ANALISIS RISIKO KEAMANAN TEKNOLOGI INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PADA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN TIMOR TENGAH SELATAN

Aji Bayu Ramadhan

NPP. 33.0657

Program Studi Teknologi Rekayasa Informasi Pemerintahan

Email: bayubeatbox16@gmail.com

Pembimbing Skripsi: M. Rezza Fahlevvi, M.Cs.

NIP. 199408142022031004

ABSTRACT

Problem Statement (Research Gap): *The development of electronic-based government systems at the local level has not always been followed by balanced strengthening of information technology risk management, security control, and ICT audit. In Timor Tengah Selatan Regency, the SPBE service domain has improved, but the management domain and ICT audit aspect remain weak, creating a need for an adaptive risk assessment and mitigation model for local government capacity.* ***Purpose:*** *This study aims to determine the level of information technology security risk in the SPBE implementation at the Department of Communication and Informatics of Timor Tengah Selatan Regency, identify relevant mitigation controls based on CIS Controls v8, and analyze the conceptual implications for SDGs 16.6 and 16.10.* ***Method:*** *This study uses a qualitative approach. Data were collected through observation, semi-structured interviews with three informants, and documentation. Risk assessment was conducted using NIST SP 800-30 Rev. 1, while mitigation recommendations were mapped to CIS Controls v8 Implementation Group 1.* ***Result:*** *The study found 11 threat events affecting hardware, software, data, network, and human resources. Most risks are moderate, while high risks are concentrated in the absence of backup power and room temperature control for server infrastructure. The mapping to CIS Controls v8 shows that several safeguards have been partially implemented, especially in configuration, account, access, data protection, and log management, but major gaps remain in enterprise asset inventory, vulnerability management, data recovery, and security awareness training.* ***Conclusion:*** *The SPBE information security posture of Diskominfo TTS requires priority strengthening of basic infrastructure, documented procedures, access control, data recovery, vulnerability monitoring, and human resource capacity to support reliable, accountable, and transparent digital governance.*

Keywords: CIS Controls v8; Information Technology Security; NIST SP 800-30 Rev. 1; Risk Assessment; SPBE

ABSTRAK

Permasalahan (Kesenjangan Penelitian/Research Gap): Pengembangan Sistem Pemerintahan Berbasis Elektronik (SPBE) di pemerintah daerah belum selalu diikuti oleh penguatan manajemen risiko, kontrol keamanan, dan audit TIK yang seimbang. Pada Pemerintah Kabupaten Timor Tengah Selatan, domain layanan SPBE menunjukkan capaian lebih baik, tetapi domain manajemen dan aspek audit TIK masih rendah sehingga diperlukan evaluasi risiko dan mitigasi yang adaptif dengan kapasitas daerah. **Tujuan:** Penelitian ini bertujuan untuk mengetahui tingkat risiko keamanan teknologi informasi pada Diskominfo TTS, menentukan kontrol mitigasi yang relevan berdasarkan CIS Controls v8, serta menganalisis implikasi konseptualnya terhadap SDGs 16.6 dan 16.10. **Metode:** Penelitian ini menggunakan pendekatan kualitatif. Data diperoleh melalui observasi, wawancara semi-terstruktur terhadap tiga informan, dan dokumentasi. Analisis risiko

dilakukan menggunakan NIST SP 800-30 Rev. 1, kemudian hasilnya dipetakan ke CIS Controls v8 Implementation Group 1. **Hasil/Temuan:** Penelitian menemukan 11 peristiwa ancaman pada aset hardware, software, data, jaringan, dan brainware. Sebagian besar risiko berada pada kategori sedang, sedangkan risiko tinggi terdapat pada gangguan operasional akibat tidak tersedianya backup listrik dan kerusakan perangkat akibat tidak adanya pengendalian suhu ruang server. Pemetaan CIS Controls v8 menunjukkan sebagian safeguard telah diterapkan secara parsial pada konfigurasi, akun, akses, perlindungan data, dan log, tetapi gap utama masih terdapat pada inventarisasi aset, manajemen kerentanan, pemulihan data, dan pelatihan kesadaran keamanan. **Kesimpulan:** Keamanan teknologi informasi SPBE Diskominfo TTS perlu diperkuat melalui prioritas pada infrastruktur dasar, SOP, kontrol akses, pemulihan data, pemantauan kerentanan, dan peningkatan kapasitas SDM agar mendukung tata kelola digital yang andal, akuntabel, dan transparan.
Kata kunci: CIS Controls v8; Keamanan Teknologi Informasi; NIST SP 800-30 Rev. 1; Penilaian Risiko; SPBE

I. PENDAHULUAN

1.1. Latar Belakang

Pembangunan berkelanjutan menuntut institusi publik yang efektif, akuntabel, transparan, dan mampu menyediakan akses informasi yang andal. Dalam konteks pemerintahan digital, tuntutan tersebut diwujudkan melalui Sistem Pemerintahan Berbasis Elektronik (SPBE) yang mengintegrasikan proses kerja, data, infrastruktur, dan layanan publik berbasis teknologi informasi. SPBE tidak hanya berhubungan dengan digitalisasi layanan, tetapi juga dengan kemampuan pemerintah menjaga kerahasiaan, integritas, dan ketersediaan data.

Pemerintah Kabupaten Timor Tengah Selatan telah mengalami peningkatan indeks SPBE dari 2,56 pada 2022 menjadi 2,83 pada 2024 dengan predikat baik. Meskipun demikian, peningkatan layanan belum diikuti penguatan manajemen dan audit secara seimbang. Domain layanan SPBE memperoleh nilai lebih tinggi, sedangkan Domain Manajemen SPBE dan aspek Audit TIK masih rendah. Kondisi ini menunjukkan bahwa aspek layanan digital berkembang, tetapi fondasi pengelolaan risiko, pengendalian, dan audit keamanan belum optimal.

Dalam konteks ancaman siber yang terus meningkat, kelemahan manajemen risiko dan audit TIK dapat berdampak terhadap keberlangsungan layanan, integritas data, dan kepercayaan publik. Oleh karena itu, evaluasi keamanan teknologi informasi pada SPBE di Dinas Komunikasi dan Informatika Kabupaten Timor Tengah Selatan menjadi penting untuk mengidentifikasi risiko secara sistematis dan menyusun rekomendasi mitigasi yang sesuai dengan kapasitas pemerintah daerah.

Tabel 1.
Skor SPBE Pemerintah Kabupaten Timor Tengah Selatan 2022-2024

Tahun	Nilai	Predikat
2022	2,56	Cukup
2023	2,74	Baik
2024	2,83	Baik

Sumber: Diolah dari dokumen skripsi peneliti.

1.2. Kesenjangan Masalah yang Diambil (Research Gap)

Penelitian terdahulu telah banyak menggunakan NIST SP 800-30 Rev. 1 untuk menilai risiko keamanan teknologi informasi, tetapi sebagian besar masih berfokus pada identifikasi dan pemeringkatan risiko. Di sisi lain, penelitian yang menggunakan CIS Controls v8 umumnya lebih menekankan rekomendasi kontrol teknis dan belum selalu dikaitkan langsung dengan hasil risk assessment pada konteks SPBE pemerintah daerah.

Kesenjangan tersebut menjadi dasar penelitian ini. Penelitian ini mengintegrasikan NIST SP 800-30 Rev. 1 sebagai kerangka analisis risiko dengan CIS Controls v8 sebagai dasar mitigasi pada konteks Dinas Komunikasi dan Informatika Kabupaten Timor Tengah Selatan. Selain itu, penelitian

ini menempatkan SDGs 16.6 dan 16.10 sebagai kerangka implikasi konseptual, bukan sebagai indikator yang diukur langsung.

1.3. Urgensi Penelitian

Penelitian ini penting dilakukan karena hasil evaluasi SPBE menunjukkan lemahnya aspek manajemen risiko, keamanan teknologi informasi, dan audit TIK. Apabila evaluasi risiko tidak dilakukan, pemerintah daerah berpotensi tidak memiliki dasar empiris yang cukup untuk menetapkan prioritas pengamanan sistem, menyusun SOP, memperkuat infrastruktur, dan meningkatkan kapasitas SDM. Akibatnya, layanan SPBE rentan mengalami gangguan operasional, kebocoran data, dan penurunan kepercayaan masyarakat.

1.4. Penelitian Terdahulu

Penelitian ini terinspirasi dari beberapa kajian terdahulu mengenai manajemen risiko keamanan teknologi informasi, pengendalian keamanan, tata kelola SPBE, dan transformasi digital yang relevan dengan SDGs. Ringkasan perbandingan penelitian terdahulu disajikan berikut.

Tabel 2.
Ringkasan penelitian terdahulu yang relevan

No	Peneliti	Fokus	Relevansi
1	Putra & Soewito (2023)	NIST SP 800-30 dan ISO untuk sektor asuransi	Menjadi dasar penggunaan NIST untuk risk assessment.
2	Amiruddin et al. (2021)	Perencanaan cyber-risk dengan NIST dan CIS Controls v8	Menjadi acuan pemetaan kontrol mitigasi.
3	Tanjung et al. (2024)	Desain keamanan SPBE dengan NIST CSF, ISO, dan CIS	Relevan dengan konteks pemerintahan berbasis elektronik.
4	Hermawan et al. (2025)	Manajemen risiko sistem informasi pada Diskominfo	Menunjukkan relevansi NIST pada instansi pemerintah daerah.
5	Aprianti et al. (2023)	NIST SP 800-30 dan kontrol ISO pada SIMBADA	Memperkuat pola analisis risiko dan rekomendasi kontrol.
6	ElMassah & Mohieldin (2020); Lubis et al. (2024)	Transformasi digital dan SDGs	Menjadi dasar implikasi konseptual terhadap SDGs 16.

Sumber: Diolah dari kajian pustaka skripsi peneliti.

1.5. Pernyataan Kebaruan Ilmiah

Kebaruan penelitian ini terletak pada integrasi NIST SP 800-30 Rev. 1 dan CIS Controls v8 dalam konteks keamanan teknologi informasi SPBE pemerintah daerah. NIST digunakan untuk menghasilkan profil risiko, sedangkan CIS Controls v8 digunakan untuk menerjemahkan risiko menjadi rekomendasi mitigasi yang praktis. Penelitian ini juga memiliki kekhususan lokasi pada Diskominfo Kabupaten Timor Tengah Selatan serta membaca hasil evaluasi keamanan sebagai implikasi konseptual terhadap SDGs 16.6 dan 16.10.

1.6. Tujuan

Penelitian ini bertujuan untuk menganalisis risiko keamanan teknologi informasi SPBE pada Dinas Komunikasi dan Informatika Kabupaten Timor Tengah Selatan serta merumuskan rekomendasi mitigasi berdasarkan CIS Controls v8.

II. METODE

Penelitian ini menggunakan pendekatan kualitatif karena diarahkan untuk memahami kondisi aktual keamanan teknologi informasi pada penyelenggaraan SPBE dalam konteks organisasi pemerintah daerah. Penggunaan NIST SP 800-30 Rev. 1 dan CIS Controls v8 tidak mengubah penelitian menjadi kuantitatif, melainkan berfungsi sebagai kerangka analisis agar temuan lapangan dapat disusun secara sistematis.

Data primer diperoleh melalui observasi dan wawancara semi-terstruktur. Observasi digunakan untuk mengidentifikasi aset dan sumber ancaman, sedangkan wawancara digunakan untuk menggali peristiwa ancaman, kerentanan, kemungkinan, dampak, dan kontrol keamanan yang

telah diterapkan. Informan dipilih secara purposive karena memiliki keterlibatan langsung dalam pengelolaan SPBE, yaitu Kepala Bidang TIK dan dua Pranata Komputer Bidang TIK.

Data sekunder diperoleh melalui dokumentasi, seperti dokumen evaluasi SPBE, data aset, kebijakan, dan dokumen pendukung pengelolaan teknologi informasi. Analisis data dilakukan melalui reduksi data, penyajian data, dan penarikan kesimpulan. Penilaian kemungkinan dan dampak menggunakan kategori kualitatif NIST, yaitu sangat rendah, rendah, sedang, tinggi, dan sangat tinggi. Hasil penilaian kemudian digabungkan melalui matriks risiko untuk menentukan tingkat risiko.

Penelitian dilaksanakan di Dinas Komunikasi dan Informatika Kabupaten Timor Tengah Selatan, Jl. Basuki Rahmat No. 10, Soe, Nusa Tenggara Timur. Pelaksanaan penelitian disesuaikan dengan tahapan akademik tahun 2025/2026 dan kebutuhan pengumpulan data lapangan.

Tabel 3.
Informan penelitian

No	Informan	Jumlah	Kode
1	Kepala Bidang Teknologi Informasi dan Komunikasi	1	I1
2	Pranata Komputer Bidang TIK	1	I2
3	Pranata Komputer Bidang TIK	1	I3

Sumber: Diolah oleh peneliti.

III. HASIL DAN PEMBAHASAN

3.1. Identifikasi Aset Teknologi Informasi

Identifikasi aset dilakukan untuk mengetahui komponen yang menopang penyelenggaraan SPBE. Aset yang ditemukan meliputi perangkat keras, perangkat lunak, sumber daya manusia, data, dan jaringan. Kelima komponen tersebut saling berkaitan sehingga kelemahan pada satu aset dapat berdampak pada keberlangsungan layanan digital pemerintah daerah.

Tabel 4.
Information assets, data, devices, and systems

No	Jenis Aset	Jumlah	Keterangan
1	Hardware	140 unit	72 unit terkait SPBE, 50 aktif, 22 rusak
2	Software	15 sistem	11 website pemda, 4 aplikasi pusat
3	Brainware	2 orang	Pranata komputer
4	Data	Data sektoral	Data Kabupaten TTS, proses integrasi ke PDN sejak 2021 dan implementasi 2024
5	Jaringan	7 unit	Internet internal, router, firewall, LAN, Wi-Fi tamu, dan media center

Sumber: Data diolah berdasarkan KIB Diskominfo TTS.

Temuan tersebut menunjukkan bahwa Diskominfo TTS memiliki aset yang cukup beragam, tetapi dukungan SDM teknis masih terbatas. Kondisi hardware juga belum seluruhnya optimal karena masih terdapat perangkat rusak dan perangkat yang melewati umur teknis. Hal ini menjadi dasar penting dalam analisis risiko karena aset yang tidak terdokumentasi dan tidak terpelihara dapat memperbesar peluang gangguan.

3.2. Identifikasi Sumber dan Peristiwa Ancaman

Mengacu pada NIST SP 800-30 Rev. 1, sumber ancaman diklasifikasikan ke dalam adversarial, accidental, structural, dan environmental. Hasil penelitian menunjukkan bahwa ancaman tidak hanya berasal dari penyerang eksternal, tetapi juga dari kesalahan manusia, kegagalan perangkat, dan kondisi lingkungan.

Tabel 5.
Klasifikasi sumber ancaman

Kategori	Sumber Ancaman	Contoh Peristiwa
Adversarial	Hacker/penyerang eksternal	Defacement website dan potensi phishing
Accidental	Pegawai/administrator sistem	Kesalahan konfigurasi dan pengelolaan akses

Structural	Kegagalan perangkat, sistem, jaringan, dan perangkat pendukung	Kerusakan hardware, error aplikasi, overload jaringan, kegagalan UPS
Environmental	Gangguan listrik, hewan, dan pemancar/sinyal	Ketidakstabilan listrik, kabel rusak akibat hewan, gangguan konektivitas

Sumber: Data diolah berdasarkan NIST SP 800-30 Rev. 1.

Peristiwa ancaman yang telah teridentifikasi mencakup kerusakan perangkat akibat usia pakai, gangguan akibat listrik, kegagalan UPS, overheating, error atau crash aplikasi, web defacement, kebocoran dan kerusakan data, overload jaringan, ketergantungan pada satu pemancar, kesalahan konfigurasi, kesalahan pengelolaan akses, dan penyalahgunaan hak akses. Dominasi peristiwa dengan relevansi confirmed menunjukkan bahwa sebagian ancaman bukan lagi bersifat hipotetis, tetapi telah terjadi atau sangat dekat dengan kondisi aktual organisasi.

3.3. Identifikasi Kerentanan

Kerentanan tertinggi ditemukan pada aspek software, data, dan brainware. Pada software, belum adanya SOP pemeliharaan serta mekanisme keamanan aplikasi yang belum memadai memperbesar risiko serangan. Pada data, kelemahan utama berada pada belum kuatnya kebijakan pengamanan, kontrol akses, dan monitoring. Pada brainware, keterbatasan kompetensi dan tidak adanya SDM tersertifikasi keamanan SPBE menjadi kerentanan paling dominan.

Tabel 6.
Kerentanan utama keamanan teknologi informasi

Aset	Kerentanan Dominan	Nilai Kualitatif
Hardware	Tidak adanya backup listrik dan pengendalian suhu ruang server	Sedang-Tinggi
Software	Tidak adanya SOP pemeliharaan dan mekanisme keamanan aplikasi belum memadai	Tinggi
Data	Kontrol akses dan monitoring data belum optimal	Tinggi
Network	Kapasitas jaringan dan ketergantungan pada satu pemancar	Sedang
Brainware	Tidak adanya SDM tersertifikasi dan perangkapan peran admin	Tinggi-Sangat Tinggi

Sumber: Data diolah oleh peneliti.

3.4. Penilaian Kemungkinan, Dampak, dan Penentuan Risiko

Hasil penilaian kemungkinan menunjukkan bahwa sebagian besar ancaman berada pada kategori sedang. Namun, gangguan operasional akibat tidak tersedianya backup listrik dan kerusakan perangkat akibat tidak adanya pengendalian suhu ruang server berada pada kategori tinggi. Pada aspek dampak, sebagian besar ancaman juga berada pada kategori sedang, sedangkan ancaman yang berkaitan dengan listrik, suhu server, dan konektivitas jaringan dapat menimbulkan dampak tinggi terhadap keberlangsungan layanan SPBE.

Tabel 7.
Level of risk berdasarkan NIST SP 800-30 Rev. 1

No	Ancaman	Kemungkinan	Dampak	Risiko
1	Serangan defacement web terhadap website Pemda TTS	Sedang	Sedang	Sedang
2	Kesalahan operasional akibat perangkapan peran admin	Sedang	Sedang	Sedang
3	Kesalahan pengelolaan sistem dan data akibat kurangnya kompetensi SDM	Sedang	Sedang	Sedang
4	Kerusakan perangkat akibat usia aset melebihi umur teknis	Sedang	Sedang	Sedang
5	Gangguan layanan akibat tidak adanya SOP pemeliharaan sistem	Sedang	Sedang	Sedang
6	Gangguan operasional akibat tidak tersedianya backup listrik	Tinggi	Tinggi	Tinggi
7	Kerusakan perangkat akibat tidak adanya pengendalian suhu ruang server	Tinggi	Tinggi	Tinggi

8	Ketidakstabilan jaringan akibat overload pemakaian	Sedang	Sedang	Sedang
9	Gangguan operasional akibat ketidakstabilan listrik	Sedang	Sedang	Sedang
10	Gangguan konektivitas akibat ketergantungan pada satu pemancar	Sedang	Tinggi	Sedang
11	Kerusakan aset jaringan akibat faktor lingkungan dan kecelakaan	Sedang	Sedang	Sedang

Sumber: Data diolah oleh peneliti.

Berdasarkan tabel tersebut, profil risiko keamanan teknologi informasi Diskominfo TTS didominasi risiko sedang dengan dua risiko tinggi. Risiko sedang tetap perlu ditangani karena berulangnya gangguan dengan dampak sedang dapat menurunkan kualitas layanan. Sementara itu, risiko tinggi memerlukan prioritas karena dapat menyebabkan gangguan serius terhadap operasional SPBE, terutama ketika layanan bergantung pada infrastruktur listrik, server, dan jaringan yang belum memiliki redundansi memadai.

3.5. Pemetaan Risiko terhadap CIS Controls v8

Hasil risiko kemudian dipetakan ke CIS Controls v8 Implementation Group 1. Pemetaan ini menunjukkan bahwa sebagian safeguard telah diterapkan secara parsial, terutama pada konfigurasi sistem, pengelolaan akun, kontrol akses, perlindungan data, inventarisasi perangkat lunak, dan audit log. Namun, masih terdapat gap besar pada inventarisasi aset, manajemen kerentanan, pemulihan data, serta pelatihan kesadaran dan keterampilan keamanan.

Tabel 8.
Ringkasan pemetaan risiko terhadap CIS Controls v8

Area Kontrol	Status Temuan	Prioritas Penguatan
C1 Inventory and Control of Enterprise Assets	Belum kuat dan belum menyeluruh	Membuat inventaris aset terpusat, lengkap, dan diperbarui berkala
C3 Data Protection	Sebagian safeguard telah diterapkan	Menyusun klasifikasi data, kebijakan pengamanan data, dan pembatasan akses
C4 Secure Configuration	Penerapan masih parsial	Menyusun baseline konfigurasi aman dan SOP perubahan sistem
C5-C6 Account and Access Control	Sebagian telah diterapkan	Menegakkan prinsip least privilege dan pengelolaan akun tidak aktif
C7 Continuous Vulnerability Management	Belum diterapkan optimal	Membuat jadwal identifikasi, pemindaian, dan perbaikan kerentanan
C8 Audit Log Management	Sebagian telah diterapkan	Menetapkan standar retensi, review, dan tindak lanjut log
C11 Data Recovery	Gap besar	Menyusun strategi backup, pengujian restore, UPS, dan rencana pemulihan
C14 Security Awareness and Skills Training	Belum diterapkan	Pelatihan rutin keamanan SPBE dan peningkatan kompetensi teknis

Sumber: Data diolah oleh peneliti berdasarkan CIS Controls v8.

3.6. Diskusi Temuan Utama Penelitian

Temuan utama penelitian menunjukkan bahwa keamanan teknologi informasi SPBE Diskominfo TTS belum berada pada kondisi kritis secara menyeluruh, tetapi memiliki kelemahan fondasional yang dapat meningkatkan risiko apabila tidak segera diperbaiki. Sama halnya dengan penelitian sebelumnya yang menggunakan NIST SP 800-30 Rev. 1, penelitian ini membuktikan bahwa pendekatan tersebut efektif untuk memetakan risiko melalui tahapan aset, ancaman, kerentanan, kemungkinan, dampak, dan level risiko.

Berbeda dengan beberapa penelitian terdahulu yang hanya berhenti pada identifikasi risiko, penelitian ini melanjutkan analisis ke pemetaan kontrol mitigasi menggunakan CIS Controls v8. Hal ini memperkuat aspek praktis penelitian karena rekomendasi tidak hanya bersifat umum, tetapi diarahkan pada safeguard yang lebih operasional. Pemetaan CIS juga menunjukkan bahwa

organisasi telah memiliki upaya awal pengamanan, namun belum konsisten dan belum terdokumentasi secara menyeluruh.

Temuan penelitian ini juga memperkuat pandangan bahwa faktor manusia merupakan elemen penting dalam keamanan teknologi informasi. Tidak adanya SDM tersertifikasi, perangkapan peran administrator, dan belum adanya pelatihan keamanan menunjukkan bahwa kerentanan tidak hanya bersifat teknis. Oleh sebab itu, mitigasi perlu memadukan penguatan infrastruktur, SOP, kontrol akses, dan peningkatan kapasitas pegawai.

3.7. Diskusi Temuan Menarik Lainnya

Temuan menarik lain dalam penelitian ini adalah adanya ketimpangan antara perkembangan layanan SPBE dan kesiapan manajemen keamanan. Layanan digital dapat terlihat berjalan, tetapi tanpa backup listrik, pengendalian suhu, dokumentasi aset, dan pemulihan data yang memadai, layanan tersebut rentan terganggu. Kondisi ini menunjukkan pentingnya melihat SPBE bukan hanya dari sisi aplikasi yang tersedia, tetapi dari kesiapan ekosistem pengamanan yang menopangnya.

Dalam kaitannya dengan SDGs 16.6, penguatan keamanan teknologi informasi berimplikasi terhadap efektivitas, akuntabilitas, dan transparansi institusi. Sistem yang terdokumentasi, memiliki log, kontrol akses, dan SOP akan lebih mudah dipertanggungjawabkan. Dalam kaitannya dengan SDGs 16.10, perlindungan data dan ketersediaan layanan digital mendukung akses informasi publik yang lebih andal. Dengan demikian, mitigasi risiko keamanan SPBE memiliki makna strategis bagi tata kelola pemerintahan digital.

IV. KESIMPULAN

Penelitian ini menyimpulkan bahwa tingkat risiko keamanan teknologi informasi pada SPBE Dinas Komunikasi dan Informatika Kabupaten Timor Tengah Selatan didominasi kategori sedang, dengan dua risiko tinggi yang perlu diprioritaskan, yaitu gangguan operasional akibat tidak tersedianya backup listrik dan kerusakan perangkat akibat tidak adanya pengendalian suhu ruang server. Pemetaan CIS Controls v8 menunjukkan bahwa beberapa safeguard telah diterapkan secara parsial, tetapi gap utama masih terdapat pada inventarisasi aset, manajemen kerentanan, pemulihan data, dan pelatihan keamanan. Oleh karena itu, penguatan keamanan SPBE perlu diarahkan pada perbaikan infrastruktur dasar, penyusunan SOP, pengendalian akses, strategi backup dan recovery, pemantauan kerentanan, serta peningkatan kompetensi SDM.

Keterbatasan Penelitian. Penelitian ini memiliki keterbatasan pada cakupan lokus yang hanya dilakukan pada satu perangkat daerah dan penggunaan pendekatan kualitatif yang berfokus pada kondisi aktual berdasarkan observasi, wawancara, dan dokumentasi.

Arah Masa Depan Penelitian (future work). Penelitian selanjutnya disarankan memperluas objek pada perangkat daerah lain, melakukan pengukuran tingkat kematangan keamanan, atau menguji efektivitas kontrol setelah rekomendasi mitigasi diterapkan.

V. UCAPAN TERIMA KASIH

Ucapan terima kasih ditujukan kepada Dinas Komunikasi dan Informatika Kabupaten Timor Tengah Selatan beserta seluruh informan yang telah memberikan kesempatan, data, dan informasi yang dibutuhkan dalam pelaksanaan penelitian. Ucapan terima kasih juga disampaikan kepada dosen pembimbing dan seluruh pihak yang membantu penyusunan penelitian ini.

VI. DAFTAR PUSTAKA

Al Fikri, M., et al. (2019). Risk assessment pada organisasi dengan kematangan tata kelola risiko terbatas. https://doi.org/10.1016/j.procs.2019.11.234

Amiruddin, Afiansyah, H. G., & Nugroho, H. A. (2021). Cyber-risk management planning using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8. https://doi.org/10.31004/riggs.v4i3.2169

Creswell, J. W. (2018). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. SAGE Publications. https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf

Destriani, M., & Putra, Y. H. (2023). Rencana Audit Tata Kelola Sistem Informasi di Universitas Subang Menggunakan Framework COBIT 2019. https://doi.org/10.34010/JTK3TI.V9I1.9164

ElMassah, S., & Mohieldin, M. (2020). Digital transformation and localizing the Sustainable Development Goals (SDGs). https://doi.org/10.1016/j.ecolecon.2019.106490

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2025). Cybersecurity in local governments: A systematic review and framework of key challenges. Urban Governance, 5(1), 1–19. https://doi.org/10.1016/j.ugj.2024.12.010

Kesuma, I. N. R. W., Hermadi, I., & Nurhadryani, Y. (2023). Evaluasi Tata Kelola Teknologi Informasi di Dinas Pertanian Gianyar Menggunakan COBIT 2019. Jurnal Teknologi Informasi Dan Ilmu Komputer, 10(3), 513–522. https://doi.org/10.25126/jtiik.2023106565

Lumingkewas, C., Mambu, J. Y., & Wahyudi, A. (2023). Identification of IT Governance Capability Level of COBIT 2019 at The KOMINFO City of Bitung, North Sulawesi. TeIKa, 13(01), 1–15. https://doi.org/10.36342/teika.v13i01.3064

Putra, A. P., & Soewito, B. (2023). Integrated methodology for information security risk management using ISO 27005:2018 and NIST SP 800-30 for insurance sector. 10.14569/IJACSA.2023.0140468

Putro, A. A., Ambarwati, A., & Setiawan, E. (2021). "Analisa Manajemen Risiko E-Learning Edlink Menggunakan Metode NIST SP 800-30 Revisi 1". *Jurnal Teknologi Dan Informasi (JATI)*, 11(2). https://doi.org/10.34010/jati.v11i2

Putro, A., Ambarwati, A., & Setiawan, E. (2021). Analisa manajemen risiko e-learning Edlink menggunakan metode NIST SP 800-30 Revisi 1. https://doi.org/10.34010/jati.v11i2

Simangunsong, F., & Hutasoit, I. (2019). Evaluation of electronic-based government system implementation in local government. Jurnal Bina Praja: Journal of Home Affairs Governance, 11(1), 89–100. https://doi.org/10.21787/jbp.13.2021.281-292

Tanjung, D. F., Nurhayati, O. D., & Wibowo, A. (2024). Design information security in electronic-based government systems using NIST CSF 2.0, ISO/IEC 27001:2022 and CIS Control. https://doi.org/10.38124/ijisrt/IJISRT24JUN1212

United Nations. (2024). E-Government Survey 2024. Technical Appendix. https://publicadministration.un.org/en/

Wisnu Alfiansyah, M., Lauw, C. M., Husain, & Fahmi, R. (2025). Audit keamanan teknologi informasi dengan NIST 800-30 pada PD Indah Permai Group. https://doi.org/10.36595/misi.v8i1.1416