

Evaluasi Tata Kelola Keamanan Informasi pada Kementerian Agama Kota Yogyakarta Menggunakan INDEKS KAMI Versi 4.2

M. Fajratul Ikhsan¹, Nur Fikri Khuluq², Muh. Naufal Muzhaffar³, Bambang Sugiantoro⁴

^{1,2,3,4} UIN Sunan Kalijaga Yogyakarta

Email: Ikhsanm288@gmail.com

Abstrak– Kemajuan teknologi informasi pada instansi pemerintah meningkatkan risiko terhadap keamanan data sensitif, sehingga diperlukan evaluasi tingkat kematangan keamanan informasi secara terukur. Penelitian ini bertujuan untuk mengevaluasi tingkat kematangan keamanan informasi pada Kementerian Agama Kota Yogyakarta menggunakan Indeks Keamanan Informasi (KAMI) versi 4.2. Metode yang digunakan adalah kuantitatif evaluatif dengan pengumpulan data melalui kuesioner terstruktur yang diisi oleh personel kunci, kemudian dianalisis menggunakan perangkat lunak Indeks KAMI untuk memperoleh skor dan level kematangan. Hasil penelitian menunjukkan bahwa tingkat keamanan informasi berada pada kategori “cukup baik” dengan skor total 469. Terdapat disparitas antar domain, di mana pengelolaan risiko mencapai level tertinggi (V), sementara kerangka kerja keamanan informasi berada pada level terendah (I+). Selain itu, aspek pengamanan pihak ketiga dan perlindungan data pribadi menunjukkan kelemahan kritis dengan skor 0%. Penelitian ini menyimpulkan bahwa diperlukan penguatan pada kerangka kerja keamanan dasar, tata kelola data pribadi, serta manajemen risiko pihak ketiga guna meningkatkan kematangan keamanan informasi dan mendukung tata kelola pemerintahan yang lebih aman dan terpercaya.

Kata Kunci: Indeks KAMI, Tingkat Kematangan Keamanan, Kementerian Agama

Abstract– Advances in information technology in government agencies such as the Ministry of Religious Affairs of Yogyakarta City increase security risks to sensitive data. This study aims to evaluate the level of information security maturity in the agency to identify existing strengths and weaknesses. The research stages include literature review, initial observation, data collection, processing and evaluation using the Information Security Index (KAMI), and the preparation of results and recommendations. The methodology used is quantitative evaluative by applying the KAMI Index instrument version 4.2 developed by the National Cyber and Crypto Agency (BSSN). Data collection was carried out through a structured questionnaire completed by key personnel, then the data was processed using KAMI Index software to generate a maturity score. The evaluation results show that the overall level of information security is in the fairly good category with a total score of 469. However, there is a significant disparity between domains, with risk management reaching the highest level (V), while the information security framework is at the lowest level (I+). The most crucial weaknesses were found in the domains of third-party engagement security and personal data protection, both of which scored 0%. The study concluded that there is an urgency for agencies to strengthen their basic security frameworks, personal data governance, and third-party risk management to achieve a more secure and reliable governance system.

Keywords: KAMI Index, Security Maturity Level, Ministry of Religious Affairs

1. PENDAHULUAN

Kemajuan teknologi informasi di era digital saat ini memberikan dampak yang signifikan terhadap berbagai aspek kehidupan, termasuk dalam pengelolaan pemerintahan. Penggunaan teknologi informasi memungkinkan administrasi, pengelolaan data, dan penyediaan layanan publik dilakukan dengan lebih cepat, efisien, dan transparan [1]. Namun, sejalan dengan bertambahnya ketergantungan pada sistem informasi, risiko terhadap keamanan data juga semakin rumit. Ancaman ini tidak hanya muncul dari serangan luar seperti peretasan dan pencurian data, tetapi juga berasal dari kelemahan dari dalam, seperti rendahnya kesadaran pengguna tentang praktik keamanan informasi yang baik [2]. Dengan demikian, perlindungan informasi yang baik. Dengan demikian, perlindungan informasi merupakan elemen penting dalam pelaksanaan pemerintahan yang menggunakan teknologi.

Kementerian Agama sebagai salah satu lembaga pemerintah memainkan peran krusial dalam memberikan layanan kepada masyarakat, terutama dalam aspek keagamaan, pendidikan, dan administrasi publik. Data yang diatur oleh Kementerian Agama sangat bervariasi, mencakup data pegawai, institusi pendidikan keagamaan, tempat ibadah, hingga berkas administrasi internal. Data tersebut sangat sensitif sebab langsung berkaitan dengan identitas individu maupun lembaga. Jika data itu tidak diurus dengan benar, maka dapat memicu risiko bocornya informasi, penyalahgunaan data, hingga berkurangnya kepercayaan masyarakat terhadap instansi pemerintah [3]. Keadaan ini menekankan betapa pentingnya

penerapan pengelolaan keamanan informasi yang cukup di lingkungan Kementerian Agama, termasuk di tingkat daerah seperti Kota Yogyakarta.

Seiring dengan kemajuan itu, Badan Siber dan Sandi Negara (BSSN) sebagai instansi yang memiliki wewenang di sektor keamanan siber di Indonesia telah merilis alat evaluasi yang disebut dengan Indeks Keamanan Informasi (KAMI) [4]. Alat ini dirancang untuk mendukung organisasi, terutama lembaga pemerintah, dalam mengevaluasi tingkat implementasi keamanan informasi yang telah dilaksanakan sesuai dengan standar yang ada. Indeks KAMI merujuk pada standar global ISO/IEC 27001 mengenai Sistem Manajemen Keamanan Informasi (ISMS), yang menekankan tiga pilar utama keamanan informasi, yaitu kerahasiaan, integritas, dan ketersediaan [5]. Dengan menggunakan instrumen ini, organisasi dapat menilai tingkat kematangan sistem keamanan informasinya, serta mengenali area yang masih perlu diperbaiki. Sejalan dengan kemajuan tersebut, Badan Siber dan Sandi Negara (BSSN) sebagai otoritas yang berwenang dalam sektor keamanan siber di Indonesia telah merilis alat evaluasi yang disebut Indeks Keamanan Informasi (KAMI). Alat ini dirancang untuk mendukung organisasi, terutama lembaga pemerintah, dalam mengevaluasi tingkat penerapan keamanan informasi yang telah dilakukan sesuai dengan standar yang ada. Indeks KAMI merujuk pada standar internasional ISO/IEC 27001 mengenai Sistem Manajemen Keamanan Informasi (ISMS), yang menekankan pada tiga pilar utama dalam keamanan informasi, yaitu kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability). Dengan alat ini, organisasi dapat menilai tingkat kematangan sistem keamanan informasi serta mengidentifikasi aspek-aspek yang masih perlu diperbaiki.

Versi terkini dari alat ini, KAMI versi 4.2, menawarkan kerangka evaluasi yang lebih menyeluruh dan sesuai dengan situasi teknologi informasi saat ini. Indeks ini tidak hanya mengevaluasi aspek teknis, tetapi juga aspek pengelolaan, kebijakan, manajemen risiko, serta kesadaran sumber daya manusia mengenai pentingnya keamanan informasi. Hal ini menjadikan KAMI versi 4.2 sebagai instrumen evaluasi yang komprehensif untuk menilai kesiapan suatu lembaga dalam menangani ancaman keamanan informasi. Dengan demikian, implementasi evaluasi memakai KAMI versi 4.2 diharapkan dapat memberikan gambaran sebenarnya mengenai posisi keamanan informasi suatu organisasi, serta menjadi landasan dalam perumusan strategi peningkatan keamanan di masa mendatang.

Kementerian Agama Yogyakarta, sebagai lembaga pemerintah di level daerah, juga menghadapi tantangan serupa dalam melindungi keamanan informasi. Layanan masyarakat yang disediakan memerlukan sistem informasi yang terpercaya, baik dari segi akurasi data maupun perlindungan terhadap kemungkinan ancaman [6]. Penilaian keamanan informasi di instansi ini sangat krusial, karena data yang dikelola tidak hanya bersifat administratif, tetapi juga melibatkan data sensitif yang berkaitan dengan aspek sosial dan keagamaan masyarakat Yogyakarta. Tanpa evaluasi yang jelas, sulit bagi lembaga untuk memahami tingkat kesiapan dan kematangan sistem keamanan informasi yang telah diterapkan.

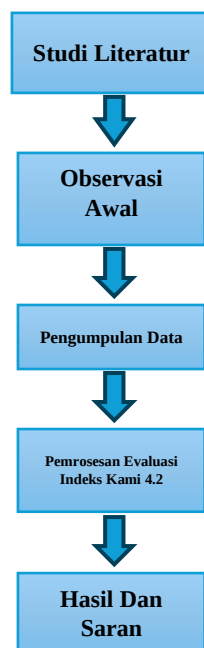
Selain itu, penilaian keamanan informasi melalui Indeks KAMI memberikan keuntungan strategis bagi lembaga. Hasil evaluasi dapat berfungsi sebagai alat ukur yang objektif untuk mengetahui posisi tingkat keamanan informasi yang ada saat ini. Kedua, hasil tersebut dapat menjadi acuan dalam merumuskan kebijakan pengelolaan keamanan informasi yang lebih efisien. Ketiga, penilaian ini mendukung pemimpin lembaga dalam menetapkan prioritas perbaikan, distribusi sumber daya, serta perencanaan program pelatihan untuk karyawan [7]. Oleh karena itu, evaluasi tidak sekadar bentuk ketaatan pada standar, melainkan juga alat untuk meningkatkan mutu layanan publik secara keseluruhan.

Pentingnya evaluasi keamanan informasi telah dibuktikan oleh berbagai penelitian terdahulu serta tingginya urgensi penelitian ini semakin jelas seiring dengan bertambahnya intensitas ancaman siber di sektor pemerintahan [8]. Berbagai lembaga melaporkan bahwa instansi pemerintah sering kali menjadi sasaran utama serangan siber karena mereka mengelola data dalam jumlah besar dan memiliki nilai strategis [9]. Insiden kebocoran data di berbagai lembaga di Indonesia menjadi pengingat jelas mengenai signifikansi penguatan elemen keamanan informasi. Dengan demikian, penerapan instrumen KAMI versi 4.2 di Kementerian Agama Kota Yogyakarta dapat menjadi langkah pencegahan untuk mengurangi risiko kebocoran data dan meningkatkan kepercayaan publik terhadap layanan pemerintah.

Berdasarkan gap tersebut, penelitian ini mengutamakan penilaian keamanan informasi di Kementerian Agama Kota Yogyakarta dengan menggunakan Indeks Keamanan Informasi (KAMI) versi 4.2. Studi ini diharapkan mampu memberikan gambaran menyeluruh tentang tingkat kesiapan penerapan keamanan informasi di lembaga tersebut. Di samping itu, temuan penelitian ini juga bisa memberikan saran praktis untuk Kementerian Agama Kota Yogyakarta dalam meningkatkan sistem keamanan informasi yang ada, serta menyumbangkan pada upaya pemerintah dalam menciptakan tata kelola pemerintahan yang transparan, akuntabel, dan aman di era digital.

2. METODOLOGI PENELITIAN

Rancangan penelitian ini mengadopsi metodologi kuantitatif yang bersifat evaluatif, Alur Penelitian ditunjukkan pada gambar 1 di bawah ini.



Gambar 1. Alur Penelitian

Rangkaian tahapan penelitian disusun secara berurutan sebagaimana ditunjukkan pada Gambar 1 alur penelitian, mulai dari studi literatur hingga penarikan kesimpulan berdasarkan hasil evaluasi yang diperoleh.

2.1 Studi Literatur

Studi literatur dilakukan dengan mengambil dokumen/rujukan resmi Indeks KAMI versi 4.2 dari laman BSSN, kemudian mempelajari konsep, ruang lingkup, domain penilaian, indikator, serta mekanisme skoring yang digunakan dalam Indeks KAMI versi 4.2. Pada tahap ini peneliti menyusun identifikasi kebutuhan penelitian dan menetapkan kerangka evaluasi yang akan digunakan sebagai dasar penyusunan instrumen pengumpulan data dan batasan objek yang dinilai [10].

2.2 Observasi Awal

Tahap observasi awal dilakukan melalui kunjungan ke lokasi penelitian Kementerian Agama Kota Yogyakarta untuk memperoleh gambaran konteks awal lingkungan sistem informasi. Observasi ini bertujuan mengenali aspek-aspek krusial terkait penerapan keamanan informasi serta mendata komponen/infrastruktur teknologi informasi yang relevan agar proses pengumpulan data berjalan lebih terarah dan sesuai dengan ruang lingkup penilaian.

2.3 Pengumpulan Data

Tahap pengumpulan data dilaksanakan dengan akuisisi data primer menggunakan kuesioner/angket terstruktur yang disusun mengacu pada kerangka kerja Indeks KAMI versi 4.2. Instrumen kemudian didistribusikan kepada personel kunci yang memiliki otoritas dan pemahaman memadai mengenai tata kelola serta implementasi keamanan informasi di instansi, sehingga respons yang terkumpul merepresentasikan kondisi aktual pada setiap area penilaian.

2.4 Pemrosesan dan Evaluasi Indeks KAMI Versi 4.2

Selanjutnya tahap pemrosesan dan evaluasi Indeks KAMI versi 4.2 dilakukan dengan mengompilasi seluruh data kuesioner, memeriksa kelengkapan jawaban, lalu memasukkan data ke perangkat lunak Indeks KAMI versi 4.2 untuk dilakukan perhitungan. Aplikasi Indeks KAMI versi 4.2 selanjutnya menghasilkan

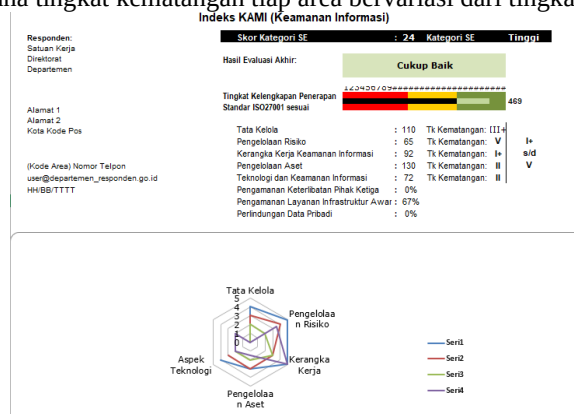
keluaran berupa skor indeks dan level kematangan keamanan informasi, baik secara keseluruhan maupun per-domain, yang menjadi dasar analisis pada tahap berikutnya [11].

2.5 Hasil dan Saran

Tahap akhir adalah hasil dan kesimpulan, yakni menginterpretasikan skor dan level kematangan yang dihasilkan untuk mengidentifikasi kekuatan, kelemahan, serta celah kontrol keamanan informasi pada instansi. Berdasarkan interpretasi tersebut, peneliti menyusun kesimpulan penelitian (serta rekomendasi perbaikan bila diperlukan) sebagai masukan peningkatan keamanan informasi secara berkelanjutan pada Kementerian Agama Kota Yogyakarta.

3. HASIL DAN PEMBAHASAN

Evaluasi menggunakan Indeks KAMI versi 4.2 menunjukkan bahwa instansi yang dinilai berada pada tahap Cukup baik untuk keamanan informasinya, dengan skor total 469. Dasbord evaluasi menyajikan gambaran lengkap, di mana tingkat kematangan tiap area bervariasi dari tingkat I+ hingga V.



Gambar 2. Hasil Dashbord Penilaian Indeks KAMI versi 4.2 pada Kemenang Kota Yogyakarta

Evaluasi keamanan sistem informasi pada Kementerian Agama Kota Yogyakarta dilakukan menggunakan Indeks Keamanan Informasi (KAMI) versi 4.2 yang mengacu pada SNI ISO/IEC 27001:2013. Penilaian mencakup 7 bagian utama yang merepresentasikan kesiapan, kelengkapan, dan kematangan pengelolaan keamanan informasi pada instansi.

Berdasarkan hasil pengisian kuesioner, verifikasi bukti dukung, serta rekapitulasi pada dashboard Indeks KAMI versi 4.2, tingkat ketergantungan sistem elektronik Kementerian Agama Kota Yogyakarta berada pada kategori Tinggi. Pada kondisi tersebut, tingkat kematangan keamanan informasi secara umum berada pada rentang Level II hingga III+, yang menunjukkan bahwa instansi telah memiliki kerangka dasar keamanan informasi, namun masih memerlukan penguatan agar mencapai kondisi yang lebih terkelola, terukur, dan optimal.

Lebih lanjut, hasil penilaian menunjukkan bahwa Skor Akhir Indeks KAMI versi 4.2 sebesar 469. Berdasarkan ambang batas penilaian untuk kategori Sistem Elektronik Tinggi, skor tersebut menempatkan status kesiapan keamanan informasi Kementerian Agama Kota Yogyakarta pada kategori “Cukup Baik”. Hal ini mengindikasikan bahwa praktik keamanan informasi telah diterapkan pada tingkat dasar hingga menengah, namun masih terdapat ruang perbaikan untuk mencapai tingkat kematangan yang lebih tinggi sesuai dengan kebutuhan kritikalitas sistem elektronik yang digunakan.

Penilaian urutan tingkat kematangan dari yang terendah hingga yang tertinggi adalah I – V. Rekapitulasi hasil penilaian untuk setiap area dapat dilihat pada Tabel 1 berikut :

Tabel 1. Rekapitulasi Hasil Evaluasi INDEKS KAMI versi 4.2

No	Area Evaluasi	Skor Diperoleh	Tingkat Kematangan (Maturity Level)
I	Kategori Sistem Elektronik	24	Tinggi
II	Tata Kelola Keamanan Informasi	110	III+
III	Pengelolaan Risiko Keamanan Informasi	65	V
IV	Kerangka Kerja Keamanan Informasi	92	I+
V	Pengelolaan Aset Informasi	130	II

VI	Teknologi dan Keamanan Informasi	72	II
	Total Skor Kelengkapan	469	Cukup Baik

3.1 Kategori Sistem Elektronik (SE)

Pada bagian ini dilakukan identifikasi tingkat ketergantungan Kementerian Agama Kota Yogyakarta terhadap layanan sistem elektronik dalam mendukung proses bisnis dan pelayanan publik. Hasil pengisian kuesioner menunjukkan bahwa instansi memperoleh skor 24, yang berada pada rentang 16–34, sehingga mengklasifikasikan Sistem Elektronik pada kategori “Tinggi”. Temuan ini memperkuat hasil penelitian sebelumnya yang menyebutkan bahwa instansi dengan ketergantungan sistem tinggi membutuhkan kontrol keamanan yang lebih ketat. Dengan demikian, kondisi ini mengindikasikan bahwa kebutuhan terhadap sistem keamanan informasi yang matang menjadi semakin krusial.

3.2 Tata Kelola Keamanan Informasi

Bagian ini mengevaluasi kelengkapan struktur organisasi serta kejelasan peran dan tanggung jawab dalam mengelola keamanan informasi. Berdasarkan hasil penilaian, Kementerian Agama Kota Yogyakarta memperoleh skor 110 dengan tingkat kematangan mencapai Level III+. Capaian ini menunjukkan bahwa tata kelola keamanan informasi telah terdefinisi dengan baik dan dilaksanakan secara konsisten oleh unit kerja terkait, meskipun mekanisme pengukuran kinerjanya masih perlu ditingkatkan agar lebih kuantitatif.

Hasil ini sejalan dengan penelitian terdahulu yang menyatakan bahwa sebagian instansi pemerintah telah memiliki kebijakan formal, namun belum sepenuhnya didukung oleh mekanisme evaluasi kinerja yang terukur. Perbedaan utama terletak pada belum optimalnya pengukuran kinerja keamanan informasi. Secara teoritis, tata kelola yang efektif tidak hanya menekankan pada struktur, tetapi juga pada mekanisme monitoring dan evaluasi. Oleh karena itu, hasil ini menunjukkan bahwa instansi masih berada pada tahap transisi menuju tata kelola yang lebih berbasis kinerja.

3.3 Pengelolaan Risiko Keamanan Informasi

Fokus evaluasi pada bagian ini adalah kemampuan instansi dalam mengidentifikasi, menganalisis, dan memitigasi risiko keamanan informasi. Hasil evaluasi mencatatkan skor 65, yang menempatkan aspek ini pada posisi sangat baik dengan tingkat kematangan Level V (Optimal). Kondisi ini mencerminkan bahwa proses pengelolaan risiko telah terintegrasi penuh dalam budaya kerja organisasi dan senantiasa mengalami perbaikan berkelanjutan (continuous improvement) guna menghadapi ancaman siber yang dinamis.

Hasil yang menunjukkan Level V (optimal) pada pengelolaan risiko merupakan temuan yang relatif lebih tinggi dibandingkan banyak penelitian sebelumnya yang umumnya berada pada level menengah. Hal ini mengindikasikan bahwa instansi telah berhasil mengintegrasikan manajemen risiko ke dalam proses bisnis.

Secara teoritis, kondisi ini sesuai dengan prinsip manajemen risiko dalam keamanan informasi yang menekankan continuous improvement. Tingginya capaian pada domain ini menunjukkan bahwa organisasi memiliki kesadaran yang baik terhadap ancaman siber.

Namun, jika dibandingkan dengan domain lain yang masih rendah, muncul ketidakseimbangan yang menunjukkan bahwa keberhasilan pada aspek risiko belum diikuti oleh penguatan pada aspek kebijakan dan implementasi teknis.

3.4 Kerangka Kerja Pengelolaan Keamanan Informasi

Pada bagian Kerangka Kerja, penilaian ditujukan terhadap ketersediaan dokumen kebijakan serta prosedur operasional standar (SOP) keamanan informasi. Instansi memperoleh skor 92, yang menempatkan tingkat kematangan pada Level I+. Hasil ini mengindikasikan bahwa penerapan kebijakan keamanan informasi masih berada pada tahap awal atau perintisan, di mana dokumentasi formal belum lengkap dan pelaksanaan prosedur keamanan sering kali masih bersifat insidental (ad-hoc) tanpa landasan aturan tertulis yang kuat.

3.5 Pengelolaan Aset Informasi

Bagian ini menyoroti tata cara instansi dalam mengelola, menginventarisasi, dan melindungi aset informasi yang meliputi perangkat keras, lunak, dan data. Kementerian Agama Kota Yogyakarta memperoleh skor 130 dengan tingkat kematangan Level II. Hal ini menandakan bahwa instansi telah menerapkan kerangka kerja dasar pengelolaan aset, seperti memiliki daftar inventaris, namun manajemen siklus hidup aset dan klasifikasi informasi belum dikelola secara sistematis dan menyeluruh.

Menurut teori manajemen aset dalam keamanan informasi, klasifikasi data merupakan elemen penting untuk menentukan tingkat perlindungan. Oleh karena itu, hasil ini menunjukkan bahwa instansi masih perlu meningkatkan pengelolaan siklus hidup aset secara menyeluruh.

3.6 Teknologi dan Keamanan Informasi

Evaluasi pada bagian ini mencakup penerapan langkah-langkah teknis untuk mengamankan sistem, jaringan, dan infrastruktur teknologi informasi. Hasil penilaian menunjukkan perolehan skor 72, yang menempatkan aspek teknologi pada tingkat kematangan Level II. Capaian ini mengisyaratkan bahwa kontrol teknis dasar (seperti penggunaan firewall atau antivirus) telah diterapkan, namun belum didukung oleh mekanisme pemantauan (monitoring) efektivitas keamanan yang proaktif dan konsisten.

3.7 Suplemen Bagian

Suplemen mengukur aspek pendukung keamanan yang meliputi keterlibatan pihak ketiga, layanan infrastruktur awan (cloud), dan perlindungan data pribadi. Berdasarkan hasil evaluasi, instansi mencatatkan skor 0,67 (67%) untuk pengamanan layanan awan, yang menunjukkan kesiapan cukup baik dalam aspek tersebut. Namun, aspek pengamanan keterlibatan pihak ketiga dan perlindungan data pribadi masing-masing mendapatkan skor 0%, yang menunjukkan belum adanya kebijakan atau kontrol spesifik yang diterapkan untuk kedua area tersebut.

Berdasarkan hasil penelitian Index KAMI versi 4.2 ditemukan bahwa kelemahan paling kritis teridentifikasi pada domain suplemen, di mana aspek Pengamanan Keterlibatan Pihak Ketiga dan Perlindungan Data Pribadi sama-sama memperoleh skor 0%, yang mengindikasikan ketiadaan kerangka kerja dan kontrol yang memadai untuk dua area vital tersebut. Dengan demikian, temuan ini menyimpulkan bahwa terdapat urgensi bagi instansi untuk memprioritaskan penguatan pada kerangka kerja keamanan dasar, tata kelola data pribadi, dan manajemen risiko pihak ketiga guna mewujudkan sistem tata kelola pemerintahan digital yang lebih tangguh, aman, dan terpercaya.

Sementara itu, prioritas perbaikan perlu difokuskan pada area keamanan informasi yang masih paling lemah. Kebijakan dan prosedur yang masih “dalam perencanaan” harus segera diformalkan dan dipublikasikan, termasuk penetapan konsekuensi pelanggaran serta prosedur audit internal. Pada pengelolaan aset, organisasi perlu memperjelas tanggung jawab keamanan informasi bagi tiap personel, serta meningkatkan praktik backup dengan uji pemulihan (restore) berkala untuk menjamin integritas data. Selain itu, inspeksi dan pemeliharaan fasilitas fisik serta perangkat pendukung perlu dilakukan secara terjadwal untuk menekan risiko fisik terhadap aset informasi. Di sisi teknologi, perbaikan mendesak diperlukan karena beberapa kontrol masih “tidak dilakukan”. Organisasi perlu menjalankan vulnerability scanning secara rutin, melakukan analisis log berkala untuk mendeteksi anomali, serta menerapkan standar enkripsi dan pengelolaan kunci untuk melindungi data sensitif. Perlindungan akses jaringan nirkabel dan akses eksternal juga harus segera diaktifkan guna menutup celah keamanan yang masih terbuka. Dengan serangkaian pengembangan tersebut, diharapkan Kementerian Agama Kota Yogyakarta mampu meningkatkan tingkat kematangan keamanan informasi ke level selanjutnya secara lebih optimal.

Dalam kajian evaluasi keamanan informasi hasil penelitian ini mengonfirmasi beberapa temuan utama dari penelitian terdahulu, sekaligus memberikan kontribusi baru yaitu :

- Menggunakan Indeks KAMI versi 4.2 sebagai dokumen/rujukan resmi dari laman Badan Siber dan Sandi Negara (BSSN) sebagai instrumen evaluasi terbaru yang cukup komprehensif dibandingkan penelitian sebelumnya.
- Menyajikan evaluasi kontekstual dan saran praktis pada instansi pemerintah tingkat daerah, yaitu Kementerian Agama Kota Yogyakarta.
- Melakukan analisis tidak hanya pada nilai agregat, tetapi juga pada disparitas tingkat kematangan antar domain keamanan informasi dan mengungkap ketidakseimbangan kematangan antar domain, yang menunjukkan bahwa implementasi keamanan informasi bersifat parsial (tidak menyeluruh).
- Jika penelitian terdahulu cenderung berfokus pada aspek umum, penelitian ini menyoroti aspek spesifik seperti keamanan pihak ketiga dan perlindungan data pribadi.

4. KESIMPULAN

Penelitian ini bertujuan untuk mengevaluasi tingkat kematangan keamanan informasi pada Kementerian Agama Kota Yogyakarta menggunakan Indeks KAMI versi 4.2. Hasil penelitian menunjukkan bahwa organisasi telah memiliki dasar penerapan keamanan informasi, namun belum mencapai tingkat kematangan yang optimal dan terintegrasi secara menyeluruh. Temuan utama mengindikasikan adanya ketidakseimbangan antar domain, di mana beberapa aspek telah berkembang dengan baik, sementara aspek fundamental lainnya masih memerlukan penguatan. Selain itu, penelitian ini menegaskan bahwa risiko keamanan tidak hanya bersumber dari internal organisasi, tetapi juga dari

keterlibatan pihak eksternal serta pengelolaan data pribadi yang belum optimal. Secara ilmiah, hasil ini menunjukkan bahwa implementasi keamanan informasi pada instansi pemerintah cenderung bersifat parsial, sehingga diperlukan pendekatan yang lebih holistik dan terintegrasi dalam pengelolaannya. Oleh karena itu, peningkatan keamanan informasi perlu difokuskan pada penguatan kerangka kerja kebijakan, tata kelola data pribadi, serta manajemen risiko pihak ketiga sebagai prioritas utama.

Untuk penelitian selanjutnya, disarankan untuk melakukan evaluasi keamanan informasi pada lebih banyak instansi pemerintahan daerah atau lainnya untuk memperoleh perbandingan yang lebih komprehensif, serta mengombinasikan pendekatan kuantitatif dengan metode kualitatif seperti wawancara atau audit langsung. Penelitian mendatang juga dapat mengembangkan model evaluasi yang lebih terintegrasi, khususnya pada aspek pengamanan pihak ketiga dan perlindungan data pribadi, agar menghasilkan strategi keamanan informasi yang lebih adaptif terhadap perkembangan ancaman siber.

UCAPAN TERIMAKASIH

Terima kasih disampaikan kepada pihak-pihak yang telah mendukung terlaksananya penelitian ini, khususnya kepada Bapak Bambang Sugiantoro selaku dosen pengampu mata kuliah Proyek Pengkajian Jaringan Komputer atas arahan dan bimbingannya. Penulis juga menyampaikan apresiasi kepada pihak IT Kementerian Agama Kota Yogyakarta atas dukungan data dan informasi yang diperlukan selama proses penelitian. Selain itu, terima kasih kepada rekan-rekan mahasiswa yang turut membantu dan memberikan dukungan sehingga penelitian ini dapat terselesaikan dengan baik.

REFERENCES

- [1] A. Iskandar Sekolah Tinggi Ilmu Administrasi YPPT Tasikmalaya Jl Perintis Kemerdekaan, K. Kawalu, and J. Barat, "CosmoGov: Jurnal Ilmu Pemerintahan PUBLIC SERVICE INNOVATION IN THE SMART GOVERNANCE ERA: STRATEGIES TO INCREASE TRANSPARENCY AND ACCOUNTABILITY IN INDONESIA," vol. 11, no. 1, 2025, doi: 10.24198/cosmogov.v11i1.62484.
- [2] J. M. Borky and T. H. Bradley, "Protecting Information with Cybersecurity," in *Effective Model-Based Systems Engineering*, Springer International Publishing, 2019, pp. 345–404. doi: 10.1007/978-3-319-95669-5_10.
- [3] S. Hamid and M. N. Huda, "Mapping the landscape of government data breaches: A bibliometric analysis of literature from 2006 to 2023," *Social Sciences and Humanities Open*, vol. 11, Jan. 2025, doi: 10.1016/j.ssaho.2024.101234.
- [4] Badan Siber dan Sandi Negara, "Pedoman Penggunaan Indeks Keamanan Informasi (KAMI) Versi 4.2," BSSN. Accessed: Feb. 22, 2026. [Online]. Available: <https://bsn.go.id/indeks-kami-versi-4-2/>
- [5] Sivitas, "INDEKS KEAMANAN INFORMASI (KAMI)," Kementerian Komunikasi dan Digital. Accessed: Feb. 22, 2026. [Online]. Available: <https://www.komdigi.go.id/berita/pengumuman/detail/indeks-keamanan-informasi-kami>
- [6] Y. Li and H. Shang, "Service quality, perceived value, and citizens' continuous-use intention regarding e-government: Empirical evidence from China," *Information and Management*, vol. 57, no. 3, Apr. 2020, doi: 10.1016/j.im.2019.103197.
- [7] G. Dagnew Gebrehiwot and P. Elantheraiyan, "A study on the effect of training on employee performance in the case of Mekelle City, Tigray, Ethiopia," *Social Sciences and Humanities Open*, vol. 8, no. 1, Jan. 2023, doi: 10.1016/j.ssaho.2023.100567.
- [8] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, "Cybersecurity in local governments: A systematic review and framework of key challenges," Mar. 01, 2025, *Elsevier B.V.* doi: 10.1016/j.ugj.2024.12.010.
- [9] M. Abdullah, M. M. Nawaz, B. Saleem, M. Zahra, E. binte Ashfaq, and Z. Muhammad, "Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data," Sep. 01, 2025, *Multidisciplinary Digital Publishing Institute (MDPI)*. doi: 10.3390/analytics4030025.
- [10] L. Bernardo, S. Malta, and J. Magalhães, "An Evaluation Framework for Cybersecurity Maturity Aligned with the NIST CSF," *Electronics (Switzerland)*, vol. 14, no. 7, Apr. 2025, doi: 10.3390/electronics14071364.
- [11] Chelyne and R. Dwi Kurniawan, "Evaluasi Tata Kelola Keamanan Informasi Indeks KAMI 5.0: Studi Kasus PT. XYZ," *CESS (Journal of Computer Engineering, System and Science)*, vol. 11, no. 1, pp. 113–126, Jan. 2026, doi: 10.24114/cess.v11i1.71701.