang ada, serta pelengkapan dokumen untuk setiap tindakan yang dijalankan dalam aspek tata kelola sistem informasi di PKBM Adi Jaya.

C. Manajemen Risiko Keamanan Informasi

Langkah ketiga melibatkan proses penilaian tingkat kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi di PKBM Adi Jaya. Ini mencakup identifikasi berbagai risiko yang mungkin muncul dan memengaruhi data maupun informasi di PKBM Adi Jaya. Adapun hasil penilaian manajemen risiko keamanan informasi dapat dilihat pada tabel 5 sebagai berikut :

TABEL 5
HASIL PENILAIAN MANAJEMEN RISIKO KEAMANAN INFORMASI

Status	Level Kematangan						
	1	Skor	2	Skor	3	Skor	Total
Tidak Dilakukan	0	0	0	0	0	0	0
Dalam Perencanaan	1	8	2	8	3	0	16
Dalam Penerapan atau Sebagian	2	4	4	0	6	0	4
Dietrapkan Secara Menyeluruh	3	0	6	0	9	0	0
Total Nilai Evaluasi Keamanan Informasi							20

Hasil penilaian di PKBM Adi Jaya menunjukkan total skor 20 poin. Hal ini menunjukkan bahwa proses manajemen risiko keamanan informasi dianggap tidak layak. Hal ini disebabkan oleh banyaknya peran dari kegiatan manajemen risiko yang sedang dalam tahap perencanaan. Selain itu, kekurangan dokumen pendukung dari tiap tahap manajemen risiko keamanan informasi yang sudah dilakukan juga menjadi kendala. Kondisi ini sangat menghambat proses evaluasi dan perbaikan yang diperlukan.

D. Kerangka Kerja Keamanan Informasi

Evaluasi terhadap kerangka kerja manajemen keamanan informasi merupakan suatu langkah evaluasi terhadap kelengkapan dan kesiapan dalam menggunakan kerangka kerja yang mencakup kebijakan dan prosedur dalam manajemen keamanan informasi, juga strategi untuk implementasinya. Tahap ini adalah implementasi dan penilaian dari tahapan sebelumnya. Dalam pengelolaan kerangka kerja manajemen keamanan informasi, terdapat dua bagian utama, yaitu:

1. Penyusunan dan pengelolaan kebijakan dan prosedur keamanan informasi. Bagian ini melibatkan pembuatan kebijakan dan prosedur yang mengatur aspek keamanan informasi dalam organisasi. Kebijakan tersebut menguraikan prinsip-prinsip dasar yang harus diikuti oleh seluruh anggota organisasi, sedangkan prosedur merinci langkah-langkah yang harus diikuti dalam implementasi kebijakan tersebut.
2. Pengelolaan strategi dan program keamanan informasi. Bagian ini melibatkan perencanaan, implementasi, dan pemantauan strategi dan program yang dirancang untuk meningkatkan keamanan informasi dalam organisasi. Ini mencakup penetapan tujuan keamanan informasi, identifikasi dan mitigasi risiko, alokasi sumber daya, serta pelaksanaan kegiatan untuk memperkuat keamanan informasi secara keseluruhan.

Adapun hasil penilaian penyusunan dan pengelolaan kebijakan dan prosedur keamanan informasi dapat dilihat pada tabel 6 sebagai berikut:

TABEL 6
HASIL PENILAIAN PENYUSUNAN DAN PENGELOLAAN KEBIJAKAN DAN PROSEDUR

Status	Level Kematangan						
	1	Skor	2	Skor	3	Skor	Total
Tidak Dilakukan	0	0	0	0	0	0	0
Dalam Perencanaan	1	2	2	12	3	0	14
Dalam Penerapan atau Sebagian	2	10	4	4	6	0	14
Dietrapkan Secara Menyeluruh	3	0	6	6	9	0	6
Total Nilai Evaluasi Keamanan Informasi							34

Adapun hasil evaluasi pengelolaan strategi dan program keamanan informasi dapat dilihat pada tabel 7 sebagai berikut:

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1948-1959

TABEL 7
HASIL PENILAIAN PENGELOLAAN STRATEGI DAN PROGRAM

Status	Level Kematangan						
	1	Skor	2	Skor	3	Skor	Total
Tidak Dilakukan	0	0	0	0	0	0	0
Dalam Perencanaan	1	2	2	4	3	0	6
Dalam Penerapan atau Sebagian	2	4	4	0	6	0	4
Dietrapkan Secara Menyeluruh	3	0	6	0	9	0	0
Total Nilai Evaluasi Keamanan Informasi							10

Evaluasi kerangka kerja pengelolaan keamanan informasi di PKBM Adi Jaya menunjukkan skor total dari kedua bagian yaitu 44. Hal ini masuk ke dalam level kesiapan II dengan status I+. Skor tersebut mencerminkan bahwa terdapat banyak komponen yang masih berada dalam status perencanaan, dan sebagian besar proses dilakukan tanpa adanya dokumen-dokumen pendukung. Kondisi ini berdampak pada penurunan nilai yang diperoleh selama proses evaluasi dilakukan.

E. Pengelolaan Aset Informasi

Hasil penilaian manajemen pengamanan aset informasi meliputi evaluasi terhadap Integritas, sirkulasi, penggunaan, dan kecukupan perlindungan aset informasi, termasuk seluruh langkah penggunaan aset informasi di PKBM Adi Jaya. Pengelolaan aset informasi terdiri dari dua bagian utama:

1. Pengelolaan Aset Informasi. Bagian ini mencakup proses pengelolaan secara keseluruhan terhadap aset informasi yang dimiliki oleh PKBM Adi Jaya. Ini termasuk identifikasi, dokumentasi, pemantauan, dan pemeliharaan aset informasi, serta penetapan kebijakan dan prosedur terkait penggunaannya.
2. Pengamanan Fisik. Bagian ini menekankan pada perlindungan fisik dari aset informasi. Ini melibatkan langkah-langkah untuk melindungi fisik aset informasi, seperti tempat penyimpanan data, perangkat keras komputer, dokumen penting, dan fasilitas fisik lainnya dari akses yang tidak sah, kerusakan, atau kehilangan.

Adapun hasil penilaian pengelolaan aset informasi dapat dilihat pada tabel 8 sebagai berikut:

TABEL 8
HASIL PENILAIAN PENGELOLAAN ASET INFOMRASI

Status	Level Kematangan						
	1	Skor	2	Skor	3	Skor	Total
Tidak Dilakukan	0	0	0	0	0	0	0
Dalam Perencanaan	1	13	2	8	3	0	21
Dalam Penerapan atau Sebagian	2	8	4	0	6	0	8
Dietrapkan Secara Menyeluruh	3	3	6	12	9	0	15
Total Nilai Evaluasi Keamanan Informasi							44

Adapun hasil penilaian pengamanan fisik dapat dilihat pada tabel 9 sebagai berikut:

TABEL 9
HASIL PENILAIAN PENGAMANAN FISIK

Status	Level Kematangan						
	1	Skor	2	Skor	3	Skor	Total
Tidak Dilakukan	0	0	0	0	0	0	0
Dalam Perencanaan	1	4	2	6	3	0	10
Dalam Penerapan atau Sebagian	2	4	4	4	6	0	8
Dietrapkan Secara Menyeluruh	3	0	6	0	9	0	0
Total Nilai Evaluasi Keamanan Informasi							18

Hasil evaluasi dalam tahap ini menunjukkan skor 62 poin dari total kedua bagian, sehingga masuk ke dalam level kesiapan II dengan status I+ yang berada pada tingkat rendah dan memerlukan perbaikan. Penilaian tersebut terpengaruh oleh kekurangan dokumen pendukung yang dapat membuktikan setiap proses yang telah dijalankan dengan lengkap dan kekurangan dalam pengamanan fisik, yang merupakan faktor yang turut memengaruhi penurunan skor. Oleh karena itu, diperlukan langkah-langkah untuk melengkapi dokumen yang berkaitan agar dapat menjadi bukti bahwa berbagai proses telah dilaksanakan sesuai dengan prosedur yang berlaku juga dilakukan langkah-langkah untuk meningkatkan pengamanan fisik dan memastikan perlindungan yang lebih baik terhadap aset informasi dari akses yang tidak sah atau kerusakan.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 4, Desember 2024, Pp. 1948-1959

F. Teknologi Informasi dan Keamanan

Hasil evaluasi dalam proses ini fokus pada kesesuaian, kestabilan, dan kinerja penggunaan teknologi untuk menjaga keamanan aset informasi di PKBM Adi Jaya. Hasil evaluasi tersedia dalam tabel 10 sebagai berikut:

TABEL 10
HASIL PENILAIAN TEKNOLOGI INFORMASI DAN KEAMANAN

Status	Level Kematangan						
	1	Skor	2	Skor	3	Skor	Total
Tidak Dilakukan	0	0	0	0	0	0	0
Dalam Perencanaan	1	12	2	20	3	3	35
Dalam Penerapan atau Sebagian	2	2	4	0	6	0	2
Dietrapkan Secara Menyeluruh	3	3	6	0	9	0	3
Total Nilai Evaluasi Keamanan Informasi							40

Hasil pada tabel menunjukkan total nilai evaluasi sebesar 40. Dari hasil ini, terlihat ada ruang untuk perbaikan dalam aspek kesesuaian, kestabilan, dan kinerja penggunaan teknologi untuk melindungi aset informasi di PKBM Adi Jaya. Disarankan untuk meningkatkan upaya dalam memperkuat perlindungan teknologi informasi guna menjaga keamanan informasi secara optimal.

G. Suplemen

Tahap ini adalah proses evaluasi yang menilai keterlibatan pihak ketiga dalam penyediaan layanan oleh badan pemerintah, organisasi, atau entitas korporat. Evaluasi ini bertujuan untuk mengidentifikasi ancaman yang mungkin timbul akibat adanya pihak ketiga. Hasil yang didapat dari tahap suplemen tidak berdampak pada nilai total dari kategori keseluruhan yang sudah dinilai sebelumnya menggunakan Indeks KAMI. Namun, evaluasi ini penting untuk memantau kemunculan ancaman baru terhadap keamanan informasi, khususnya terkait dengan keterlibatan pihak ketiga dalam berbagai aspek yang ada.

Dalam tahap suplemen, evaluasi dilakukan untuk memantau kemungkinan ancaman yang muncul dari keterlibatan pihak ketiga, layanan infrastruktur awan, dan perlindungan data pribadi di lingkungan PKBM Adi Jaya. Rincian evaluasi adalah sebagai berikut:

1. Keterlibatan pihak pihak ketiga.
   Hasil evaluasi ini menghasilkan tingkat kematangan 33%. Nilai ini mengindikasikan sejauh mana PBKM Adi Jaya melindungi informasi dari ancaman yang mungkin berasal dari pihak ketiga. Hasil evaluasi mengisyaratkan bahwa upaya keamanan terhadap keterlibatan pihak ketiga masih perlu diperkuat, karena ada potensi risiko keamanan yang belum sepenuhnya ditangani.
2. Layanan Infrastruktur Awan.
   Hasil evaluasi ini menghasilkan tingkat kematangan 33%. Nilai ini mencerminkan tingkat keamanan layanan yang disediakan oleh infrastruktur awan yang digunakan oleh PBKM Adi Jaya. Nilai 33% menunjukkan bahwa ada ruang untuk perbaikan dalam hal keamanan infrastruktur awan seperti peningkatan dalam konfigurasi keamanan atau implementasi praktik terbaik dalam manajemen keamanan awan.
3. Perlindungan Data Pribadi.
   Hasil evaluasi ini menghasilkan tingkat kematangan 48%. Nilai ini mengukur sejauh mana PBKM Adi Jaya melindungi data pribadi. Meskipun nilai ini lebih tinggi dari dua indikator sebelumnya, masih ada ruang untuk peningkatan. Nilai tersebut menunjukan bahwa ada ruang untuk perbaikan dalam hal perlindungan data sehingga perlu diperkuat kebijakan dan prosedur perlindungan data, serta mengimplementasikan kontrol keamanan tambahan untuk memastikan keamanan data pribadi yang optimal.

F. Implikasi Temuan

Penelitian menghasilkan sejumlah temuan yang dapat digunakan untuk meningkatkan praktik keamanan informasi di PKBM Adi Jaya dan organisasi serupa. Temuan tersebut mencakup kebutuhan akan peningkatan kesadaran dan komitmen manajemen terhadap kebijakan keamanan informasi, perlunya perencanaan yang lebih baik dalam mengelola risiko, pentingnya pengembangan SOP dan dokumentasi kegiatan, serta perlunya pelatihan dan peningkatan kompetensi staf terkait dengan keamanan informasi. Selain itu, temuan juga menyoroti pentingnya evaluasi dan monitoring berkelanjutan, peningkatan infrastruktur dan teknologi, serta manajemen yang lebih baik terhadap keterlibatan pihak ketiga dan perlindungan data pribadi. Dengan menerapkan temuan-temuan ini secara praktis, PKBM Adi Jaya dapat meningkatkan keamanan informasi

mereka, menciptakan lingkungan belajar yang lebih aman dan terpercaya, serta meningkatkan efisiensi operasional organisasi.

G. Perbandingan Dengan Penelitian Terdahulu

Pada tahap ini membandingkan temuan dari penelitian ini dengan hasil penelitian terkait yang telah dilakukan sebelumnya. Dalam perbandingan dengan penelitian sebelumnya, terdapat beberapa perbedaan yang signifikan. Penelitian ini menunjukkan bahwa PKBM Adi Jaya mencapai pemenuhan kerangka kerja dasar dengan total skor akhir mencapai 201 dan tingkat kematangan berada pada rentang Level I hingga Level II. Sementara itu, dalam penelitian "Evaluasi Keamanan Informasi Pada SMAN 1 Tanggamus Menggunakan Indeks KAMI Versi 4.2", meskipun tingkat integritas mencapai skor 245, namun hasil evaluasi akhirnya dinilai "Tidak Layak" [15]. Rekomendasi diberikan untuk melakukan perbaikan pada keamanan informasi guna meningkatkan kelayakan sistem. Di sisi lain, penelitian lain berjudul “Evaluasi Manajemen Keamanan Informasi Pada Perusahaan Pemula Berbasis Teknologi Menggunakan Indeks Kami” yang mengevaluasi manajemen keamanan informasi di perusahaan pemula berbasis teknologi menemukan bahwa tingkat kematangan secara keseluruhan dinilai sebagai "Tidak Layak" dengan tingkat kematangan pada level I hingga I+ [16]. Ini menunjukkan bahwa perusahaan tersebut masih dalam tahap awal penerapan manajemen keamanan informasi. Meskipun demikian, temuan penelitian ini menunjukkan bahwa PKBM Adi Jaya memiliki tingkat kematangan yang lebih baik dalam pengelolaan keamanan informasi, meskipun masih terdapat ruang untuk perbaikan dan peningkatan lebih lanjut. Perbandingan ini memberikan konteks yang lebih luas untuk memahami signifikansi dan kontribusi temuan dalam konteks keamanan informasi di organisasi atau lembaga sejenis.

IV. KESIMPULAN

Berdasarkan hasil evaluasi tingkat kesiapan keamanan informasi dengan menggunakan Indeks KAMI versi 4.2 di PKBM Adi Jaya, dapat disimpulkan bahwa pada tingkat kebutuhan perangkat elektronik, nilai yang diperoleh adalah 11 poin dan berada pada rentang Level I hingga Level II. PBKM Adi Jaya telah berhasil memenuhi kerangka kerja dasar dalam menjaga keamanan informasi dengan total skor akhir mencapai 201, hal ini menunjukkan efektivitas upaya yang dilakukan dalam mengelola dan melindungi aset informasi. Namun agar memenuhi kriteria yang sesuai dengan standar ISO/IEC 27001:2013, PKBM Adi Jaya perlu meningkatkan keamanan informasi internal dan eksternal, dan terus-menerus melakukan evaluasi keamanan.

Langkah-langkah yang dapat diambil untuk meningkatkan keamanan informasi di PKBM Adi Jaya antara lain adalah menyusun *Road Map* pengelolaan keamanan informasi kemudian mempublikasikannya kepada semua staff terkait, menyusun dan memperbarui daftar aset dan pengelolaan risiko yang senantiasa diperbaharui, merumuskan dan menyempurnakan SOP untuk setiap tahap pengelolaan, serta melengkapi dokumentasi pelaksanaan kegiatan yang signifikan agar memiliki pedoman dokumen pendukung saat dibutuhkan, serta mengamati dan mengutamakan perbaikan tingkat keamanan pada penerapan sistem informasi yang ada.

Selain itu, hasil pada tahap suplemen juga perlu diperhatikan. Keterlibatan pihak ketiga sebesar 33%, Layanan Infrastruktur Awan 33%, dan Perlindungan Data Pribadi 48% menunjukkan adanya potensi risiko yang perlu dipertimbangkan secara lebih mendalam. Dengan demikian, PKBM Adi Jaya perlu meningkatkan pengamanan terkait keterlibatan pihak ketiga, infrastruktur awan, dan perlindungan data pribadi guna meminimalkan potensi ancaman terhadap keamanan informasi mereka.

DAFTAR PUSTAKA

[1] P. Jayadi, P. Sarwono, and M. D. Nanda, “Pengukuran Kinerja Teknologi Informasi di Indonesia dalam General Control: Literature Review,” *JIMP J. Inform. Merdeka Pasuruan*, vol. 7, no. 1, pp. 6–13, 2022.

[2] A. Ghufran Yuda, D. Takratama Savra, F. Rahmat Halim, M. Ripaldo Pratama, and N. Safiq Tama, “AUDIT TATA KELOLA UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU KULIAH KERJA NYATA SISTEM MENGGUNAKAN COBIT 2019,” *J. Test. dan Implementasi Sist. Inf.*, vol. 2, no. 1, pp. 10–17, 2024.

[3] E. Novianto, E. H. Heri Ujianto, and R. Rianto, “Keamanan Informasi (Information Security) Pada Aplikasi Sistem Informasi Manajemen Sumber Daya Manusia,” *Rabit J. Teknol. dan Sist. Inf. Univrab*, vol. 8, no. 1, pp. 10–15, 2023, doi: 10.36341/rabit.v8i1.2966.

[4] Faradhiya Aulia Rahma, Najwa Hamidah Erwin, Bintang Nuari Atno Nichada, and Reisa Permatasari, “Analisis Keamanan Informasi Menggunakan Aplikasi Indeks Kami Pada Sekretariat Dprd Kabupaten Jombang,” *Pros. Semin. Nas. Teknol. dan Sist. Inf.*, vol. 3, no. 1, pp. 279–288, 2023, doi: 10.33005/sitasi.v3i1.396.

[5] I. G. P. K. Juliharta, I. N. Y. A. Wijaya, and A. S. Laksana, “PENGUKURAN TINGKAT KEAMANAN SISTEM INFORMASI MENGGUNAKAN INDEKS KAMI VERSI 3.1, DAN MENGUKUR TINGKAT KERENTANAN SERVER MENGGUNAKAN NETWORK SECURITY ASSESSMENT STUDI KASUS KOMINFO KABUPATEN GIANYAR I Gede Putu Krisna Juliharta 1), I Nyoman Yudi Anggara Wij,” *J. Teknol. Inf. dan Komput.*, vol. 7, pp. 319–325, 2021.

[6] S. Yuliani, N. T. Ramadhini, A. I. Gustisyaf, and A. Wahyudin, “Asesmen Keamanan Informasi Menggunakan Indeks Kami,” *Naratif J. Nas. Riset, Apl. dan Tek. Inform.*, vol. 2, no. 1, pp. 1–5, 2020, doi: 10.53580/naratif.v2i1.76.

[7] T. N. Khusna and B. Sugiantoro, "Pengukuran Tingkat Keamanan Informasi Pada Upt-Psi Universitas Muria Kudus Berdasarkan Indeks Keamanan Informasi (Kami) Versi 4.2," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 8, no. 3, pp. 847–856, 2023, doi: 10.29100/jipi.v8i3.3720.

[8] R. Hidayat, M. Suyanto, and A. Sunyoto, "Indeks Penilaian Keamanan Informasi Untuk Mengukur Kematangan Manajemen Keamanan Layanan TI," *Pengemb. Apl. Untuk Mendeteksi Pergerakan Sendi Pada Pasien Pasca Stroke Menggunakan Sens. Accelerom. Di Smartphone Android*, vol. 3, no. 1, pp. 1–7, 2018, [Online]. Available: http://e-journal.janabadra.ac.id/index.php/informasiinteraktif/article/view/671

[9] E. Soesanto, M. R. Adrian, and ..., "Analisis Keamanan Sistem Informasi di PT. Telkom Menggunakan Indeks KAMI," *IJM Indones. …*, vol. 1, pp. 169–175, 2023, [Online]. Available: https://journal.csspublishing.com/index.php/ijm/article/view/105%0Ahttps://journal.csspublishing.com/index.php/ijm/article/download/105/60

[10] M. Yunella, A. Dwi Herlambang, W. Hayuhardhika, and N. Putra, "Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Malang Menggunakan Indeks KAMI," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 10, pp. 9552–9559, 2019, [Online]. Available: http://j-ptiik.ub.ac.id

[11] M. Bakri and N. Irmayana, "Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi Simhp Bpkp Menggunakan Standar Iso 27001," *J. Tekno Kompak*, vol. 11, no. 2, p. 41, 2017, doi: 10.33365/jtk.v11i2.162.

[12] L. Munaroh, Y. Amrozi, and R. A. Nurdian, "Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC 27001:2013," *Technomedia J.*, vol. 5, no. 2 Februari, pp. 167–181, 2020, doi: 10.33050/tmj.v5i2.1377.

[13] P. Sundari and W. Wella, "SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)," *Ultim. InfoSys J. Ilmu Sist. Inf.*, vol. 12, no. 1, pp. 35–42, 2021, doi: 10.31937/si.v12i1.1701.

[14] A. Kornelia and D. Irawan, "Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1," *J. Pengemb. Sist. Inf. dan Inform.*, vol. 2, no. 2, pp. 78–86, 2021, doi: 10.47747/jpsii.v2i2.548.

[15] 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.

[16] A. L. Maryanto, M. N. Al Azam, and A. Nugroho, "Evaluasi Manajemen Keamanan Informasi Pada Perusahaan Pemula Berbasis Teknologi Menggunakan Indeks Kami," *J. Simantec*, vol. 11, no. 1, pp. 1–12, 2022, doi: 10.21107/simantec.v11i1.14099.

[17] S. N. Azizah, "Strategi Pengembangan Kegiatan Pembelajaran di PKBM," *J. Pract. Learn. Educ. Dev.*, vol. 1, no. 2, pp. 46–49, 2021, doi: 10.58737/jpled.v1i2.18.

[18] A. Irmawati, "DALAM MENGURANGI BUTA AKSARA DI KABUPATEN KARIMUN *) THE ROLE OF COMMUNITY LEARNING CENTER TO REDUCE ILLITERACY RATE IN KARIMUN REGENCY," vol. 2, pp. 81–98, 2017.

[19] D. Rahmat, "Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar SNI ISO/IEC 27001," *J. Inform.*, vol. 37, no. 41, pp. 37–41, 2019, [Online]. Available: https://ejournal.unibba.ac.id/index.php/computing/article/view/203/186

[20] S. R. Musyarofah and R. Bisma, "Analisis kesenjangan sistem manajemen keamanan informasi (SMKI) sebagai persiapan sertifikasi ISO/IEC 27001:2013 pada institusi pemerintah," *Teknologi*, vol. 11, no. 1, pp. 1–15, 2021, doi: 10.26594/teknologi.v11i1.2152.