Jurnal Keamanan Nasional , Vol. 11 Nomor 2 (2025), pp 185-198
ISSN 2442-7985 (print) | ISSN 2579-7727 (online)
Available online at: https://ejurnal.ubharajaya.ac.id/index.php/kamnas/index

Strategi Peningkatan Keamanan Siber dan Sandi di Kementerian Agama: Analisis Tingkat Kematangan Berdasarkan IKASANDI 2.1

Strategies for Enhancing Cybersecurity and Cryptographic Security at the Ministry of Religious Affairs: A Maturity Level Analysis Based on IKASANDI 2.1

Abdul Rozak Nurdiansyah[1], Setiadi Yazid[2], Yudho Giri Sucahyo[3]
[1,2,3]Fakultas Ilmu Komputer, Universitas Indonesia, Jakarta, Indonesia
Korespondensi: abdul.rozak31@ui.ac.id

Received:	Revised :	Accepted:	Published :
December 4, 2025	December 15, 2025	December 18, 2025	December 31, 2025

Abstract : *Cybersecurity is a crucial aspect in the implementation of Electronic Systems in the government sector, including in the Ministry of Religion of the Republic of Indonesia. 330,527,636 anomalous traffic incidents in Indonesia in 2024 indicate potential cybersecurity threats that could undermine public trust. One of the strategic systems managed is the Education Management Information System (EMIS) version 4.0 which contains large-scale and sensitive data. This study aims to measure the level of cybersecurity and cryptography maturity in the Ministry of Religion using the IKASANDI framework version 2.1 from BSSN and to prepare strategic recommendations for its improvement. The research methods used are qualitative and quantitative approaches through literature studies, interviews with the Head of the Application Development and Information Security Team, and filling in indicators in five IKASANDI domains, namely identification, protection, detection, countermeasures and recovery, and cryptography. The research findings indicate that the EMIS 4.0 system falls into the category of High-Level Electronic Systems, with its Cybersecurity maturity level at level 3, while its Cryptographic Security stands at level 2 overall. This condition indicates the need for further strengthening of information security within the Ministry of Religious Affairs and underscores the importance of policy alignment and collaboration with BSSN to ensure integrated and effective national security standards.*

Keywords : *Cybersecurity, Password Security, IKASANDI, EMIS, Ministry of Religion*

Abstrak : *Keamanan siber menjadi aspek krusial dalam penyelenggaraan Sistem Elektronik sektor pemerintahan, termasuk di Kementerian Agama Republik Indonesia. Sebanyak 330.527.636 trafik anomali di Indonesia tahun 2024 menunjukkan potensi ancaman siber yang dapat menyebabkan menurunnya kepercayaan publik. Salah satu sistem strategis yang dikelola*

Kementerian Agama adalah Education Management Information System (EMIS) versi 4.0 yang memuat data berskala besar dan sensitif. Penelitian ini bertujuan untuk mengukur tingkat kematangan keamanan siber dan sandi di Kementerian Agama menggunakan kerangka kerja IKASANDI versi 2.1 dari BSSN serta menyusun rekomendasi strategis peningkatannya. Metode penelitian yang digunakan adalah pendekatan kualitatif dan kuantitatif melalui studi literatur, wawancara dengan Tim Pengembangan Aplikasi dan Keamanan Informasi, serta pengisian indikator pada lima domain IKASANDI, yaitu identifikasi, proteksi, deteksi, penanggulangan dan pemulihan, serta persandian. Hasil penelitian menunjukkan bahwa sistem EMIS versi 4.0 termasuk dalam kategori Sistem Elektronik Tinggi dengan tingkat kematangan Keamanan Siber berada pada level 3 sementara Keamanan Sandi berada pada level 2 secara keseluruhan. Kondisi ini menandakan perlunya penguatan lebih lanjut terhadap aspek keamanan informasi di Kementerian Agama dan menegaskan pentingnya keselarasan kebijakan dan kolaborasi dengan BSSN untuk memastikan standar keamanan nasional yang terpadu dan efektif.

Kata kunci : *Keamanan Siber, Keamanan Sandi, IKASANDI, EMIS, Kementerian Agama*

PENDAHULUAN

Keamanan siber telah menjadi isu yang penting bagi individu, organisasi kecil, maupun organisasi besar dari berbagai sektor.[1] Sebanyak 330.527.636 trafik anomali di Indonesia Tahun 2024 menunjukkan tingginya aktivitas mencurigakan dan potensi ancaman siber yang dapat menyebabkan penurunan kinerja perangkat dan jaringan,[2] kebocoran data sensitif, serta menurunnya kepercayaan publik terhadap suatu organisasi. Berbagai serangan siber yang terjadi pada sektor publik di Indonesia telah menimbulkan dampak signifikan secara materi dan ekonomi.[3] Kerugian global akibat kejahatan siber diperkirakan akan terus meningkat hingga mencapai $12,2 triliun per tahun pada tahun 2031,[4] dengan laju pertumbuhan sekitar 2,5 persen per tahun. Tingginya frekuensi dan kompleksitas serangan siber menunjukkan bahwa Indonesia juga menjadi salah satu sasaran utama serangan siber yang berupaya mengganggu infrastruktur vital, mencuri informasi sensitif, serta memengaruhi opini publik.[5] Kolaborasi dan koordinasi antara pemerintah dan sektor swasta adalah kunci untuk memastikan keberhasilan strategi pertahanan siber di berbagai sektor.[6] Tercatat 56.128.160 temuan data eksposur yang berdampak

[1] Deny Budiyanto and Muhammad Mabruri, "Pentingnya Keamanan Siber Dalam Era Digital: Tinjauan Global Dan Kondisi Di Indonesia," *Prosiding Seminar Nasional Sains Dan Teknologi "SainTek"* 2, no. 1 (February 2025): 981–94, https://conference.ut.ac.id/index.php/saintek/article/view/5134.

[2] Badan Siber dan Sandi Negara (BSSN), *Lanskap Keamanan Siber Indonesia 2024* (2024).

[3] Muhammad Alfi, Ni Yundari, and Ahnaf Tsaqif, "Analisis Risiko Keamanan Siber Dalam Transformasi Digital Pelayanan Publik Di Indonesia," *Jurnal Kajian Stratejik Ketahanan Nasional* 6, no. 2 (December 2023): 1–11, https://doi.org/10.7454/jkskn.v6i2.10082.

[4] Cybersecurity Ventures, *Cybersecurity Ventures Report on Cybercrime*, November 25, 2025, https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime.

[5] Ria Wulandari, Priyanto Priyanto, and Afrizal Hendra, "The Indonesia's Cyber Security Strategy in the Face of Evolving Modern Warfare Threats," *Formosa Journal of Applied Sciences* 4, no. 2 (February 2025): 615–26, https://doi.org/10.55927/fjas.v4i2.5.

[6] Arinaldo Adma, Yusuf Surbakti, and Puspita Sari, "Transformasi Sistem Pertahanan Siber Indonesia Dengan BSSN Sebagai Poros & Motor Penggerak Menuju Angkatan Siber Mandiri Di Masa Depan," *Jurnal Kajian Stratejik Ketahanan Nasional* 6, no. 1 (June 2023): 1–14, https://doi.org/10.7454/jkskn.v6i1.10077.

pada 461 instansi di Indonesia.[7] Dari jumlah tersebut, sektor Administrasi Pemerintahan menjadi yang paling terdampak dengan porsi 58,34% dari total kasus, disusul oleh sektor Lainnya sebesar 30,14%, Keuangan sebesar 3,58%, Teknologi Informasi dan Komunikasi (TIK) sebesar 2,73%, Transportasi sebesar 2,70%, Energi dan Sumber Daya Mineral (ESDM) sebesar 1,88%, Kesehatan sebesar 0,34%, Pangan sebesar 0,19%, serta Pertahanan sebesar 0,11% dari keseluruhan temuan data eksposur tersebut. Salah satu insiden serangan siber adalah kebocoran Pusat Data Nasional pada tahun 2024. Penyebab utama insiden kebocoran data nasional pada PDN adalah kelemahan sistem, kurangnya kesiapan SDM, dan lemahnya regulasi.[8]

Kementerian Agama (Kemenag) sebagai sektor administrasi pemerintahan juga memiliki berbagai aplikasi dan data berskala besar, salah *satunya Education Management Information System* (EMIS). EMIS adalah sistem pendataan pendidikan yang dikelola untuk mengumpulkan, mengelola, dan menyediakan data yang akurat untuk mendukung perencanaan dan pengambilan kebijakan di bidang pendidikan agama dan keagamaan. Versi 4.0 EMIS ini sudah mengintegrasikan data lembaga, tenaga pendidik, peserta didik, serta sarana dan prasarana untuk semua jenjang pendidikan di bawah Kemenag.[9] Sebagai Penyelenggara Sistem Elektronik Kemenag harus menyelenggarakan Sistem Elektronik,[10] salah satunya EMIS secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. Kemenag wajib melindungi data pribadi dari setiap bentuk pemrosesan yang tidak sah, dengan menerapkan sistem keamanan yang andal, aman, dan bertanggung jawab terhadap data pribadi yang diproses dan/atau dikelola melalui Sistem Elektronik sesuai amanat UU PDP.[11]

Kemenag telah berupaya menghindari gangguan, kegagalan dan kerugian dalam penyelenggaraan Sistem Elektronik melalui sistem manajemen keamanan informasi yang tertuang dalam Keputusan Menteri Agama.[12] Namun, implementasi dan efektivitas penerapan sistem tersebut masih memerlukan evaluasi untuk memastikan bahwa seluruh satuan kerja telah mematuhi standar keamanan informasi secara konsisten. Penelitian terdahulu mengungkapkan adanya beberapa risiko keamanan, seperti kebocoran data siswa dan guru, serangan siber, serta akses tidak sah.[13] Penelitian tersebut menyoroti kurangnya kesadaran pengguna mengenai pentingnya keamanan data yang turut memperbesar risiko tersebut. Penelitian ini penting dilakukan sebagai sarana untuk memerhatikan lebih lanjut bagaimana sektor pemerintah khususnya Kemenag dapat mengukur tingkat kematangan untuk mengidentifikasi celah keamanan dan inkonsistensi penerapan standar keamanan. Maka dari itu pertanyaan penelitian yang dirumuskan untuk penelitian ini adalah: (1). Bagaimana tingkat kematangan keamanan siber dan sandi di Kementerian Agama berdasarkan kerangka kerja IKASANDI versi 2.1? (2). Rekomendasi

---

[7] Badan Siber dan Sandi Negara (BSSN), *Lanskap Keamanan Siber Indonesia 2024*.

[8] Imanuel Toding Bua and Nur Isdah Idris, "Analisis Kebijakan Keamanan Siber Di Indonesia: Studi Kasus Kebocoran Data Nasional Pada Tahun 2024," *Desentralisasi : Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan* 2, no. 2 (May 2025): 100–114, https://doi.org/10.62383/desentralisasi.v2i2.653.

[9] Hikmah Romalina and Moh Khoeron, "EMIS 4.0 GTK Madrasah Dirilis, Gantikan Simpatika," Kementerian Agama Republik Indonesia, January 16, 2025, https://kemenag.go.id/nasional/emis-4-0-gtk-madrasah-dirilis-gantikan-simpatika-VPhlG.

[10] Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

[11] Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

[12] Keputusan Menteri Agama Republik Indonesia Nomor 412 Tahun 2023 Tentang Sistem Manajemen Keamanan Informasi.

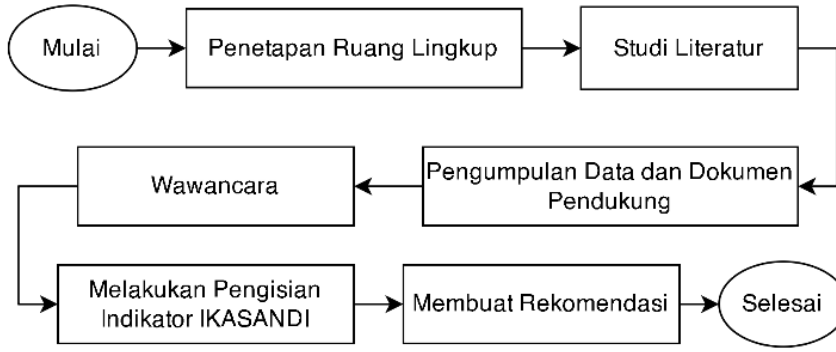
[13] Yasin Wahyudi and Sugiyono, "Analisis Keamanan Data Penerapan Aplikasi Emis Di MI Ma'arif NU 001 Samarinda," *Rayah Al-Islam* 8, no. 4 (December 2024): 2822–31, https://doi.org/10.37274/rais.v8i4.1277.

apa yang dapat diterapkan untuk meningkatkan keamanan siber di Kementerian Agama berdasarkan hasil pengukuran tingkat kematangan tersebut?

Penelitian ini disusun menjadi lima bagian. Bagian I berisi pendahuluan. Bagian II berisi studi literatur yang digunakan dalam penelitian ini. Bagian III menyajikan metodologi penelitian. Bagian IV berisi pembahasan hasil penelitian. Terakhir, Bagian V menyajikan kesimpulan, rekomendasi, dan keterbatasan untuk penelitian selanjutn

METODE

Penelitian ini menggunakan dua metodologi utama, yaitu kualitatif dan kuantitatif. Pendekatan kualitatif[14] digunakan untuk memberikan data yang rinci dan ilustratif guna mendapatkan pemahaman tentang berbagai karakteristik yang terkait dengan topik keamanan siber di Kemenag. Pendekatan kuantitatif mengukur tingkat kematangan keamanan siber dan sandi di Kementerian Agama menggunakan instrumen IKASANDI versi 2.1 dari BSSN.



Gambar 1. Tahapan Penelitian

Penetapan Ruang Lingkup

Penentuan ruang lingkup dalam pengategorian Sistem Elektronik (SE) akan berpengaruh pada pemilihan kontrol yang harus dipenuhi, yang kemudian diklasifikasikan ke dalam kategori Rendah, Tinggi, atau Strategis. Tabel 1 menggambarkan pembagian nilai maksimum pada masing-masing kategori Sistem Elektronik. Nilai tersebut disusun berdasarkan bobot kontrol keamanan yang ditetapkan oleh BSSN.

Sistem Elektronik dengan kategori Strategis memiliki nilai maksimum tertinggi, yakni 193, disusul oleh kategori Tinggi sebesar 179, dan Rendah sebesar 112. Perbedaan total nilai ini menunjukkan adanya variasi tingkat kompleksitas serta prioritas keamanan pada masing-masing kategori Sistem Elektronik. Tabel ini berfungsi sebagai acuan dalam penentuan bobot penilaian IKASANDI sesuai klasifikasi sistem yang dinilai, serta menegaskan bahwa semakin strategis suatu sistem, semakin besar pula kebutuhan penerapan kontrol keamanan informasi yang harus dipenuhi.

[14] Zanyar Nathir Ghafar, "The Evaluation Research: A Comparative Analysis of Qualitative and Quantitative Research Methods," *Journal of Language, Literature, Social and Cultural Studies* 2, no. 1 (February 2024): 1–10, https://doi.org/10.58881/jllscs.v2i1.122.

Tabel 1. Kategorisasi Sistem Elektronik

Uraian	RENDAH	TINGGI	STRATEGIS
Kontrol Kamsiber	**96**	**163**	**177**
> Kontrol Identifikasi	31	56	59
> Kontrol Proteksi	52	75	79
> Kontrol Deteksi	4	9	12
> Kontrol Gulih	9	23	27
Kontrol Persandian	**39**	**39**	**39**
> Irisan Kontrol Keamanan Siber dan Persandian	23	23	23
TOTAL	**112**	**179**	**193**

Studi Literatur

Peneliti melakukan identifikasi organisasi dan indikator IKASANDI. Identifikasi organisasi berisi tentang visi, misi, struktur organisasi sesuai KMA terbaru, rencana strategis Kementerian Agama Tahun 2025-2029 serta hasil tingkat kematangan indeks KAMI tahun 2023. Dokumen yang juga dipelajari adalah undang-undang PDP dan undang-undang ITE.

Pengumpulan Data dan Dokumen Pendukung

Populasi dalam penelitian ini adalah anggota CSIRT Kemenag yang berada di Pusdatin Kemenag. Teknik sampling yang digunakan adalah accidental sampling, yaitu teknik pengambilan sampel berdasarkan subjek yang tersedia dan bersedia saat penelitian dilakukan. Data dikumpulkan melalui wawancara oleh Ketua Tim Infrastruktur dan Jaringan, Ketua Tim Pengembangan Aplikasi dan Keamanan Informasi dan Penanggung Jawab Tata Kelola Keamanan Data Dan Informasi Pusdatin Kemenag. Data dukung yang telah diperoleh kemudian digunakan untuk melakukan pengisian indikator dari 5 domain IKASANDI. Domain disusun berdasarkan penerapan Kontrol Keamanan meliputi: (1). Identifikasi, (2). Proteksi, (3). Deteksi, (4). Penanggulangan dan Pemulihan, dan (5). Persandian

Data yang terkumpul dari setiap responden dipetakan ke dalam setiap domain untuk dinilai berdasarkan skor kelengkapan dan kematangan, kemudian dibandingkan dengan level skala 0-5. Langkah terakhir adalah penyusunan rekomendasi berdasarkan hasil pengisian indikator dan analisis tingkat kematangan.

STUDI LITERATUR

Keamanan Siber

Keamanan siber adalah gabungan dan pengaturan berbagai sumber daya termasuk personel, infrastruktur, struktur dan proses untuk melindungi jaringan dan sistem komputer berbasis siber dari kejadian yang mengompromikan integritas dan mengganggu hak milik, yang mengakibatkan beberapa tingkat kerugian.[15]

a. Indeks KAMI

[15] Francesco Schiliro, "Towards a Contemporary Definition of Cybersecurity," version 1, preprint, arXiv, 2023, https://doi.org/10.48550/ARXIV.2302.02274.

Indeks Keamanan Informasi (KAMI) BSSN merupakan aplikasi yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001.[16] Pengelompokan dilakukan berdasarkan tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT atau CMMI. Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di Kementerian / Lembaga.[17] Dengan adanya pembaruan pada SNI ISO/IEC 27001:2022, telah dilakukan revisi Indeks KAMI dan dilakukan pembaruan dari Indeks KAMI versi 4.2 menjadi Indeks KAMI versi 5.0, dengan penambahan sesuai kontrol baru pada SNI ISO/IEC 27001:2022.[18]

Tabel 2. Restrukturisasi Kategori pada Indeks KAMI 5.0

Kontrol Baru pada SNI ISO/IEC 27001:2022	Penambahan pada Indeks KAMI
Threat intelligence, ICT readiness for business continuity, Information security for cloud services	Aspek Kerangka Kerja
Information deletion, Data masking	Aspek Pengelolaan Aset
Physical security monitoring, Configuration management, Data leakage prevention, Monitoring activities, Web filtering, Secure coding	Aspek Teknologi

b. Kerangka Kerja ISO 27001:2022

ISO 27001:2022 adalah standar yang diakui secara luas dan diakui secara global sebagai kerangka kerja komprehensif untuk mengelola risiko keamanan informasi organisasi secara efektif melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi.[19] ISO/IEC 27001:2022 menegaskan bahwa organisasi tidak cukup hanya menetapkan kebijakan keamanan informasi, tetapi juga harus membangun dan menerapkan sistem manajemen yang menyatukan seluruh tahapan pengamanan yang dimulai dari identifikasi risiko, penentuan kontrol, pelaksanaan, hingga proses evaluasi serta peningkatan berkelanjutan.

c. IKASANDI

IKASANDI merupakan instrumen dari BSSN yang digunakan untuk mengukur Tingkat Kematangan Keamanan Siber dan Sandi sebuah organisasi atau Penyelenggaraan PSE. Instrumen IKASANDI memiliki dua bagian pengukuran, yaitu Pengukuran Tingkat Kematangan Keamanan Siber dan Pengukuran Tingkat Kematangan Persandian. IKASANDI juga merupakan hasil pemetaan dari berbagai instrumen yaitu instrumen Indeks Keamanan Informasi (Indeks KAMI), instrumen pengukuran tingkat kematangan keamanan siber/*Cyber Security Maturity* (CSM), instrumen Tingkat Maturitas Penanganan Insiden Siber (TMPI), dan CIS *Critical Security Controls* versi 8 (CIS *Controls* v8). Tingkat kematangan menggambarkan sejauh mana penerapan keamanan

[16] BSSN, *Indeks KAMI*, November 3, 2025, [Online]. Available: https://www.bssn.go.id/indeks-kami/
[17] BSSN.
[18] BSSN.
[19] Athallariq Rafii Nugroho and Nilo Legowo, "Risk Assessment at It Company by Focusing on Information Security Area Using Iso 27001:2022," *Syntax Literate ; Jurnal Ilmiah Indonesia* 7, no. 12 (February 2024): 20307–24, https://doi.org/10.36418/syntax-literate.v7i12.15349.

siber dan sandi telah dilakukan secara sistematis dan terdokumentasi melalui prosedur yang terorganisir. Terdapat lima level kematangan yang menunjukkan perkembangan kemampuan organisasi dalam mengelola keamanan informasi sesuai Peraturan Badan BSSN nomor 10 Tahun 2023.

Gambar 2. Level Kematangan IKASANDI

Level 1 – Awal, nilai kematangan pada rentang indeks 0 – 1,50. Pada tahap ini, menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi awal, belum memiliki prosedur yang terorganisir dan bersifat informal. Level 2 – Berulang, nilai kematangan pada rentang indeks 1,51 – 2,50. Menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi yang berulang, sudah memiliki prosedur yang terorganisir namun masih bersifat informal. Level 3 – Terdefinisi, nilai kematangan pada rentang indeks 2,51 – 3,50. Pada tahap ini, menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi yang telah terdefinisi dengan baik, sudah terorganisir dengan jelas dan bersifat formal. Level 4 – Terkelola, nilai kematangan pada rentang indeks 3,51 – 4,50. Pada tahap ini, menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi yang telah terkelola dengan baik, elah terorganisir dengan baik namun belum dilakukan proses otomatisasi dan bersifat formal. Level 5 – Inovatif, nilai kematangan pada rentang indeks 4,51 – 5,00. Pada tahap ini, menggambarkan kondisi penerapan Keamanan Siber telah diimplementasikan secara optimal, telah terorganisir dengan baik dan telah dilakukan proses otomatisasi dan bersifat formal.

PEMBAHASAN

Penentuan Ruang Lingkup

Sebelum penentuan ruang lingkup, dilakukan analisis kesenjangan terlebih dahulu antara kondisi aktual dengan nilai yang diharapkan. Sistem Elektronik yang dinilai dipilih berdasarkan hasil kesepakatan responden. Setelah dilakukan penilaian, kategori Sistem Elektronik pada Pusdatin Kemenag dengan sistem yang dinilai adalah adalah EMIS versi 4.0 mendapat kategori tinggi dengan total skor 28.

Tabel 3. Hasil Penilaian Kategorisasi Sistem Elektronik

Skor penetapan Kategori Sistem Elektronik	28

Tingkat Ketergantungan / Kategori SE	Tinggi

Domain Identifikasi

Identifikasi mencakup inventarisasi aset, penilaian risiko, dan analisis ancaman. Tahap awal yang penting untuk mengetahui apa yang perlu dilindungi dan memahami potensi risiko. Identifikasi digunakan untuk perencanaan strategis.

Tabel 4. Indikator Domain Identifikasi

Kategori	Indikator
Mengidentifikasi Peran dan tanggung jawab Organisasi	7
Menyusun strategi, kebijakan, dan prosedur keamanan siber	18
Mengelola aset informasi	7
Menilai dan mengelola risiko Keamanan Siber	14
Mengelola risiko rantai pasok	10
Total	56

Berdasarkan hasil penilaian pada masing-masing indikator pada domain identifikasi, diperoleh nilai dengan total skor 133.

Tabel 5. Hasil Penilaian Domain Identifikasi

Kategori	Skor
Mengidentifikasi Peran dan tanggung jawab Organisasi	18
Menyusun strategi, kebijakan, dan prosedur keamanan siber	54
Mengelola aset informasi	14
Menilai dan mengelola risiko Keamanan Siber	27
Mengelola risiko rantai pasok	20
Total	133

Domain Proteksi

Proteksi berfokus pada implementasi kontrol untuk melindungi sistem dan data dari ancaman yang mencakup kontrol akses, enkripsi, dan kebijakan keamanan.

Tabel 6. Indikator Domain Proteksi

Kategori	Indikator
Mengelola identitas, autentikasi, dan kendali akses	10
Melindungi aset fisik	9
Melindungi data	18
Melindungi aplikasi	26
Melindungi jaringan	7
Melindungi sumber daya manusia	5
Total	75

Berdasarkan hasil penilaian pada masing-masing indikator pada domain proteksi, diperoleh nilai dengan total skor 214.

Tabel 7. Hasil Penilaian Domain Proteksi

Kategori	Skor
Mengelola identitas, autentikasi, dan kendali akses	31
Melindungi aset fisik	21
Melindungi data	39
Melindungi aplikasi	84
Melindungi jaringan	24
Melindungi sumber daya manusia	15
Total	214

Domain Deteksi

Deteksi melibatkan pemantauan, analisis log, dan penggunaan alat untuk mengidentifikasi aktivitas mencurigakan atau pelanggaran. Deteksi bertujuan memastikan bahwa ancaman dapat dikenali segera setelah muncul dan sebelum menyebabkan kerusakan signifikan.

Tabel 8. Indikator Domain Deteksi

Kategori	Indikator
Mengelola deteksi Peristiwa Siber	4
Menganalisis anomali dan Peristiwa Siber	3
Memantau Peristiwa Siber berkelanjutan	2
Total	9

Berdasarkan hasil penilaian pada masing-masing indikator pada domain deteksi, diperoleh nilai dengan total skor 20.

Kategori	Skor
Mengelola deteksi Peristiwa Siber	10
Menganalisis anomali dan Peristiwa Siber	4
Memantau Peristiwa Siber berkelanjutan	6
Total	20

Domain Penanggulangan dan Pemulihan

Respon insiden mencakup tanggapan terhadap dan mitigasi dampak dari insiden yang telah terdeteksi meliputi isolasi sistem yang terpengaruh, perbaikan, dan pemulihan. Bertujuan untuk meminimalkan dampak insiden yang sudah terjadi dan untuk memastikan pemulihan yang cepat dan efektif.

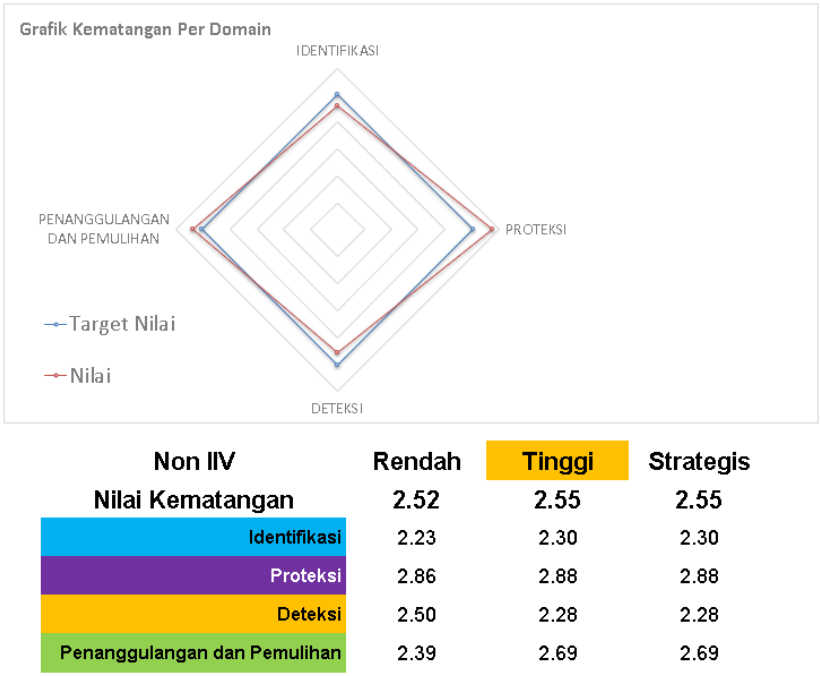
Tabel 9. Indikator Domain Penanggulangan dan Pemulihan

Kategori	Indikator
Menyusun perencanaan penanggulangan dan pemulihan Insiden Siber	13
Menganalisis dan melaporkan Insiden Siber	3
Melaksanakan penanggulangan dan pemulihan Insiden Siber	3
Meningkatkan keamanan setelah terjadinya Insiden Siber	4
Total	23

Berdasarkan hasil penilaian pada masing-masing indikator pada domain Penanggulangan dan Pemulihan, diperoleh nilai dengan total skor 63.

Tabel 10. Hasil Penilaian Indikator Domain Gulih

Kategori	Skor
Menyusun perencanaan penanggulangan dan pemulihan Insiden Siber	35
Menganalisis dan melaporkan Insiden Siber	8
Melaksanakan penanggulangan dan pemulihan Insiden Siber	5
Meningkatkan keamanan setelah terjadinya Insiden Siber	15
Total	63



Non IIV	Rendah	Tinggi	Strategis
Nilai Kematangan	2.52	2.55	2.55
Identifikasi	2.23	2.30	2.30
Proteksi	2.86	2.88	2.88
Deteksi	2.50	2.28	2.28
Penanggulangan dan Pemulihan	2.39	2.69	2.69

Gambar 3. Dashboard Keamanan Siber

Gambar 3 menunjukkan tingkat kematangan pada empat domain keamanan siber, yaitu Identifikasi, Proteksi, Deteksi, serta Penanggulangan dan Pemulihan. tingkat kematangan keseluruhan berada pada kategori Tinggi dengan nilai 2,55. Proteksi merupakan domain dengan tingkat kematangan tertinggi.

Domain Persandian

Area ini mengukur tingkat kepatuhan dan pemenuhan kondisi terhadap pelaksanaan identifikasi pola hubungan komunikasi sandi dan pelaksanaan analisis pola hubungan komunikasi sandi.

Tabel 11. Indikator Domain Persandian

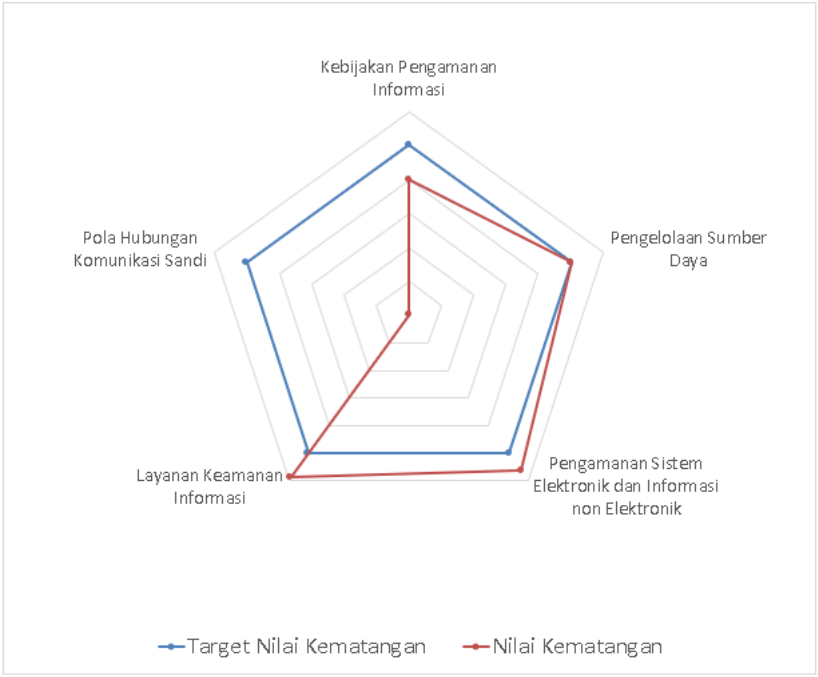
Kategori	Indikator
Kebijakan Pengamanan Informasi	1
Pengelolaan Sumber Daya	4
Pengamanan Sistem Elektronik dan Informasi non Elektronik	7
Layanan Keamanan Informasi	1
Pola Hubungan Komunikasi Sandi	4
Total	17

Berdasarkan hasil penilaian pada masing-masing indikator pada domain Persandian, diperoleh nilai dengan total skor 33.

Tabel 12. Hasil Penilaian Indikator Domain Persandian

Kategori	Indikator
Kebijakan Pengamanan Informasi	1
Pengelolaan Sumber Daya	8
Pengamanan Sistem Elektronik dan Informasi non Elektronik	21
Layanan Keamanan Informasi	3
Pola Hubungan Komunikasi Sandi	0
Total	33

Gambar 4 menunjukkan adanya kesenjangan yang signifikan antara nilai aktual dan target mengindikasikan bahwa kerangka kebijakan yang ada belum sepenuhnya memenuhi standar kematangan yang diharapkan. Kemenag juga masih berada pada tahap pengembangan dalam penerapan persandian.



Gambar 4. Dashboard Persandian

PENUTUP

Berdasarkan hasil dan pembahasan, kesimpulannya adalah kategori Sistem Elektronik EMIS versi 4.0 yang dikelola Pusdatin Kemenag adalah "Tinggi". Nilai tertinggi dari evaluasi Sistem Elektronik terdapat pada pengguna Sistem Elektronik yang berjumlah lebih dari 5.000 pengguna dan dan tingkat ancaman serangannya berisiko mengganggu hajat hidup orang banyak dan berdampak langsung pada pelayanan publik. Berdasarkan hasil evaluasi akhir penilaian mandiri IKASANDI untuk Pusdatin Kemenag Tingkat Kematangan keamanan siber berada pada level 3 – Terdefinisi. Artinya menggambarkan kondisi penerapan Keamanan Siber Kemenag dalam tahap implementasi yang telah terdefinisi dengan baik, dilakukan secara berulang dan konsisten serta direviu secara berkala. Sedangkan Tingkat Kematangan Persandian Kemenag berada di level 2 – berulang. Persandian dilakukan secara berulang namun masih bersifat informal, belum konsisten dan belum berkelanjutan.

Setiap domain dievaluasi berdasarkan skor yang diperoleh, yang kemudian dianalisis untuk mengidentifikasi implikasi kematangan serta area yang memerlukan penguatan. Untuk meningkatkan nilai kematangan keamanan siber pada domain identifikasi adalah:

1) Klasifikasikan dan lakukan audit berkala untuk memastikan inventaris selalu akurat dan terkini.
2) Terapkan kontrol akses berbasis kebutuhan (role-based access control) untuk mencegah akses berlebihan.
3) Terapkan kebijakan retensi dan pemusnahan aman sesuai klasifikasi aset.
4) Gunakan risk register untuk mencatat ancaman, kerentanan, dampak, kemungkinan, dan tingkat risiko.
5) Integrasikan penilaian risiko dalam proses pengadaan dan pengembangan sistem.
6) Masukkan persyaratan keamanan dalam kontrak/SLA, termasuk perlindungan data, batas akses, dan kewajiban notifikasi insiden.

Untuk meningkatkan nilai kematangan keamanan siber pada domain proteksi adalah:

1) Klasifikasikan data berdasarkan sensitivitas.
2) Terapkan kebijakan retensi data dan hapus data sensitif secara aman menggunakan metode secure deletion.
3) Lindungi data pribadi sesuai undang-undang PDP.

Untuk meningkatkan nilai kematangan keamanan siber pada domain deteksi adalah:

1) Sediakan dashboard pemantauan real-time untuk tim keamanan guna meningkatkan visibilitas.
2) Terapkan prosedur analisis insiden standar agar penanganan konsisten.
3) Beri pelatihan khusus kepada tim keamanan terkait teknik deteksi, investigasi, dan analisis ancaman modern.
4) Dokumentasikan setiap temuan dan pola anomali untuk memperkaya basis data insiden dan pembelajaran organisasi.

Untuk meningkatkan nilai kematangan keamanan siber pada domain penanggulangan dan pemulihan adalah:

1) Lakukan uji pemulihan secara berkala.

2) Lakukan komunikasi insiden terstruktur kepada pimpinan, pemilik sistem, dan pihak terkait sesuai tingkat keparahan.
3) Perbarui kontrol keamanan seperti patching, hardening, berdasarkan temuan evaluasi insiden sebelumnya.
4) Sosialisasikan hasil kepada pegawai terkait agar kesadaran dan ketahanan organisasi meningkat.

Untuk meningkatkan nilai kematangan keamanan siber pada domain persandian adalah:

1) Buat kebijakan turunan seperti kebijakan manajemen aset, akses, kriptografi, pemulihan bencana, penggunaan perangkat, cloud, dan email.
2) Lakukan monitoring dan audit komunikasi sandi untuk mendeteksi anomali, penyalahgunaan, atau kegagalan enkripsi.
3) Siapkan SOP tanggap insiden sandi.
4) Tetapkan prosedur autentikasi kuat seperti *two factor authentication* di setiap system.

Daftar Pustaka

Adma, Arinaldo, Yusuf Surbakti, dan Puspita Sari. "Transformasi Sistem Pertahanan Siber Indonesia dengan BSSN sebagai Poros dan Motor Penggerak Menuju Angkatan Siber Mandiri di Masa Depan." *Jurnal Kajian Stratejik Ketahanan Nasional* 6, no. 1 (2023): 1–14. https://doi.org/10.7454/jkskn.v6i1.10077.

Alfi, Muhammad, Ni Yundari, and Ahnaf Tsaqif. "Analisis Risiko Keamanan Siber Dalam Transformasi Digital Pelayanan Publik Di Indonesia." *Jurnal Kajian Stratejik Ketahanan Nasional* 6, no. 2 (December 2023): 1–11. https://doi.org/10.7454/jkskn.v6i2.10082.

Badan Siber dan Sandi Negara (BSSN). *Lanskap Keamanan Siber Indonesia 2024*. 2024.

BSSN. *Indeks KAMI*. November 3, 2025. [Online]. Available: https://www.bssn.go.id/indeks-kami/

Budiyanto, Deny, and Muhammad Mabruri. "PENTINGNYA KEAMANAN SIBER DALAM ERA DIGITAL:: TINJAUAN GLOBAL DAN KONDISI DI INDONESIA." *Prosiding Seminar Nasional Sains Dan Teknologi "SainTek"* 2, no. 1 (February 2025): 981–94. https://conference.ut.ac.id/index.php/saintek/article/view/5134.

Cybersecurity Ventures. *Cybersecurity Ventures Report on Cybercrime*. November 25, 2025. https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime.

Ghafar, Zanyar Nathir. "The Evaluation Research: A Comparative Analysis of Qualitative and Quantitative Research Methods." *Journal of Language, Literature, Social and Cultural Studies* 2, no. 1 (February 2024): 1–10. https://doi.org/10.58881/jllscs.v2i1.122.

Imanuel Toding Bua and Nur Isdah Idris. "Analisis Kebijakan Keamanan Siber Di Indonesia: Studi Kasus Kebocoran Data Nasional Pada Tahun 2024." *Desentralisasi : Jurnal Hukum, Kebijakan Publik, Dan Pemerintahan* 2, no. 2 (May 2025): 100–114. https://doi.org/10.62383/desentralisasi.v2i2.653.

Keputusan Menteri Agama Republik Indonesia Nomor 412 Tahun 2023 Tentang Sistem Manajemen Keamanan Informasi.

Nugroho, Athallariq Rafii, and Nilo Legowo. "Risk Assessment at It Company by Focusing on Information Security Area Using Iso 27001:2022." *Syntax Literate ; Jurnal Ilmiah Indonesia* 7, no. 12 (February 2024): 20307–24. https://doi.org/10.36418/syntax-literate.v7i12.15349.

Romalina, Hikmah, and Moh Khoeron. "EMIS 4.0 GTK Madrasah Dirilis, Gantikan Simpatika." Kementerian Agama Republik Indonesia, January 16, 2025. https://kemenag.go.id/nasional/emis-4-0-gtk-madrasah-dirilis-gantikan-simpatika-VPhlG.

Schiliro, Francesco. "Towards a Contemporary Definition of Cybersecurity." Version 1. Preprint, arXiv, 2023. https://doi.org/10.48550/ARXIV.2302.02274.

Undang-Undang Nomor 1 Tahun 2024 Tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

Wahyudi, Yasin and Sugiyono. "Analisis Keamanan Data Penerapan Aplikasi Emis Di MI Ma'arif NU 001 Samarinda." *Rayah Al-Islam* 8, no. 4 (December 2024): 2822–31. https://doi.org/10.37274/rais.v8i4.1277.

Wulandari, Ria, Priyanto Priyanto, and Afrizal Hendra. "The Indonesia's Cyber Security Strategy in the Face of Evolving Modern Warfare Threats." *Formosa Journal of Applied Sciences* 4, no. 2 (February 2025): 615–26. https://doi.org/10.55927/fjas.v4i2.5.