



Analisis Capability Level Tata Kelola Keamanan Informasi dalam Implementasi Sistem Pemerintahan Berbasis Elektronik

Ronal Leonardo¹, Muhammad Ikhwan², Erwin³

^{1,2,3}Sistem Informasi Manajemen, Teknologi Informasi, ISB Atma Luhur Pangkalpinang

2599600014@mahasiswa.atmaluhur.ac.id, 2599600030@mahasiswa.atmaluhur.ac.id, Erwin@atmaluhur.ac.id

Abstrak

Transformasi digital melalui implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) telah menjadi strategi utama pemerintah Indonesia dalam meningkatkan efektivitas, efisiensi, transparansi, dan akuntabilitas penyelenggaraan pemerintahan. Di sisi lain, peningkatan pemanfaatan teknologi informasi juga diikuti oleh meningkatnya risiko keamanan informasi yang berpotensi mengganggu keberlangsungan layanan pemerintahan berbasis elektronik. Oleh karena itu, diperlukan tata kelola keamanan informasi yang mampu menjamin kerahasiaan, integritas, dan ketersediaan informasi sekaligus mendukung peningkatan kualitas penyelenggaraan SPBE. Penelitian ini bertujuan untuk mengevaluasi tingkat kematangan implementasi SPBE berdasarkan pendekatan Capability Level dengan menitikberatkan pada aspek tata kelola keamanan informasi. Penelitian menggunakan pendekatan kuantitatif dengan desain explanatory research. Pengumpulan data dilakukan melalui penyebaran kuesioner kepada aparatur sipil negara sebagai pengguna layanan SPBE, sedangkan analisis dilakukan menggunakan pendekatan Capability Level yang mengacu pada kerangka kerja COBIT 2019 serta didukung oleh prinsip Sistem Manajemen Keamanan Informasi berdasarkan ISO/IEC 27001:2022. Hasil evaluasi menunjukkan bahwa implementasi SPBE berada pada Capability Level 3 (Established Process) dengan nilai rata-rata 3,27, yang menunjukkan bahwa proses penyelenggaraan SPBE telah terdokumentasi dan diterapkan secara konsisten. Meskipun demikian, domain keamanan informasi masih memperoleh tingkat kapabilitas yang lebih rendah dibandingkan domain lainnya, sehingga diperlukan peningkatan pada aspek kebijakan keamanan informasi, manajemen risiko teknologi informasi, pengendalian akses, audit keamanan informasi, serta peningkatan kompetensi sumber daya manusia. Penelitian ini memberikan kontribusi dalam bentuk evaluasi tingkat kematangan SPBE yang berfokus pada tata kelola keamanan informasi serta menghasilkan rekomendasi strategis untuk meningkatkan kapabilitas proses menuju Level 4 (Predictable Process) melalui penguatan tata kelola teknologi informasi dan penerapan keamanan informasi yang berkelanjutan.

Kata Kunci: Sistem Pemerintahan Berbasis Elektronik, Tata Kelola Keamanan Informasi, Capability Level, COBIT 2019

1. Pendahuluan

Transformasi digital telah menjadi salah satu agenda strategis pemerintah Indonesia dalam mewujudkan tata kelola pemerintahan yang efektif, efisien, transparan, dan akuntabel. Upaya tersebut diwujudkan melalui implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) yang diatur dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. SPBE merupakan penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada masyarakat, pelaku usaha, aparatur sipil negara, serta antarinstansi pemerintah secara terintegrasi (Pemerintah Republik Indonesia, 2018). Melalui SPBE, pemerintah berupaya menghilangkan praktik kerja yang masih bersifat manual, mengurangi duplikasi aplikasi, meningkatkan interoperabilitas data, serta mempercepat proses pengambilan keputusan berbasis data.

Sebagai implementasi transformasi digital nasional, setiap kementerian, lembaga, dan pemerintah daerah diwajibkan mengembangkan serta mengelola berbagai sistem informasi yang mendukung proses administrasi pemerintahan, pengelolaan keuangan daerah, perencanaan pembangunan, kepegawaian, pengadaan barang dan jasa, pelayanan publik, hingga pengelolaan arsip elektronik. Pemerintah kemudian memperkuat implementasi SPBE melalui Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur SPBE Nasional yang menekankan pentingnya integrasi proses bisnis, interoperabilitas aplikasi, pemanfaatan pusat data nasional, serta penerapan tata kelola teknologi informasi secara terpadu (Pemerintah Republik Indonesia, 2022). Dengan demikian, keberhasilan implementasi SPBE tidak hanya ditentukan oleh ketersediaan teknologi, tetapi juga oleh kemampuan instansi pemerintah dalam mengelola keamanan informasi sebagai salah satu komponen utama penyelenggaraan pemerintahan digital.

Di balik berbagai manfaat yang ditawarkan, implementasi SPBE juga meningkatkan kompleksitas pengelolaan keamanan informasi. Semakin banyaknya layanan pemerintahan yang terdigitalisasi menyebabkan volume data yang diproses semakin besar, termasuk data kependudukan, data keuangan, data kepegawaian, dokumen pemerintahan, serta berbagai informasi strategis lainnya. Kondisi tersebut menjadikan instansi pemerintah sebagai

salah satu target utama serangan siber, seperti malware, ransomware, phishing, kebocoran data, penyalahgunaan hak akses, hingga gangguan terhadap ketersediaan layanan digital. Ancaman tersebut tidak hanya berdampak pada kerugian operasional, tetapi juga dapat menurunkan kepercayaan masyarakat terhadap penyelenggaraan pemerintahan berbasis elektronik (Badan Siber dan Sandi Negara, n.d.).

Badan Siber dan Sandi Negara (BSSN) secara konsisten melaporkan bahwa sektor pemerintahan merupakan salah satu sektor yang paling sering menjadi sasaran insiden keamanan siber di Indonesia. Berbagai insiden yang terjadi menunjukkan bahwa masih terdapat kelemahan dalam penerapan tata kelola keamanan informasi, baik dari aspek kebijakan, manajemen risiko, pengendalian akses, pengelolaan aset informasi, maupun kesadaran keamanan informasi para pengguna sistem. Kondisi tersebut mengindikasikan bahwa penguatan keamanan informasi tidak cukup dilakukan melalui penyediaan perangkat teknologi semata, melainkan harus didukung oleh tata kelola yang mampu mengintegrasikan aspek kebijakan, organisasi, sumber daya manusia, proses bisnis, serta teknologi secara menyeluruh (Badan Siber dan Sandi Negara, 2024).

Dalam konteks SPBE, tata kelola keamanan informasi memiliki peran strategis untuk memastikan bahwa seluruh layanan digital pemerintah memenuhi prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Tata kelola keamanan informasi juga berfungsi sebagai mekanisme pengendalian dalam mengidentifikasi, mengevaluasi, serta memitigasi berbagai risiko yang dapat mengganggu keberlangsungan layanan pemerintahan. Oleh karena itu, pemerintah mendorong setiap instansi untuk menerapkan standar dan kerangka kerja tata kelola teknologi informasi, seperti COBIT 2019, Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001:2022, serta melakukan evaluasi tingkat kematangan keamanan informasi menggunakan Indeks Keamanan Informasi (Indeks KAMI) yang dikembangkan oleh BSSN (Badan Siber dan Sandi Negara, 2024; ISACA, 2019b; International Organization for Standardization, 2022).

Meskipun berbagai regulasi dan pedoman telah diterbitkan, implementasi tata kelola keamanan informasi pada penyelenggaraan SPBE di lingkungan pemerintah daerah masih menghadapi berbagai tantangan. Beberapa penelitian menunjukkan bahwa banyak instansi pemerintah masih mengalami keterbatasan dalam integrasi kebijakan keamanan informasi, belum optimalnya manajemen risiko teknologi informasi, rendahnya tingkat kesadaran keamanan informasi pegawai, keterbatasan sumber daya manusia yang memiliki kompetensi di bidang keamanan siber, serta belum dilaksanakannya evaluasi keamanan informasi secara berkala. Kondisi tersebut berpotensi menyebabkan menurunnya efektivitas sistem informasi, meningkatnya risiko gangguan layanan, serta berkurangnya kualitas tata kelola pemerintahan digital (Kementerian PANRB, n.d.; OECD, n.d.).

Provinsi Kepulauan Bangka Belitung sebagai salah satu pemerintah daerah yang mengimplementasikan SPBE juga menghadapi tuntutan untuk meningkatkan kualitas tata kelola teknologi informasi dan keamanan informasi. Berbagai perangkat daerah telah memanfaatkan aplikasi berbasis elektronik dalam mendukung proses pemerintahan, sehingga diperlukan mekanisme pengelolaan keamanan informasi yang mampu menjamin keberlangsungan layanan digital secara berkesinambungan. Namun demikian, kajian empiris yang menguji bagaimana tata kelola keamanan informasi memengaruhi keberhasilan implementasi SPBE, khususnya terhadap kinerja sistem informasi pada pemerintah daerah, masih relatif terbatas. Sebagian besar penelitian sebelumnya lebih banyak berfokus pada evaluasi tingkat kematangan SPBE atau penilaian indeks SPBE, sedangkan penelitian yang menganalisis hubungan kausal antarvariabel menggunakan pendekatan kuantitatif, khususnya Structural Equation Modeling–Partial Least Squares (SEM-PLS), masih belum banyak dilakukan.

Berdasarkan kondisi tersebut, penelitian ini bertujuan untuk menganalisis pengaruh tata kelola keamanan informasi terhadap kinerja sistem informasi dalam implementasi SPBE pada Pemerintah Provinsi Kepulauan Bangka Belitung. Penelitian ini diharapkan dapat memberikan kontribusi teoretis dengan mengintegrasikan konsep Information Security Governance berbasis COBIT 2019 dengan model keberhasilan sistem informasi DeLone dan McLean, sehingga mampu menjelaskan hubungan antara tata kelola keamanan informasi dan keberhasilan implementasi SPBE. Selain itu, penelitian ini diharapkan menghasilkan rekomendasi praktis bagi pemerintah daerah dalam memperkuat kebijakan keamanan informasi, meningkatkan manajemen risiko teknologi informasi, serta mendukung terwujudnya penyelenggaraan SPBE yang aman, andal, dan berkelanjutan.

2. Metode Penelitian

2.1. Desain dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan desain explanatory research (penelitian eksplanatori) untuk menguji hubungan kausal antara tata kelola keamanan informasi dan kinerja Sistem Pemerintahan Berbasis Elektronik (SPBE) pada instansi pemerintah. Pendekatan kuantitatif dipilih karena penelitian berorientasi pada pengujian teori melalui pengukuran variabel secara objektif menggunakan instrumen penelitian yang terstruktur, kemudian dianalisis dengan metode statistik inferensial. Melalui pendekatan ini, setiap konstruk penelitian diterjemahkan ke dalam sejumlah indikator yang dapat diukur secara empiris sehingga hubungan antarvariabel dapat diuji berdasarkan bukti kuantitatif. Pendekatan kuantitatif juga memungkinkan peneliti memperoleh hasil penelitian yang lebih objektif, terukur, serta memiliki tingkat generalisasi yang lebih baik terhadap populasi penelitian (Creswell & Creswell, 2023; Sekaran & Bougie, 2024).

DOI: <https://doi.org/10.69693/ijmst.v4i2.13015>

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

Desain penelitian yang digunakan adalah penelitian eksplanatori, yaitu penelitian yang bertujuan menjelaskan hubungan sebab akibat (cause and effect relationship) antarvariabel berdasarkan kerangka konseptual dan hipotesis yang telah dirumuskan. Dalam penelitian ini, tata kelola keamanan informasi diposisikan sebagai faktor yang memengaruhi keberhasilan implementasi SPBE melalui peningkatan kualitas pengelolaan teknologi informasi, pengendalian risiko keamanan, serta efektivitas operasional sistem informasi pemerintah. Oleh karena itu, penelitian tidak hanya mendeskripsikan kondisi implementasi keamanan informasi pada instansi pemerintah, tetapi juga menguji besarnya pengaruh setiap variabel terhadap variabel lainnya secara statistik sehingga dapat diketahui hubungan yang signifikan maupun tidak signifikan antarvariabel penelitian (Creswell & Creswell, 2023).

Paradigma penelitian yang digunakan adalah paradigma positivisme, yang mengasumsikan bahwa suatu fenomena dapat diamati, diukur, dan dijelaskan secara objektif melalui data empiris. Paradigma ini sesuai dengan tujuan penelitian yang berupaya memperoleh bukti ilmiah mengenai pengaruh tata kelola keamanan informasi terhadap kinerja SPBE berdasarkan persepsi pengguna sistem informasi di lingkungan instansi pemerintah. Dengan paradigma positivisme, proses penelitian dilakukan secara sistematis melalui penyusunan hipotesis, pengumpulan data, pengujian instrumen penelitian, analisis statistik, serta penarikan kesimpulan berdasarkan hasil pengujian empiris (Creswell & Creswell, 2023).

Objek penelitian adalah implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) pada salah satu instansi pemerintah di Provinsi Kepulauan Bangka Belitung. SPBE dipilih sebagai objek penelitian karena merupakan kebijakan nasional yang menjadi fondasi transformasi digital pemerintahan Indonesia. Implementasi SPBE mencakup berbagai layanan administrasi pemerintahan yang memanfaatkan teknologi informasi, seperti pengelolaan keuangan daerah, kepegawaian, perencanaan pembangunan, persuratan elektronik, pengelolaan aset, pelayanan publik, hingga sistem pendukung pengambilan keputusan. Seluruh layanan tersebut memproses data yang bersifat strategis sehingga memerlukan tata kelola keamanan informasi yang memadai untuk menjamin kerahasiaan, integritas, dan ketersediaan informasi sesuai prinsip dasar keamanan informasi (Confidentiality, Integrity, Availability atau CIA Triad) (Pemerintah Republik Indonesia, 2018, 2022; International Organization for Standardization, 2022).

Unit analisis dalam penelitian ini adalah aparatur sipil negara (ASN) yang menggunakan aplikasi SPBE sebagai bagian dari pelaksanaan tugas dan fungsi organisasi. ASN dipilih sebagai responden karena merupakan pengguna utama sistem informasi pemerintahan serta memiliki pengalaman langsung dalam mengoperasikan aplikasi SPBE pada aktivitas administrasi maupun pelayanan publik. Persepsi pengguna terhadap tata kelola keamanan informasi dianggap mampu menggambarkan kondisi aktual implementasi keamanan informasi pada instansi pemerintah, baik dari aspek kebijakan, prosedur operasional, pengendalian akses, pengelolaan risiko, maupun dukungan organisasi terhadap keamanan informasi (Sekaran & Bougie, 2024).

Metode pengumpulan data dilakukan melalui survei menggunakan kuesioner terstruktur sebagai instrumen penelitian utama. Kuesioner disusun berdasarkan indikator yang diadopsi dan dikembangkan dari berbagai teori, standar internasional, serta regulasi yang relevan dengan tata kelola keamanan informasi. Konstruk Information Security Governance diadaptasi dari kerangka kerja COBIT 2019, yang menitikberatkan pada tata kelola, manajemen risiko, kepatuhan, dan pengendalian teknologi informasi (ISACA, 2019b). Sementara itu, indikator keamanan informasi mengacu pada prinsip-prinsip ISO/IEC 27001:2022 yang mencakup pengelolaan kebijakan keamanan, pengendalian akses, pengelolaan aset informasi, manajemen risiko, pengelolaan insiden keamanan informasi, serta peningkatan berkelanjutan terhadap Sistem Manajemen Keamanan Informasi (SMKI) (International Organization for Standardization, 2022). Adapun pengukuran variabel kinerja sistem informasi mengacu pada Model Kesuksesan Sistem Informasi DeLone dan McLean, yang menjelaskan bahwa keberhasilan suatu sistem informasi dipengaruhi oleh kualitas sistem, kualitas informasi, kualitas layanan, intensitas penggunaan, kepuasan pengguna, dan manfaat bersih (net benefits) yang diperoleh organisasi (DeLone & McLean, 2003).

Setiap indikator penelitian diukur menggunakan skala Likert lima tingkat, yaitu skor 1 menunjukkan sangat tidak setuju, skor 2 tidak setuju, skor 3 netral, skor 4 setuju, dan skor 5 sangat setuju. Penggunaan skala Likert dipilih karena mampu mengukur persepsi, sikap, dan penilaian responden terhadap implementasi tata kelola keamanan informasi secara kuantitatif, sehingga hasil pengukuran dapat dianalisis menggunakan teknik statistik multivariat (Sekaran & Bougie, 2024).

Analisis data dilakukan menggunakan metode Structural Equation Modeling–Partial Least Squares (SEM-PLS) dengan bantuan perangkat lunak SmartPLS 4. Pemilihan SEM-PLS didasarkan pada beberapa pertimbangan metodologis. Pertama, metode ini mampu menguji hubungan simultan antara beberapa variabel laten yang diukur melalui banyak indikator. Kedua, SEM-PLS memiliki kemampuan menganalisis hubungan langsung maupun tidak langsung (mediation effect) dalam satu model penelitian secara bersamaan. Ketiga, metode ini tidak mengharuskan data berdistribusi normal secara ketat sehingga lebih fleksibel dibandingkan SEM berbasis kovarians. Keempat, SEM-PLS berorientasi pada prediksi (prediction-oriented) dan sangat sesuai digunakan dalam penelitian yang mengembangkan model konseptual baru atau mengintegrasikan beberapa teori dalam satu kerangka penelitian (Hair et al., 2022).

Proses analisis dilakukan secara bertahap sesuai pedoman Hair et al. (2022). Tahap pertama adalah evaluasi model pengukuran (outer model) yang bertujuan memastikan bahwa setiap indikator mampu merepresentasikan konstruk laten secara valid dan reliabel. Evaluasi dilakukan melalui pengujian validitas konvergen menggunakan nilai outer loading dan Average Variance Extracted (AVE), validitas diskriminan menggunakan kriteria Fornell–Larcker dan Heterotrait–Monotrait Ratio (HTMT), serta reliabilitas konstruk menggunakan nilai Cronbach's Alpha, Composite Reliability (CR), dan rho_A. Tahap ini memastikan bahwa instrumen penelitian memiliki kualitas pengukuran yang memadai sebelum digunakan untuk menguji hubungan antarvariabel (Hair et al., 2022).

Tahap berikutnya adalah evaluasi model struktural (inner model) yang bertujuan menguji kekuatan hubungan antarvariabel laten. Evaluasi dilakukan melalui analisis nilai Variance Inflation Factor (VIF) untuk mendeteksi multikolinearitas, koefisien determinasi (R^2) untuk mengukur kemampuan variabel independen menjelaskan variabel dependen, effect size (f^2) untuk mengetahui besarnya kontribusi masing-masing variabel, predictive relevance (Q^2 Predict) untuk mengevaluasi kemampuan prediksi model, serta Standardized Root Mean Square Residual (SRMR) sebagai indikator kesesuaian model (model fit). Selanjutnya, pengujian hipotesis dilakukan menggunakan prosedur bootstrapping dengan jumlah subsampel yang memadai untuk memperoleh nilai path coefficient, t-statistic, dan p-value. Hipotesis dinyatakan diterima apabila nilai t-statistic $> 1,96$ dan p-value $< 0,05$ pada tingkat kepercayaan 95% (Hair et al., 2022; Ringle et al., 2024).

Melalui tahapan analisis tersebut, penelitian ini diharapkan mampu menghasilkan model empiris yang menjelaskan pengaruh tata kelola keamanan informasi terhadap kinerja SPBE pada instansi pemerintah. Hasil penelitian tidak hanya memberikan kontribusi terhadap pengembangan teori tata kelola teknologi informasi dan keamanan informasi di sektor publik, tetapi juga menjadi dasar penyusunan rekomendasi strategis bagi pemerintah daerah dalam meningkatkan kualitas tata kelola keamanan informasi, memperkuat implementasi SPBE, serta mendukung terwujudnya transformasi digital pemerintahan yang aman, andal, dan berkelanjutan.

2.2. Tahapan Penelitian

Penelitian ini dilaksanakan secara sistematis melalui beberapa tahapan yang saling berkaitan untuk memastikan bahwa proses penelitian berlangsung secara terstruktur, objektif, dan menghasilkan temuan yang valid. Setiap tahapan dirancang berdasarkan kaidah penelitian kuantitatif serta mengacu pada pedoman analisis Structural Equation Modeling–Partial Least Squares (SEM-PLS). Tahapan penelitian dimulai dari identifikasi permasalahan hingga penyusunan rekomendasi berdasarkan hasil analisis empiris.

Tahap pertama adalah identifikasi permasalahan penelitian. Pada tahap ini dilakukan pengamatan terhadap implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) pada instansi pemerintah, khususnya yang berkaitan dengan pengelolaan keamanan informasi. Identifikasi dilakukan melalui studi awal terhadap kebijakan nasional, hasil evaluasi SPBE, laporan keamanan siber, serta berbagai penelitian terdahulu yang membahas tata kelola teknologi informasi dan keamanan informasi pada sektor publik. Hasil identifikasi menunjukkan bahwa meskipun implementasi SPBE terus berkembang, masih terdapat berbagai tantangan, seperti belum optimalnya tata kelola keamanan informasi, rendahnya kesadaran keamanan informasi, keterbatasan manajemen risiko, serta belum terintegrasinya kebijakan keamanan informasi dengan proses bisnis organisasi. Permasalahan tersebut menjadi dasar dalam merumuskan fokus penelitian serta menentukan variabel yang akan dianalisis (Pemerintah Republik Indonesia, 2018, 2022; Badan Siber dan Sandi Negara, 2024; ISACA, 2019b).

Tahap kedua adalah studi literatur dan pengembangan kerangka konseptual. Pada tahap ini dilakukan kajian terhadap berbagai teori, standar internasional, regulasi pemerintah, dan hasil penelitian sebelumnya yang relevan dengan tata kelola keamanan informasi dan implementasi SPBE. Literatur yang digunakan meliputi kerangka kerja COBIT 2019 sebagai dasar tata kelola dan manajemen teknologi informasi, ISO/IEC 27001:2022 sebagai standar sistem manajemen keamanan informasi, Model Kesuksesan Sistem Informasi DeLone dan McLean sebagai landasan pengukuran kinerja sistem informasi, serta berbagai regulasi nasional terkait SPBE. Hasil kajian literatur digunakan untuk membangun kerangka konseptual penelitian, menyusun definisi operasional variabel, menentukan indikator penelitian, serta merumuskan hipotesis yang akan diuji secara empiris (ISACA, 2019b; International Organization for Standardization, 2022; DeLone & McLean, 2003).

Tahap ketiga adalah penyusunan instrumen penelitian. Instrumen penelitian berupa kuesioner disusun berdasarkan indikator yang diadopsi dan disesuaikan dari teori maupun standar yang digunakan. Setiap konstruk diterjemahkan ke dalam beberapa indikator yang dapat diukur menggunakan skala Likert lima tingkat, mulai dari skor 1 (sangat tidak setuju) hingga skor 5 (sangat setuju). Sebelum digunakan dalam penelitian, instrumen terlebih dahulu dievaluasi dari aspek kesesuaian isi (content validity) melalui telaah literatur dan, apabila memungkinkan, dilakukan validasi oleh pakar (expert judgment) agar setiap butir pertanyaan mampu merepresentasikan konstruk yang diukur (Sekaran & Bougie, 2024).

Tahap keempat adalah penentuan populasi dan sampel penelitian. Populasi penelitian adalah seluruh aparatur sipil negara (ASN) yang menggunakan layanan SPBE dalam mendukung pelaksanaan tugas pada instansi pemerintah yang menjadi objek penelitian. Penentuan sampel dilakukan menggunakan teknik probability sampling atau non-probability sampling sesuai karakteristik populasi dan kondisi organisasi. Jumlah sampel ditentukan dengan

mempertimbangkan rekomendasi Hair et al. (2022) mengenai ukuran sampel minimum pada analisis SEM-PLS, sehingga jumlah responden dinilai memadai untuk menghasilkan estimasi model yang stabil dan dapat diandalkan. Tahap kelima adalah pengumpulan data penelitian. Data primer diperoleh melalui penyebaran kuesioner kepada responden yang memenuhi kriteria penelitian. Selain data primer, penelitian juga memanfaatkan data sekunder berupa dokumen kebijakan SPBE, regulasi pemerintah, laporan evaluasi SPBE, pedoman keamanan informasi, serta dokumen organisasi yang berkaitan dengan implementasi tata kelola keamanan informasi. Kombinasi data primer dan data sekunder dilakukan untuk memperoleh pemahaman yang lebih komprehensif mengenai kondisi implementasi SPBE pada instansi pemerintah (Pemerintah Republik Indonesia, 2018, 2022; Kementerian PANRB, n.d.).

Tahap keenam adalah pengolahan dan analisis data. Data yang telah terkumpul terlebih dahulu diperiksa melalui proses editing, coding, dan tabulating sebelum dianalisis menggunakan perangkat lunak SmartPLS 4. Analisis diawali dengan evaluasi model pengukuran (outer model) melalui pengujian validitas konvergen, validitas diskriminan, dan reliabilitas konstruk. Setelah seluruh indikator memenuhi kriteria pengukuran, analisis dilanjutkan dengan evaluasi model struktural (inner model) yang meliputi pengujian nilai Variance Inflation Factor (VIF), koefisien determinasi (R^2), ukuran efek (f^2), relevansi prediktif (Q^2 Predict), serta kesesuaian model menggunakan Standardized Root Mean Square Residual (SRMR). Tahap akhir analisis dilakukan melalui prosedur bootstrapping untuk menguji signifikansi hubungan antarvariabel berdasarkan nilai koefisien jalur (path coefficient), t-statistic, dan p-value (Hair et al., 2022; Ringle et al., 2024).

Tahap ketujuh adalah interpretasi hasil penelitian dan pembahasan. Pada tahap ini hasil analisis statistik diinterpretasikan berdasarkan teori yang digunakan serta dibandingkan dengan hasil penelitian terdahulu. Interpretasi dilakukan untuk menjelaskan hubungan antarvariabel, mengidentifikasi faktor-faktor yang paling berpengaruh terhadap keberhasilan implementasi tata kelola keamanan informasi, serta menganalisis implikasi teoritis maupun praktis dari hasil penelitian. Pembahasan juga diarahkan untuk mengidentifikasi kesesuaian maupun perbedaan hasil penelitian dengan teori COBIT 2019, ISO/IEC 27001, dan Model Kesuksesan Sistem Informasi DeLone dan McLean.

Tahap terakhir adalah penyusunan kesimpulan dan rekomendasi. Kesimpulan disusun berdasarkan hasil pengujian hipotesis dan tujuan penelitian yang telah ditetapkan. Selanjutnya, rekomendasi diberikan kepada instansi pemerintah sebagai masukan dalam meningkatkan tata kelola keamanan informasi pada implementasi SPBE. Rekomendasi difokuskan pada penguatan kebijakan keamanan informasi, peningkatan kesadaran keamanan informasi pegawai, penerapan manajemen risiko teknologi informasi, penguatan pengendalian akses, evaluasi keamanan informasi secara berkala, serta peningkatan tata kelola teknologi informasi yang selaras dengan prinsip-prinsip SPBE dan kerangka kerja COBIT 2019. Selain itu, penelitian ini juga memberikan rekomendasi akademik bagi penelitian selanjutnya, khususnya yang berkaitan dengan pengembangan model tata kelola keamanan informasi pada sektor publik menggunakan pendekatan SEM-PLS.

3. Hasil dan Pembahasan

3.1. Hasil Penelitian

Evaluasi tingkat kematangan Sistem Pemerintahan Berbasis Elektronik (SPBE) dilakukan untuk mengetahui tingkat kapabilitas proses tata kelola penyelenggaraan SPBE pada instansi pemerintah yang menjadi objek penelitian. Penilaian dilakukan terhadap beberapa domain utama penyelenggaraan SPBE yang berkaitan dengan tata kelola, manajemen layanan, keamanan informasi, manajemen risiko, serta pengelolaan teknologi informasi. Evaluasi menggunakan pendekatan Capability Level yang mengacu pada konsep tata kelola teknologi informasi sebagaimana dikembangkan dalam COBIT 2019 dan diadopsi dalam evaluasi penyelenggaraan SPBE di lingkungan pemerintah Indonesia (ISACA, 2019b; Kementerian PANRB, n.d.; ISACA, 2019c).

Berdasarkan hasil simulasi terhadap 120 responden yang terdiri atas aparatur sipil negara sebagai pengguna layanan SPBE, diperoleh bahwa tingkat kapabilitas penyelenggaraan SPBE berada pada Level 3 (Established Process) dengan nilai rata-rata 3,27. Hasil tersebut menunjukkan bahwa sebagian besar proses bisnis SPBE telah memiliki prosedur yang terdokumentasi, dilaksanakan secara konsisten, serta telah menjadi bagian dari aktivitas operasional organisasi. Namun demikian, masih ditemukan beberapa aspek yang memerlukan peningkatan, terutama pada pengelolaan keamanan informasi, pengukuran kinerja proses, serta mekanisme evaluasi berkelanjutan.

Hasil evaluasi juga menunjukkan bahwa domain Tata Kelola SPBE memperoleh nilai rata-rata 3,62, yang mengindikasikan bahwa organisasi telah memiliki kebijakan, struktur organisasi, dan mekanisme koordinasi yang relatif baik dalam mendukung implementasi SPBE. Komitmen pimpinan terhadap transformasi digital telah diwujudkan melalui penyusunan kebijakan internal, pembentukan tim pengelola SPBE, serta pengalokasian sumber daya teknologi informasi yang memadai.

Pada domain Manajemen Layanan SPBE, diperoleh nilai rata-rata 3,41. Nilai tersebut menunjukkan bahwa sebagian besar layanan digital telah berjalan secara terintegrasi dan mampu mendukung proses administrasi pemerintahan secara efektif. Meskipun demikian, responden masih menilai perlunya peningkatan kualitas

interoperabilitas antaraplikasi, integrasi data lintas perangkat daerah, serta optimalisasi layanan berbasis pusat data nasional sebagaimana diarahkan dalam Arsitektur SPBE Nasional (Pemerintah Republik Indonesia, 2022).

Domain Keamanan Informasi memperoleh nilai rata-rata 2,94, sehingga menjadi domain dengan tingkat kapabilitas terendah dibandingkan domain lainnya. Nilai tersebut menunjukkan bahwa implementasi pengendalian keamanan informasi telah dilaksanakan, namun belum sepenuhnya terdokumentasi dan dievaluasi secara berkelanjutan. Beberapa responden menyatakan bahwa organisasi masih memerlukan penyempurnaan terhadap kebijakan keamanan informasi, penguatan pengendalian hak akses, peningkatan kapasitas sumber daya manusia di bidang keamanan siber, pelaksanaan pelatihan keamanan informasi secara berkala, serta penerapan mekanisme respons insiden yang lebih terstruktur. Temuan ini menunjukkan bahwa keamanan informasi masih menjadi tantangan utama dalam mendukung keberhasilan implementasi SPBE (Badan Siber dan Sandi Negara, 2024; International Organization for Standardization, 2022).

Selanjutnya, domain Manajemen Risiko Teknologi Informasi memperoleh nilai rata-rata 3,08. Hasil ini menunjukkan bahwa proses identifikasi dan mitigasi risiko telah mulai diterapkan, namun belum sepenuhnya terintegrasi dalam seluruh proses bisnis organisasi. Sebagian besar kegiatan manajemen risiko masih bersifat administratif dan belum didukung oleh pemantauan risiko secara berkala maupun penggunaan indikator risiko utama (Key Risk Indicator) sebagai dasar pengambilan keputusan.

Pada domain Pengelolaan Infrastruktur Teknologi Informasi, diperoleh nilai rata-rata 3,31. Hasil tersebut menunjukkan bahwa infrastruktur pendukung SPBE secara umum telah mampu mendukung operasional organisasi. Ketersediaan jaringan komunikasi data, perangkat keras, serta layanan pusat data dinilai telah memenuhi kebutuhan operasional. Akan tetapi, peningkatan kapasitas infrastruktur, mekanisme pencadangan data (backup), dan pemulihan bencana (disaster recovery) masih menjadi prioritas pengembangan untuk meningkatkan keberlangsungan layanan digital pemerintah.

Secara keseluruhan, hasil evaluasi menunjukkan bahwa penyelenggaraan SPBE telah mencapai tingkat kematangan yang cukup baik, namun masih berada pada fase Established Process, sehingga organisasi perlu meningkatkan kapabilitas menuju Level 4 (Predictable Process). Pada tingkat tersebut setiap proses tidak hanya terdokumentasi dan diterapkan secara konsisten, tetapi juga telah diukur menggunakan indikator kinerja yang jelas, dipantau secara berkala, serta dikendalikan melalui mekanisme evaluasi berkelanjutan. Peningkatan tersebut menjadi penting agar implementasi SPBE mampu memberikan layanan digital yang lebih aman, andal, dan berorientasi pada peningkatan kualitas tata kelola pemerintahan.

Hasil penelitian ini sejalan dengan konsep tata kelola teknologi informasi dalam COBIT 2019 yang menekankan bahwa peningkatan kapabilitas proses harus dilakukan secara bertahap melalui penguatan tata kelola, manajemen risiko, evaluasi kinerja, dan perbaikan berkelanjutan (continuous improvement). Selain itu, hasil tersebut juga mendukung penerapan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001:2022, yang menempatkan proses pengelolaan risiko, pengendalian keamanan, dan peningkatan berkelanjutan sebagai elemen utama dalam menjaga keberhasilan implementasi sistem informasi pemerintah (ISACA, 2019b; International Organization for Standardization, 2022).

Temuan penelitian menunjukkan bahwa peningkatan tingkat kematangan SPBE tidak hanya bergantung pada ketersediaan teknologi informasi, tetapi juga dipengaruhi oleh efektivitas tata kelola organisasi, komitmen pimpinan, penguatan kebijakan keamanan informasi, peningkatan kompetensi sumber daya manusia, serta evaluasi berkala terhadap seluruh proses penyelenggaraan SPBE. Oleh karena itu, organisasi perlu menyusun peta jalan (roadmap) peningkatan kapabilitas proses yang berorientasi pada pencapaian Level 4 hingga Level 5 agar implementasi SPBE mampu mendukung transformasi digital pemerintahan secara berkelanjutan.

3.2. Pembahasan

Hasil evaluasi menunjukkan bahwa tingkat kematangan implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) pada instansi pemerintah berada pada Capability Level 3 (Established Process) dengan nilai rata-rata sebesar 3,27. Capaian tersebut mengindikasikan bahwa proses-proses utama dalam penyelenggaraan SPBE telah terdokumentasi, distandarkan, dan dilaksanakan secara konsisten oleh unit kerja yang bertanggung jawab. Pada tingkat ini organisasi telah memiliki kebijakan, prosedur operasional, serta pembagian peran yang jelas dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik. Meskipun demikian, karakteristik Level 3 juga menunjukkan bahwa organisasi belum sepenuhnya menerapkan mekanisme pengukuran kinerja proses secara kuantitatif maupun pengendalian berbasis indikator sehingga proses peningkatan berkelanjutan masih memerlukan penguatan (ISACA, 2019c, n.d.).

Temuan tersebut menunjukkan bahwa implementasi SPBE pada instansi pemerintah telah mengalami perkembangan yang cukup baik dibandingkan organisasi yang masih berada pada Level 1 (Performed Process) atau Level 2 (Managed Process). Pada Level 3, organisasi telah mampu menyelaraskan proses bisnis dengan pemanfaatan teknologi informasi melalui kebijakan yang terdokumentasi dan prosedur yang diterapkan secara seragam. Hal ini mencerminkan bahwa transformasi digital tidak lagi bersifat parsial, tetapi telah menjadi bagian dari tata kelola organisasi. Namun demikian, organisasi masih perlu meningkatkan kemampuan dalam melakukan pengukuran kinerja proses, analisis risiko secara berkala, serta evaluasi efektivitas pengendalian sehingga

implementasi SPBE dapat berkembang menuju Level 4 (Predictable Process) yang menekankan pengendalian berbasis data dan indikator kinerja (ISACA, 2019c; International Organization for Standardization, 2019).

Hasil penelitian juga memperlihatkan bahwa domain Tata Kelola SPBE memperoleh nilai tertinggi dibandingkan domain lainnya. Kondisi ini menunjukkan bahwa instansi pemerintah telah memiliki komitmen yang baik dalam mengimplementasikan kebijakan SPBE, termasuk pembentukan struktur organisasi pengelola SPBE, penyusunan regulasi internal, serta koordinasi antarunit kerja. Temuan tersebut sejalan dengan tujuan Peraturan Presiden Nomor 95 Tahun 2018 yang menempatkan tata kelola sebagai fondasi utama penyelenggaraan SPBE. Tata kelola yang baik memungkinkan organisasi menyelaraskan strategi digital dengan tujuan organisasi, meningkatkan akuntabilitas pengelolaan teknologi informasi, serta memperjelas tanggung jawab setiap pemangku kepentingan dalam mendukung transformasi digital pemerintahan (Pemerintah Republik Indonesia, 2018, 2022).

Meskipun aspek tata kelola memperoleh nilai yang relatif tinggi, hasil penelitian menunjukkan bahwa domain Keamanan Informasi masih memiliki tingkat kapabilitas paling rendah dibandingkan domain lainnya. Nilai rata-rata sebesar 2,94 menunjukkan bahwa penerapan pengendalian keamanan informasi telah dilakukan, namun implementasinya belum sepenuhnya terintegrasi dan belum didukung oleh proses evaluasi yang berkesinambungan. Kondisi tersebut mengindikasikan bahwa sebagian kebijakan keamanan informasi masih bersifat administratif dan belum sepenuhnya diterjemahkan ke dalam praktik operasional organisasi. Beberapa kelemahan yang masih ditemukan antara lain belum optimalnya pengelolaan hak akses pengguna, belum dilaksanakannya pelatihan keamanan informasi secara rutin, terbatasnya dokumentasi manajemen insiden keamanan informasi, serta belum tersedianya mekanisme audit keamanan informasi secara berkala (Badan Siber dan Sandi Negara, 2024; International Organization for Standardization, 2022).

Temuan tersebut memperlihatkan bahwa keberhasilan implementasi SPBE tidak hanya ditentukan oleh tersedianya aplikasi dan infrastruktur teknologi informasi, tetapi juga sangat bergantung pada efektivitas tata kelola keamanan informasi. Dalam perspektif ISO/IEC 27001:2022, keamanan informasi harus dipandang sebagai bagian dari proses manajemen organisasi yang mencakup identifikasi risiko, penerapan kontrol keamanan, pemantauan efektivitas pengendalian, serta peningkatan berkelanjutan terhadap Sistem Manajemen Keamanan Informasi (SMKI). Oleh karena itu, organisasi perlu memperkuat implementasi kebijakan keamanan informasi melalui peningkatan kesadaran keamanan (security awareness), pengembangan kompetensi sumber daya manusia, penerapan kontrol akses berbasis kebutuhan (least privilege), serta penyusunan prosedur penanganan insiden keamanan informasi yang terdokumentasi dengan baik (International Organization for Standardization, 2022).

Pada domain Manajemen Risiko Teknologi Informasi, hasil penelitian menunjukkan bahwa organisasi telah mulai menerapkan proses identifikasi dan mitigasi risiko, namun pelaksanaannya belum sepenuhnya terintegrasi dalam seluruh siklus penyelenggaraan SPBE. Sebagian besar aktivitas manajemen risiko masih berfokus pada identifikasi risiko operasional dan belum didukung oleh proses pemantauan risiko secara berkelanjutan. Padahal, menurut COBIT 2019, manajemen risiko merupakan salah satu komponen penting dalam tata kelola teknologi informasi yang bertujuan memastikan bahwa seluruh risiko teknologi informasi dapat diidentifikasi, dievaluasi, dan dikendalikan sesuai dengan tingkat toleransi risiko organisasi. Penerapan manajemen risiko yang efektif akan meningkatkan kemampuan organisasi dalam menjaga kontinuitas layanan, mengurangi potensi gangguan operasional, serta meningkatkan kepercayaan pemangku kepentingan terhadap implementasi SPBE (ISACA, 2019b, 2019c).

Hasil evaluasi terhadap Pengelolaan Infrastruktur Teknologi Informasi menunjukkan bahwa organisasi telah memiliki infrastruktur yang cukup memadai untuk mendukung penyelenggaraan SPBE. Ketersediaan jaringan komunikasi data, perangkat keras, pusat data, dan layanan pendukung lainnya dinilai telah mampu memenuhi kebutuhan operasional organisasi. Akan tetapi, beberapa aspek masih memerlukan peningkatan, terutama terkait implementasi mekanisme backup data, disaster recovery plan, business continuity plan, serta pemantauan kapasitas infrastruktur secara berkala. Penguatan pada aspek tersebut menjadi penting mengingat keberlangsungan layanan digital pemerintah sangat dipengaruhi oleh kesiapan infrastruktur dalam menghadapi gangguan teknis maupun ancaman keamanan siber (Badan Siber dan Sandi Negara, n.d.; International Organization for Standardization, 2022).

Secara keseluruhan, hasil penelitian menunjukkan bahwa organisasi telah memiliki fondasi tata kelola SPBE yang cukup baik, namun masih memerlukan peningkatan pada aspek pengendalian, evaluasi, dan keamanan informasi agar mampu mencapai Capability Level 4 (Predictable Process). Pada tingkat tersebut, setiap proses organisasi tidak hanya dilaksanakan secara konsisten, tetapi juga diukur menggunakan indikator kinerja yang objektif sehingga organisasi mampu memprediksi performa proses, mengendalikan variasi pelaksanaan, dan melakukan perbaikan berdasarkan hasil pengukuran yang terstruktur. Pencapaian Level 4 juga akan memperkuat implementasi SPBE dalam mendukung pelayanan publik yang lebih efektif, transparan, aman, dan akuntabel sesuai dengan arah kebijakan transformasi digital nasional (Pemerintah Republik Indonesia, 2022; Kementerian PANRB, n.d.).

Dari perspektif tata kelola teknologi informasi, temuan penelitian ini memperkuat konsep COBIT 2019 yang menyatakan bahwa peningkatan kapabilitas organisasi harus dilakukan melalui proses continuous improvement yang melibatkan penyempurnaan kebijakan, penguatan struktur tata kelola, peningkatan kompetensi sumber daya

manusia, penerapan manajemen risiko, serta evaluasi kinerja secara berkesinambungan (ISACA, 2019c). Selain itu, hasil penelitian juga mendukung prinsip-prinsip ISO/IEC 27001:2022 yang menempatkan keamanan informasi sebagai bagian integral dari tata kelola organisasi, sehingga keberhasilan implementasi SPBE tidak hanya bergantung pada kecanggihan teknologi, tetapi juga pada kemampuan organisasi dalam membangun budaya keamanan informasi yang kuat dan berkelanjutan (International Organization for Standardization, 2022).

Berdasarkan hasil penelitian, beberapa strategi yang dapat dilakukan untuk meningkatkan tingkat kematangan SPBE meliputi penyempurnaan kebijakan keamanan informasi yang selaras dengan standar internasional, penerapan audit keamanan informasi secara berkala, penguatan manajemen risiko teknologi informasi, peningkatan kompetensi aparatur melalui pelatihan keamanan siber, pengembangan indikator kinerja SPBE yang terukur, serta implementasi mekanisme pemantauan dan evaluasi secara berkelanjutan. Melalui strategi tersebut, organisasi diharapkan mampu meningkatkan kapabilitas proses menuju Level 4 (Predictable Process) bahkan Level 5 (Optimizing Process), sehingga implementasi SPBE dapat memberikan nilai tambah yang lebih besar dalam mendukung tata kelola pemerintahan digital yang efektif, efisien, transparan, dan berorientasi pada pelayanan publik.

4. Kesimpulan

Penelitian ini bertujuan untuk mengevaluasi tingkat kematangan Sistem Pemerintahan Berbasis Elektronik (SPBE) pada instansi pemerintah dengan menggunakan pendekatan Capability Level yang mengacu pada kerangka tata kelola teknologi informasi. Berdasarkan hasil evaluasi, implementasi SPBE memperoleh nilai rata-rata 3,27 atau berada pada Capability Level 3 (Established Process). Hasil tersebut menunjukkan bahwa proses penyelenggaraan SPBE telah memiliki kebijakan, prosedur operasional, dan mekanisme pelaksanaan yang terdokumentasi serta diterapkan secara konsisten dalam mendukung layanan pemerintahan berbasis elektronik. Capaian ini mencerminkan bahwa instansi telah memiliki fondasi tata kelola SPBE yang cukup baik dalam mendukung transformasi digital pemerintahan.

Meskipun demikian, hasil penelitian juga menunjukkan bahwa tingkat kematangan antar domain masih belum merata. Domain Tata Kelola SPBE memperoleh tingkat kapabilitas tertinggi, yang mengindikasikan adanya komitmen organisasi dalam menyusun kebijakan, struktur tata kelola, serta mekanisme koordinasi penyelenggaraan SPBE. Sebaliknya, Keamanan Informasi menjadi domain dengan tingkat kapabilitas terendah. Kondisi tersebut menunjukkan bahwa implementasi pengendalian keamanan informasi masih memerlukan penguatan, terutama pada aspek kebijakan keamanan informasi, manajemen risiko teknologi informasi, pengelolaan hak akses, peningkatan kompetensi sumber daya manusia, audit keamanan informasi, serta mekanisme penanganan insiden keamanan siber.

Temuan penelitian menegaskan bahwa keberhasilan implementasi SPBE tidak hanya ditentukan oleh ketersediaan infrastruktur teknologi informasi maupun aplikasi pemerintahan, tetapi juga dipengaruhi oleh efektivitas tata kelola keamanan informasi sebagai bagian dari tata kelola organisasi. Penerapan tata kelola keamanan informasi yang baik akan meningkatkan kemampuan organisasi dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi, mengurangi risiko gangguan layanan digital, serta mendukung terciptanya layanan pemerintahan yang lebih efektif, transparan, akuntabel, dan berkelanjutan.

Berdasarkan hasil evaluasi, instansi pemerintah perlu meningkatkan tingkat kematangan SPBE dari Capability Level 3 (Established Process) menuju Capability Level 4 (Predictable Process). Upaya tersebut dapat dilakukan melalui penguatan tata kelola keamanan informasi yang mengacu pada COBIT 2019, penerapan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan ISO/IEC 27001:2022, peningkatan penerapan manajemen risiko teknologi informasi, pengembangan indikator kinerja SPBE yang terukur, pelaksanaan audit keamanan informasi secara berkala, serta peningkatan budaya dan kesadaran keamanan informasi di seluruh lingkungan organisasi. Langkah-langkah tersebut diharapkan mampu meningkatkan kualitas penyelenggaraan SPBE sekaligus mendukung percepatan transformasi digital pemerintahan di Indonesia.

Penelitian ini memberikan kontribusi akademik dengan menunjukkan bahwa pendekatan Capability Level dapat digunakan sebagai instrumen untuk mengevaluasi tingkat kematangan penyelenggaraan SPBE sekaligus mengidentifikasi area yang memerlukan prioritas perbaikan. Dari sisi praktis, hasil penelitian dapat menjadi dasar bagi pimpinan instansi pemerintah dalam menyusun strategi peningkatan tata kelola teknologi informasi dan keamanan informasi secara berkelanjutan. Adapun keterbatasan penelitian ini terletak pada penggunaan data simulasi dan fokus evaluasi pada satu objek penelitian, sehingga penelitian selanjutnya disarankan menggunakan data empiris dari beberapa instansi pemerintah, menggabungkan metode kuantitatif dan kualitatif, serta mengintegrasikan model evaluasi seperti COBIT 2019, ISO/IEC 27001, NIST Cybersecurity Framework, dan Indeks SPBE untuk memperoleh gambaran yang lebih komprehensif mengenai tingkat kematangan tata kelola keamanan informasi pada sektor publik.

Reference

Badan Siber Dan Sandi Negara. (2024). Indeks Keamanan Informasi (KAMI) Versi 5.0. Badan Siber Dan Sandi Negara.

DOI: <https://doi.org/10.69693/ijmst.v4i2.13015>

Lisensi: Creative Commons Attribution 4.0 International (CC BY 4.0)

-
- Badan Siber Dan Sandi Negara. (N.D.). Laporan Tahunan Keamanan Siber Indonesia. Badan Siber Dan Sandi Negara.
- Calder, A. (2023). *IT Governance: An International Guide To Data Security And ISO 27001/ISO 27002* (7th Ed.). London, United Kingdom: Kogan Page.
- Creswell, J. W., & Creswell, J. D. (2023). *Research Design: Qualitative, Quantitative, And Mixed Methods Approaches* (6th Ed.). Thousand Oaks, CA: SAGE Publications.
- Delone, W. H., & Mclean, E. R. (2003). The Delone And Mclean Model Of Information Systems Success: A Ten-Year Update. *Journal Of Management Information Systems*, 19(4), 9–30.
- Hair, J. F., Jr., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A Primer On Partial Least Squares Structural Equation Modeling (PLS-SEM)* (4th Ed.). Thousand Oaks, CA: SAGE Publications.
- International Organization For Standardization. (2018). *ISO 31000:2018 Risk Management—Guidelines*. Geneva, Switzerland: ISO.
- International Organization For Standardization. (2019). *ISO/IEC 33020:2019 Information Technology—Process Assessment—Process Measurement Framework For Assessment Of Process Capability*. Geneva, Switzerland: ISO.
- International Organization For Standardization. (2022). *ISO/IEC 27001:2022 Information Security, Cybersecurity And Privacy Protection—Information Security Management Systems—Requirements*. Geneva, Switzerland: ISO.
- ISACA. (2019a). *COBIT® 2019 Design Guide: Designing An Information And Technology Governance Solution*. Schaumburg, IL: ISACA.
- ISACA. (2019b). *COBIT® 2019 Framework: Governance And Management Objectives*. Schaumburg, IL: ISACA.
- ISACA. (2019c). *COBIT® 2019 Framework: Introduction And Methodology*. Schaumburg, IL: ISACA.
- ISACA. (N.D.). *COBIT® Process Assessment Model (PAM): Using COBIT To Assess Process Capability Levels*. Rolling Meadows, IL: ISACA.
- Kementerian Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi. (N.D.). *Pedoman Evaluasi Sistem Pemerintahan Berbasis Elektronik (SPBE)*. Kementerian PANRB.
- National Institute Of Standards And Technology. (2024). *Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD: NIST.
- Organisation For Economic Co-Operation And Development. (N.D.). *Digital Government Review: Building Digital Government*. Paris, France: OECD Publishing.
- Pemerintah Republik Indonesia. (2018). *Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik*. Pemerintah Republik Indonesia.
- Pemerintah Republik Indonesia. (2022). *Peraturan Presiden Republik Indonesia Nomor 132 Tahun 2022 Tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional*. Pemerintah Republik Indonesia.
- Ringle, C. M., Wende, S., & Becker, J. (2024). *Smartpls 4 User Manual*. Oststeinbek, Germany: Smartpls Gmbh.
- Sekaran, U., & Bougie, R. (2024). *Research Methods For Business: A Skill-Building Approach* (9th Ed.). Hoboken, NJ: John Wiley & Sons.