TATA KELOLA PERSANDIAN DALAM MENINGKATKAN KEAMANAN PELAYANAN PUBLIK DI DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN MADIUN

Abidah Ardelia Alfita
NPP. 33.0510
Program Studi Teknologi Rekayasa Informasi Pemerintahan
Email: abidahdella06@gmail.com

Pembimbing Skripsi: Dr. Ir. Ika Sartika, MT
Email: ika_sartika@ipdn.ac.id

ABSTRACT

Problem Statement (Kesenjangan Penelitian/Research Gap): *This study focuses on the increasingly critical challenge of cryptographic governance in local government information systems. Despite the enactment of national cybersecurity regulations, local government agencies particularly at the district level remain highly vulnerable to cyber threats due to limited technical human resources, inadequate infrastructure, and incomplete Standard Operating Procedures. The Communication and Informatics Department (Diskominfo) of Madiun Regency exemplifies this condition, having experienced repeated web defacement attacks on its official websites.* ***Purpose:*** *This study analyzes cryptography governance to enhance public service security at Diskominfo Madiun Regency.* ***Method:*** *This descriptive qualitative case study gathered data through documentation, observations, and in-depth interviews with six informants. Data were analyzed using NVivo 12 Plus and a Risk-Based Governance framework via the Octave Allegro method (covering risk measurement, asset profiling, and risk identification/mitigation), combined with the Index KAMI 5.0 to measure information security readiness.* ***Result:*** *The findings indicate that cryptographic governance at Diskominfo Madiun Regency currently stands at the "Basic Framework Fulfillment" status based on the KAMI 5.0 Index. Risk measurement reveals that public trust and institutional reputation constitute the highest-priority risk, evidenced by the web defacement incident. The cryptographic asset profile has been classified into five categories: hardware, software, data, network, and people. However, only 4 of 48 civil servant staff hold information security certifications. Risk identification and mitigation are carried out through multi-layered technical security measures including Next-Generation firewall, IDS/IPS systems, data encryption, and 24-hour SOC monitoring, yet Personal Data Protection and Risk Management areas remain at maturity level II.* ***Conclusion:*** *Cryptographic governance at Diskominfo Madiun Regency has not yet reached optimal implementation, primarily due to limited qualified technical human resources and the absence of comprehensive derivative regulations for risk management. It is recommended to strengthen the organizational structure through the formulation of periodic cyber incident mitigation SOPs and enhancement of official competency to ensure sustainable, secure, and trusted public services.*

Keywords: *Cryptography; Governance; Information Security; Public Services*

ABSTRAK

Permasalahan (Kesenjangan Penelitian/Research Gap): Penelitian ini berfokus pada semakin kritisnya tantangan tata kelola persandian dalam sistem informasi pemerintahan daerah. Meskipun regulasi keamanan siber nasional telah diterbitkan, instansi pemerintah daerah khususnya di tingkat kabupaten tetap sangat rentan terhadap ancaman siber akibat keterbatasan sumber daya manusia teknis, infrastruktur yang belum memadai, dan belum lengkapnya Standar Operasional Prosedur. Dinas Komunikasi dan Informatika Kabupaten Madiun menjadi contoh nyata kondisi tersebut, dengan mengalami serangan web defacement berulang pada situs web resminya. **Tujuan:** Penelitian ini bertujuan untuk menganalisis tata kelola persandian dalam meningkatkan keamanan pelayanan publik di Dinas Komunikasi dan Informatika Kabupaten Madiun. **Metode:** Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan studi kasus di Dinas Komunikasi dan Informatika Kabupaten Madiun. Pengumpulan data dilakukan melalui wawancara mendalam terhadap enam informan, observasi, dan dokumentasi. Analisis data menggunakan perangkat lunak NVivo 12 Plus dan diintegrasikan dengan kerangka *Risk-Based Governance* menggunakan metode Octave Allegro yang mencakup tiga dimensi: pengukuran risiko, profil aset persandian, serta identifikasi dan mitigasi risiko ditambah instrumen Indeks KAMI 5.0 untuk mengukur tingkat kesiapan keamanan informasi. **Hasil/Temuan:** Temuan menunjukkan bahwa tata kelola persandian Diskominfo Kabupaten Madiun berada pada status "Pemenuhan Kerangka Kerja Dasar" berdasarkan Indeks KAMI 5.0. Pengukuran risiko menunjukkan bahwa kepercayaan publik dan reputasi institusi merupakan prioritas risiko tertinggi. Profil aset persandian telah diklasifikasikan dalam lima kategori: hardware, software, data, network, dan people. Namun, hanya 4 dari 48 ASN yang memiliki sertifikasi keamanan informasi. Identifikasi dan mitigasi risiko dilaksanakan melalui pengamanan teknis berlapis, namun Area Perlindungan Data Pribadi dan Pengelolaan Risiko masih berada pada tingkat kematangan II. **Kesimpulan:** Tata kelola persandian di Diskominfo Kabupaten Madiun belum optimal, terutama disebabkan keterbatasan kualitas SDM teknis dan belum adanya regulasi turunan yang komprehensif mengenai manajemen risiko. Diperlukan penguatan struktur organisasi persandian melalui penyusunan SOP mitigasi insiden siber secara periodik serta peningkatan kapasitas kompetensi aparatur.

Kata kunci: Keamanan Informasi; Pelayanan Publik; Persandian; Tata Kelola

I. PENDAHULUAN

1.1. Latar Belakang

Transformasi digital pelayanan publik melalui Sistem Pemerintahan Berbasis Elektronik (SPBE) sesuai Perpres No. 95/2018 meningkatkan efisiensi, tetapi sekaligus memperluas risiko serangan siber. Berdasarkan data BSSN tahun 2024, Indonesia menghadapi 330.527.636 serangan siber, di mana sektor administrasi pemerintahan menjadi yang paling rentan dengan mendominasi 74% kasus (183 dugaan kebocoran data) (Id-SIRTII /CC, 2024). Kondisi ini menegaskan perlunya manajemen risiko dan penguatan keamanan informasi yang serius.

Sebagai respons atas ancaman tersebut, UU No. 23/2014 menetapkan persandian sebagai urusan pemerintahan wajib di daerah untuk menjaga tiga pilar keamanan informasi (*Confidentiality, Integrity, Availability*). Tata kelola persandian yang efektif sangat krusial agar standar keamanan dapat diimplementasikan dengan baik (Saputra et al., 2023). Selain itu, kehadiran UU No. 27/2022 tentang

Perlindungan Data Pribadi (UU PDP) kini mewajibkan instansi pemerintah daerah menerapkan pelindungan data yang ketat guna menghindari sanksi hukum dan runtuhnya reputasi publik.

Namun pada realisasinya, Dinas Komunikasi dan Informatika Kabupaten Madiun menghadapi tantangan besar. Dokumen Renstra 2025–2029 mengidentifikasi belum optimalnya penyelenggaraan persandian serta terbatasnya kuantitas dan kualitas SDM aparatur bidang TIK. Dampak dari celah ini terlihat dari insiden peretasan berulang (*deface*) pada situs OPD Kabupaten Madiun (seperti Dinas Tenaga Kerja periode 2019–2020) yang mengakibatkan hilangnya data publik.

Oleh karena itu, penelitian ini dilakukan untuk menganalisis tata kelola persandian di Diskominfo Kabupaten Madiun menggunakan pendekatan *Risk-Based Governance* melalui metode *Octave Allegro* dan instrumen Indeks KAMI 5.0 guna mengukur tingkat kesiapan keamanan informasinya.

1.2. Kesenjangan Masalah yang Diambil (Research Gap)

Penelitian ini berfokus pada kesenjangan antara regulasi persandian pusat dengan implementasi di pemerintah daerah. Secara nasional, data BSSN 2025 menunjukkan mayoritas instansi daerah masih berada pada kategori "Dasar" dalam kematangan keamanan informasi, yang menandakan lemahnya kapasitas kelembagaan dalam menghadapi ancaman siber. Di Kabupaten Madiun, kesenjangan tersebut terlihat nyata dari empat kondisi faktual, yaitu krisis SDM terampil di mana hanya 4 dari 48 ASN Diskominfo yang memiliki sertifikasi keamanan informasi, serta belum tersedianya SOP teknis yang rinci dan operasional meskipun Perbup Madiun Nomor 46 Tahun 2020 sudah diterbitkan. Selain itu, hasil evaluasi Indeks KAMI 5.0 juga menempatkan instansi ini pada status “Pemenuhan Kerangka Kerja Dasar” dengan Area Pengelolaan Risiko dan Area Kerangka Kerja Pengelolaan Keamanan Informasi yang masih tertahan di tingkat kematangan II, ditambah dengan aspek perlindungan data pribadi yang belum terintegrasi sesuai amanat UU PDP. Meskipun studi keamanan informasi daerah sudah banyak dilakukan, penelitian yang secara khusus mengombinasikan metode Octave Allegro dan Indeks KAMI 5.0 ke dalam satu kerangka *Risk-Based Governance* pada tingkat kabupaten masih sangat terbatas, sehingga kesenjangan literatur dan kondisi empiris inilah yang menjadi urgensi utama penelitian ini dilakukan.

1.3. Urgensi Penelitian

Penelitian ini memiliki tiga dimensi urgensi yang saling berkaitan, yaitu keilmuan, permasalahan, dan kebijakan. Dari sisi keilmuan, penelitian ini berkontribusi mengisi celah literatur mengenai tata kelola persandian pemerintah daerah berbasis *Risk-Based Governance* melalui integrasi metode *Octave Allegro* dan Indeks KAMI 5.0, di mana analisis bibliometrik VOSviewer menunjukkan klaster ini masih sangat terbuka untuk dieksplorasi. Dari sisi permasalahan, penelitian ini krusial untuk mencegah mitigasi siber yang bersifat reaktif dan tidak terukur; tanpa adanya analisis profil risiko yang sistematis berbasis data, instansi akan kesulitan memprioritaskan pengamanan secara tepat sasaran di tengah keterbatasan anggaran dan SDM. Terakhir, dari sisi kebijakan, hasil penelitian ini memberikan gambaran empiris bagi Diskominfo Kabupaten Madiun dalam menyusun SOP teknis, merumuskan strategi peningkatan kapasitas SDM, serta memperkuat pengelolaan keamanan informasi, sehingga perumusan kebijakan di masa depan tidak salah sasaran dan tata kelola persandian tidak berjalan stagnan.

1.4. Penelitian Terdahulu

Penelitian ini terinspirasi oleh sejumlah kajian terdahulu yang relevan dalam konteks keamanan informasi, tata kelola persandian, dan penilaian risiko di sektor pemerintahan maupun swasta. Secara umum, penelitian-penelitian tersebut menunjukkan variasi fokus, metode, serta pendekatan yang saling melengkapi.

Penelitian Alfarisi & Surantha (2022) mengkaji penilaian risiko dalam sistem *fleet management* menggunakan metode Octave Allegro dan menemukan 10 risiko yang dapat memengaruhi keamanan operasional, di mana 4 di antaranya terkait keamanan aplikasi dan perangkat keras. Penelitian ini

berlokasi di perusahaan swasta dengan fokus analisis risiko pada sistem transportasi, sehingga berbeda dengan penelitian penulis yang berfokus pada tata kelola persandian di instansi pemerintahan daerah.

Penelitian Emmanuel & Maulany (2023) menganalisis keamanan website Dinas Perhubungan Provinsi Jawa Timur menggunakan kombinasi metode Octave Allegro dan FMEA. Temuan menunjukkan ancaman DDoS, perubahan konten, dan pencurian data sebagai risiko utama. Perbedaannya terletak pada penggunaan teori FMEA sebagai alat penilaian dampak risiko dan fokus yang hanya pada keamanan website, sedangkan penelitian penulis mencakup tata kelola persandian secara menyeluruh. Penelitian M. S. Hasibuan et al. (2025) mengevaluasi keamanan informasi sistem komputerisasi terintegrasi di kementerian menggunakan Indeks KAMI dan Octave Allegro, dengan hasil skor KAMI 570 yang mengindikasikan masih adanya kelemahan sistem. Persamaannya terletak pada penggunaan kombinasi Indeks KAMI dan Octave Allegro, namun penelitian ini dilakukan di tingkat kementerian (pemerintah pusat), berbeda dengan penelitian penulis yang berlokasi di pemerintah daerah tingkat kabupaten.

Penelitian Budarsa (2022)meneliti risiko keamanan informasi pada data center Pemerintah Kabupaten Buleleng menggunakan Octave Allegro dan Analytical Hierarchy Process (AHP). Hasil penelitian menemukan risiko besar terhadap serangan siber dan kerusakan perangkat keras. Perbedaannya terletak pada penggunaan AHP sebagai metode pengolahan data tambahan dan fokus yang spesifik pada data center, berbeda dengan penelitian penulis yang mencakup seluruh dimensi tata kelola persandian. Penelitian Saputra et al. (2023) mengkaji pengelolaan keamanan informasi dan persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur menggunakan metode deskriptif kualitatif dan Indeks KAMI. Temuan menunjukkan tingkat kematangan berada pada level I+ hingga II+, belum memenuhi standar minimum ISO/IEC 27001:2013. Persamaannya terletak pada penggunaan Indeks KAMI dan objek penelitian yang sama-sama Diskominfo, namun berbeda dari segi lokasi penelitian (provinsi vs kabupaten) dan tidak menggunakan Octave Allegro sebagai instrumen analisis risiko. Penelitian Irsheid et al. (2022) melakukan studi komparatif terhadap enam model manajemen risiko keamanan informasi yaitu ISO27005, NIST SP 800-30, CRAMM, CORAS, OCTAVE Allegro, dan COBIT 5 dalam konteks sistem berbasis cloud hosting, dengan mengevaluasi ketiga dimensi utama yaitu applicability, adaptability, dan involvement masing-masing model.

Secara umum, penelitian-penelitian tersebut menunjukkan dominasi penggunaan metode Octave Allegro secara parsial dengan beragam metode pendamping serta variasi konteks objek penelitian, baik di sektor swasta maupun berbagai tingkatan pemerintahan. Perbedaan konteks, lokasi, dan kombinasi metode ini sekaligus membuka ruang bagi penelitian penulis untuk hadir sebagai kajian yang lebih komprehensif di konteks pemerintahan daerah kabupaten.

1.5. Pernyataan Kebaruan Ilmiah

Kebaruan ilmiah penelitian ini terletak pada integrasi metode *Octave Allegro* sebagai instrumen analisis risiko berbasis aset dengan Indeks KAMI 5.0 untuk evaluasi kesiapan keamanan informasi dalam satu kerangka *Risk-Based Governance* yang terpadu, sebuah kombinasi yang jarang ditemui pada level pemerintah daerah berdasarkan peta bibliometrik VOSviewer. Selain itu, penelitian ini mengoperasionalkan teori *Risk-Based Governance* dari Richard A. Caralli melalui dimensi pengukuran risiko, profil aset, serta identifikasi dan mitigasi risiko, yang membedakannya dari tren riset terdahulu yang didominasi oleh teori CIA Triad atau FMEA. Keunikan lainnya tampak pada fokus objek riset yang diarahkan pada Diskominfo tingkat kabupaten dengan karakteristik khas berupa keterbatasan SDM, anggaran, dan infrastruktur yang selama ini masih jarang dieksplorasi dibanding tingkat kementerian atau provinsi. Terakhir, seluruh analisis ini diaktualisasikan dalam konteks pemberlakuan UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), sehingga temuan yang dihasilkan menjadi sangat relevan dalam mendukung kepatuhan regulasi siber terbaru di lingkungan pemerintah daerah.

1.6. Tujuan

Penelitian ini bertujuan untuk menganalisis tata kelola persandian dalam meningkatkan keamanan pelayanan publik di Dinas Komunikasi dan Informatika Kabupaten Madiun.

II. METODE

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan desain studi kasus tunggal. Pendekatan ini dipilih karena tata kelola persandian merupakan fenomena kompleks yang tidak cukup dijelaskan melalui angka semata, melainkan membutuhkan pemahaman mendalam terhadap proses, dinamika, dan konteks implementasinya di lapangan (Creswell et al. 2023). Pendekatan kualitatif memungkinkan peneliti menggali makna, pola, dan interaksi antar-elemen tata kelola yang tidak tertangkap oleh pendekatan kuantitatif, sehingga relevan untuk menganalisis kondisi riil persandian di Dinas Komunikasi dan Informatika Kabupaten Madiun.

Data dikumpulkan melalui tiga teknik yang saling melengkapi: wawancara mendalam dengan pertanyaan terbuka, observasi langsung terhadap aktivitas pelayanan publik dan aset persandian, serta studi dokumentasi berupa profil instansi, struktur organisasi, regulasi, dan laporan kinerja. Keabsahan data dijamin melalui triangulasi sumber dan triangulasi teknik, yaitu membandingkan informasi dari berbagai informan dan memverifikasi lintas metode (wawancara, observasi, dan dokumen), sehingga temuan bersifat kredibel dan dapat dipertanggungjawabkan secara ilmiah.

Pemilihan informan dilakukan dengan teknik purposive sampling berdasarkan kriteria relevansi jabatan, kedalaman pengetahuan, dan keterlibatan langsung dalam tata kelola persandian. Terdapat enam informan yang ditetapkan sesuai dengan peran dan bidang informan. Informan kunci dalam penelitian ini adalah Kepala Dinas (I1) selaku pengambil keputusan tertinggi yang memiliki kewenangan penuh atas kebijakan dan alokasi anggaran persandian, sehingga perspektifnya merepresentasikan arah strategis tata kelola secara keseluruhan. Informan I3 (Kepala Bidang Persandian) juga berperan penting sebagai sumber data teknis karena mengelola implementasi harian sistem keamanan informasi.

Analisis data dilaksanakan menggunakan bantuan perangkat lunak NVivo 12 Plus melalui tiga tahapan berurutan: (1) reduksi data, yaitu pemilahan dan pengkodean (*coding*) data transkrip wawancara berdasarkan dimensi dan indikator teori *Risk-Based Governance*; (2) penyajian data, yaitu penyusunan temuan dalam bentuk naratif, tabel, dan visualisasi *Word Cloud, Word Frequency Query,* serta *Hierarchy Chart*; dan (3) penarikan kesimpulan dan verifikasi secara induktif berdasarkan pola dan kategori yang teridentifikasi dari data lapangan.

Penelitian ini dilaksanakan di Dinas Komunikasi dan Informatika Kabupaten Madiun, beralamat di Jl. Mastrip No. 23, Kelurahan Klegen, Kecamatan Kartoharjo, Kabupaten Madiun, Jawa Timur. Lokasi ini dipilih karena instansi tersebut merupakan leading sector teknologi informasi dan persandian di lingkungan Pemerintah Kabupaten Madiun yang secara langsung bertanggung jawab atas keamanan informasi pelayanan publik digital. Pengumpulan data lapangan dilaksanakan selama kurang lebih dua bulan, yaitu pada bulan Maret hingga April 2026, mencakup proses observasi awal, pelaksanaan wawancara mendalam, pengisian instrumen Indeks KAMI 5.0, serta pengumpulan dokumentasi. Keseluruhan proses penelitian, mulai dari pengajuan judul hingga penyusunan skripsi akhir, berlangsung dalam rentang tahun akademik 2025/2026 sesuai kalender akademik IPDN Angkatan XXXIII.

III. HASIL DAN PEMBAHASAN

3.1. Pengukuran Risiko (*Establish Drivers*)

Dimensi pengukuran risiko mencakup penetapan kriteria dampak yang digunakan untuk mengevaluasi tingkat risiko berdasarkan pengaruhnya terhadap misi organisasi (Caralli et al., 2007)

1. Reputasi dan Kepercayaan Publik

Kemampuan instansi dalam menjaga kepercayaan publik melalui pengelolaan keamanan informasi yang andal dan bebas dari insiden siber yang merugikan masyarakat. Penilaian terhadap indikator reputasi dan kepercayaan publik menunjukkan posisi prioritas tertinggi di antara seluruh indikator risiko, dilihat dari dampak langsung yang ditimbulkan oleh insiden keamanan terhadap persepsi masyarakat atas layanan digital pemerintah. Temuan ini sejalan dengan hasil penelitian Temuan ini sejalan dengan Nainggolan & Aqil (2023) yang menegaskan bahwa keamanan platform digital merupakan prasyarat mutlak terpeliharanya kepercayaan masyarakat, serta Nainggolan (2024) yang menyatakan bahwa penggunaan website dan media sosial pemerintah memiliki hubungan positif dengan kepercayaan masyarakat, sehingga keamanan platform digital menjadi prasyarat mutlak terpeliharanya kepercayaan. Ancaman siber pada infrastruktur layanan publik digital, termasuk sistem transportasi cerdas yang menjadi tulang punggung smart city, terbukti dapat berdampak langsung pada keselamatan dan keberlangsungan layanan masyarakat sebagaimana ditunjukkan oleh Joshi et al. (2026), sehingga memperkuat urgensi pengelolaan risiko yang sistematis di lingkungan pemerintah daerah."Diperkuat pula oleh Rasyid et al. (2024) yang menemukan bahwa insiden siber pada sistem transportasi cerdas dan layanan publik digital dapat secara langsung mengguncang kepercayaan masyarakat serta keberlangsungan layanan.

2. Keuangan/Finansial

Kemampuan instansi dalam mengalokasikan dan mengelola anggaran persandian secara efektif untuk menghadapi insiden keamanan tanpa mengganggu kesinambungan operasional layanan publik. Penilaian terhadap indikator keuangan menunjukkan adanya komitmen yang meningkat namun disertai keterbatasan struktural, dilihat dari tren kenaikan anggaran persandian dan tantangan fleksibilitas yang dihadapi dalam merespons ancaman siber secara cepat. Hal ini terlihat dari data anggaran persandian Diskominfo Kabupaten Madiun yang menunjukkan peningkatan konsisten dari Rp87.625.850 (2022) menjadi Rp122.370.668 (2024). Temuan ini selaras dengan kajian M. said Hasibuan et al. (2023) yang menyimpulkan bahwa keterbatasan anggaran merupakan salah satu faktor struktural yang paling menghambat optimalisasi tata kelola keamanan informasi di pemerintah daerah.

3. Produktivitas

Kemampuan sistem persandian dalam menjaga keberlangsungan alur kerja elektronik seluruh OPD tanpa gangguan yang menghambat produktivitas operasional. Penilaian terhadap indikator produktivitas menunjukkan potensi dampak yang signifikan apabila terjadi gangguan persandian, dilihat dari terhentinya alur kerja elektronik yang bergantung pada keandalan sistem keamanan informasi. Dampak gangguan persandian terhadap produktivitas diklasifikasikan ke dalam tiga tingkatan mulai dari tingkat rendah berupa kendala teknis minor, tingkat sedang berupa gangguan akses aplikasi dalam waktu singkat, dan tingkat tinggi berupa ancaman integritas data yang berimplikasi hukum dan sosial. Dimensi produktivitas perlu mendapat perhatian serius karena skala dampaknya yang berlapis, sejalan dengan argumen Hidayah & Almadani (2022)yang menemukan bahwa dalam evaluasi tingkat kematangan SPBE di Sulawesi Selatan, isu keamanan data menjadi salah satu kendala utama yang menghambat

keberhasilan sistem pemerintahan berbasis elektronik tidak hanya bergantung pada ketersediaan infrastruktur, melainkan juga pada keandalan sistem keamanan yang menopangnya.

4. Keselamatan dan Kesehatan SDM

Kemampuan tata kelola persandian dalam melindungi identitas dan keselamatan psikologis aparatur dari penyalahgunaan data pribadi akibat celah keamanan informasi. Penilaian terhadap indikator keselamatan dan kesehatan SDM menunjukkan posisi prioritas terakhir di antara lima indikator risiko, dilihat dari karakteristik ancaman siber yang lebih dominan berdampak pada aset informasi dan integritas institusi dibandingkan keselamatan fisik aparatur. Dimensi keselamatan dan kesehatan SDM meskipun berada pada prioritas terakhir, tetap tidak mengurangi pentingnya perlindungan data personal staf sebagai bagian dari tata kelola persandian yang bertanggung jawab.

5. Kepatuhan dan Sanksi Hukum

Kemampuan instansi dalam memenuhi kerangka regulasi persandian yang berlaku guna menghindari sanksi hukum dan memastikan pengelolaan keamanan informasi sesuai dengan ketentuan peraturan perundang-undangan. Penilaian terhadap indikator kepatuhan dan sanksi hukum menunjukkan adanya kesenjangan yang signifikan antara regulasi yang tersedia dengan implementasi teknis di lapangan, dilihat dari belum tersedianya SOP yang rinci dan operasional sebagai turunan regulasi yang ada. Kesenjangan regulasi berkontribusi pada status Pemenuhan Kerangka Kerja Dasar pada evaluasi Indeks KAMI 5.0, khususnya pada Area Kerangka Kerja Pengelolaan Keamanan Informasi yang masih berada pada tingkat kematangan II. Dimensi kepatuhan dan sanksi hukum perlu mendapat perhatian utama dalam penyusunan regulasi teknis turunan, sejalan dengan penekanan Susila & Salim (2024) yang membandingkan kerangka regulasi siber Indonesia dan Jerman bahwa infrastruktur hukum Indonesia dalam menghadapi ancaman siber masih jauh tertinggal dan memerlukan reformasi mendesak dengan memprioritaskan operasionalisasi regulasi turunan yang konkret sebagai kunci pencegahan eksploitasi celah keamanan pada sistem informasi pemerintah.

3.2. Profil Aset Persandian (*Profile Assets*)

Dimensi profil aset persandian mencakup identifikasi dan karakterisasi aset-aset informasi kritis beserta tanggung jawab pengelolaannya dalam mendukung penyelenggaraan pelayanan publik digital (Caralli et al., 2007). Aset persandian Diskominfo Kabupaten Madiun telah teridentifikasi dan terklasifikasi ke dalam lima kategori utama yang mencakup seluruh komponen infrastruktur keamanan informasi instansi. Mengacu pada klasifikasi Alberts et al. (2021), aset persandian Diskominfo Kabupaten Madiun diklasifikasikan dalam lima kategori berikut:

Tabel 1.1 Klasifikasi Aset Persandian Dinas Komunikasi dan Informatika Kabupaten Madiun

Kategori	Daftar Aset
Hardware	Perangkat enkripsi, server penyimpanan data, kunci keamanan, komputer kerja (PC), laptop, printer, scanner
Software	Firewall, antivirus, IDS; aplikasi e-government berbasis web/mobile; Aplikasi Manajemen Sertifikat Elektronik; Sistem TTE; tools enkripsi data
Data	Naskah dinas dan laporan strategis; data sertifikat elektronik; database aplikasi e-government
Network	Infrastruktur VPN dan Firewall; jaringan LAN dan Wi-Fi internal
People	Tim teknis persandian; pengelola keamanan informasi dan sistem digital

Sumber: Hasil pengolahan data riset (2026)

Kejelasan peran dan tanggung jawab dalam pengelolaan aset persandian yang terbagi secara berjenjang untuk memastikan setiap komponen infrastruktur terjaga secara optimal. Pembagian tanggung jawab yang terstruktur mencerminkan kesiapan instansi dalam mengoperasikan sistem keamanan informasi secara sistematis dan akuntabel. Kesiapan pembagian peran mencakup tiga lapisan: pimpinan sebagai pemilik kebijakan strategis, Bidang Persandian sebagai pengelola teknis harian, serta staf internal dan admin OPD sebagai pengguna aset yang bertanggung jawab menjaga kedisiplinan operasional sistem. Dimensi tanggung jawab pengelolaan aset sudah cukup baik dari sisi struktur organisasi, namun perlu ditingkatkan dari sisi kompetensi teknis SDM, sejalan dengan penegasan Wardana et al. (2025) dalam kajian good governance digital Kabupaten Sumedang bahwa keberhasilan transformasi digital pemerintahan tidak semata ditentukan oleh teknologi, melainkan juga oleh regulasi, kepemimpinan, dan SDM yang kompeten secara teknis dalam mengelola infrastruktur digital dan mengatasi isu keamanan data.

3.3. Identifikasi dan Mitigasi Risiko (*Identify and Mitigate*)

Dimensi identifikasi dan mitigasi risiko mencakup proses pengenalan ancaman dan kerentanan terhadap aset kritis serta perumusan strategi penanganannya untuk menjaga keberlangsungan penyelenggaraan layanan publik digital (Caralli et al., 2007). Visualisasi *Hierarchy Chart* menunjukkan indikator Strategi Mitigasi mendominasi data wawancara dibandingkan Pelatihan dan Pengembangan Kompetensi, mencerminkan perhatian lebih besar informan pada tindakan teknis pengamanan.

Pada indikator Pelatihan dan Pengembangan Kompetensi, Diskominfo Kabupaten Madiun melaksanakan tiga jalur pengembangan secara bersamaan: (1) pelatihan formal eksternal melalui Bimtek dan sertifikasi BSSN; (2) penguatan internal melalui knowledge sharing dan penyusunan prosedur formal; serta (3) sosialisasi eksternal kepada operator OPD dan masyarakat. Anggaran pelatihan terus meningkat seiring dengan tren kenaikan total anggaran persandian. Namun kondisi faktual menunjukkan masih minimnya personil bersertifikat, mengingat frekuensi pelatihan belum mencukupi kebutuhan menghadapi dinamika ancaman siber yang terus berkembang.

Pada indikator Strategi Mitigasi, Diskominfo Kabupaten Madiun menerapkan pengamanan berlapis yang mencakup: firewall Next-Generation, sistem IDS/IPS, enkripsi data pada aset-aset informasi prioritas, backup data berkala ke server cadangan yang terpisah, pemantauan jaringan 24 jam melalui *Security Operations Center* (SOC), segmentasi jaringan, dan pembaruan antivirus/patching rutin. Seluruh OPD diwajibkan mengintegrasikan standar keamanan informasi sesuai Perbup No. 46/2020 dan arahan BSSN. Meskipun demikian, aspek Perlindungan Data Pribadi (skor 56, level II) masih menjadi kelemahan signifikan mengingat mekanisme pemetaan alur pertukaran data dengan pihak ketiga belum terintegrasi penuh sesuai amanat UU PDP.

Tabel 1.2 Rekapitulasi Capaian Tata Kelola Persandian

Dimensi	Indikator	Capaian	Keterangan
Pengukuran Risiko	Reputasi & Kepercayaan Publik	Tercapai	Prioritas risiko tertinggi; insiden web defacement berdampak langsung pada kepercayaan publik
	Keuangan/Finansial	Tercapai	Anggaran meningkat konsisten, namun fleksibilitas terbatas akibat mekanisme e-Procurement
	Produktivitas	Tercapai	Klasifikasi dampak tiga tingkatan teridentifikasi; prosedur pemulihan belum terstandar menyeluruh
	Keselamatan & Kesehatan SDM	Tercapai	Risiko pada data personal staf diakui; prioritas terakhir
	Kepatuhan & Sanksi Hukum	Belum Tercapai	Regulasi tersedia namun SOP teknis turunan belum lengkap; kematangan II pada KAMI 5.0
Profil Aset Persandian	Klasifikasi Sarana & Prasarana	Tercapai	Lima kategori aset teridentifikasi; sebagian perangkat berusia >5 tahun

Identifikasi & Mitigasi Risiko	Pihak yang Bertanggung Jawab	Tercapai	Pembagian berjenjang terbentuk; hanya 4 dari 48 ASN bersertifikat
	Pelatihan & Pengembangan Kompetensi	Belum Tercapai	Tiga jalur pelatihan berjalan; jumlah personil bersertifikat masih sangat terbatas
	Strategi Mitigasi	Tercapai	Pengamanan berlapis melalui firewall, IDS/IPS, enkripsi, SOC 24 jam; PDP masih level II

Sumber: Diolah oleh Penulis (2026)

3.4. Evaluasi Kesiapan Keamanan Informasi melalui Indeks KAMI 5.0

Tingkat kesiapan keamanan informasi Diskominfo Kabupaten Madiun yang diukur menggunakan Indeks KAMI 5.0 berdasarkan kriteria SNI ISO/IEC 27001 sebagai instrumen komplementer dalam menilai kelengkapan dan kematangan penerapan keamanan informasi.

Tabel 1.3 Hasil Evaluasi Indeks KAMI 5.0 Dinas Komunikasi dan Informatika Kabupaten Madiun

Area Evaluasi	Skor	Kematangan	Keterangan
Kategori Sistem Elektronik	31	Tinggi	Ketergantungan sangat besar pada TI; memerlukan pengamanan ketat
Tata Kelola Keamanan Informasi	104	III+	Telah berjalan layak; pimpinan memberikan dukungan penuh secara resmi
Pengelolaan Risiko Keamanan Informasi	46	II	Ambang batas risiko masih dalam tahap perencanaan; kajian risiko rutin belum terdokumentasi
Kerangka Kerja Pengelolaan Keamanan Informasi	91	II	SOP belum tersosialisasi maksimal; kepatuhan rutin masih perlu ditingkatkan
Pengelolaan Aset Informasi	153	II	Inventarisasi dilakukan, namun klasifikasi kerahasiaan & masa retensi data belum terdefinisi
Teknologi dan Keamanan Informasi	127	III+	Pilar terkuat; firewall berlapis dan segmentasi jaringan telah diterapkan dengan baik
Perlindungan Data Pribadi	56	II	Mekanisme pertukaran data dengan pihak ketiga & penghapusan data belum terintegrasi sesuai UU PDP

Sumber: Dinas Komunikasi dan Informatika Kabupaten Madiun (2026)

3.4. Diskusi Temuan Utama Penelitian

Temuan utama penelitian ini menunjukkan bahwa tata kelola persandian Diskominfo Kabupaten Madiun telah berjalan dengan berpedoman pada regulasi yang ada, namun implementasinya masih memerlukan penguatan pada aspek operasional dan manajemen risiko. Kondisi ini sejalan dengan temuan Saputra et al. (2023) pada Diskominfo Provinsi Kalimantan Timur yang menemukan tingkat kematangan Indeks KAMI berada pada level I+ hingga II+, mengindikasikan kerentanan serupa pada ekosistem pemerintah daerah secara umum. Berbeda dengan temuan M. S. Hasibuan et al. (2025) di level kementerian yang menunjukkan skor lebih tinggi, pemerintah kabupaten memiliki keterbatasan kapasitas kelembagaan yang lebih signifikan.

Temuan mengenai prioritas risiko pada reputasi dan kepercayaan publik memperkuat penelitian Nainggolan (2024) yang mengungkapkan hubungan positif antara kualitas layanan digital pemerintah dan kepercayaan masyarakat. Insiden *web defacement* yang berulang membuktikan bahwa kepercayaan publik terhadap layanan digital sangat bergantung pada jaminan CIA Triad (kerahasiaan, keutuhan, dan ketersediaan) sebagaimana ditekankan oleh Rochmadi & Ike Yunia Pasa (2021). Temuan mengenai keterbatasan SDM bersertifikat (hanya 4 dari 48 ASN) sejalan dengan laporan BSSN (2025) yang

mencatat sebagian besar instansi pemerintah daerah masih berada pada kategori "Dasar" dalam hal kematangan keamanan informasi nasional.

3.5. Diskusi Temuan Menarik Lainnya

Penulis menemukan faktor penghambat yang saling berkaitan dalam pelaksanaan tata kelola persandian: (1) keterbatasan SDM bersertifikat yang menyebabkan beban kerja tidak terdistribusi merata; (2) keterbatasan infrastruktur, di mana sebagian perangkat berusia >5 tahun tidak lagi mendapat patch keamanan vendor; (3) keterbatasan fleksibilitas anggaran akibat mekanisme e-Procurement yang panjang; (4) belum tersedianya SOP teknis turunan dari Perbup No. 46/2020; serta (5) rendahnya kesadaran keamanan informasi pengguna OPD yang menjadikan human error sebagai pemicu utama insiden siber, suatu temuan yang selaras dengan identifikasi Supriyanto et al. (2025) mengenai alignment standar keamanan.

IV. KESIMPULAN

Penelitian ini menyimpulkan bahwa tata kelola persandian di Dinas Komunikasi dan Informatika Kabupaten Madiun belum optimal, yang dibuktikan dengan status "Pemenuhan Kerangka Kerja Dasar" pada Indeks KAMI 5.0. Berdasarkan analisis Octave Allegro: (1) Pengukuran risiko menunjukkan reputasi dan kepercayaan publik menjadi prioritas risiko tertinggi yang terbukti dari insiden web defacement; (2) Profil aset persandian telah teridentifikasi dalam lima kategori namun klasifikasi kerahasiaan data dan retensi belum terdefinisi formal; (3) Identifikasi dan mitigasi risiko dilakukan melalui pengamanan berlapis, namun keterbatasan SDM bersertifikat dan belum optimalnya SOP teknis turunan menjadi kendala utama. Diperlukan penguatan struktur organisasi persandian melalui penyusunan SOP mitigasi insiden siber secara periodik dan peningkatan kapasitas kompetensi aparatur guna menjamin keberlanjutan pelayanan publik yang aman dan terpercaya.

Keterbatasan Penelitian. Penelitian ini memiliki keterbatasan utama pada cakupan satu instansi sebagai studi kasus serta keterbatasan waktu pengumpulan data selama dua bulan. Selain itu, penilaian Indeks KAMI 5.0 yang dijadikan acuan merupakan hasil *self-assessment* instansi per Juli 2025 sehingga bersifat subjektif.

Arah Masa Depan Penelitian (*future work*). Penelitian lanjutan disarankan untuk melakukan studi komparatif tata kelola persandian di beberapa kabupaten/kota di Jawa Timur agar diperoleh gambaran yang lebih representatif. Integrasi dengan analisis kuantitatif melalui pengujian validitas SOP berbasis ISO/IEC 27001:2022 juga perlu dipertimbangkan.

V. UCAPAN TERIMA KASIH

Ucapan terima kasih terutama ditujukan kepada Ibu Dr. Ir. Ika Sartika, M.T. selaku Dosen Pembimbing Skripsi atas bimbingan, arahan, dan motivasi intelektual yang luar biasa. Terima kasih kepada seluruh jajaran Dinas Komunikasi dan Informatika Kabupaten Madiun yang telah memberikan kesempatan dan kemudahan akses selama penelitian berlangsung. Ucapan terima kasih juga kepada Institut Pemerintahan Dalam Negeri serta seluruh pihak yang telah membantu dan mendukung penyelesaian penelitian ini.

VI. DAFTAR PUSTAKA

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2021). *OCTAVE®-S Implementation Guide, Version 1.0 Volume*. *8*(January), 167–186. https://doi.org/10.1184/R1/6575852

Alfarisi, S., & Surantha, N. (2022). Risk assessment in fleet management system using OCTAVE allegro. *Bulletin of Electrical Engineering and Informatics*, *11*(1), 530–540. https://doi.org/10.11591/eei.v11i1.3241

BSSN. (2025). *Peraturan Badan Siber dan Sandi Negara Nomor 5 Tahun 2025 tentang Pedoman Tata Kelola Keamanan Informasi dan Infrastruktur Informasi Vital Sektor Administrasi Pemerintahan.* https://peraturan.bpk.go.id/Details/315044/peraturan-bssn-no-5-tahun-2025

Budarsa, N. (2022). Analisis Risiko Keamanan Informasi Menggunakan Metode Octave Allegro dan Analytical Hirarchy Process pada Data Center Pemerintah Kabupaten Buleleng. *Jurnal Ilmu Komputer Indonesia (JIK)*, *7*(1), 13–15. https://ejournal-pasca.undiksha.ac.id/index.php/jik/article/view/3769

Caralli, R. a R. a. C., Stevens, J. F., Young, L. R., & Wilson, W. R. (2007). Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process. *Young*, (May), 1–113. https://doi.org/10.1184/R1/6574790

Creswell, J. W., & Creswell, J. D. (2023). Research Design: Qualitative, quantitative and mixed methods approaches. In *SAGE Publications,Inc.* https://books.google.co.id/books/about/Research_Design.html?hl=id&id=Rkh4EAAAQBAJ&redir_esc=y

Emmanuel, P. N., & Maulany, R. (2023). Penilaian Risiko Sistem Informasi Menggunakan Metode OCTAVE Allegro pada Indonesia Publishing House. *Krea-Tif: Jurnal Teknik Informatika*, *11*(1), 37–52. https://garuda.kemdiktisaintek.go.id/documents/detail/3690900

Hasibuan, M. S., Romadhoni, N. R., & Muludi, K. (2025). Analisis Keamanan Informasi pada Sistem Komputerisasi Terpadu Menggunakan Metode Indeks KAMI dan Octave Allegro. *Jurnal Ilmu Komputer Dan Agri-Informatika*, *12*(1), 38–49. https://doi.org/10.29244/jika.12.1.38-49

Hasibuan, M. said, & Rahman, R. Y. (2023). Evaluasi Keamanan Informasi Pada Sman 1 Xyz Menggunakan Indeks Kami Versi 4.2. *Jurnal Fasilkom*, *13*(02), 181–187. https://doi.org/10.37859/jf.v13i02.4916

Hidayah, E. S., & Almadani, M. (2022). Analisis Tingkat Kematangan Sistem Pemerintahan Berbasis Elektronik (SPBE) pada Pemerintah Provinsi Sulawesi Selatan. *Jurnal Teknologi Dan Komunikasi Pemerintahan*, *4*(2), 49–67. https://www.researchgate.net/publication/366835573_Analisis_Tingkat_Kematangan_Sistem_Pemerintahan_Berbasis_Elektronik_SPBE_pada_Pemerintah_Provinsi_Sulawesi_Selatan

Id-SIRTII /CC. (2024). Lanskap Keamanan Siber Indonesia. *Id-SIRTII /CC*, (70), 1–107. https://alika.pesisirbaratkab.go.id/ebook/lanskap-keamanan-siber-indonesia-2024

Irsheid, A., Murad, A., Alnajdawi, M., & Qusef, A. (2022). Information security risk management models for cloud hosted systems: A comparative study. *Procedia Computer Science*, *204*, 205–217. https://doi.org/10.1016/j.procs.2022.08.025

Joshi, S., Baviskar, A., & Rajmane, S. (2026). A review of cybersecurity in smart cities and intelligent transport systems. *Discover Internet of Things*, *6*(1). https://doi.org/10.1007/s43926-026-00312-y

Nainggolan, R. R. E. (2024). Analisis Penggunaan Website dan Media Sosial Pemerintah untuk Pelayanan Publik. *Jurnal Teknologi Dan Komunikasi Pemerintahan*, *6*(1), 1–21. https://scholar.google.com/citations?view_op=view_citation&hl=id&user=d9FOk0YAAAAJ&citation_for_view=d9FOk0YAAAAJ:Tyk-4Ss8FVUC

Nainggolan, R. R. E., & Aqil, M. H. (2023). Analisis Faktor-Faktor yang Mempengaruhi Kepuasan Pengguna Aplikasi Pemerintah Kota Pagar Alam. *Jurnal Teknologi Dan Komunikasi Pemerintahan*, *5*(2), 229–249. https://scholar.google.com/citations?view_op=view_citation&hl=id&user=d9FOk0YAAAAJ&citation_for_view=d9FOk0YAAAAJ:2osOgNQ5qMEC

Rasyid, M. F. F., Muh. Akhdharisa, S. J., Mamu, K. Z., Paminto, S. R., Hidaya, W. A., & Hamadi, A. (2024). Cybercrime Threats and Responsibilities: The Utilization of Artificial Intelligence in Online Crime. *Jurnal Ilmiah Mizani*, *11*(1), 49–63. https://doi.org/10.29300/mzn.v11i1.3318

Rochmadi, T., & Ike Yunia Pasa. (2021). Pengukuran Risiko Dan Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi Di Bkd Xyz Berdasarkan Iso 27001 / Sni. *Cyber Security Dan Forensik Digital*, *4*(1), 38–43. https://doi.org/10.14421/csecurity.2021.4.1.2439

Saputra, A. D., Dione, F., & Uluputty, I. (2023). Pengelolaan Keamanan Informasi dan Persandian di Dinas Komunikasi dan Informatika Provinsi Kalimantan Timur. *Jurnal Teknologi Dan Komunikasi Pemerintahan*, *5*(2), 159–187. https://www.researchgate.net/publication/377505917_Pengelolaan_Keamanan_Informasi_dan_Persandian_di_Dinas_Komunikasi_dan_Informatika_Provinsi_Kalimantan_Timur

Supriyanto, A., Jananto, A., Razaq, J. A., Hartono, B., & Damaryanti, F. (2025). Alignment of KAMI Index with Global Security Standards in Information Security Risk Maturity Evaluation. *Cybernetics and Information Technologies*, *25*(2), 173–192. https://doi.org/10.2478/cait-2025-0018

Susila, M. E., & Salim, A. A. (2024). Cyber Espionage Policy and Regulation: A Comparative Analysis of Indonesia and Germany. *Padjadjaran Jurnal Ilmu Hukum*, *11*(1), 122–144. https://doi.org/10.22304/pjih.v11n1.a6

Wardana, R., Meilya Putri, K. A., & Fatati, K. (2025). Good Governance di Era Digital: Pemerintah Kabupaten Sumedang Sebagai Model Transformasi Pelayanan Publik. *Jurnal Teknologi Dan Komunikasi Pemerintahan*, *7*(1), 66–80. https://doi.org/10.33701/jtkp.v7i1.5094