JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7, Nomor 4, Juli – Agustus 2026, Page 1072-1079
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Evaluasi Tingkat Kesiapan Keamanan Teknologi Informasi Menggunakan Indeks KAMI 4.2 di Madrasah Aliyah Nurul Ummah Yogyakarta

Hanif Amarudin[1], Bambang Sugiantoro[2]

[1,2)]Informatika, Universitas Islam Negeri Sunan Kalijaga, Yogyakarta, Indonesia
Email: [1]hanifamar17@email.com, [2]bambang.sugiantoro@uin-suka.ac.id
Email Penulis Korespondensi: [2]hanifamar17@email.com

Abstrak− Teknologi informasi memiliki peran vital dalam proses manajemen pendidikan serta penunjang aktivitas akademik di sekolah. Namun, ketergantungan yang semakin meningkat pada teknologi informasi dapat menimbulkan risiko keamanan informasi, sehingga pemahaman tentang risiko, pemantauan dan evaluasi terhadap kesiapan keamanan menjadi kebutuhan untuk instansi pendidikan. Oleh karena itu, penelitian ini bertujuan untuk mengevaluasi tingkat kesiapan keamanan teknologi informasi di Madrasah Aliyah Nurul Ummah Yogyakarta. Instrumen penelitian menggunakan Indeks KAMI 4.2 yang diterbitkan oleh BSSN, dan selaras dengan standar SNI ISO/IEC 27001. Data melalui observasi dan wawancara bersama beberapa *stakeholder* yang memiliki wewenang dan pemahaman terkait pengelolaan teknologi informasi di instansi tersebut dan dianalisis berdasarkan kerangka penilaian dan tingkat kematangan Indeks KAMI. Hasil penelitian menunjukkan bahwa kesiapan keamanan teknologi informasi instansi diklasifikasikan sebagai Tidak Layak, dengan total skor 182 dengan Tingkat Kematangan berkisar pada level I s/d I+. Kesiapan yang rendah ditemukan di semua aspek penilaian, menunjukkan bahwa praktik keamanan informasi masih berada pada tahap awal dan belum diterapkan secara sistematis. Kondisi ini menyoroti kebutuhan untuk meningkatkan tata kelola keamanan informasi melalui penetapan kebijakan formal, manajemen risiko, dan pengendalian teknis yang ditingkatkan. Hasil ini dapat berfungsi sebagai dasar untuk perbaikan keamanan di masa depan dan penelitian lebih lanjut mengenai tingkat kematangan keamanan informasi di instansi pendidikan.

Kata Kunci: Keamanan Informasi, Indeks KAMI, ISO/IEC 27001

Abstract− Information technology plays a vital role in education management and supports academic activities in schools. However, an increasing dependence on IT can pose information security risks, so it is important for educational institutions to understand these risks and monitor and evaluate their security readiness. Therefore, this study aims to evaluate the level of information technology security readiness at Madrasah Aliyah Nurul Ummah Yogyakarta. The research instrument used the KAMI 4.2 Index that BSSN published, which is in line with the SNI ISO/IEC 27001 standard. Data was collected through observation and interviews with several stakeholders who have authority and understanding related to information technology management at the institution, and it was then analysed based on the KAMI Index assessment framework and maturity level. The results show that the institution's IT security readiness is classified as unfit, with a total score of 182 and a maturity level ranging from I to I+. Low readiness was found in all areas assessed, indicating that information security practices are still in their infancy and have not yet been implemented systematically. This condition highlights the need to improve information security governance through the establishment of formal policies, risk management, and enhanced technical controls. These results can serve as a basis for future security improvements. They can also inform further research. This research can look into the maturity level of information security in educational institutions.

Keywords: Information Security, Indeks KAMI, ISO/IEC 27001

1. PENDAHULUAN

Informasi adalah aset berharga bagi sebuah institusi Pendidikan. Mobilisasi informasi yang tinggi tidak lepas dari hadirnya teknologi informasi yang semakin berkembang. Hal positif yang diberikan misalnya pada kegiatan belajar-mengajar seperti pemberian materi menjadi lebih mudah, menyenangkan dan bervariasi dengan berbasis TIK, web/blog atau multimedia [1]. Kemudahan lainnya seperti pencarian informasi penunjang materi, fleksibilitas pembelajaran dan memperluas wawasan karena tidak bergantung pada informasi cetak saja [2]. Berdampingan dengan itu, teknologi informasi menjadi penting untuk diterapkan sebagai pendorong utama dalam manajemen pendidikan di sekolah [3]. Dalam mendukung aktivitas akademik, sekolah tidak bisa lepas dari pengelolaan informasi-informasi seperti data siswa-siswi, guru, keuangan dan dokumen-dokumen kelembagaan sebagai aset penting instansi. Secara garis besar, teknologi informasi memiliki peranan vital dalam pendidikan sebagai penunjang informasi akademik, administrasi dan layanan umum. Teknologi informasi telah diterapkan dalam beberapa proses pengelolaan administrasi di Madrasah Aliyah (MA) Nurul Ummah Yogyakarta, seperti pada area pengelolaan administrasi perpustakaan, tata usaha, keuangan, pembelajaran, aset madrasah, dan masih banyak lainnya.

Ketergantungan pada penerapan teknologi informasi memiliki risiko keamanan informasi, seperti penyalahgunaan teknologi, pencurian informasi digital, infrastruktur yang tidak memadai penanganan kejahatan siber atau karena *human error* [2]. Pengelolaan sistem administrasi berbasis digital yang tidak diiringi dengan manajemen risiko yang baik dapat meningkatkan tingkat risiko keamanan informasi, terutama dalam hal perlindungan data pribadi

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **03/06/2026**; Accepted: **28/06/2026**; Published: **30/07/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7, Nomor 4, Juli – Agustus 2026, Page 1072-1079
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

dan pengendalian ancaman siber [4]. Berdasarkan data yang dilaporkan oleh Badan Siber dan Sandi Negara (BSSN), periode 2024 terdeteksi sebanyak 241 dugaan insiden kebocoran data, 330.527.636 trafik anomali, 2.487.041 aktivitas *Advanced Persistent Threat* (APT), 514.508 aktivitas *Ransomware*, dan sebanyak 26.771.610 aktivitas *Phising* [5]. Sebagai pimpinan instansi, hal ini merupakan aspek penting yang harus menjadi perhatian dalam manajemen instansi. Pemahaman tentang risiko-risiko yang mungkin bisa terjadi, mengatur, monitoring dan mengevaluasi penggunakan teknologi informasi secara tepat sehingga dapat meminimalisir risiko yang tidak diinginkan. Dalam rangka memahami dan mengenali sejauh mana kesiapan instansi dalam menerapkan keamanan teknologi informasi, maka perlu untuk menyiapkan instrumen dalam mengevaluasi kondisi instansi.

Salah satu instrumen yang bisa digunakan untuk mengevaluasi tingkat kesiapan keamanan informasi adalah instrumen yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN), yaitu Indeks Keamanan Informasi (KAMI). Dikutip dari laman resmi BSSN, Indeks KAMI adalah alat *self-assesment* kesiapan keamanan informasi yang mengacu pada SNI ISO/IEC 27001 [6]. Pemilihan Indeks KAMI dilakukan dengan mempertimbangkan beberapa aspek, salah satunya adalah Indeks KAMI dirancang sesuai dengan kultur operasional organisasi/instansi di Indonesia. Karena dikembangkan oleh BSSN, instrumen ini mampu memberikan potret kondisi keamanan siber yang sesuai dengan infrastruktur dan regulasi di Indonesia. Selain itu, instrumen ini tidak berdiri sendiri, melainkan diturunkan dari standar internasional ISO/IEC 27001.

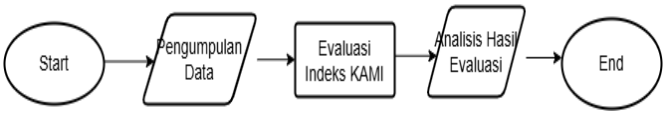
Beberapa penelitian lain yang serupa melakukan penelitian untuk mengevaluasi tingkat kesiapan keamanan informasi menggunakan Indeks KAMI 4.2 pada sebuah instansi SMK XYZ. Hasilnya adalah Indeks KAMI 4.2 dapat memberikan gambaran kondisi kesiapan instansi dengan hasil status kesiapan Tidak Layak dan skor Tingkat Penerapan Standar ISO27001 sesuai Kategori SE yaitu 314 [7]. Penelitian serupa dilakukan menggunakan Indeks KAMI 4.0 ISO 27001:2013 pada studi kasus SMK N 1 Banyumas. Hasil evaluasinya menyatakan status kesiapan Baik dengan total skor 629 [8]. Penelitian lainnya menggunakan instrumen Indeks KAMI 5.0 dan Cobit 5 dengan studi kasus Pondok Pesantren Sunni Darussalam Yogyakarta. Hasil evaluasi Indeks KAMI menyatakan keamanan informasi belum optimal atau masih rendah dengan skor hasil evaluasi 170 dan 284. Begitu pula dengan hasil evaluasi dengan kerangka kerja Cobit 5 yang mendapatkan status rendah dan perlu ditingkatkan [9].

Penelitian-penelitian di atas telah menerapkan evaluasi tingkat keamanan informasi Indeks KAMI pada sebuah instansi Pendidikan, baik formal maupun non-formal. Namun, meskipun demikian, celah penelitian yang jelas masih tetap ada. Sebagian besar penelitian ada berfokus pada pelaporan skor kematangan dan status kesiapan dengan pembahasan yang terbatas tentang bagaimana hasil evaluasi dapat secara sistematis diterapkan menjadi strategi perbaikan berdasarkan kondisi institusi. Selain itu, banyak studi yang menekankan pada sekolah negeri atau lembaga non-formal, sementara analisis terhadap sekolah swasta yang dikelola oleh pesantren masih terbatas, terutama dalam hal struktur tata kelola, keterbatasan sumber daya, dan pila penggunaan teknologi. Selain itu, penelitian sebelumnya menyajikan hasil evaluasi secara deskriptif tanpa melihat kelemahan yang timbul di beberapa aspek untuk memberikan rekomendasi yang realistis untuk peningkatan tingkat kematangan institusi. Oleh karena itu, penelitian ini akan mengatasi kesenjangan tersebut dengan tidak hanya mengevaluasi kesiapan keamanan informasi menggunakan Indeks KAMI 4.2, tetapi juga melakukan analisis terhadap kelemahan di seluruh komponen untuk mengidentifikasi prioritas perbaikan yang realistis untuk dapat meningkatkan tingkat kematangan institusi. Pendekatan ini memberikan nilai tambah dengan menawarkan wawasan yang dapat ditindaklanjuti oleh pimpinan institusi dari pada sekadar menyajikan skor penilaian.

Tujuan utama penelitian ini adalah menilai tingkat kesiapan keamanan teknologi informasi pada studi kasus instansi swasta MA Nurul Ummah Yogyakarta menggunakan instrumen evaluasi Indeks KAMI 4.2. Instrumen evaluasi kemudian digunakan untuk mengidentifikasi area-area kelemahan keamanan dan menyusun rekomendasi perbaikan kebijakan dan prosedur keamanan dalam penyelenggaraan teknologi informasi untuk meningkatkan tingkat kesiapan pada instansi tersebut. Penelitian ini diharapkan dapat memberikan pemahaman yang menyeluruh untuk MA Nurul Ummah Yogyakarta tentang kondisi keamanan teknologi informasi sehingga dapat menyesuaikan dan menentukan kebijakan-kebijakan dalam meningkatkan aspek-aspek yang belum optimal agar aset informasi institusi tetap terjaga dengan baik.

2. METODOLOGI PENELITIAN

Metodologi penelitian ini disusun ke dalam beberapa tahap sistematis untuk memastikan evaluasi Indeks KAMI yang komprehensif. Gambaran rinci mengenai tahapan penelitian ini, mulai dari pengumpulan data awal hingga analisis akhir dapat dilihat pada Gambar 1.



Gambar 1. Alur Penelitian

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **03/06/2026**; Accepted: **28/06/2026**; Published: **30/07/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7, Nomor 4, Juli – Agustus 2026, Page 1072-1079
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

2.1 Pengumpulan Data

Penelitian ini berfokus pada pengumpulan skor penilaian yang dapat diukur untuk mencerminkan tingkat kematangan implementasi keamanan informasi di institusi. Data dikumpulkan melalui observasi dan wawancara. Observasi dilakukan untuk mengamati secara langsung kondisi infrastruktur teknologi informasi, penggunaan sistem, serta prosedur pengelolaan sistem informasi. Wawancara dilakukan dengan responden terpilih untuk mengisi kuesioner Indeks KAMI untuk memperoleh informasi mengenai kebijakan, prosedur dan implementasi yang bersifat teknis.

Subjek penelitian ini mencakup beberapa *stakeholder* yang memiliki kewenangan dan pemahaman terkait pengelolaan teknologi informasi di instansi, seperti pimpinan instansi sebagai penanggung jawab kebijakan yang berlaku dan tim IT atau operator sekolah sebagai pelaksana teknis infrastruktur teknologi informasi. Responden dipilih menggunakan *purposive sampling*, berdasarkan wewenang, keterlibatan dan peran yang paling dominan dan memiliki pemahaman dalam pengelolaan teknologi informasi di instansi [10]. Data yang dikumpulkan kemudian digunakan untuk menghitung skor Indeks KAMI untuk setiap aspek penilaian sebagai dasar untuk analisis lebih lanjut.

2.2 Evaluasi Indeks KAMI

Penilaian tingkat kesiapan keamanan informasi dilakukan menggunakan Indeks KAMI 4.2 berdasarkan kriteria SNI ISO/IEC 27001 sebagai instrumen evaluasi Indeks KAMI 4.2 dipilih karena terbukti mampu memetakan kondisi kesiapan keamanan informasi khususnya dilingkungan Perguruan Tinggi maupun di lingkup sekolah [8], [11]. Proses evaluasi dilakukan dengan melakukan penilaian dari beberapa aspek seperti pada Tabel 1.

Tabel 1. Kriteria penilaian Indeks KAMI 4.2

Kriteria	**Keterangan**
Bagian 1: Kategori Sistem Elektronik	Evaluasi tingkat atau kategori sistem elektronik yang digunakan
Bagian II: Tata Kelola Keamanan Informasi	Evaluasi kesiapan bentuk beserta fungsi, tugas dan tanggung jawab pengelola.
Bagian III: Pengelolaan Risiko Keamanan Informasi	Evaluasi kesiapan penerapan pengelolaan risiko sebagai dasar penerapan strategi keamanan informasi.
Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi	Evaluasi kelengkapan dan kesiapan kerangka kerja pengelolaan dan strategi penerapan keamanan informasi.
Bagian V: Pengelolaan Aset Informasi	Evaluasi kelengkapan pengamanan dan penggunaan aset informasi.
Bagian VI: Teknologi dan Keamanan Informasi	Evaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.
Bagian VII: Suplemen	Evaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

Pertanyaan dalam instrumen Indeks KAMI dikelompokkan untuk dua keperluan. Kelompok pertanyaan pertama dikategorikan untuk menilai tingkat kesiapan penerapan pengamanan dengan kelengkapan dokumen pengawasan sesuai dengan ISO/IEC 27001:2013. Hasil penilaian tingkat kesiapan yang ditampilkan dalam *dashboard* akan dikelompokkan menjadi beberapa tingkatan seperti pada Tabel 2.

Tabel 2**.** Pengelompokkan status kesiapan berdasarkan kategori 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**		**Status Kesiapan**
16	34	0	272	Tidak Layak
		273	455	Pemenuhan Kerangka Kerja Dasar
		456	583	Cukup Baik
		584	645	Baik
Strategis		**Skor Akhir**		**Status Kesiapan**
35	50	0	333	Tidak Layak
		334	535	Pemenuhan Kerangka Kerja Dasar
		536	609	Cukup Baik
		610	645	Baik

Kelompok pertanyaan kedua kedua dikategorikan berdasarkan tingkat kematangan penerapan keamanan teknologi informasi dengan kategorisasi yang mengacu pada kerangka kerja COBIT atau CMMI [6]. Penilaian ini menggunakan skala lima tingkat kematangan untuk mengukur seberapa efektif dan konsisten cara kerja pengamanan yang diterapkan dalam organisasi atau instansi yang dapat dilihat pada Tabel 3.

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **03/06/2026**; Accepted: **28/06/2026**; Published: **30/07/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7, Nomor 4, Juli – Agustus 2026, Page 1072-1079
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

Tabel 3. Tingkat kematangan Indeks KAMI 4.2

Tingkat	Deskripsi
I	Kondisi Awal
II	Penerapan Kerangka Kerja Dasar
III	Terdefinisi dan Konsisten
IV	Terkelola dan Terukur
V	Optimal

BSSN menambahkan tingkat kematangan dengan tingkat I+, II+, III+, dan IV+. Tujuannya adalah agar lebih memudahkan dalam memberikan gambaran dan uraian yang lebih detail. Adapun tingkat kematangan yang diharapkan dari penilaian ini sesuai standar ISO/IEC 27001:2013 adalah pada tingkat III+ [6].

Pada pelaksanaannya, penilaian dalam penelitian ini dilakukan menggunakan penilaian mandiri berdasarkan wawancara terstruktur dengan pemangku kepentingan utama. Penelitian ini hanya bergantung pada penjelasan dan konfirmasi responden mengenai kebijakan, prosedur, dan implementasi teknis yang berlaku. Dokumen pendukung tidak dikumpulkan secara formal sebagai data penelitian. Oleh karena itu, hasil penilaian mencerminkan tingkat implementasi keamanan informasi yang dirasakan oleh instansi pada saat penelitian dilakukan.

2.3 Analisis Hasil Evaluasi

Hasil pengisian instrumen Indeks KAMI yang telah dilakukan bersama instansi akan diuraikan pada bagian Hasil dan Pembahasan untuk memetakan tingkat kesiapan keamanan teknologi informasi. Informasi yang didapatkan dari hasil evaluasi ini akan menjadi laporan dan rekomendasi saran bagi pimpinan dalam pengelolaan kebijakan yang disesuaikan untuk keamanan teknologi informasi instansi.

3. HASIL DAN PEMBAHASAN

Bagian ini akan memaparkan dan membahas hasil evaluasi yang telah dilakukan menggunakan Indeks KAMI 4.2 melalui *dashboard* penilaian pada Gambar 2. *Dashboard* ini akan memberikan gambaran umum tingkat kematangan keamanan informasi di instansi berdasarkan beberapa kriteria penilaian untuk kemudian diidentifikasi kelebihan dan kelemahan dari pengelolaan yang sudah ada.

Gambar 2. *Dashboard* penilaian Indeks KAMI 4.2

Berdasarkan *dashboard* pada Gambar 2 di atas, dapat dilihat bahwa tingkat kesiapan yang diperoleh instansi saat ini adalah "Tidak Layak" dengan skor total sebesar 182. Tingkat kematangan instansi saat ini berkisar pada tingkat I hingga I+, menunjukkan instansi masih berada pada kondisi awal dan belum mencapai kondisi yang terkelola dan terukur. Sebagian kriteria seperti Tata Kelola, Pengelolaan Risiko, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset berada pada tingkat kematangan I+. Hal ini menunjukkan bahwa pengelolaan dasar sudah mulai diterapkan namun belum menyeluruh secara lengkap dan konsisten. Di samping itu, aspek Teknologi dan Keamanan Informasi masih berada pada tingkat kematangan I, menunjukkan kelemahan dalam implementasi pengelolaan aspek keamanan informasi yang bersifat teknis.

Skor yang lebih rendah pada aspek teknologi ini merupakan temuan kritis. Meskipun lembaga telah mulai membuat aturan dan dokumentasi, namun alat yang secara teknis untuk mendukung kebijakan tersebut masih belum memadai atau masih lemah. Tingkat kematangan I hingga I+ terkadang menunjukkan bahwa proses keamanan informasi instansi bersifat reaktif, di mana instansi cenderung memperbaiki masalah sebagai respons dari insiden yang muncul akibat kurangnya pemantauan dan perbaikan berkala, sehingga upaya pencegahan belum berjalan dengan baik [12]. Kondisi ini menunjukkan bahwa keamanan informasi saat ini terlalu bergantung pada individu tertentu daripada tim dengan sistem yang lengkap dan terdokumentasi. Jika sumber daya manusia ini tidak tersedia atau membuat

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **03/06/2026**; Accepted: **28/06/2026**; Published: **30/07/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7, Nomor 4, Juli – Agustus 2026, Page 1072-1079
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

kesalahan, maka keamanan instansi menjadi lebih berisiko. Selisih antara skor Tata Kelola (I+) dan skor Teknologi (I) menunjukkan adanya sedikit perbedaan perencanaan dan pelaksanaan pengelolaan. Instansi sudah mulai melakukan perencanaan keamanan, namun kontrol yang bersifat teknis belum cukup memadai untuk melaksanakan perencanaan tersebut secara efektif. Temuan yang serupa juga terdapat pada penelitian sebelumnya [7], [8], [9], yang menunjukkan bahwa institusi pendidikan sering memprioritaskan ketersediaan layanan dan fungsionalitas administratif daripada langkah-langkah keamanan teknis yang bersifat preventif. Berikut ini adalah paparan lengkap hasil penilaian Indeks KAMI 4.2 berdasarkan tujuh kriteria penilaian.

3.1 Kategori Sistem Elektronik

Pada bagian pertama ini, instansi memperoleh skor sebesar 18 dengan tingkat ketergantungan yang tinggi. Berdasarkan penilaian pada bagian ini, ditemukan bahwa skala investasi dan anggaran masih tergolong rendah. Di samping itu, instansi juga mengelola data yang bersifat sensitif yang saling terkait dan data yang bersifat rahasia. Melihat sifat data yang dikelola maka proses mitigasi diperlukan, namun teknik kriptografi belum dihadirkan dalam proses pengamanan data. Hal ini menjadi kelemahan instansi karena implementasi enkripsi data memiliki peran penting dalam perlindungan data dan tidak/belum diterapkan [4]. Langkah perbaikan yang bisa dilakukan instansi seperti perlu meningkatkan alokasi anggaran yang berfokus pada keamanan informasi, khususnya penerapan teknik kriptografi seperti enkripsi data.

3.2 Tata Kelola Keamanan Informasi

Bagian kedua pada instrumen ini menunjukkan skor sebesar 36. Instansi secara umum mengembangkan tata kelola namun belum maksimal. Struktur instansi dan fungsi pengelolaan pengamanan informasi sudah ada diterapkan sebagian, koordinasi antar tim dalam lingkup internal dan eksternal sudah berjalan, serta tanggung jawab terhadap kelangsungan layanan TIK di instansi juga sudah ditentukan. Namun, masih ada beberapa kelemahan meliputi pemetaan peran dan segregasi wewenang, penentuan metrik kinerja dan evaluasi, serta kebijakan yang mencakup aspek hukum terkait penanggulangan insiden keamanan informasi. Kondisi ini juga terjadi dalam temuan literatur lain yang mengatakan bahwa rendahnya tingkat keamanan informasi biasanya terjadi karena kurang atau tidak adanya pembagian tugas yang baik dan kurangnya kebijakan formal yang mendukung tata kelola dari pimpinan [13]. Untuk memperbaiki bagian ini, instansi perlu menyusun pembagian tugas secara jelas dengan menentukan tiap aktor serta wewenangnya dalam tata kelola, menetapkan indikator kerja dan membuat kebijakan terkait penanggulangan insiden.

3.3 Pengelolaan Risiko Keamanan Informasi

Bagian ketiga menunjukkan hasil evaluasi sebesar 19, yang menggambarkan proses pengelolaan risiko keamanan informasi mulai diterapkan namun belum menyeluruh dan belum lengkap. Beberapa elemen dari tingkat dasar (II) sudah diterapkan seperti bagian penanggung jawab risiko dan pendefinisian pemilik aset informasi. Beberapa elemen di tingkat selanjutnya (III-V) seperti pada bagian mitigasi risiko sudah direncanakan namun belum diterapkan dan dipantau secara berkala. Secara umum, bagian ini masih berada pada tahap dasar dan masih membutuhkan penguatan kerangka kerja serta mitigasi risiko ke dalam tata kelola keamanan informasi instansi. Sementara itu, manajemen risiko yang baik tidak berhenti pada identifikasi aset saja, tapi bertahap menuju pengelolaan mitigasi dan pemantauan secara berkala untuk meminimalisir dampak ancaman keamanan informasi [14]. Sebagai langkah perbaikan yang bisa dilakukan oleh instansi yaitu dengan menerapkan mitigasi risiko yang sudah direncanakan dan menetapkan langkah penerapan prosedur pemantauannya. Selain itu, penerapan evaluasi juga perlu direncanakan dan direalisasikan terhadap prosedur mitigasi yang ada.

3.4 Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian keempat pada instrumen ini menunjukkan hasil evaluasi sebesar 42, menunjukkan sebagian kebijakan dan prosedur seperti komunikasi kebijakan, proses identifikasi kondisi dan kerangka kerja pengelolaan kelangsungan TIK sudah berjalan, meskipun masih diterapkan sebagian. Sedangkan, aspek seperti kebijakan formal untuk semua stakeholder, manajemen pelaporan pengamanan, serta strategi keamanan informasi masih dalam perencanaan. Di sisi lain, aspek yang berhubungan dengan rencana pemulihan insiden terhadap layanan TIK, program audit internal dan monitoring secara berkala masih belum diterapkan, padahal audit keamanan internal secara berkala dapat membantu instansi menilai dan mengindentifikasi potensi kerentanan sebelum insiden terjadi [15]. Secara keseluruhan, kondisi ini menunjukkan bahwa instansi perlu membuat kebijakan secara formal yang terdokumentasi dengan baik, mempertimbangkan evaluasi, audit dan rencana pemulihan insiden agar kerangka kerja menjadi lebih baik.

3.5 Pengelolaan Aset Informasi

Berdasarkan hasil evaluasi instrumen Indeks KAMI pada bagian kelima, ditemukan bahwa skor yang didapatkan sebesar 53. Pengelolaan aset informasi yang berkaitan dengan proses teknologi informasi, pengamanan fisik dan beberapa aspek dasar instrumen sudah diterapkan sebagian atau setidaknya masih dalam proses perencanaan. Beberapa pengelolaan yang sudah diterapkan secara menyeluruh mencakup inventarisasi aset informasi dan proses pengecekan latar belakang SDM. Namun, bagian pengelolaan aset informasi memiliki status tidak dilakukan dan

Terakreditasi SINTA 5 SK :72/E/KPT/2024 Submitted: **03/06/2026**; Accepted: **28/06/2026**; Published: **30/07/2026**

JURNAL MEDIA INFORMATIKA [JUMIN]
Volume 7, Nomor 4, Juli – Agustus 2026, Page 1072-1079
ISSN 2808-005X (media online)
Available Online at http://ejournal.sisfokomtek.org/index.php/jumin

dalam perencanaan yang paling banyak dibandingkan bagian pengamanan fisik. Aspek ini berkaitan dengan klasifikasi aset informasi, pengelolaan tingkat akses berdasarkan klasifikasi, perlindungan data pribadi, proses penghancuran data dan prosedur pencadangan atau pemulihan aset. Tidak adanya prosedur pencadangan dan pemulihan pada bagian ini menjadikan institusi rentan terhadap kehilangan data saat terjadi insiden [8]. Saran perbaikan yang bisa dilakukan adalah instansi perlu menyusun ulang dan menerapkan kebijakan yang berkaitan dengan klasifikasi aset informasi dan pengaturan hak akses serta pengamanannya agar sesuai dengan tingkat kepentingan aset (berdasarkan klasifikasi). Selain itu, pengelolaan pencadangan dan pemulihan data/aset juga perlu direncanakan atau setidaknya mulai diterapkan pada instansi untuk menjamin ketersediaan aset informasi secara aman.

3.6 Teknologi dan Keamanan Informasi

Pada bagian ini, instansi memperoleh skor sebesar 32. Pemanfaatan teknologi untuk pengelolaan keamanan masih sangat rendah dan masih sedikit yang berada pada tahap penerapan, dan sebagian besar aspek instrumen belum dilakukan. Beberapa aspek yang sudah mulai diterapkan sebagian seperti pengamanan berlapis dalam penggunaan internet, penjaminan ketersediaan infrastruktur jaringan/sistem/aplikasi, pengelolaan kata sandi, penggunaan antivirus, serta pengamanan pada *environment* pengembang dan pengujian sistem. Sedangkan aspek yang belum dilakukan seperti segmentasi pada jaringan, penggunaan konfigurasi keamanan, pemindaian celah keamanan, standar penggunaan enkripsi, serta penerapan analisis log. Lemahnya aspek teknis pada bagian ini biasanya disebabkan karena biasanya institusi hanya berfokus pada pemenuhan ketersediaan layanan tanpa begitu memperhatikan aspek keamanan [11]. Berdasarkan hal ini, instansi perlu memprioritaskan penggunaan segmentasi jaringan dan penyusunan standar pengelolaan keamanan lainnya. Selain itu, pencatatan log dan pemindaian terhadap kerentanan ancaman dan penerapan enkripsi juga perlu mulai direncanakan untuk melindungi aset informasi penting instansi.

3.7 Suplemen

Berdasarkan hasil evaluasi pada bagian terakhir ini, dapat disimpulkan bahwa pengelolaan aspek keamanan informasi tambahan masih berada pada tahap awal dan belum sepenuhnya diterapkan. Dalam hal seperti keterlibatan pihak ketiga, sebagian besar instrumen berada dalam status belum dilakukan dan masih dalam proses perencanaan. Hal ini menunjukkan bahwa manajemen risiko, ketentuan keamanan dalam kontrak, mekanisme audit, penanganan insiden, atau pengelolaan kelangsungan layanan pihak ketiga yang masih belum memadai dan belum dipenuhi. Aspek pengamanan *cloud service* juga menunjukkan kondisi belum dilakukan dan masih dalam perencanaan. Sementara itu, aspek perlindungan data pribadi sudah mulai diterapkan sebagian meskipun juga masih banyak yang berada pada kondisi dalam perencanaan. Setidaknya ada empat langkah dasar dalam melakukan perlindungan data pribadi, seperti mengindentifikasi data, menemukan lokasi dan aliran data, mengklasifikasikan sesuai sensitivitas dan mengamankan dengan langkah-langkah yang sesuai . Intinya, instansi perlu untuk mengembangkan dan menerapkan kebijakan dan prosedur formal terkait pengelolaan pihak ketiga, penggunaan *cloud service*, dan perlindungan data pribadi, ketentuan keamanan dalam perjanjian kerja sama, serta mekanisme pemantauan dan pelaporan insiden, sehingga implementasi keamanan informasi dapat lebih konsisten dan berkelanjutan.

Untuk memahami posisi institusi ini dengan lebih baik, perlu untuk membandingkan hasil-hasil penilaian tingkat kesiapan keamanan teknologi informasi pada tiga studi berbeda yang telah disebutkan di latar belakang penelitian ini. Perbandingan ini membantu untuk melihat sejauh mana kinerja instansi ini dibandingkan dengan instansi-instansi yang serupa. Studi pertama pada SMK XYZ menggunakan Indeks KAMI 4.2 mendapatkan status "Tidak Layak" dengan total skor sebesar 314 [7]. Terdapat perbedaan yang besar jika kita bandingkan dengan total skor yang diperoleh instansi di penelitian ini, yaitu 182. Meskipun keduanya memperoleh status "Tidak Layak", SMK XYZ jauh lebih dekat untuk mencapai standar ISO 27001, sedangkan instansi ini masih tertinggal dan perlu bekerja lebih keras untuk mencapai status yang lebih baik. Studi kedua menunjukkan perbedaan hasil yang sangat signifikan. SMKN 1 Banyumas memperoleh status "Baik" dengan total skor sebesar 629 [8]. Perbandingan ini sangat penting karena menunjukkan bahwa sebuah instansi dapat mencapai tingkat kematangan tinggi dalam keamanan teknologi informasi jika mengikuti standar ISO yang telah ditetapkan. Selisih yang sangat besar menunjukkan instansi ini masih banyak kekurangan pada berbagai aspek keamanan seperti dokumentasi yang lengkap dan penerapan teknis yang kuat. Studi yang terakhir di Pondok Pesantren Sunni Darussalam Yogyakarta menunjukkan skor sebesar 170 dan 284 dengan status rendah dan tidak optimal [9]. Hasil ini hampir sama dengan total skor yang diperoleh instansi ini. Hal ini menunjukkan bahwa instansi-instansi yang berada di bawah lembaga non-formal sering menghadapi masalah yang sama, yaitu fokus pada operasional sehari-hari dan mengabaikan pentingnya keamanan informasi.

Dominasi tingkat kematangan I dan I+ juga menunjukkan bahwa praktik keamanan informasi di instansi masih bersifat reaktif daripada proaktif. Tindakan keamanan umumnya diambil setelah masalah muncul, daripada didorong oleh penilaian risiko berkelanjutan dan kontrol pencegahan. Kondisi ini meningkatkan kerentanan institusi terhadap kebocoran data, kegagalan sistem, dan kesalahan manusia *(human error)* terutama mengingat meningkatnya jumlah insiden siber yang telah dilaporkan secara nasional [5]. Oleh karena itu, temuan ini menekankan perlunya institusi untuk melampaui kepatuhan dasar dan mulai mengintegrasikan kontrol teknis yang mendukung kerangka kerja tata kelola dan manajemen risiko. Secara keseluruhan, analisis perbandingan menegaskan bahwa tingkat kematangan yang

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **03/06/2026**; Accepted: **28/06/2026**; Published: **30/07/2026**

rendah yang telah diamati dalam penelitian ini bukanlah permasalahan yang terisolasi, tetapi ada bagian dari pola yang lebih luas yang ditemukan di instansi pendidikan serupa. Namun, kesenjangan yang signifikan antara instansi ini dan instansi lain yang berkinerja lebih tinggi menunjukkan bahwa perbaikan adalah hal yang mungkin.

Rekomendasi yang bisa dilakukan untuk meningkatkan skor total dan mencapai tingkat kematangan yang lebih baik, dari level I ke level yang lebih tinggi, instansi perlu fokus pada peningkatan yang terstruktur dan realistis berdasarkan evaluasi Indeks KAMI. Masalah utama yang diidentifikasi bukanlah kurangnya upaya, melainkan kurangnya pengelolaan secara formal, terdokumentasi dan implementasi yang konsisten. Oleh karena itu, langkah penting untuk dilakukan instansi dengan beralih dari sistem kerja yang hanya berorientasi pada individu ke sistem kerja yang berorientasi pada proses yang didukung oleh kebijakan dan prosedur yang jelas.

Di antara ketujuh komponen kriteria penilaian, Tata Kelola Keamanan Informasi serta Teknologi dan Keamanan Informasi adalah area paling strategis untuk meningkatkan tingkat kematangan. Peningkatan tata kelola dapat dicapai dengan mendefinisikan peran, wewenang, indikator kinerja, dan kebijakan dalam penanganan insiden secara jelas. Proses manajemen risiko harus dikembangkan, mulai dari identifikasi aset hingga implementasi dan pemantauan secara rutin sebagai bentuk dari tindakan mitigasi risiko. Langkah-langkah ini lebih membutuhkan komitmen instansi dari pada biaya yang tinggi.

Dari aspek teknis, tindakan prioritas yang perlu dilakukan meliputi implementasi enkripsi data, prosedur pencadangan dan pemulihan, pencatatan dan pemantauan, dan pemeriksaan keamanan secara rutin. Langkah ini secara langsung mengatasi kelemahan utama di beberapa komponen dan dapat secara signifikan mampu meningkatkan skor secara keseluruhan. Selain itu, sangat penting untuk memberikan pelatihan keamanan dasar kepada seluruh elemen di instansi untuk meningkatkan kesadaran pentingnya keamanan informasi agar dapat diberlakukan sebagai tanggung jawab bersama. Dengan memprioritaskan aspek-aspek ini dan secara konsisten menggunakan Indeks KAMI sebagai referensi, instansi diharapkan mampu meningkatkan tingkat kematangannya dan semakin mendekati standar kepatuhan ISO 27001.

4. KESIMPULAN

Berdasarkan hasil evaluasi dan analisis Indeks KAMI 4.2, status penilaian keseluruhan yang diperoleh dapat diklasifikasikan “Tidak Layak”. Hal ini dapat disimpulkan bahwa kesiapan keamanan teknologi informasi di Madrasah Aliyah Nurul Ummah Yogyakarta masih tergolong sangat rendah atau pada tahap awal. Tingkat kematangan yang dicapai menunjukkan bahwa praktik keamanan informasi telah diterapkan, namun belum sistematis, konsisten, atau sepenuhnya terintegrasi di seluruh bidang tata Kelola, manajemen risiko, dan teknis. Temuan ini menegaskan bahwa instansi ini belum memenuhi tingkat kesiapan yang diharapkan sesuai dengan standar ISO/IEC 27001.

Kelemahan utama yang ditemukan tidak hanya terletak pada tidak adanya kebijakan formal, tetapi pada ketidakseimbangan antara perencanaan dan penerapam. Aspek tata Kelola telah mulai berkembang, sementara aspek kontrol keamanan teknis dan mitigasi risiko masih sangat terbatas. Berdasarkan hal itu, penerapan keamanan informasi cenderung reaktif dan bergantung pada peran beberapa individu saja daripada didukung oleh kontrol yang terstruktur. Kondisi ini yang kemudian bisa menjelaskan mengapa instansi akan tetap rentan terhadap risiko keamanan informasi karena ketergantungan pada teknologi untuk proses akademik dan administrasi yang semakin meningkat.

Hasil ini juga menegaskan dan konsisten dengan temuan penelitian sebelumnya pada intansi serupa, terutama yang beroperasi dengan sumber daya terbatas dan berdiri pada pengelolaan informal. Namun, kesenjangan yang wsignifikan antara instansi ini dengan instansi dengan kinerja yang lebih tinggi juga menunjukkan bahwa perbaikan dapat dicapai melalui upaya bertahap dan terfokus, khususnya dalam memprioritaskan kebijakan formal keamanan dan penerapan kontrol teknis yang lebih baik lagi.

Penelitian ini memiliki beberapa keterbatasan. Evaluasi yang dilakukan menggunakan pendekatan penilaian mandiri berdasarkan wawacara tanpa verifikasi formal melalui dokumen pendukung atau audit teknis. Selain itu, penelitian ini terbatas pada satu instansi, yang membatasi generalisasi temuan. Oleh karena itu, hasil penelitian akan mencerminkan konteks dan kondisi spesifik pada instansi studi kasus saja. Penelitian lebih lanjut disarankan untuk melibatkan analisis dokumen, pengujian teknis, atau audit untuk memvalidasi hasil penilaian dan meningkatkan akurasi data. Studi perbandingan yang melibatkan beberapa instansi juga disarankan untuk memahami perkembangan kematangan keamanan informasi seiring waktu. Pendekatan-pendekatan ini diharapkan dapat memberikan wawasan yang lebih mendalam dan bukti empiris yang lebih kuat untuk mendukung strategi peningkatan keamanan informasi di instansi pendidikan.

UCAPAN TERIMAKASIH

Terima kasih yang sebesar-besarnya kami ucapkan kepada Dr. Ir. Bambang Sugiantoro, M.T., IPU., ASEAN Eng., sebagai dosen pada mata kuliah “Proyek Pengkajian Jaringan Komputer” di Magister Informatika UIN Sunan Kalijaga Yogyakarta atas segala bimbingan, arahan, dan dukungan yang sangat berarti selama penelitian ini. Kami

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **03/06/2026**; Accepted: **28/06/2026**; Published: **30/07/2026**

sangat berterima kasih atas masukan konstruktif, dorongan, dan dedikasinya yang telah memberikan kontribusi yang signifikan dalam memperkaya pembelajaran dan pengembangan kami di bidang ini.

REFERENCES

[1] C. P. N. Azizah and Subiyantoro, "Pemanfaatan Teknologi Informasi Dalam Menunjang Mutu Pendidikan Sekolah," *Kelola J. Islam. Educ. Manag.*, vol. 8, no. 1, pp. 11–28, Apr. 2023, doi: 10.24256/KELOLA.V8I1.3452.

[2] I. K. A. Subagio and A. M. N. Limbong, "Dampak Teknologi Informasi Dan Komunikasi Terhadap Aktivitas Pendidikan," *J. Learn. Technol.*, vol. 2, no. 1, pp. 43–52, Jun. 2023, doi: 10.33830/jlt.v2i1.5844.

[3] M. Suhardi and A. Fahmi, "The Role of Information Technology in the Development of Education Management Systems in the Digital Age: A Literature Review."

[4] F. Azzahra, Irsyad, and M. Setiawati, "Analisis Risiko Keamanan Data Siswa Dalam Sistem Administrasi Berbasis Digital," *Glob. Res. Innov. J.*, vol. 1, no. 3, pp. 3150–3154, Dec. 2025, Accessed: Dec. 23, 2025. [Online]. Available: https://journaledutech.com/index.php/great/article/view/866

[5] Badan Siber dan Sandi Negara, "Lanskap Keamanan Siber Indonesia 2024," 2024.

[6] "Indeks KAMI - www.bssn.go.id." Accessed: Dec. 06, 2025. [Online]. Available: https://www.bssn.go.id/indeks-kami/

[7] H. I. Azmi, M. T. Akbar, B. T. K. Dewi, and B. Sugiantoro, "Evaluasi Tingkat Kesiapan Keamanan Informasi Pada SMK XYZ Menggunakan Indeks KAMI Versi 4.2," *Cyber Secur. dan Forensik Digit.*, vol. 7, no. 1, pp. 42–49, Nov. 2024, doi: 10.14421/csecurity.2024.7.1.4422.

[8] R. Nugroho, I. Setiawan, R. N. Akmal, and N. Azka, "Evaluasi Keamanan Sistem Informasi Pada SMKN 1 Banyumas Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013," *Merkurius J. Ris. Sist. Inf. dan Tek. Inform.*, vol. 2, no. 6, pp. 110–118, Oct. 2024, doi: 10.61132/MERKURIUS.V2I6.423.

[9] S. Bahri, Y. Wijayanti, R. Dewantara, and A. T. Hidayat, "Evaluasi Sistem Keamanan Teknologi Informasi Menggunakan Indeks Kami dan Cobit 5 Di Pondok Pesantren," *J. Janitra Inform. dan Sist. Inf.*, vol. 4, no. 2, pp. 119–128, Feb. 2024, doi: 10.59395/PXZWYD38.

[10] N. Suriani, Risnita, and M. S. Jailani, "Konsep Populasi dan Sampling Serta Pemilihan Partisipan Ditinjau Dari Penelitian Ilmiah Pendidikan." [Online]. Available: http://ejournal.yayasanpendidikandzurriyatulquran.id/index.php/ihsan

[11] 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, Aug. 2023, doi: 10.29100/JIPI.V8I3.3720.

[12] D. Ayu, A. Faroqi, and A. Wulansari, "Evaluation of Information Security Management Capability Level with COBIT 5," *bit-Tech*, vol. 8, no. 1, pp. 726–737, Aug. 2025, doi: 10.32877/BT.V8I1.2682.

[13] Evariani, M. I. Herdiansyah, E. S. Negara, and T. Sutabri, "Analisis Keamanan Informasi Dan Tata Kelola Sistem Di Sekolah Tinggi Ilmu Kesehatan Bina Husada Menggunakan Indeks-KAMI," *Djtechno J. Teknol. Inf.*, vol. 6, no. 1, pp. 219–236, Apr. 2025, doi: 10.46576/DJTECHNO.V6I1.6126.

[14] M. T. Anwar, U. Aryanti, M. Wijana, and D. Atmoko, "Mitigasi Risiko Keamanan Informasi Menggunakan SNI ISO/IEC 27001:2013 Berbasis Manajemen Risiko OCTAVE Allegro di Perguruan Tinggi : Studi kasus Perguruan Tinggi x," *INFORMATICS Educ. Prof. J. Informatics*, vol. 9, no. 1, p. 73, Jun. 2024, doi: 10.51211/ITBI.V9I1.2913.

[15] Š. Grigaliūnas, M. Schmidt, R. Brūzgienė, P. Smyrli, S. Andreou, and A. Lopata, "Holistic Information Security Management and Compliance Framework," *Electron. 2024, Vol. 13, Page 3955*, vol. 13, no. 19, p. 3955, Oct. 2024, doi: 10.3390/ELECTRONICS13193955.

Terakreditasi SINTA 5 SK :72/E/KPT/2024
Submitted: **03/06/2026**; Accepted: **28/06/2026**; Published: **30/07/2026**