EVALUASI TATA KELOLA KEAMANAN INFORMASI PADA DINAS PERPUSTAKAAN DAN KEARSIPAN PROVINSI RIAU MENGGUNAKAN INDEKS KAMI

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Komputer pada
Program Studi Sistem Informasi

Oleh:

AHSAN KHOIRUL ANAM
12150312334

UIN SUSKA RIAU

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2026

LEMBAR PERSETUJUAN

EVALUASI TATA KELOLA KEAMANAN INFORMASI PADA DINAS PERPUSTAKAAN DAN KEARSIPAN PROVINSI RIAU MENGGUNAKAN INDEKS KAMI

TUGAS AKHIR

Oleh:

AHSAN KHOIRUL ANAM
12150312334

Telah diperiksa dan disetujui sebagai Laporan Tugas Akhir
di Pekanbaru, pada tanggal 12 Januari 2026

Ketua Program Studi	Pembimbing
Angraini, S.Kom., M.Eng., Ph.D.	M. Jazman, S.Kom., M.Infosys.
NIP. 198408212009012008	NIP. 198206042015031004

LEMBAR PENGESAHAN

EVALUASI TATA KELOLA KEAMANAN INFORMASI PADA DINAS PERPUSTAKAAN DAN KEARSIPAN PROVINSI RIAU MENGGUNAKAN INDEKS KAMI

TUGAS AKHIR

Oleh:

AHSAN KHOIRUL ANAM
12150312334

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
di Pekanbaru, pada tanggal 25 November 2025

Pekanbaru, 25 November 2025
Mengesahkan,

Dekan	Ketua Program Studi
Dr. Yuslenita Muda, S.Si., M.Sc.	**Angraini, S.Kom., M.Eng., Ph.D.**
NIP. 197701032007102001	**NIP. 198408212009012008**

DEWAN PENGUJI:

Ketua : **Arif Marsal, Lc.,M.A.**

Sekretaris : **M. Jazman, S.Kom., M.Infosys.**

Anggota 1 : **Angraini, S.Kom., M.Eng., Ph.D.**

Anggota 2 : **Mona Fronita, S.Kom., M.Kom.**

Lampiran Surat :
Nomor : Nomor 25/2021
Tanggal : 10 September 2021

SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini:

Nama : Ahsan khoirul Anam
NIM : 12150312334
Tempat/Tgl. Lahir : Tanjung kapal / 20 Maret 2003
Fakultas/Pascasarjana : Sains dan Teknologi
Prodi : Sistem Informasi
Judul Disertasi/Thesis/Skripsi/Karya Ilmiah lainnya*:
EVALUASI TATA KELOLA KEAMANAN INFORMASI PADA DINAS PERPUSTAKAAN DAN KEARSIPAN PROVINSI RIAU MENGGUNAKAN INDEKS KAMI.

Menyatakan dengan sebenar-benarnya bahwa :

1. Penulisan Disertasi/Thesis/Skripsi/Karya Ilmiah lainnya* dengan judul sebagaimana tersebut di atas adalah hasil pemikiran dan penelitian saya sendiri.
2. Semua kutipan pada karya tulis saya ini sudah disebutkan sumbernya.
3. Oleh karena itu Disertasi/Thesis/Skripsi/Karya Ilmiah lainnya* saya ini, saya nyatakan bebas dari plagiat.
4. Apa bila dikemudian hari terbukti terdapat plagiat dalam penulisan Disertasi/Thesis/Skripsi/(Karya Ilmiah lainnya)* saya tersebut, maka saya besedia menerima sanksi sesua peraturan perundang-undangan.

Demikianlah Surat Pernyataan ini saya buat dengan penuh kesadaran dan tanpa paksaan dari pihak manapun juga.

Pekanbaru, 22 Januari 2026
Yang membuat pernyataan

Ahsan khoirul Anam
NIM : 12150312334

*pilih salah satu sasuai jenis karya tulis

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL

Tugas Akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum, dengan ketentuan bahwa hak cipta ada pada peneliti. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan atas izin peneliti dan harus dilakukan mengikuti kaedah dan kebiasaan ilmiah serta menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh Tugas Akhir ini harus memperoleh izin tertulis dari Peneliti, Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan dapat meminjamkan Tugas Akhir ini untuk anggotanya dengan mengisi nama, tanda peminjaman, dan tanggal pinjam pada *form* peminjaman.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Pekanbaru, 12 Januari 2026
Yang membuat pernyataan,

AHSAN KHOIRUL ANAM
NIM. 12150312334

LEMBAR PERSEMBAHAN

Assalamu'alaikum Warahmatullahi Wabarakaatuh.

Alhamdulillahi Rabbil 'Alamin, segala puji bagi Allah *Subhanahu Wa Ta'ala* sebagai bentuk rasa syukur atas segala nikmat yang telah diberikan tanpa ada kekurangan sedikitpun. Shalawat beserta salam tak lupa pula kita ucapkan kepada Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam* dengan mengucapkan *Allahumma Sholli'ala Sayyidina Muhammad Wa'ala Ali Sayyidina Muhammad*. Semoga kita semua selalu senantiasa mendapat syafa'at-Nya di dunia maupun di akhirat, *aamiin ya rabbal'alaamiin*. Kupersembahkan karya kecil ini sebagai salah satu hadiah istimewa bentuk bakti, rasa terimakasih, dan hormatku kepada orang tuaku tercinta, Ayah dan Ibu.

Ayah dan Ibu tersayang, terimakasih atas setiap perjuangan, do'a, bimbingan, serta dukungan yang kalian berikan kepada saya. Terimakasih atas segala kebaikan dan selalu ada saat keadaan tersulit sekalipun. Terimakasih untuk segala pengorbanan yang kalian lakukan. Sampai kapanpun tiada rasa dan cara yang dapat membalas semuanya. Saya akan selalu mendo'akan yang terbaik untuk Ayah dan Ibu agar bahagia dunia dan akhirat, serta diberikan tempat istimewa di sisi-Nya kelak sehingga kita bisa berkumpul kembali bersama-sama di Jannah-Nya.

Terimakasih juga saya ucapkan kepada abang dan kakak saya yang sangat saya cintai. Terimakasih untuk segala waktu berharga yang telah dilalui bersama, do'a, dan dukungan yang tiada hentinya. Kemudian saya ucapkan terimakasih kepada Bapak dan Ibu Dosen Program Studi Sistem Informasi yang telah mewariskan ilmu yang bermanfaat dan arahan kepada saya untuk menyelesaikan studi di Program Studi Sistem Informasi ini. Semoga kita semua selalu diberikan kemudahan, rahmat, serta karunia-Nya. *Aamiin*.

Wassalamu'alaikum Warahmatullahi Wabarakaatuh.

KATA PENGANTAR

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Alhamdulillahi Rabbil 'Alamin, Puji Syukur saya ucapkan kepada Allah SWT yang telah memberikan Rahmat dan hidayah-Nya sehingga saya bisa menyelesaikan Tugas Akhir ini *inshaallah* dengan hasil yang baik. *Sholawat* serta salam juga senantiasa dihadiahkan kepada Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam*dengan lafadz *Allahumma Sholli'ala Sayyidina Muhammad Wa'ala Alihi Sayyidina Muhammad*.

Laporan ini disusun sebagai syarat untuk memperoleh gelar sarjana dan sebagai pembelajaran akademis maupun spiritual, saya mengucapkan terimakasih kepada semua pihak yang membantu dalam segala proses penelitian yang telah saya lakukan baik berupa materi maupun motivasi dan do'a, untuk itu pada kesempatan ini saya mengucapkan terimakasih yang sangat mendalam kepada:

1. Ibu Prof. Dr. Hj. Leny Nofianti MS, SE, M.Si, Ak sebagai Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Ibu Dr. Yuslenita Muda, S.Si., M.Sc sebagai Dekan Fakultas Sains dan Teknologi.
3. Ibu Angraini, S.Kom., M.Eng., Ph.D sebagai Ketua Program Studi Sistem Informasisekaligus Penguji I yang telah banyak membantu dan meluangkan waktu untuk memberikan masukan, saran, serta motivasi dalam penyelesaian Tugas Akhir ini.
4. Bapak M. Jazman, S.Kom., M.Infosys selaku Dosen Pembimbing Akademik yang telah banyak membantu dan membimbing peneliti sejak awal perkuliahan, sekaligus sebagai Dosen Pembimbing Tugas Akhir yang dengan penuh kesabaran telah meluangkan waktu untuk memberikan bimbingan, masukan, saran, serta motivasi hingga terselesaikannya penelitian ini.
5. Bapak Arif Marsal, Lc., MA selaku Ketua Sidang yang telah memberikan arahan dan masukan berharga.
6. Ibu Mona Fronita, S.Kom., M.Kom sebagai Penguji II yang telah banyak membantu dan meluangkan waktu untuk memberikan masukan, saran, serta motivasi dalam penyelesaian Tugas Akhir ini.
7. Seluruh Bapak dan Ibu Dosen Program Studi Sistem Informasi yang telah memberikan ilmunya kepada peneliti. Semoga ilmu yang diberikan dapat peneliti amalkan dan menjadi amal jariyah.
8. Kedua orang tua tercinta yaitu Bapak Sumari Zen dan Ibu Rofikoh yang

selalu memberikan dukungan serta senantiasa mendo'akan peneliti.

9. Saudara kandung yaitu Rita Nurun Ni'mah dan Anas Asrori Zen yang menjadi penyemangat untuk menyelesaikan Laporan Tugas Akhir.
10. Seluruh teman-teman kelas A yang sudah berjuang bersama dalam bangku perkuliahan. Serta, semua pihak yang namanya tidak dapat disebutkan yang telah banyak membantu dalam penyelesaian Tugas Akhir ini.

Peneliti menyadari bahwa dalam penulisan Tugas Akhir ini masih terdapat berbagai kekurangan dan jauh dari kata sempurna. Oleh karena itu, peneliti dengan rendah hati membuka diri untuk menerima kritik dan saran yang membangun yang dapat disampaikan melalui email 12150312334@students.uin-suska.ac.id. Peneliti berharap semoga Laporan Tugas Akhir ini dapat memberikan manfaat bagi kita semua. Akhir kata, peneliti mengucapkan terimakasih atas segala perhatian dan dukungan yang telah diberikan

Wassalamu'alaikum Warahmatullahi Wabarakaatuh.

Pekanbaru, 12 Januari 2026

peneliti,

AHSAN KHOIRUL ANAM

NIM. 12150312334

EVALUASI TATA KELOLA KEAMANAN INFORMASI PADA DINAS PERPUSTAKAAN DAN KEARSIPAN PROVINSI RIAU MENGGUNAKAN INDEKS KAMI

AHSAN KHOIRUL ANAM
NIM: 12150312334

Tanggal Sidang: 25 November 2025
Periode Wisuda:

Universitas Islam Negeri Sultan Syarif Kasim Riau
Jl. Soebrantas, No. 155, Pekanbaru

ABSTRAK

Pemanfaatan teknologi informasi pada instansi pemerintahan untuk meningkatkan efisiensi dan kualitas layanan publik. Namun disisi lain juga menimbulkan risiko terhadap keamanan informasi. Hal ini terjadi pada Dinas Perpustakaan dan Kearsipan Provinsi Riau yang mengalami insiden peretasan pada sistem perpustakaan Soeman H.S pada Juli-Agustus 2024, menandakan bahwa tata kelola keamanan informasi belum optimal. Selain itu, instansi belum melakukan evaluasi keamanan informasi sesuai permenkominfo Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Untuk mengatasi masalah tersebut, dilakukan evaluasi keamanan informasi menggunakan Indeks KAMI versi 5.0. Hasil evaluasi akan digunakan sebagai dasar menyusun rekomendasi perbaikan tata kelola keamanan Informasi agar sejalan dengan standar ISO/IEC 27001:2022. Hasil evaluasi menunjukkan bahwa sistem elektronik di Dinas Perpustakaan dan Kearsipan Provinsi Riau termasuk dalam kategori tinggi, dengan tingkat kelengkapan 253 dan tingkat kematangan berada pada level I+ pada area tata kelola, kerangka kerja, pengelolaan aset, teknologi informasi, dan perlindungan data pribadi (PDP), serta level I pada area pengelolaan risiko. Berdasarkan hasil tersebut, instansi dikategorikan belum layak terhadap penerapan standar ISO/IEC 27001. Evaluasi menghasilkan 9 rekomendasi pada area tata kelola, 13 pada pengelolaan risiko, 12 pada kerangka kerja, 16 pada pengelolaan aset, 9 pada teknologi dan keamanan, serta 9 pada area suplemen untuk meningkatkan penerapan keamanan informasi.

Kata Kunci: Indeks KAMI, ISO/IEC 27001:2022, Keamanan Informasi

EVALUATION OF INFORMATION SECURITY GOVERNANCE AT THE LIBRARY AND ARCHIVES DEPARTMENT RIAU PROVINCE USING INDEX KAMI

AHSAN KHOIRUL ANAM
NIM: 12150312334

Date of Final Exam: November 25th 2025
Graduation Period:

Department of Information System
Faculty of Science and Technology
State Islamic University of Sultan Syarif Kasim Riau
Soebrantas Street, No. 155, Pekanbaru

ABSTRACT

The use of information technology in government agencies to improve the efficiency and quality of public services. However, on the other hand, it also poses risks to information security. This happened at the Riau Provincial Library and Archives Office, which experienced a hacking incident on the Soeman H.S library system in July-August 2024, indicating that information security management was not yet optimal. In addition, the agency has not conducted an information security evaluation in accordance with Permenkominfo No. 4 of 2016 concerning the Information Security Management System. To overcome this problem, an information security evaluation was conducted using the KAMI Index version 5.0. The results of the evaluation will be used as a basis for compiling recommendations for improving information security governance in line with the ISO/IEC 27001:2022 standard. The evaluation results show that the electronic system at the Riau Provincial Library and Archives Office is in the high category, with a completeness level of 253 and a maturity level of I+ in the areas of governance, framework, asset management, information technology, and personal data protection, as well as a level I in the area of risk management. Based on these results, the agency was categorised as not yet eligible for the implementation of the ISO/IEC 27001 standard. The evaluation resulted in 9 recommendations in the area of governance, 13 in risk management, 12 in framework, 16 in asset management, 9 in technology and security, and 9 in the area of supplements to improve the implementation of information security.

Keywords: *Indeks KAMI, Information Security, ISO/IEC 27001:2022*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

Dipersip Provinsi Riau	:	Dinas Perpustakaan dan Kearsipan Provinsi Riau
e-Government	:	*electronic Government*
IEC	:	*International Electrotechnical Commission*
ISO	:	*International Organization for Standardization*
PDP	:	Perlindungan Data Pribadi
PII	:	Perlindungan Informasi Identitas
SE	:	Sistem Elektronik
SMKI	:	Sistem Manajemen Keamanan Informasi
SMPI	:	Sistem Manajemen Pengamanan Informasi
SOP	:	*Standard Operating Procedure*
SPBE	:	Sistem Pemerintahan Berbasis Elektronik

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Penggunaan teknologi informasi pada organisasi berperan untuk mempercepat proses kerja, meningkatkan efisiensi, dan mendukung layanan lebih responsif. Teknologi informasi memungkinkan organisasi mengelola informasi secara sistematis dan real-time sehingga memudahkan pimpinan dalam proses mengambil keputusan. Dalam konteks ini, informasi merupakan aset berharga yang perlu dijaga keberadaannya karna bersangkutan langsung dengan operasional dan arah kebijakan organisasi (Suprianto, 2023). Selain itu, kemampuan mengelola dan melindungi informasi yang baik akan memberikan keunggulan kompetitif bagi organisasi dibandingkan dengan organisasi lain (Rachmadi, 2020).

Salah satu wujud nyata penerapan teknologi informasi di sektor pemerintahan adalah melalui *electronic government (e-government)*. *E-government* memanfaatkan jaringan internet dan sistem informasi untuk mendukung proses komunikasi, pelayanan, dan penyebaran informasi dari pemerintah kepada masyarakat atau ke instansi lain (Taufik, Sudarsono, Sudaryana, Muryono, dkk., 2022). Transformasi ini mengubah pola komunikasi pemerintah yang sebelumnya satu arah menjadi dua arah. Menurut Amalia dan Anwar (2024) keinginan untuk menciptakan pemerintahan yang lebih transparan dan akuntabel menjadi pendorong utama bagi negara-negara berkembang dalam menerapkan sistem *e-goverment*.

Selain itu, pemerintah Indonesia telah menerapkan Sistem Pemerintahan Berbasis Elektronik (SPBE) sebagai upaya untuk mewujudkan tata kelola pemerintahan yang lebih efektif, efisien, dan terintegrasi. Pelaksanaan SPBE memiliki landasan hukum yang diatur dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik. Sistem elektronik sendiri didefinisikan sebagai sekumpulan perangkat, mekanisme, dan prosedur yang dimanfaatkan dalam pengelolaan informasi elektronik, mulai dari proses pengumpulan, pengolahan, penyimpanan, hingga pendistribusian informasi (Badan Siber dan Sandi Negara, 2023). Proses penyebaran informasi di lingkungan instansi pemerintahan memerlukan perlindungan yang memadai untuk menjaga kerahasiaan informasi dari pihak yang tidak berwenang. Risiko kebocoran data dapat menimbulkan gangguan serius terhadap keberlangsungan layanan pemerintah.

Keamanan informasi adalah langkah untuk menjaga data agar terhindar dari akses, penggunaan, perubahan, maupun perusakan yang tidak sah. Sistem yang aman harus menjamin tiga aspek utama yang meliputi kerahasiaan untuk memas-

tikan bahwa data hanya bisa diakses oleh pihak yang memiliki wewenang, integritas untuk memastikan data akurat dan lengkap, dan ketersediaan agar informasi dapat diakses ketika dibutuhkan (Kementerian Komunikasi dan Digital, 2022). Selain itu, penerapan keamanan informasi turut mendukung peningkatan mutu layanan publik yang disediakan oleh instansi pemerintah. Keamanan informasi juga berperan sebagai indikator penting dalam menilai tingkat efektivitas dan akuntabilitas pelaksanaan tata kelola pemerintahan.

Dinas Perpustakaan dan Kearsipan Provinsi Riau (Dipersip Provinsi Riau) telah menerapkan teknologi informasi guna mendukung pelaksanaan kebijakan daerah, khususnya pada layanan perpustakaan dan pengelolaan arsip, dengan tujuan memberikan layanan informasi yang transparan, akurat, dan dapat dipertanggungjawabkan. Sejalan dengan transformasi digital pemerintah, Pemerintah Provinsi Riau telah menetapkan Pergub Nomor 28 Tahun 2023 tentang penerapan SPBE. Peraturan ini mengatur aspek tata kelola SPBE, manajemen Risiko, manajemen keamanan informasi, audit teknologi informasi dan komunikasi, serta integrasi layanan publik digital. Meskipun telah tersedia kebijakan SPBE secara formal, implementasi teknis terkait manajemen keamanan informasi di Dipersip Provinsi Riau masih belum menyeluruh. Hal ini terlihat dari insiden peretasan yang terjadi pada Juli-Agustus 2024 terhadap sistem informasi perpustakaan Soeman H.S, di mana tampilan antarmuka sistem berhasil diubah menjadi lama judi *online*.

Mengacu pada Permenkominfo Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi mewajibkan setiap penyelenggara sistem elektronik untuk menerapkan Sistem Manajemen Pengamanan Informasi (SMPI) berdasarkan tingkat risiko (Menteri Komunikasi dan Informatika Republik Indonesia, 2016). Dalam Pasal 7 dijelaskan bahwa sistem dikelompokkan ke dalam tiga klasifikasi, yaitu strategis, tinggi, dan rendah. Sistem yang berada pada kategori strategis dan tinggi diwajibkan untuk menerapkan standar ISO/IEC 27001, sedangkan sistem dengan klasifikasi rendah harus mengacu pada pedoman Indeks KAMI. Di pasal 28 dijelaskan bahwa sertifikasi keamanan informasi paling lambat dilakukan maksimal sejak dua tahun sejak peraturan diberlakukan bagi sistem yang sudah berjalan, dan satu tahun bagi sistem baru. Aturan ini bertujuan memastikan keamanan informasi dalam pelayanan publik memiliki standar dan berkelanjutan.

Berdasarkan masalah-masalah yang telah diurai sebelumnya serta mengacu pada peraturan pemerintah, Dipersip Provinsi Riau memerlukan evaluasi untuk memastikan penerapan keamanan informasi suda sesuai aturan yang berlaku. Evaluasi ini juga untuk melihat gambaran menyeluruh mengenai pengelolaan keamanan informasi di Dipersip Provinsi Riau. Melalui evaluasi ini, diharapkan hasil

evaluasi bisa menjadi pertimbangan dalam pengambilan keputusan yang berhubungan dengan keamanan informasi, dan diharapkan bisa meningkatkan hasil evaluasi SPBE, sekaligus menjadi langkah awal mempersiapkan sertifikasi keamanan sesuai Permenkominfo Nomor 4 Tahun 2016.

Setelah dilakukan observasi sistem elektronik Dipersip Provinsi Riau berada di kategori rendah, yang artinya evaluasi akan dilakukan menggunakan indeks KAMI. Indeks KAMI berfungsi sebagai alat untuk mengevaluasi sejauh mana kesiapan dan penerapan keamanan informasi telah dilaksanakan dalam sebuah instansi. Penilaian ini didasarkan pada acuan standar internasional ISO/IEC 27001 yang menetapkan prinsip-prinsip utama dalam menjaga keamanan informasi (Ningrum, Riwanto, Pratiwi, dan Fikri, 2024).

Berdasarkan pemaparan tersebut, penulis mengajukan sebuah penelitian yang berjudul "Evaluasi Tata Kelola Keamanan Informasi pada Dinas Perpustakaan dan Kearsipan Provinsi Riau Menggunakan Indeks KAMI". Penelitian ini diharapkan menghasilkan rekomendasi perbaikan yang dapat dimanfaatkan untuk meningkatkan kualitas tata kelola keamanan informasi pada instansi terkait.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dapat dirumuskan beberapa pokok permasalahan yang akan dikaji dalam penelitian ini, yaitu:

a. Bagaimana hasil evaluasi keamanan informasi pada Dipersip Provinsi Riau menggunakan alat ukur Indeks KAMI?
b. Bagaimana rekomendasi perbaikan yang dapat diusulkan untuk meningkatkan tingkat kelengkapan dan kematangan keamanan informasi di Dinas Perpustakaan dan Kearsipan Provinsi Riau?

1.3 Batasan Masalah

Dari masalah yang dipaparkan di atas, peneliti menetapkan batasan masalah guna mempersempit fokus penelitian agar tetap terarah. Berikut batasan pada penelitian ini:

a. Evaluasi tingkat kelengkapan dan kematangan keamanan informasi akan dilakukan menggunakan Indeks KAMI versi 5.0 yang dirilis pada Maret 2023. Penilaian mencakup seluruh area keamanan informasi ditetapkan dalam Indeks KAMI. Penilaian secara menyeluruh ini bertujuan untuk mendapat gambaran nyata mengenai kondisi keamanan informasi saat ini.
b. Data yang digunakan diperoleh melalui proses wawancara dan pengisian kuisioner berdasarkan instrumen yang terdapat pada Indeks KAMI versi 5.0. Pengumpulan data dilakukan untuk memperoleh data yang tepat dan mencerminkan kondisi sebenarnya di lapangan yang selanjutnya menjadi dasar dalam proses analisis tingkat kematangan keamanan informasi.

c. Pemilihan responden dilakukan menggunakan RACI chart yang disusun berdasarkan pembagian peran dan tanggung jawab di lingkungan Dipersip Provinsi Riau. Metode ini dipilih agar setiap penilaian Indeks KAMI diisi oleh responden yang memiliki pemahaman terhadap area-area Indeks KAMI, sehingga penilaian dilakukan dengan akurat sesuai kondisi yang ada.
d. Usulan rekomendasi perbaikan berdasarkan ISO/IEC 27001:2022, merupakan standar internasional yang digunakan sebagai dasar tentang Sistem Manajemen Keamanan Informasi (SMKI).

1.4 Tujuan

Dengan mempertimbangkan rumusan serta batasan masalah yang telah disampaikan, penelitian ini bertujuan sebagai berikut:

a. Mengevaluasi tingkat kelengkapan dan kematangan keamanan informasi pada Dipersip Provinsi Riau menggunakan Indeks KAMI sebagai alat penilaian.
b. Memberikan rekomendasi perbaikan agar dapat diterapkan untuk meningkatkan hasil penilaian Indeks KAMI pada Dipersip Provinsi Riau.

1.5 Manfaat

Berikut merupakan manfaat yang diharapkan dari penelitian ini:

a. Melalui perhitungan Indeks KAMI, Dipersip Provinsi Riau dapat memperoleh gambaran mengenai tingkat kesiapan, kelengkapan, serta kematangan pengelolaan keamanan informasi yang telah diterapkan.
b. Melalui perhitungan Indeks KAMI, Dipersip Provinsi Riau dapat memperoleh gambaran mengenai tingkat kesiapan, kelengkapan, serta kematangan pengelolaan keamanan informasi yang diterapkan di instansi tersebut.

1.6 Sistematika Penulisan

Sistematika penulisan ini disusun untuk memastikan laporan penelitian tersaji secara terstruktur dan sejalan dengan tujuan yang ingin dicapai. Adapun susunan penulisan Tugas Akhir ini adalah sebagai berikut:

BAB 1. PENDAHULUAN

Bab ini menjelaskan secara umum arah dan ruang lingkup penelitian yang dilaksanakan. Pembahasan dalam bab ini mencakup latar belakang penelitian, perumusan masalah, pembatasan masalah, tujuan penelitian, manfaat penelitian, serta sistematika penulisan Tugas Akhir sebagai pedoman penyusunan laporan.

BAB 2. LANDASAN TEORI

Bab ini membahas uraian teori-teori, konsep, dan hasil penelitian terdahulu yang diperoleh dari buku, jurnal, maupun referensi ilmiah lainnya yang menjadi

dasar teori dan acuan penelitian.

BAB 3. METODOLOGI PENELITIAN

Bab ini menguraikan secara rinci pendekatan, metode, serta tahapan penelitian yang digunakan dalam pelaksanaan studi ini, meliputi tahap perencanaan, pemilihan responden, pengumpulan data, pengolahan data, validasi, analisis, penyusunan rekomendasi, serta penarikan kesimpulan.

BAB 4. HASIL DAN ANALISIS

Bab ini menjeaskan hasil analisis terhadap sistem manajemen keamanan informasi di Dipersip Provinsi Riau berdasarkan penilaian Indeks KAMI, serta temuan yang diperoleh.

BAB 5. PEMBAHASAN

Bab ini berisi rekomendasi perbaikan yang disusun berdasarkan hasil analisis dan setiap rekomendasi mengacu pada ISO 27001.

BAB 6. PENUTUP

Bab ini menyajikan hasil akhir penelitian berupa rangkuman kesimpulan dan rekomendasi yang disusun berdasarkan temuan selama proses penelitian berlangsung.

BAB 2
LANDASAN TEORI

2.1 Kajian Pustaka

Berikut penelitian-penelitian yang membahas topik keamanan informasi dari berbagai perspektif. Penelitian-penelitian tersebut mencakup aspek kebijakan, manajemen risiko, dan standar keamanan informasi. Lebih lanjut, penelitian-penelitian berikut menyoroti pula implementasi keamanan informasi di berbagai sektor seperti pada Tabel 2.1, Tabel 2.2, Tabel 2.3, Tabel 2.4, dan Tabel 2.5.

Tabel 2.1. Kajian Terdahulu I

Nama Peneliti	Faradhiya Aulia, Najwa Hamidah, Bintang Nuari, Reisa Permatasari
Judul Penelitian	Analisis Keamanan Informasi Menggunakan Aplikasi Indeks KAMI pada Sekretariat DPRD Kabupaten Jombang
Tahun	2023
Kesimpulan	Sistem elektronik di Sekretariat DPRD Kabupaten Jombang memiliki peran penting dalam keamanan informasi, namun penerapannya belum menyeluruh. Perlu peningkatan pada aspek area keamanan informasi, serta pembaruan sesuai perkembangan teknologi untuk meningkatkan keamanan secara komprehensif.
Perbedaan Penelitian	Penggunaan Indeks KAMI versi 4.1 yang berpedoman pada ISO/IEC 27001:2013 dan objek penelitian.
Persamaan Penelitian	Penggunaan metode yang sama yaitu Indeks KAMI.

Sumber: Aulia, Hamidah Erwin Effendi, dan Nuari (2023)

Tabel 2.2. Kajian Terdahulu II

Nama Peneliti	Piski Sundari, Wella
Judul Penelitian	SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR)
Tahun	2021
Kesimpulan	Penelitian ini menunjukkan bahwa Pusdatin berada pada kategori ”Kritis” dengan level kematangan keamanan informasi level I+, yang artinya masih memerlukan perbaikan. Pusdatin perlu meningkatkan keamanan informasi untuk mencapai standar ISO 27001:2013 dan melindungi sistem dari potensi ancaman yang dapat mengganggu operasional.
Perbedaan Penelitian	Penggunaan Indeks KAMI versi 4.1 yang berpedoman pada ISO/IEC 27001:2013 dan objek penelitian.
Persamaan Penelitian	Penggunaan metode yang sama yaitu Indeks KAMI.

Sumber: Sundari dan Wella (2021)

Tabel 2.3. Kajian Terdahulu III

Nama Peneliti	Reynaldo Adi Putra Pratama Gala, Rizal Sengkey, Charles Punusingon
Judul Penelitian	Analisis Keamanan Informasi Pemerintah Kabupaten Minahasa Tenggara Menggunakan Indeks KAMI
Tahun	2020
Kesimpulan	Penelitian tentang tingkat kematangan keamanan informasi di Pemerintah Kabupaten Minahasa Tenggara menunjukkan bahwa, walaupun tingkat ketergantungan terhadap teknologi informasi tergolong tinggi, pengelolaan keamanan informasi masih sangat rendah dengan skor 264, tidak memenuhi standar ISO/IEC 27001:2013. Perbaikan diperlukan pada semua aspek keamanan informasi.
Perbedaan Penelitian	Penggunaan Indeks KAMI versi 4.1 yang berpedoman pada ISO/IEC 27001:2013 dan objek penelitian.
Persamaan Penelitian	Penggunaan metode yang sama yaitu Indeks KAMI.

Sumber: Gala, Sengkey, dan Punusingon (2020)

Tabel 2.4. Kajian Terdahulu IV

Nama Peneliti	Fauzia Anis Sekar Ningrum, Yudha Riwanto,Inggrid Yanuar Risca Pratiwi, Muhammad Ainul Fikri
Judul Penelitian	Analisis Keamanan Sistem Informasi Perguruan Tinggi Berbasis Indeks KAMI
Tahun	2024
Kesimpulan	Hasil penelitian ini memperlihatkan adanya perbedaan yang signifikan dalam tingkat keamanan informasi antara perguruan tinggi A dan perguruan tinggi B. Perguruan tinggi A meraih skor 713 dengan kategori "Tinggi" berdasarkan Indeks KAMI versi 5.0, dan dinilai sudah layak untuk mengajukan sertifikasi ISO/IEC 27001, meskipun masih diperlukan peningkatan pada aspek manajemen risiko. Sementara itu, perguruan tinggi B memperoleh skor 321 dengan kategori "Rendah" dan dinyatakan "Belum Layak" untuk memperoleh sertifikasi tersebut.
Perbedaan Penelitian	objek penelitian.
Persamaan Penelitian	Penggunaan metode yang sama yaitu Indeks KAMI versi 5.0.

Sumber: Ningrum dkk. (2024)

Tabel 2.5. Kajian Terdahulu V

Nama Peneliti	Lucia Devlina Adventia Jelita, Moh Noor Al Azam, Aryo Nugroho
Judul Penelitian	Evaluasi Keamanan Teknologi Informasi Menggunakan Indeks Keamanan Informasi 5.0 dan ISO/IEC 27001:2022

Tabel 2.5. Kajian Terdahulu V (Tabel Lanjutan...)

Tahun	2024
Kesimpulan	Penilaian dengan Indeks KAMI versi 5.0 menunjukkan nilai kesiapan pengamanan teknologi ”Cukup Baik” dengan nilai 674. Hanya area tata kelola dan teknologi serta keamanan informasi yang sesuai dengan ISO 27001:2022. Area lainnya, masih pada level dasar. Perbaikan diperlukan agar seluruh aspek dapat memenuhi standar ISO/IEC 27001:2022.
Perbedaan Penelitian	objek penelitian.
Persamaan Penelitian	Penggunaan metode yang sama yaitu Indeks KAMI versi 5.0.

Sumber: Jelita, Al Azam, dan Nugroho (2024)

2.2 Evaluasi Sistem Informasi

Evaluasi adalah upaya untuk menilai atau mengukur sejauh mana suatu *artifact* berfungsi dengan baik dalam organisasi yang mengimplementasikannya (Cronholm dan Goldkuhl, 2003). Dalam konteks teknologi informasi, *artifact* merujuk pada sebuah sistem komputer yang diterapkan untuk membantu proses bisnis organisasi. Tujuan dari evaluasi adalah untuk mendapatkan informasi yang dapat dimanfaatkan dalam menemukan solusi terhadap permasalahan yang timbul, serta memperbaiki atas *artifact* yang telah ada. Evaluasi dapat dilakukan melalui pendekatan kuantitatif, kualitatif, atau gabungan keduanya (Cronholm dan Göbel, 2016). Tahapan evaluasi dibagi menjadi tiga tahap yakni perencanaan, pelaksanaan, dan setelah pelaksanaan. Pada tahap perencanaan akan ditentukan permasalahan dan solusi yang akan digunakan. Tahap pelaksanaan merupakan proses menjalankan rencana tersebut. Terakhir, tahap pasca pelaksanaan melibatkan analisis hasil untuk melihat dampaknya terhadap tujuan evaluasi (Cronholm dan Goldkuhl, 2003).

2.3 Teknologi Informasi

Teknologi adalah hasil penerapan ilmu pengetahuan yang diciptakan manusia untuk menghasilkan produk, proses, jasa, atau sistem yang digunakan guna meningkatkan kesejahteraan dan kualitas hidup (Riyana, 2008). Sementara itu, Informasi merupakan data yang telah melalui proses pengolahan sehingga disajikan dalam bentuk yang bermakna dan memiliki nilai, sehingga dapat dijadikan dasar dalam proses mengambil keputusan (Wahyono, 2004). Menurut (Wardiana, 2002) teknologi informasi merupakan teknologi yang difungsikan sebagai pengolah data menjadi sebuah informasi yang sesuai, akurat, dan tepat waktu guna mendukung proses pengambilan keputusan. teknologi ini memanfaatkan komputer, jaringan, dan telekomunikasi untuk mengakses dan menyebarkan informasi.

2.4 Tata Kelola Teknologi Informasi

Tata kelola teknologi informasi merupakan pendekatan yang digunakan oleh organisasi dalam mengatur dan mengendalikan pemanfaatan teknologi informasi agar sejalan dengan strategi serta tujuan bisnis yang ingin dicapai. Tata kelola ini mencakup unsur kepemimpinan, struktur organisasi, dan proses kerja yang dirancang untuk memastikan bahwa teknologi informasi memberikan kontribusi nyata terhadap peningkatan kinerja dan kemajuan bisnis organisasi (De Haes dan Van Grembergen, 2008). Mendorong peningkatan efisiensi operasional serta mendukung proses pengambilan keputusan yang lebih akurat dan tepat sasaran, serta memperkuat sinergi antara strategi bisnis dan pemanfaatan teknologi.

Tujuan pokok dari tata kelola teknologi informasi yaitu tercapainya keselarasan antara teknologi informasi dan strategi bisnis yang dikenal sebagai *strategic alignment*. Keselarasan ini menjadi kunci dalam menciptakan value lebih dan keunggulan kompetitif untuk organisasi. Agar tercapai, diperlukan koordinasi yang baik antara tujuan teknologi informasi dan tujuan bisnis. Tujuan teknologi informasi berfokus untuk menjamin layanan TI bisa mencegah serta mengatasi gangguan atau segala bentuk ancaman, sekaligus berperan sebagai pendukung dalam pencapaian tujuan bisnis. Sementara itu, tujuan bisnis berfungsi mempertahankan reputasi serta memperkuat posisi kepemimpinan suatu organisasi, dan bertindak sebagai penggerak dalam arah, dan pengembangan tujuan teknologi informasi (De Haes dan Van Grembergen, 2008).

2.5 ISO/IEC 27001:2022

ISO/IEC 27001:2022 merupakan standar internasional yang membantu organisasi melindungi data dari risiko keamanan dengan sistem manajemen yang terstruktur. Standar ini, hasil kerja sama *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC), menetapkan langkah-langkah untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi. Penerapan ISO/IEC 27001:2022 menunjukkan bahwa suatu organisasi memiliki sistem keamanan informasi yang kuat serta mampu menghadapi berbagai ancaman (Junaid, 2023). ISO/IEC 27001:2022 dapat diterapkan oleh semua organisasi tanpa mempertimbangkan jenis industri, ukuran, atau jumlah karyawan. Tujuan utama standar ini adalah untuk menyediakan keamanan informasi dan menjaga aset informasi suatu perusahaan (Başaran, 2016). ISO/IEC 27001:2022 dikeluarkan sebagai respons terhadap kebutuhan bisnis akan teknologi informasi dan manajemen keamanan (Wu, Shi, Wu, dan Liu, 2021).

2.6 Indeks KAMI

Indeks KAMI adalah alat ukur kematangan sistem manajemen keamanan informasi pada organisasi atau instansi pemerintah di Indonesia (Gala dkk., 2020). Sejak versi pertamanya yang dirilis pada 2009, Indeks KAMI telah diperbarui beberapa kali, dan versi terbaru yakni versi 5.0 yang dirilis pada 16 Agustus 2023. Versi ini mengacu pada standar ISO/IEC 27001:2022 yang mencerminkan perkembangan terbaru dalam keamanan informasi.

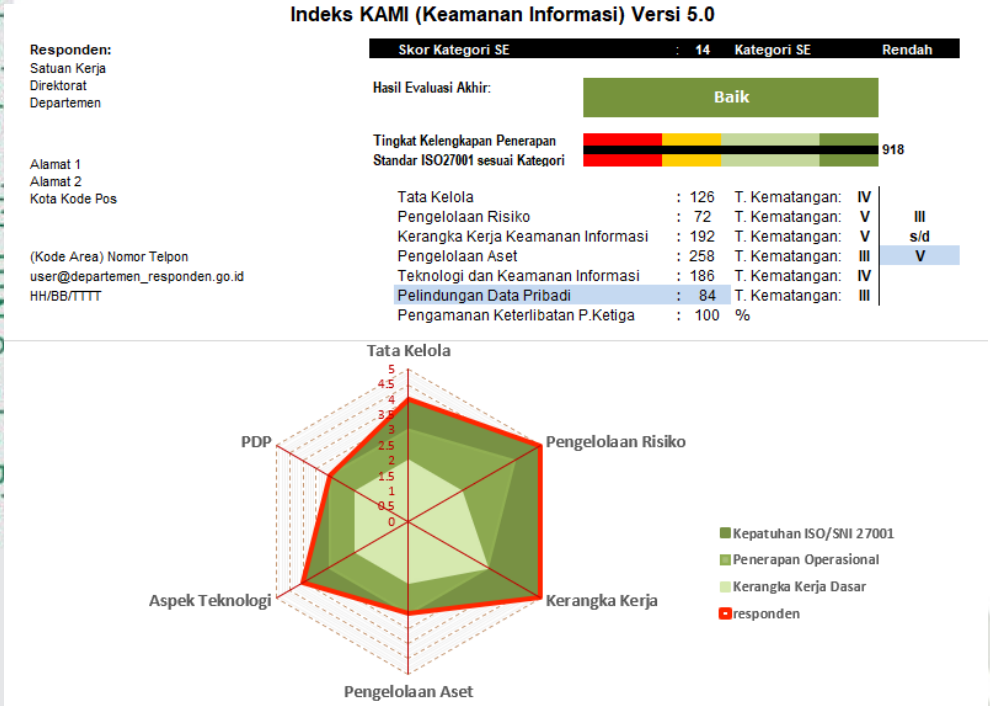
Pada versi 5.0, terdapat beberapa perubahan penting, di antaranya penambahan area evaluasi baru yang meliputi aspek kerangka kerja keamanan informasi, pengelolaan aset, dan teknologi. Selain itu, area evaluasi yang sebelumnya berada dalam kategori Suplemen, yaitu "Penggunaan Infrastruktur Layanan Awan," kini dipindahkan ke area utama di bawah pengelolaan aset. Perubahan lainnya adalah pemisahan area evaluasi untuk perlindungan data pribadi menjadi satu area mandiri untuk menggarisbawahi pentingnya aspek privasi. Versi terbaru ini juga mencakup penyesuaian rumus perhitungan skor dan penyempurnaan dasbor agar hasil evaluasi lebih akurat dan mudah dipahami seperti pada Gambar 2.1. Pembaruan-pembaruan ini menunjukkan peningkatan fokus pada pengelolaan aset, perlindungan data pribadi, serta adaptasi terhadap perkembangan risiko dan tata kelola informasi yang terus berubah (Badan Siber dan Sandi Negara, 2023).

Alat ukur Indeks KAMI dibuat untuk bisa digunakan oleh organisasi dari berbagai ukuran, baik yang beroperasi di tingkat nasional maupun dalam skala lebih kecil. Khusus untuk instansi pemerintah, penerapan evaluasi ini bisa dilakukan di tingkat pusat hingga di unit kerja, seperti Direktorat Jenderal, Badan, Pusat, atau Direktorat, dengan tujuan untuk mendapat gambaran tentang tingkat kematangan keamanan informasi yang dijalankan. Proses evaluasi ini disarankan dikelola oleh pejabat yang memiliki tanggung jawab langsung atas pengelolaan keamanan informasi lingkup instansinya (Badan Siber dan Sandi Negara, 2023).

Proses evaluasi dilakukan melalui pengisian dan penilaian terhadap sejumlah pertanyaan yang mencakup beberapa area penilaian, yaitu kategori sistem elektronik, tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, serta aspek teknologi dan keamanan informasi. Selain itu, evaluasi juga mencakup pelindungan data pribadi serta suplemen berupa ruang lingkup penilaian pengendalian keamanan yang berkaitan dengan kerja sama dengan pihak ketiga sebagai penyedia layanan.

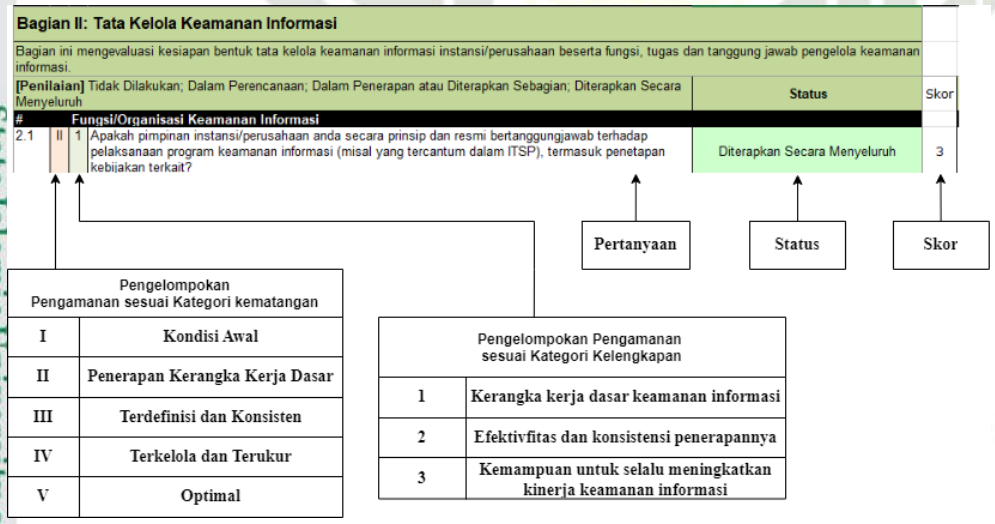
Dalam proses pengisian kuesioner Indeks KAMI, setiap pertanyaan dinilai berdasarkan tingkat penerapan elemen keamanan informasi di instansi. Penentuan opsi jawaban dilakukan dengan melihat dua aspek utama, yaitu: (1) keberadaan

dasar atau dokumen pendukung seperti kebijakan, pedoman, atau standar, dan (2) tingkat implementasi dari elemen tersebut dalam operasional.



Gambar 2.1. *Dashboard* Penilaian Dokumen Indeks KAMI

Sumber: Badan Siber dan Sandi Negara (2023)



Gambar 2.2. Bagian Penilaian Indeks KAMI

Sumber: Badan Siber dan Sandi Negara (2023)

Gambar 2.3 adalah empat opsi jawaban yang digunakan memiliki definisi sebagai berikut:

1. Tidak dilakukan, Tidak terdapat kebijakan, pedoman, maupun implementasi terkait elemen yang ditanyakan.

2. Dalam perencanaan, Sudah terdapat konsep atau rancangan awal, namun belum diterapkan dalam kegiatan operasional.
3. Diterapkan sebagian, Sudah ada kebijakan atau pedoman serta telah dilakukan implementasi, tetapi belum berjalan secara penuh atau belum dilaksanakan secara konsisten.
4. Diterapkan menyeluruh, Kebijakan atau pedoman telah disahkan dan implementasinya sudah diterapkan secara lengkap dan konsisten di seluruh ruang lingkup organisasi.

Untuk beberapa pertanyaan tertentu terdapat opsi tambahan "Tidak relevan", yang digunakan apabila elemen tersebut berada di luar ruang lingkup organisasi, misalnya prosesnya dilakukan oleh pihak ketiga.

Seperti yang tertera pada Gambar 2.2 terdapat dua jenis kategori yaitu berdasarkan kematangan dan kelengkapan. Dalam pengelompokan pengamanan sesuai dengan kelengkapan responden akan diminta untuk memberikan tanggapan mulai dari area yang terkait sesuai dengan kategori kelengkapan yang meliputi:

i. Label 1: kerangka kerja dasar keamanan informasi.
ii. Label 2: efektifitas dan konsistensi penerapannya.
iii. Label 3: kemampuan untuk selalu meningkatkan kinerja keamanan informasi.

Mengacu pada persyaratan minimum yang diperlukan untuk sertifikasi ISO/IEC 27001:2022, penilaian dilakukan dengan memberikan skor pada setiap jawaban. Skor-skor ini kemudian dijumlahkan untuk memperoleh nilai indeks keseluruhan. Nilai indeks ini nantinya akan digunakan sebagai referensi dalam evaluasi akhir yang akan ditampilkan di *dashboard* (Muahidin, Nasiri, dkk., 2022).

	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Gambar 2.3. Nilai Status Pengamanan Berdasarkan Kategori Pengamanan

Pada penilaian di bagian kematangan adalah di nilai dari tingkat kematangan terendah terlebih dahulu, setelah itu akan naik ke level selanjutnya untuk pengecekan apakah kematangan akan naik atau berhenti di level tersebut. Penilaian dimulai dari di level II ke level V. Berikut penilaian untuk menentukan skor:

i. Pertama jika nilai di tingkat kematangan lebih besar atau sama dengan nilai pencapaian tingkat kematangan, hasilnya adalah tingkat penilaian tersebut lulus dan mendapatkan validitas untuk dapat melakukan pengecekan ke level berikutnya hingga level terakhir di level V.

ii. Kedua, jika nilai tingkat kematangan lebih besar atau sama dengan nilai minimum tingkat kematangan, hasilnya adalah tingkat kematangan sebelumnya yang bernilai +. Contoh jika melakukan pengecekan di level II dan mendapatkan nilai seperti di atas artinya bagian tersebut mempunyai tingkat kematangan I+.

iii. Jika kedua kondisi di atas tidak terpenuhi, maka hasilnya adalah ”No” artinya tingkat kematangan tersebut tidak terpenuhi dan hasil tingkat kematangan berada di tingkat sebelumnya.

Bagian Indeks KAMI juga disusun berdasarkan aspek-aspek evaluasi yang dinilai melalui sejumlah pertanyaan pada beberapa area berikut:

2.6.1 Kategori Sistem Elektronik

Penilaian dimulai dari evaluasi Sistem Elektronik (SE) yang menilai tingkat implementasi sistem elektronik di tingkat instansi secara keseluruhan hingga ke unit satuan kerja. Tujuan dari proses ini untuk menilai sejauh mana sistem elektronik yang diimplementasikan oleh instansi berada pada kategori rendah, tinggi, atau strategis. Hasil dari penilaian sistem elektronik ini akan mempengaruhi skor akhir pada tujuh bagian penilaian lainnya dalam Indeks KAMI.

KATEGORI SISTEM ELEKTRONIK				
Rendah		**Skor Akhir**		**Status Kesiapan**
10	15	0	247	Tidak Layak
		248	443	Pemenuhan Kerangka Kerja Dasar
		444	760	Cukup Baik
		761	916	Baik
Tinggi		**Skor Akhir**		**Status Kesiapan**
16	34	0	387	Tidak Layak
		388	646	Pemenuhan Kerangka Kerja Dasar
		647	828	Cukup Baik
		829	916	Baik
Strategis		**Skor Akhir**		**Status Kesiapan**
35	50	0	472	Tidak Layak
		473	760	Pemenuhan Kerangka Kerja Dasar
		761	864	Cukup Baik
		865	916	Baik

Gambar 2.4. Pengelompokan nilai Indeks KAMI berdasarkan nilai SE

Berdasarkan Gambar 2.4, skor akhir yang sama dapat menghasilkan status

kesiapan yang berbeda, tergantung pada kategori sistem elektronik yang dimiliki.

2.6.2 Tata Kelola Keamanan Informasi

Bagian ini mengevaluasi kesiapan dalam hal struktur tata kelola keamanan informasi, mencakup fungsi, tugas, dan tanggung jawab yang ada. Terdapat 22 pertanyaan yang terkait dengan Kebijakan/Standar/Peraturan, Prosedur/Petunjuk/Pedoman, Rekaman/Formulir/*Record*, dan Reviu. Penilaian ini meliputi beberapa aspek, antara lain kebijakan Sistem Manajemen Keamanan Informasi (SMKI), audit internal, kompetensi, kesadaran, perlindungan data pribadi, konteks eksternal, Rencana Kelangsungan Bisnis, Rencana Pemulihan Bencana, pemantauan dan reviu, serta kebijakan dan prosedur (SOP) terkait insiden.

Total nilai skor untuk bagian ini adalah 126 dengan tingkat kematangan tertinggi yang dapat dicapai adalah tingkat IV. Tabel 2.6 adalah rincian nilai penilaian berdasarkan tingkat kematangan.

Tabel 2.6. Tingkat Kematangan Tata Kelola

Tingkat Kematangan II	
Jumlah Pertanyaan	13
Skor Minimum	12
Skor Pencapaian	36
Tingkat Kematangan III	
Jumlah Pertanyaan	3
Skor Minimum	8
Skor Pencapaian	14
Tingkat Kematangan IV	
Jumlah Pertanyaan	6
Skor Minimum	24
Skor Pencapaian	54

2.6.3 Pengelolaan Risiko Keamanan Informasi

Bagian ini berfokus pada penilaian implementasi pengelolaan risiko keamanan informasi yang digunakan sebagai landasan dalam penetapan strategi keamanan informasi. Dari hasil evaluasi, bagian ini memperoleh total skor sebesar 72, dengan tingkat kematangan maksimum yang dapat dicapai berada pada level V. Adapun perincian hasil penilaian pada bagian ini disajikan berdasarkan masing-masing tingkat kematangan pada Tabel 2.7.

Tabel 2.7. Tingkat Kematangan Pengelolaan Risiko

Tingkat Kematangan II	
Jumlah Pertanyaan	10

Tabel 2.7. Tingkat Kematangan Pengelolaan Risiko (Tabel Lanjutan...)

Skor Minimum	14
Skor Pencapaian	20
Tingkat Kematangan III	
Jumlah Pertanyaan	2
Skor Minimum	4
Skor Pencapaian	8
Tingkat Kematangan IV	
Jumlah Pertanyaan	2
Skor Minimum	8
Skor Pencapaian	12
Tingkat Kematangan V	
Jumlah Pertanyaan	2
Skor Minimum	12
Skor Pencapaian	18

2.6.4 Kerangka Kerja Keamanan Informasi

Pada area ini akan mengevaluasi bagaimana implementasi pengelolaan risiko keamanan informasi sebagai landasan untuk menerapkan strategi pada keamanan informasi. Total nilai yang didapat dari bagian ini adalah 192, dengan tingkat kematangan tertinggi yang dapat dicapai adalah tingkat V. Tabel 2.8 adalah rincian penilaian berdasarkan tingkat kematangan kerangka kerja.

Tabel 2.8. Tingkat Kematangan Kerangka Kerja

Tingkat Kematangan II	
Jumlah Pertanyaan	11
Skor Minimum	15
Skor Pencapaian	24
Tingkat Kematangan III	
Jumlah Pertanyaan	17
Skor Minimum	56
Skor Pencapaian	84
Tingkat Kematangan IV	
Jumlah Pertanyaan	3
Skor Minimum	15
Skor Pencapaian	27
Tingkat Kematangan V	
Jumlah Pertanyaan	2
Skor Minimum	12
Skor Pencapaian	18

2.6.5 Pengelolaan Aset Informasi

Area ini bertujuan untuk menilai sejauh mana penerapan pengamanan terhadap aset informasi, mencakup seluruh penggunaan aset dari awal hingga akhir. Total skor yang diperoleh pada bagian ini adalah 258, dengan tingkat kematangan maksimal yang dapat dicapai berada pada tingkat III. Adapun rincian hasil penilaian untuk bagian ini berdasarkan tingkat kematangan pada Tabel 2.9.

Tabel 2.9. Tingkat Kematangan Pengelolaan Aset

Tingkat Kematangan II	
Jumlah Pertanyaan	32
Skor Minimum	39
Skor Pencapaian	88
Tingkat Kematangan III	
Jumlah Pertanyaan	21
Skor Minimum	83
Skor Pencapaian	118

2.6.6 Teknologi dan Keamanan Informasi

Area ini berfokus pada penilaian terhadap tingkat kelengkapan serta efektivitas penerapan teknologi dalam melindungi aset informasi. Total skor yang diperoleh pada bagian ini adalah 186, dengan tingkat kematangan tertinggi yang dapat dicapai berada pada tingkat IV. Tabel 2.10 merupakan rincian hasil penilaian berdasarkan tingkat kematangan teknologi.

Tabel 2.10. Tingkat Kematangan Teknologi

Tingkat Kematangan II	
Jumlah Pertanyaan	14
Skor Minimum	18
Skor Pencapaian	28
Tingkat Kematangan III	
Jumlah Pertanyaan	18
Skor Minimum	68
Skor Pencapaian	92
Tingkat Kematangan III	
Jumlah Pertanyaan	3
Skor Minimum	12
Skor Pencapaian	21

2.6.7 Pelindungan Data Pribadi

Bagian ini berfungsi untuk mengevaluasi kelengkapan, konsistensi, dan efektivitas dalam menerapkan kontrol keamanan terkait PDP. Selain itu, disini juga mengevaluasi kesiapan dalam menerapkan pengelolaan risiko keamanan informasi

sebagai dasar bagi strategi keamanan informasi. Total skor yang diperoleh dari bagian ini adalah 84, dengan tingkat kematangan tertinggi yang dapat dicapai adalah tingkat III. Tabel 2.11 adalah rincian penilaian berdasarkan tingkat kematangan perlindungan data pribadi.

Tabel 2.11. Tingkat Kematangan Perlindungan Data Pribadi

Tingkat Kematangan II	
Jumlah Pertanyaan	6
Skor Minimum	8
Skor Pencapaian	16
Tingkat Kematangan III	
Jumlah Pertanyaan	10
Skor Minimum	36
Skor Pencapaian	48

2.6.8 Suplemen

Menilai aspek kesiapan pengamanan yang digunakan. Khusus hasil evaluasi kesiapan pengamanan keterlibatan pihak ketiga akan disajikan dalam bentuk persentase (%) yang mencerminkan pencapaian maksimal sesuai dengan obyektif atau target yang telah ditetapkan.

2.7 Gambaran Umum Instansi

2.7.1 Sejarah

Dinas Perpustakaan dan Kearsipan (Dipersip) Provinsi Riau dibentuk melalui pengembangan kelembagaan yang mengacu pada Peraturan Daerah Nomor 8 Tahun 2008. Perjalanan perpustakaan di Provinsi Riau dimulai pada tahun 1959 dengan berdirinya Perpustakaan Negara di Tanjung Pinang, yang kemudian dipindahkan ke Pekanbaru pada tahun 1967 seiring dengan pemindahan ibu kota provinsi. Pada tahun 1978, lembaga ini beralih status menjadi Perpustakaan Wilayah di bawah naungan Departemen Pendidikan dan Kebudayaan, dan sejak tahun 1989 berperan sebagai Perpustakaan Daerah yang berada di bawah pembinaan Perpustakaan Nasional Republik Indonesia. Pengelolaan bidang kearsipan mulai dirintis sejak pembentukan Subbagian Arsip dan Ekspedisi pada tahun 1992, yang selanjutnya berkembang menjadi Kantor Arsip Daerah pada tahun 1996. Pada tahun 2001, pengelolaan perpustakaan dan kearsipan disatukan dalam satu lembaga yang kemudian dikenal sebagai Dinas Perpustakaan dan Kearsipan Provinsi Riau, sesuai dengan ketentuan Undang-Undang Nomor 23 Tahun 2017. Gedung Perpustakaan Soeman HS yang diresmikan pada 24 Juni 2008 menjadi ikon layanan perpustakaan di Riau, dengan dukungan fasilitas modern serta pemanfaatan teknologi informasi

dalam pelayanannya (Dinas Perpustakaan dan Kearsipan Provinsi Riau, 2025).

2.7.2 Visi Misi

Visi:

"Terwujudnya Dinas Perpustakaan dan Kearsipan Provinsi Riau yang Profesional dalam Pengelolaan Perpustakaan, Arsip dan Dokumentasi sebagai sumber pengetahuan dan Informasi untuk mencapai Sumber Daya Manusia Riau yang berkualitas menunjang visi Riau 2020".

Misi:

Misi pada Dipersip Provinsi Riau adalah sebagai berikut:

1. Peningkatan kualitas Sumber Daya Manusia Dipersip Provinsi Riau.
2. Peningkatan pelayanan Perpustakaan, Kearsipan dan Dokumentasi kepada masyarakat.
3. Peningkatan minat dan budaya baca masyarakat serta pentingnya nilai guna arsip.
4. Peningkatan kualitas prasarana dan sarana Dipersip Provinsi Riau.
5. Peningkatan upaya-upaya pembinaan dalam rangka pemantapan pengelolaan Perpustakaan Arsip dan Dokumentasi.
6. Peningkatan upaya dokumentasi pada usaha pembangunan Provinsi Riau.

2.7.3 Tugas dan Fungsi

Tugas:

Tugas Pokok Dinas Perpustakaan dan Kearsipan Provinsi Riau sebagai berikut:

1. Merumuskan serta menetapkan arah kebijakan Pemerintah Provinsi Riau dalam bidang perpustakaan, kearsipan, dan dokumentasi.
2. Mengkoordinasikan, menyinergikan, serta memastikan keselarasan pelaksanaan kebijakan dan kegiatan di bidang perpustakaan, arsip, dan dokumentasi di tingkat daerah.
3. Menetapkan pedoman dan standar dalam pengelolaan perpustakaan, arsip, serta dokumentasi.
4. Menyusun rencana kerja dan program pembangunan yang berkaitan dengan bidang perpustakaan, arsip, dan dokumentasi.
5. Menetapkan kebijakan strategis terkait pengelolaan perpustakaan, arsip, dan dokumentasi di lingkungan Pemerintah Provinsi Riau.
6. Mengimplementasikan rencana kerja serta program pembangunan sesuai bidang tugas berdasarkan ketentuan dan mekanisme yang berlaku.
7. Menjalin kerja sama dengan berbagai lembaga yang bergerak di bidang per-

pustakaan, arsip, dan dokumentasi dalam upaya pelestarian bahan pustaka dan arsip sebagai warisan budaya serta sumber informasi, ilmu pengetahuan, dan kebudayaan.

8. Melaksanakan kegiatan pemantauan dan evaluasi terhadap pelaksanaan seluruh kegiatan perpustakaan, arsip, dan dokumentasi di daerah.
9. Memberikan layanan umum dan layanan teknis dalam bidang perpustakaan, arsip, dan dokumentasi kepada masyarakat dan instansi terkait.
10. Menangani serta menyelesaikan berbagai permasalahan yang muncul dalam lingkup tugas dan tanggung jawabnya.
11. Melakukan pendokumentasian terhadap berbagai peristiwa penting atau bersejarah yang terjadi dalam proses pembangunan di Provinsi Riau.
12. Menyusun dan mengembangkan sistem pengelolaan dokumen daerah agar lebih tertata dan mudah diakses.
13. Melakukan pembinaan terhadap pengelolaan dan penataan dokumen daerah agar sesuai dengan ketentuan yang berlaku.
14. Menyusun serta menyampaikan laporan kegiatan sesuai dengan prosedur dan peraturan yang telah ditetapkan.
15. Melaksanakan tugas tambahan lainnya sesuai arahan dan petunjuk dari Gubernur.

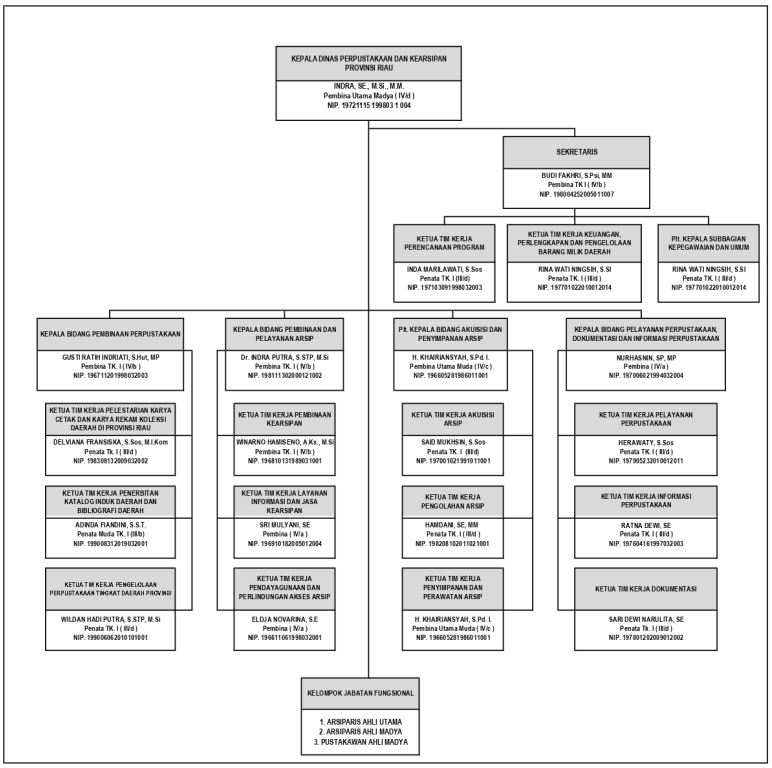
Fungsi:

Fungsi Dinas Perpustakaan dan Kearsipan Provinsi Riau sebagai berikut:

1. Merumuskan Kebijaksanaan
2. Pengambilan Keputusan
3. Perencanaan
4. Pengorganisasian
5. Pelayanan umum dan Teknis
6. Pengendalian / Pengarahan / Pembinaan dan Bimbingan.
7. Pengawasan, Pemantauan dan Evaluasi
8. Pelaksanaan
9. Pembiayaan
10. Penelitian dan Pengkajian
11. Pelaporan

2.7.4 Struktur Organisasi

Gambar 2.5 merupakan struktur organisai pada Dipersip Provinsi Riau.

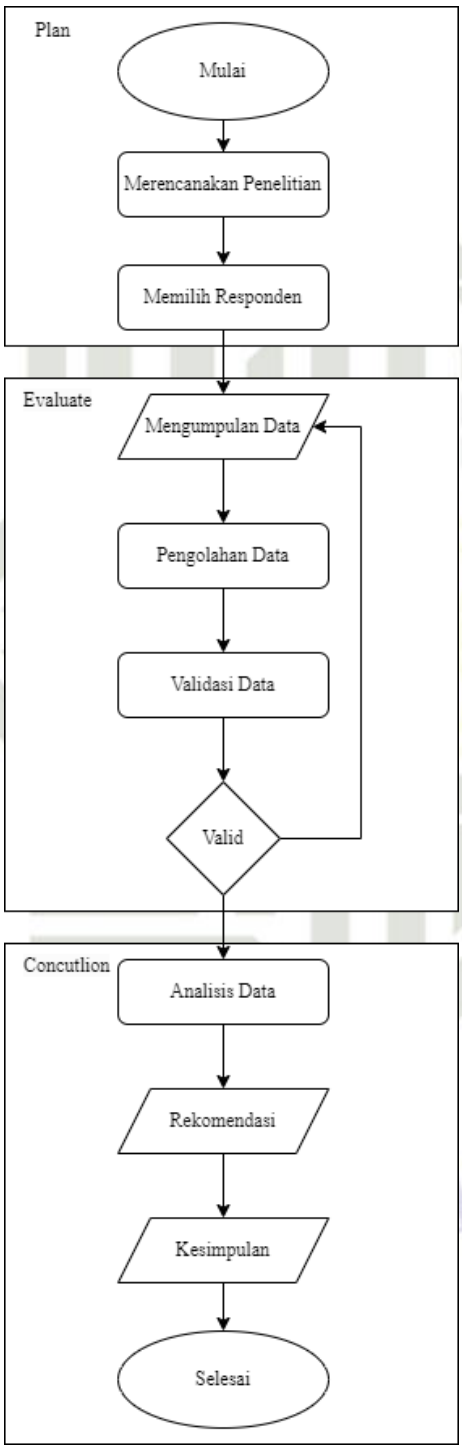


Gambar 2.5. Struktur Organisasi Dipersip Provinsi Riau

Sumber: Dinas Perpustakaan dan Kearsipan Provinsi Riau (2025)

BAB 3
METODOLOGI PENELITIAN

Pada Gambar 3.1 akan digambarkan tahapan pada penelitian ini.



Gambar 3.1. Metodologi Penelitian

3.1 Perencanaan Penelitian

Penelitian ini diawali dengan tahap perencanaan yang disusun berdasarkan hasil observasi awal serta kajian pustaka yang relevan. Perumusan rencana penelitian mengacu pada kerangka kerja metode Indeks KAMI. Pada tahap ini, seluruh kebutuhan penelitian dipersiapkan terlebih dahulu sebelum pelaksanaan evaluasi secara langsung pada instansi yang menjadi objek penelitian.

3.2 Pemilihan Responden

Responden yang dipilih adalah orang yang berwenang dan tanggung jawab terhadap keamanan informasi. Pemilihan ini bertujuan agar responden bisa mengisi kuesioner Indeks KAMI dan dapat memberi penjelasan yang memadai saat dilakukan wawancara. Pemilihan responden ini menggunakan RACI Matrix untuk memastikan individu yang tepat terlibat seperti pada Lampiran A.

3.3 Pengumpulan Data

Metode pengambilan data pada penelitian ini adalah dengan metode kuisioner, dengan cara memberikan seperangkat pernyataan tertulis dan diberikan kepada responden terpilih agar dapat memilih opsi jawaban. Kuisioner yang dipakai sesuai Indeks KAMI seperti pada Lampiran B dan Lampiran C. Penyusunan kuisioner sesuai dengan format yang disediakan di *website* BSSN. Kuisioner yang digunakan adalah versi terbaru yakni Indeks KAMI versi 5.0 yang mencakup area kategori sistem elektronik dan 6 area keamanan informasi.

3.4 Pengolahan Data

Setelah kuesioner berhasil dikumpulkan, data selanjutnya diproses mengikuti Panduan Indeks KAMI versi 5.0. Semua informasi, termasuk data responden dan juga yyang terdapat pada Lampiran D, di *input* ke dalam *file* Excel yang sudah diformat sesuai standar Indeks KAMI versi 5.0. Langkah ini bertujuan mengubah data mentah menjadi informasi yang sistematis dan mudah dianalisis. Hasil penilaian terbagi menjadi dua area utama, yakni: area kategori sistem elektronik dan area keamanan informasi.

3.5 Validasi Data

Setelah pengolahan data selesai, data akan divalidasi dengan metode *checklist* untuk memastikan kebenaran hasil kuisioner. Validasi dilakukan secara tatap muka dengan responden guna menggali informasi lebih dalam dan mendapatkan bukti pendukung dari jawaban yang telah dapat. Secara khusus, bukti diperlukan untuk pertanyaan yang dijawab dengan status “dalam perencanaan atau diterapkan sebagian“ dan “diterapkan menyeluruh”.

3.6 Analisis Data

Setelah data dinyatakan valid, tahap selanjutnya adalah melakukan analisis menggunakan Indeks KAMI versi 5.0. Data dari area keamanan informasi yang telah dianalisis akan menghasilkan rekomendasi perbaikan. Proses analisis dilakukan dengan memetakan hasil kuisioner berdasarkan tingkat kematangannya, kemudian hasilnya ditampilkan dalam bentuk tabel nilai serta diagram radar.

3.7 Rekomendasi perbaikan

Rekomendasi penelitian dirumuskan berdasarkan hasil evaluasi yang disesuaikan dengan pengendalian pada standar ISO/IEC 27001:2022. Penyusunan rekomendasi dilakukan melalui proses pencocokan antara temuan penelitian dan persyaratan yang tercantum dalam kontrol ISO/IEC 27001:2022.

3.8 Kesimpulan

Kesimpulan disusun sebagai tahap akhir penelitian berdasarkan hasil analisis dan pembahasan yang telah dilakukan. Bagian ini menggambarkan kondisi tata kelola keamanan informasi di Dinas Perpustakaan dan Kearsipan Provinsi Riau serta tingkat kesesuaiannya dengan standar yang berlaku.

BAB 6
PENUTUP

6.1 Kesimpulan

Berdasarkan hasil penelitian terkait penilaian sistem manajemen keamanan informasi Dipersip provinsi Riau menggunakan Indeks Keamanan Informasi (KAMI) adalah sebagai berikut:

1. Hasil evaluasi akhir menunjukkan bahwa status penerapan keamanan informasi di instansi ini adalah "tidak layak", dengan tingkat kelengkapan penerapan ISO/IEC 27001 mencapai skor 253. Secara rinci, tingkat kematangan pada masing-masing area adalah: Tata Kelola I+, Pengelolaan Risiko I, Kerangka Kerja Keamanan Informasi I+, Pengelolaan Aset I+, Teknologi dan Keamanan Informasi I+, Pelindungan Data Pribadi I+, dan Pengamanan Keterlibatan Pihak Ketiga 25%.
2. Dari hasil analisis tersebut, disusun rekomendasi perbaikan yang dapat menjadi pertimbangan bagi Dipersip Provinsi Riau untuk meningkatkan penerapan keamanan informasi dan skor Indeks KAMI. Rekomendasi yang diusulkan setiap area adalah: Tata Kelola 16 rekomendasi, Pengelolaan Risiko Keamanan Informasi 15 rekomendasi, Kerangka Kerja Keamanan Informasi 29 rekomendasi, Pengelolaan Aset 42 rekomendasi, Teknologi dan Keamanan Informasi 29 rekomendasi, Pelindungan Data Pribadi 15 rekomendasi, dan Suplemen 27 rekomendasi.

6.2 Saran

Berdasarkan hasil kesimpulan sebelumnya terdapat saran kepada Dipersip Provinsi Riau adalah:

1. Melakukan beberapa rekomendasi yang diberikan untuk memperbaiki tingkat keamanan informasi pada Dipersip Provinsi Riau.
2. Melakukan sertifikasi ISO 27001:2022 saat sudah siap menerapkan semua ketentuan standar yang ada.

Lalu terdapat saran pada penelitian ini adalah memanfaatkan forum diskusi yang lebih memadai agar seluruh kebutuhan penelitian dapat terpenuhi secara optimal.

DAFTAR PUSTAKA

Amalia, S. F., dan Anwar, M. K. (2024). Dampak penerapan e-government terhadap perubahan budaya birokrasi untuk mencapai transparansi dan akuntabilitas dalam sistem pemerintahan modern. *PENTAHELIX*, *2*(1), 25–40.

Aulia, F., Hamidah Erwin Effendi, N., dan Nuari, B. (2023). Analisis keamanan informasi menggunakan aplikasi indeks kami pada sekretariat dprd kabupaten jombang. Dalam *Seminar nasional teknologi dan sistem informasi* (Vol. 4).

Badan Siber dan Sandi Negara. (2023). *Peraturan badan siber dan sandi negara republik indonesia nomor 7 tahun 2023 tentang identifikasi infrastruktur informasi vital* (Tech. Rep.). Badan Siber dan Sandi Negara Republik Indonesia. (Peraturan BSSN)

Başaran, B. (2016). The effect of iso quality management system standards on industrial property rights in turkey. *World Patent Information*, *45*, 33–46.

Cronholm, S., dan Göbel, H. (2016). Evaluation of the information systems research framework: Empirical evidence from a design science research project. *Electronic Journal of Information Systems Evaluation*, *19*(3), pp158–168.

Cronholm, S., dan Goldkuhl, G. (2003). Strategies for information systems evaluation-six generic types. *Electronic Journal of Information Systems Evaluation*, *6*(2), 65–74.

De Haes, S., dan Van Grembergen, W. (2008). Analysing the relationship between it governance and business/it alignment maturity. Dalam *Proceedings of the 41st annual hawaii international conference on system sciences (hicss 2008)* (hal. 428–428).

Dinas Perpustakaan dan Kearsipan Provinsi Riau. (2025). *Sejarah dinas perpustakaan dan kearsipan provinsi riau.* Retrieved from `https://dipersip.riau.go.id/` (Situs resmi)

Gala, R. A., Sengkey, R., dan Punusingon, C. (2020). Analisis keamanan informasi pemerintah kabupaten minahasa tenggara menggunakan indeks kami. *Jurnal Teknik Informatika*, *15*(3), 189–198.

Jelita, L. D. A., Al Azam, M. N., dan Nugroho, A. (2024). Evaluasi keamanan teknologi informasi menggunakan indeks keamanan informasi 5.0 dan iso/eic 27001: 2022. *Jurnal Saintekom: Sains, Teknologi, Komputer dan Manajemen*, *14*(1), 84–94.

Junaid, T.-S. (2023). *Iso 27001: information security management systems* (Unpublished doctoral dissertation). Ph. D. thesis, Unspecified Institution. https://doi. org/10.13140/RG. 2.2 ....

Kementerian Komunikasi dan Digital. (2022, October 6). *Keamanan informasi.* Retrieved from https://bpptik.komdigi.go.id/Publikasi/detail/keamanan-informasi (Publikasi resmi)

Menteri Komunikasi dan Informatika Republik Indonesia. (2016). *Peraturan menteri komunikasi dan informatika republik indonesia nomor 4 tahun 2016 tentang sistem manajemen pengamanan informasi* (Tech. Rep.). Kementerian Komunikasi dan Informatika Republik Indonesia. (Peraturan Menteri)

Muahidin, Z., Nasiri, A., dkk. (2022). Analisis manajemen keamanan informasi menggunakan indeks keamanan informasi pada it support di universitas teknologi mataram. *Explore*, *12*(2), 126–130.

Ningrum, F. A. S., Riwanto, Y., Pratiwi, I. Y. R., dan Fikri, M. A. (2024). Analisis keamanan sistem informasi perguruan tinggi berbasis indeks kami. *Jurnal Informatika Polinema*, *10*(3).

Rachmadi, T. (2020). *Pengantar teknologi informasi* (Vol. 1). Tiga Ebook.

Riyana, C. (2008). Peranan teknologi dalam pembelajaran. *Universitas Indonesia, Jakarta*.

Sundari, P., dan Wella, W. (2021). Sni iso/iec 27001 dan indeks kami: Manajemen risiko pusdatin (pupr). *Ultima InfoSys: Jurnal Ilmu Sistem Informasi*, *12*(1), 35–42.

Suprianto, B. (2023). Literature review: penerapan teknologi informasi dalam meningkatkan kualitas pelayanan publik. *Jurnal Pemerintahan Dan Politik*, *8*(2), 123–128.

Taufik, A., Sudarsono, G., Sudaryana, I. K., Muryono, T. T., dkk. (2022). Pengantar teknologi informasi. *Yayasan Drestanta Pelita Indonesia*, 1–113.

Wahyono, T. (2004). Sistem informasi. *Yogyakarta: Graha Ilmu*.

Wardiana, W. (2002). *Perkembangan teknologi informasi di indonesia.*

Wu, W., Shi, K., Wu, C.-H., dan Liu, J. (2021). Research on the impact of information security certification and concealment on financial performance: Impact of iso 27001 and concealment on performance. *Journal of Global Information Management (JGIM)*, *30*(3), 1–16.

LAMPIRAN A
TRANSKRIP WAWANCARA

Nama Responden : Adinda Fiandini
Jabatan : Koordinator Tim IT
Hari/Tanggal : Jum'at, 10 Oktober 2025

Tabel A.1. Transkrip Wawancara Kepada Koordinator IT

	Pertanyaan
1	Apakah Dipersip Riau telah menerapkan keamanan informasi pada tata kelola IT?
	Jawab
	Ya, sudah menerapkan. Contoh penerapan keamanan informasi yang dilakukan berfokus pada investasi Sumber Daya Manusia (SDM) melalui workshop terkait IT setiap tahun, yang biasanya dalam hal keamanan data.
	Pertanyaan
2	Apakah terdapat kebijakan khusus mengatur tentang keamanan informasi?
	Jawab
	Belum ada kebijakan khusus yang mengatur tentang keamanan informasi di Dipersip Riau.
	Pertanyaan
3	Permasalahan apa saja yang pernah dihadapi Dipersip Riau dalam konteks keamanan informasi?
	Jawab
	Permasalahan terbesar yang pernah dihadapi terkait keamanan dan operasional IT adalah insiden peretasan server. Peretasan terjadi ketika SDM yang bertanggung jawab mengurus server sedang berada di luar kota. Akibatnya, server sempat mengalami down sekitar empat jam sebelum dapat diakses dan diperbaiki.
	Pertanyaan
4	Apakah pernah dilakukan evaluasi keamanan informasinya?
	Jawab
	Pernah, evaluasi dan penilaian terhadap tata kelola IT dilakukan oleh DISKOMINFOTIK Riau. Penilaian ini biasanya dilakukan setahun sekali. Dalam konteks Sistem Pemerintahan Berbasis Elektronik (SPBE), nilai yang diperoleh Perpustakaan Soeman H.S. dinilai baik.
	Pertanyaan
5	Apa harapan utama Anda dan tim terkait pengembangan tata kelola IT dan keamanan informasi di Dipersip Riau ke depannya?
	Jawab
	Harapan utama terkait tata kelola IT dan keamanan informasi di Perpustakaan Soeman H.S. (Dipersip Riau) adalah penambahan anggaran untuk perbaikan infrastruktur kritis, peningkatan keamanan melalui pembaruan lisensi perangkat lunak, serta pengembangan SDM IT melalui pelatihan bersertifikasi.

Mengetahui,
Koordinator Tim IT

Adinda Fiandini, S.S.T.
Nip. 199008.71 201903 2. 001

Nama Responden : Abdul Rohman Wahid
Jabatan : Staf IT
Hari/Tanggal : Senin, 20 Januari 2025

Tabel A.2. Transkrip Wawancara Kepada Staf IT

	Pertanyaan
1	Apa saja sistem informasi yang ada di Dinas Perpustakaan dan Kearsipan Provinsi Riau?
	Jawab
	Dinas Perpustakaan dan Kearsipan Provinsi Riau memanfaatkan beberapa sistem informasi utama untuk mendukung layanan dan pengelolaan data, yaitu INLISLite sebagai sistem pengelolaan koleksi dan layanan perpustakaan dengan rata-rata sekitar 100 akses per hari, SRIKANDI sebagai sistem pengelolaan arsip dinamis dan surat-menyurat elektronik dengan rata-rata sekitar 500 transaksi per hari, serta SIKN sebagai sistem pengelolaan arsip statis yang terintegrasi dengan Arsip Nasional Republik Indonesia (ANRI) dengan rata-rata sekitar 200 akses per hari.
	Pertanyaan
2	Apakah Dinas Perpustakaan dan Kearsipan Provinsi Riau pernah mengalami serangan siber, seperti peretasan atau serangan virus?
	Jawab
	Ya, Dinas Perpustakaan dan Kearsipan Provinsi Riau pernah mengalami insiden serangan siber pada periode Juli hingga Agustus 2024. Pada saat itu, sistem informasi perpustakaan Soeman H.S. (INLISLite) mengalami peretasan, di mana tampilan antarmuka sistem berhasil diubah menjadi laman judi online.
	Pertanyaan
3	Apakah Dipersip Provinsi Riau sudah mengikuti standar untuk keamanan informasi?
	Jawab
	Belum, Dinas Perpustakaan dan Kearsipan Provinsi Riau belum menerapkan standar keamanan informasi secara formal, seperti standar ISO/IEC 27001.
	Pertanyaan
4	Apakah ada evaluasi rutin terhadap keamanan informasi?
	Jawab
	Belum, Dinas Perpustakaan dan Kearsipan Provinsi Riau belum melakukan evaluasi rutin yang secara khusus menilai aspek keamanan informasi.

Mengetahui Responden

Abdul Rohman Wahid

LAMPIRAN B
KUESIONER

Tabel B.1. Kuesioner Kategori Sistem Elektronik

Bagian I: Kategori Sistem Elektronik		
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan.		
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis		**Status**
#	**Karakteristik Instansi / Perusahaan**	
1.1	Nilai investasi sistem elektronik yang terpasang a. Lebih dari Rp 30 Miliar b. Lebih dari Rp 3 Miliar s.d. Rp 30 Miliar c. Kurang dari Rp 3 Miliar	A
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik a. Lebih dari Rp 10 Miliar b. Lebih dari Rp 1 Miliar s.d. Rp 10 Miliar c. Kurang dari Rp 1 Miliar	C
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu a. Peraturan atau Standar nasional dan internasional b. Peraturan atau Standar nasional c. Tidak ada Peraturan khusus	B
1.4	Menggunakan teknik kriptografi untuk keamanan informasi dalam Sistem Elektronik a. Teknik kriptografi bersertifikasi negara b. Teknik kriptografi sesuai standar industri c. Tidak menggunakan teknik kriptografi	B
1.5	Jumlah pengguna Sistem Elektronik a. Lebih dari 5.000 pengguna b. 1.000 sampai dengan 5.000 pengguna c. Kurang dari 1.000 pengguna	C
1.6	Data pribadi yang dikelola Sistem Elektronik a. Data pribadi saling terkait b. Data pribadi individu dan/atau badan usaha c. Tidak ada data pribadi	B

Tabel B.1. Kuesioner Kategori Sistem Elektronik (Tabel Lanjutan...)

Bagian I: Kategori Sistem Elektronik (Lanjutan)		
#	**Karakteristik Instansi / Perusahaan**	**Status**
1.7	Tingkat klasifikasi/kekritisan data dalam Sistem Elektronik a. Sangat rahasia b. Rahasia dan/atau terbatas c. Biasa	B
1.8	Tingkat kekritisan proses dalam Sistem Elektronik a. Berdampak langsung pada layanan publik b. Berdampak tidak langsung c. Berdampak pada bisnis internal	C
1.9	Dampak kegagalan Sistem Elektronik a. Membahayakan pertahanan keamanan negara b. Gangguan layanan publik nasional c. Gangguan layanan regional atau internal	C
1.10	Potensi kerugian akibat insiden keamanan informasi a. Menimbulkan korban jiwa b. Kerugian finansial c. Gangguan operasional sementara	C

Tabel B.2. Kuesioner Area Tata Kelola Keamanan Informasi

Bagian II: Tata Kelola Keamanan Informasi				
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi instansi/perusahaan beserta fungsi, tugas, dan tanggung jawab pengelola keamanan informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Fungsi / Organisasi Keamanan Informasi**	
2.1	II	1	Apakah pimpinan instansi/perusahaan Anda secara prinsip dan resmi bertanggung jawab terhadap pelaksanaan program keamanan informasi, termasuk penetapan kebijakan terkait?	Dalam Perencanaan
2.2	II	1	Apakah instansi/perusahaan Anda memiliki fungsi atau bagian khusus yang bertugas mengelola keamanan informasi dan menjaga kepatuhannya?	Dalam Penerapan / Diterapkan Sebagian

Tabel B.2. Kuesioner Area Tata Kelola Keamanan Informasi (Tabel Lanjutan...)

Bagian II: Tata Kelola Keamanan Informasi (Lanjutan)				
2.3	II	1	Apakah pejabat atau petugas pelaksana pengamanan informasi memiliki wewenang yang memadai untuk menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
2.4	II	1	Apakah penanggung jawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
2.5	II	1	Apakah peran pelaksana pengamanan informasi telah dipetakan secara lengkap termasuk kebutuhan audit internal dan segregasi kewenangan?	Dalam Perencanaan
2.6	II	1	Apakah instansi/perusahaan telah mendefinisikan persyaratan atau standar kompetensi pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
2.7	II	1	Apakah seluruh pelaksana pengamanan informasi memiliki kompetensi dan keahlian sesuai standar yang berlaku?	Dalam Penerapan / Diterapkan Sebagian
2.8	II	1	Apakah instansi/perusahaan telah menerapkan program sosialisasi dan peningkatan pemahaman keamanan informasi bagi seluruh pihak terkait?	Dalam Perencanaan
2.9	II	2	Apakah instansi/perusahaan menerapkan program peningkatan kompetensi dan keahlian bagi pejabat dan petugas pengelola keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian
2.10	II	2	Apakah keperluan dan persyaratan keamanan informasi telah diintegrasikan dalam proses kerja yang ada?	Dalam Perencanaan
2.11	II	2	Apakah data pribadi yang digunakan dalam proses kerja telah diidentifikasi dan diamankan sesuai peraturan perundangan?	Dalam Perencanaan
2.12	II	2	Apakah pengelolaan keamanan informasi mencakup koordinasi dengan pihak internal dan eksternal untuk memenuhi kebutuhan pengamanan informasi?	Dalam Perencanaan
2.13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan unit terkait dan pihak eksternal untuk menjamin kepatuhan pengamanan informasi?	Dalam Perencanaan

Tabel B.2. Kuesioner Area Tata Kelola Keamanan Informasi (Tabel Lanjutan...)

Bagian II: Tata Kelola Keamanan Informasi (Lanjutan)				
2.14	III	2	Apakah tanggung jawab perencanaan dan pengelolaan kelangsungan layanan TIK telah didefinisikan dan dialokasikan secara resmi?	Dalam Perencanaan
2.15	III	2	Apakah penanggung jawab keamanan informasi melaporkan kondisi dan kinerja program keamanan informasi secara rutin kepada pimpinan?	Dalam Perencanaan
2.16	III	2	Apakah isu keamanan informasi menjadi bagian dari proses pengambilan keputusan strategis instansi?	Dalam Perencanaan
2.17	IV	3	Apakah pimpinan satuan kerja menerapkan program khusus untuk memastikan kepatuhan pengamanan informasi?	Tidak Dilakukan
2.18	IV	3	Apakah metrik dan proses pengukuran kinerja keamanan informasi telah ditetapkan secara resmi?	Tidak Dilakukan
2.19	IV	3	Apakah program penilaian kinerja pengelolaan keamanan informasi bagi individu telah diterapkan?	Tidak Dilakukan
2.20	IV	3	Apakah target dan sasaran pengelolaan keamanan informasi telah ditetapkan dan dievaluasi secara berkala?	Tidak Dilakukan
2.21	IV	3	Apakah legislasi dan standar keamanan informasi yang relevan telah diidentifikasi dan dianalisis tingkat kepatuhannya?	Tidak Dilakukan
2.22	IV	3	Apakah kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum telah ditetapkan?	Tidak Dilakukan

Tabel B.3. Kuesioner Pengelolaan Risiko Keamanan Informasi

Bagian III: Pengelolaan Risiko Keamanan Informasi				
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Kajian Risiko Keamanan Informasi**	
3.1	II	1	Apakah instansi/perusahaan Anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Perencanaan
3.2	II	1	Apakah instansi/perusahaan Anda telah menetapkan penanggung jawab manajemen risiko serta mekanisme eskalasi pelaporan status pengelolaan risiko keamanan informasi hingga tingkat pimpinan?	Dalam Perencanaan
3.3	II	1	Apakah instansi/perusahaan Anda memiliki kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan digunakan secara resmi?	Dalam Penerapan / Diterapkan Sebagian
3.4	II	1	Apakah kerangka kerja pengelolaan risiko mencakup definisi dan hubungan klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman, serta dampak kerugian bagi instansi/perusahaan?	Dalam Perencanaan
3.5	II	1	Apakah instansi/perusahaan Anda telah menetapkan ambang batas tingkat risiko yang dapat diterima?	Dalam Perencanaan
3.6	II	1	Apakah kepemilikan dan pengelolaan (custodian) aset informasi telah didefinisikan, termasuk aset utama dan proses kerja yang menggunakannya?	Dalam Perencanaan
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, khususnya aset utama, telah diidentifikasi?	Dalam Perencanaan
3.8	II	1	Apakah dampak kerugian akibat hilangnya atau terganggunya fungsi aset utama telah ditetapkan sesuai definisi yang berlaku?	Dalam Perencanaan
3.9	II	1	Apakah instansi/perusahaan Anda telah melaksanakan analisis atau kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada?	Dalam Perencanaan

Tabel B.3. Kuesioner Pengelolaan Risiko Keamanan Informasi (Tabel Lanjutan...)

Bagian III: Pengelolaan Risiko Keamanan Informasi (Lanjutan)				
3.10	II	1	Apakah langkah mitigasi dan penanggulangan risiko keamanan informasi telah disusun?	Dalam Perencanaan
3.11	III	2	Apakah langkah mitigasi risiko disusun berdasarkan prioritas, target penyelesaian, dan penanggung jawabnya dengan mempertimbangkan efektivitas penggunaan sumber daya?	Dalam Perencanaan
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala untuk memastikan kemajuan atau penyelesaiannya?	Dalam Perencanaan
3.13	IV	2	Apakah langkah mitigasi risiko yang telah diterapkan dievaluasi melalui proses yang objektif dan terukur untuk memastikan konsistensi dan efektivitasnya?	Dalam Perencanaan
3.14	IV	2	Apakah profil risiko beserta mitigasinya dikaji ulang secara berkala untuk memastikan akurasi dan validitasnya, termasuk revisi apabila terjadi perubahan signifikan?	Dalam Perencanaan
3.15	V	3	Apakah kerangka kerja pengelolaan risiko dikaji secara berkala untuk memastikan dan meningkatkan efektivitasnya?	Tidak Dilakukan
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria penilaian objektif kinerja efektivitas pengamanan informasi?	Tidak Dilakukan

Tabel B.4. Kuisioner Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi				
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan dan prosedur) pengelolaan keamanan informasi serta strategi penerapannya.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**	
4.1	II	1	Apakah kebijakan dan prosedur keamanan informasi telah disusun secara jelas dengan mencantumkan peran dan tanggung jawab pihak yang berwenang menerapkannya?	Dalam Penerapan / Diterapkan Sebagian

Tabel B.4. Kuisioner Kerangka Kerja Pengelolaan Keamanan Informasi (Tabel Lanjutan...)

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi (Lanjutan)				
4.2	II	1	Apakah kebijakan keamanan informasi telah ditetapkan secara formal, dipublikasikan, dan mudah diakses oleh pihak yang membutuhkan?	Dalam Perencanaan
4.3	II	1	Apakah tersedia mekanisme pengelolaan dokumen kebijakan dan prosedur keamanan informasi, termasuk distribusi dan penyimpanannya?	Dalam Perencanaan
4.4	II	1	Apakah tersedia proses untuk mengkomunikasikan kebijakan keamanan informasi beserta perubahannya kepada seluruh pihak terkait termasuk pihak ketiga?	Dalam Penerapan / Diterapkan Sebagian
4.5	II	1	Apakah kebijakan dan prosedur keamanan informasi mencerminkan hasil kajian risiko serta sasaran yang ditetapkan pimpinan?	Dalam Perencanaan
4.6	II	1	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden?	Dalam Perencanaan
4.7	II	1	Apakah aspek keamanan informasi tercantum dalam kontrak dengan pihak ketiga?	Dalam Perencanaan
4.8	II	2	Apakah konsekuensi pelanggaran kebijakan keamanan informasi telah didefinisikan dan ditegakkan?	Dalam Perencanaan
4.9	II	2	Apakah tersedia prosedur resmi untuk mengelola pengecualian penerapan keamanan informasi?	Dalam Perencanaan
4.10	III	2	Apakah kebijakan dan prosedur pengelolaan security patch telah diterapkan secara operasional?	Dalam Perencanaan
4.11	III	2	Apakah aspek keamanan informasi telah dibahas dalam manajemen proyek sistem?	Dalam Perencanaan
4.12	III	2	Apakah terdapat proses evaluasi risiko terkait pembelian atau implementasi sistem baru?	Dalam Perencanaan
4.13	III	2	Apakah instansi menerapkan proses pengembangan sistem yang aman (Secure SDLC)?	Dalam Perencanaan
4.14	III	2	Apakah terdapat proses penanggulangan risiko baru akibat penerapan sistem?	Dalam Perencanaan

Tabel B.4. Kuisioner Kerangka Kerja Pengelolaan Keamanan Informasi (Tabel Lanjutan...)

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi (Lanjutan)				
4.15	III	2	Apakah tersedia fungsi khusus untuk mengelola perkembangan ancaman keamanan informasi (threat intelligence)?	Dalam Perencanaan
4.16	III	2	Apakah tersedia kerangka kerja perencanaan kelangsungan layanan TIK (BCP)?	Dalam Perencanaan
4.17	III	3	Apakah kebijakan terkait threat intelligence telah disusun secara resmi?	Tidak Dilakukan
4.18	III	3	Apakah hasil analisis ancaman keamanan informasi disampaikan kepada pihak terkait mitigasi risiko?	Tidak Dilakukan
4.19	III	3	Apakah disaster recovery plan telah mendefinisikan peran dan tanggung jawab tim?	Tidak Dilakukan
4.20	III	3	Apakah uji coba disaster recovery plan dilakukan secara berkala?	Tidak Dilakukan
4.21	IV	3	Apakah hasil DRP dievaluasi untuk perbaikan berkelanjutan?	Tidak Dilakukan
4.22	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi secara berkala?	Tidak Dilakukan
# Pengelolaan Strategi dan Program Keamanan Informasi				
4.23	II	1	Apakah instansi memiliki strategi penerapan keamanan informasi berdasarkan hasil analisis risiko?	Dalam Perencanaan
4.24	II	1	Apakah terdapat strategi penggunaan teknologi keamanan informasi yang disesuaikan dengan profil risiko?	Dalam Perencanaan
4.25	III	1	Apakah strategi keamanan informasi direalisasikan dalam program kerja organisasi?	Dalam Penerapan / Diterapkan Sebagian
4.26	III	1	Apakah tersedia program audit internal keamanan informasi oleh pihak independen?	Dalam Perencanaan
4.27	III	1	Apakah audit internal mengevaluasi kepatuhan dan efektivitas penerapan keamanan informasi?	Dalam Perencanaan
4.28	III	2	Apakah hasil audit dievaluasi untuk perbaikan dan peningkatan keamanan informasi?	Dalam Perencanaan
4.29	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi?	Dalam Perencanaan

Tabel B.4. Kuisioner Kerangka Kerja Pengelolaan Keamanan Informasi (Tabel Lanjutan...)

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi (Lanjutan)				
4.30	IV	3	Apakah terdapat analisis dampak finansial sebelum revisi kebijakan keamanan informasi?	Tidak Dilakukan
4.31	V	3	Apakah tingkat kepatuhan program keamanan informasi diuji dan dievaluasi secara berkala?	Tidak Dilakukan
4.32	V	3	Apakah tersedia rencana peningkatan keamanan informasi jangka menengah dan panjang?	Tidak Dilakukan

Tabel B.5. Kuesioner Area Pengelolaan Aset Informasi

Bagian V: Pengelolaan Aset Informasi				
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Pengelolaan Aset Informasi**	
5.1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat, dan terpelihara termasuk kepemilikan aset?	Diterapkan Secara Menyeluruh
5.2	II	1	Apakah tersedia definisi klasifikasi aset informasi sesuai peraturan perundangan yang berlaku?	Dalam Penerapan / Diterapkan Sebagian
5.3	II	1	Apakah tersedia proses evaluasi dan klasifikasi aset informasi sesuai tingkat kepentingan dan kebutuhan pengamanannya?	Dalam Perencanaan
5.4	II	1	Apakah tersedia definisi tingkatan akses dan matriks alokasi akses untuk setiap klasifikasi aset informasi?	Dalam Perencanaan
5.5	II	1	Apakah tersedia proses identifikasi dan inventarisasi syarat retensi aset informasi serta penghapusannya?	Dalam Perencanaan
5.6	II	1	Apakah tersedia proses evaluasi kepatuhan terhadap syarat retensi aset informasi?	Dalam Perencanaan
5.7	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis, dan proses TI yang diterapkan secara konsisten?	Dalam Perencanaan

Tabel B.5. Kuesioner Area Pengelolaan Aset Informasi (Tabel Lanjutan...)

Bagian V: Pengelolaan Aset Informasi (Lanjutan)				
5.8	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Dalam Perencanaan
5.9	II	1	Apakah tersedia proses untuk merilis aset baru dan memutakhirkan inventaris aset informasi?	Dalam Perencanaan
Kontrol Keamanan sebagai Kelanjutan Mitigasi Risiko				
5.10	II	1	Definisi tanggung jawab pengamanan informasi secara individual untuk seluruh personel instansi/perusahaan	Dalam Penerapan / Diterapkan Sebagian
5.11	II	1	Tata tertib penggunaan komputer, email, internet, dan intranet	Diterapkan Secara Menyeluruh
5.12	II	1	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	Dalam Perencanaan
5.13	II	1	Peraturan terkait instalasi piranti lunak di aset TI instansi/perusahaan	Dalam Perencanaan
5.14	II	1	Peraturan penggunaan data pribadi yang mensyaratkan izin tertulis dari pemilik data	Dalam Perencanaan
5.15	II	1	Pengelolaan identitas elektronik dan proses otentikasi termasuk kebijakan pelanggaran	Dalam Perencanaan
5.16	II	1	Persyaratan dan prosedur pemberian akses, otentikasi, dan otorisasi aset informasi	Dalam Perencanaan
5.17	II	1	Ketetapan waktu penyimpanan data dan syarat penghancurannya	Dalam Perencanaan
5.18	II	1	Ketetapan pertukaran data dengan pihak eksternal dan pengamanannya	Dalam Perencanaan
5.19	II	1	Proses investigasi insiden kegagalan keamanan informasi	Dalam Perencanaan
5.20	II	1	Prosedur backup dan uji pemulihan data secara berkala	Diterapkan Secara Menyeluruh
5.21	II	2	Ketentuan pengamanan fisik sesuai zona dan klasifikasi aset	Dalam Perencanaan
5.22	III	2	Proses pengecekan latar belakang SDM	Dalam Perencanaan
5.23	III	2	Proses pelaporan insiden keamanan informasi ke pihak eksternal	Dalam Perencanaan
5.24	III	2	Proses dan metode penghancuran informasi sesuai klasifikasi termasuk bukti penghancuran	Dalam Perencanaan
5.25	III	2	Prosedur kajian dan peninjauan hak akses pengguna	Dalam Perencanaan
5.26	III	2	Prosedur untuk pengguna mutasi/keluar atau tenaga kontrak	Dalam Perencanaan

Tabel B.5. Kuesioner Area Pengelolaan Aset Informasi (Tabel Lanjutan...)

Bagian V: Pengelolaan Aset Informasi (Lanjutan)				
5.27	III	3	Apakah tersedia daftar data yang wajib dibackup dan laporan kepatuhan backup?	Tidak Dilakukan
5.28	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi?	Tidak Dilakukan
5.29	III	3	Apakah telah diterapkan metode pengaburan data (data masking)?	Tidak Dilakukan
5.30	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga?	Tidak Dilakukan
Pengamanan Layanan Infrastruktur Awan (Cloud Service)				
5.31	III	2	Apakah dilakukan kajian risiko penggunaan layanan cloud?	Dalam Perencanaan
5.32	III	2	Apakah telah ditetapkan data yang disimpan dan diolah melalui layanan cloud?	Dalam Perencanaan
5.33	III	2	Apakah kebijakan pengamanan data pribadi pada layanan cloud telah ditetapkan?	Dalam Perencanaan
5.34	III	2	Apakah pembagian tanggung jawab keamanan cloud telah ditetapkan?	Dalam Perencanaan
5.35	III	2	Apakah aspek hukum penggunaan layanan cloud telah dikaji?	Dalam Perencanaan
5.36	III	2	Apakah reputasi penyedia layanan cloud telah dievaluasi?	Dalam Perencanaan
5.37	III	2	Apakah standar keamanan teknis penggunaan cloud telah ditetapkan?	Dalam Perencanaan
5.38	III	2	Apakah keamanan dan sertifikasi ISO 27001 layanan cloud telah dievaluasi?	Dalam Perencanaan
5.39	III	2	Apakah tersedia proses pelaporan insiden layanan cloud?	Dalam Perencanaan
5.40	III	3	Apakah tersedia kebijakan penggantian layanan cloud saat gangguan?	Tidak Dilakukan
5.41	III	3	Apakah tersedia proses penghentian layanan cloud dan pengamanan data?	Tidak Dilakukan
Pengamanan Fisik				
5.42	II	1	Apakah pengamanan fasilitas fisik diterapkan sesuai klasifikasi aset secara berlapis?	Diterapkan Secara Menyeluruh
5.43	II	1	Apakah tersedia proses pengelolaan alokasi kunci akses fisik dan elektronik?	Diterapkan Secara Menyeluruh
5.44	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan?	Diterapkan Secara Menyeluruh
5.45	II	1	Apakah infrastruktur terlindungi dari gangguan listrik dan petir?	Dalam Penerapan / Diterapkan Sebagian

Tabel B.5. Kuesioner Area Pengelolaan Aset Informasi (Tabel Lanjutan...)

Bagian V: Pengelolaan Aset Informasi (Lanjutan)				
5.46	II	1	Apakah infrastruktur dipantau menggunakan CCTV?	Dalam Penerapan / Diterapkan Sebagian
5.47	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi di luar kantor?	Dalam Perencanaan
5.48	II	1	Apakah tersedia proses pemindahan aset TIK beserta pemutakhiran inventaris?	Dalam Perencanaan
5.49	II	2	Apakah ruang penyimpanan aset dirancang tahan risiko kebakaran?	Dalam Perencanaan
5.50	II	2	Apakah tersedia proses inspeksi dan perawatan keamanan fasilitas?	Diterapkan Secara Menyeluruh
5.51	II	2	Apakah tersedia mekanisme pengamanan pengiriman aset oleh pihak ketiga?	Dalam Perencanaan
5.52	II	2	Apakah tersedia peraturan pengamanan ruang kerja penting?	Dalam Perencanaan
5.53	III	3	Apakah tersedia proses pengamanan lokasi kerja dari pihak ketiga?	Tidak Dilakukan

Tabel B.6. Kuesioner Area Teknologi dan Keamanan Informasi

Bagian VI: Teknologi dan Keamanan Informasi				
Bagian ini mengevaluasi kelengkapan, konsistensi, dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Pengamanan Teknologi**	
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari satu lapis pengamanan?	Dalam Perencanaan
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dan lain-lain)?	Dalam Perencanaan
6.3	II	1	Apakah tersedia konfigurasi standar keamanan sistem untuk seluruh aset jaringan, sistem, dan aplikasi yang dimutakhirkan sesuai perkembangan standar industri?	Dalam Perencanaan
6.4	III	2	Apakah tersedia proses pengelolaan konfigurasi perangkat komputasi (server, perangkat jaringan, sistem operasi, dan aplikasi) yang diterapkan secara konsisten?	Dalam Perencanaan

Tabel B.6. Kuesioner Area Teknologi dan Keamanan Informasi (Tabel Lanjutan...)

Bagian VI: Teknologi dan Keamanan Informasi (Lanjutan)				
6.5	IV	3	Apakah perangkat komputasi dikaji ulang secara berkala sesuai konfigurasi standar keamanan dan dimutakhirkan melalui proses manajemen perubahan?	Dalam Perencanaan
6.6	II	1	Apakah jaringan, sistem, dan aplikasi dipindai secara rutin untuk mengidentifikasi celah keamanan atau perubahan konfigurasi?	Dalam Perencanaan
6.7	II	1	Apakah infrastruktur jaringan, sistem, dan aplikasi dirancang untuk menjamin ketersediaan melalui rancangan redundan?	Dalam Perencanaan
6.8	II	1	Apakah infrastruktur jaringan, sistem, dan aplikasi dimonitor untuk memastikan kapasitas dan efektivitas keamanannya?	Diterapkan Secara Menyeluruh
6.9	II	1	Apakah setiap perubahan dalam sistem informasi terekam secara otomatis dalam log?	Dalam Perencanaan
6.10	II	1	Apakah upaya akses oleh pihak yang tidak berhak terekam secara otomatis dalam log?	Dalam Perencanaan
6.11	II	1	Apakah seluruh log dianalisis secara berkala untuk kepentingan audit dan forensik?	Dalam Perencanaan
Catatan Periksa Log Minimal: 1. Trafik jaringan inbound dan outbound; 2. Akses ke sistem, server, perangkat jaringan, dan aplikasi kritis; 3. Penggunaan file sistem dan konfigurasi jaringan; 4. Log perangkat keamanan (antivirus, IDS/IPS, firewall, web filter, DLP); 5. Event log sistem dan aktivitas jaringan.				
6.12	II	1	Apakah instansi/perusahaan menerapkan enkripsi untuk melindungi aset informasi penting?	Dalam Perencanaan
6.13	III	2	Apakah instansi/perusahaan memiliki standar penggunaan enkripsi?	Dalam Perencanaan
6.14	III	2	Apakah pengelolaan kunci enkripsi termasuk sertifikat elektronik telah diterapkan?	Tidak Dilakukan
6.15	III	2	Apakah sistem dan aplikasi menerapkan pengelolaan password otomatis dan kebijakan kompleksitas password?	Tidak Dilakukan
6.16	III	2	Apakah akses administrasi sistem menggunakan pengamanan berlapis?	Tidak Dilakukan
6.17	III	2	Apakah sistem dan aplikasi menerapkan pembatasan waktu akses dan mekanisme lockout?	Tidak Dilakukan

Tabel B.6. Kuesioner Area Teknologi dan Keamanan Informasi (Tabel Lanjutan...)

Bagian VI: Teknologi dan Keamanan Informasi (Lanjutan)				
6.18	III	2	Apakah tersedia pengamanan untuk mendeteksi dan mencegah akses jaringan tidak resmi?	Tidak Dilakukan
6.19	II	1	Apakah diterapkan pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Dalam Penerapan / Diterapkan Sebagian
6.20	II	1	Apakah sistem operasi desktop dan server dimutakhirkan ke versi terkini?	Dalam Penerapan / Diterapkan Sebagian
6.21	II	1	Apakah setiap desktop dan server dilindungi dari malware?	Dalam Penerapan / Diterapkan Sebagian
6.22	III	2	Apakah tersedia audit trail pemutakhiran antivirus/antimalware?	Dalam Penerapan / Diterapkan Sebagian
6.23	III	2	Apakah laporan insiden malware ditindaklanjuti dan diselesaikan?	Dalam Perencanaan
6.24	III	2	Apakah dilakukan analisis dan pemblokiran website berbahaya?	Dalam Perencanaan
6.25	III	2	Apakah sistem menggunakan mekanisme sinkronisasi waktu yang akurat?	Dalam Perencanaan
6.26	III	2	Apakah prinsip pengembangan aplikasi aman (secure coding) telah diterapkan?	Tidak Dilakukan
6.27	III	2	Apakah diterapkan proses perencanaan pengembangan sistem yang aman?	Dalam Perencanaan
6.28	III	2	Apakah source code direview sebelum diterapkan di lingkungan produksi?	Dalam Perencanaan
6.29	II	1	Apakah diterapkan kontrol akses terhadap source code aplikasi?	Dalam Perencanaan
6.30	III	2	Apakah spesifikasi dan fungsi keamanan aplikasi diverifikasi saat pengembangan?	Tidak Dilakukan
6.31	III	3	Apakah dilakukan analisis dan perbaikan terhadap ancaman baru?	Dalam Perencanaan
6.32	III	3	Apakah lingkungan pengembangan dan pengujian telah diamankan?	Dalam Perencanaan
6.33	III	3	Apakah diterapkan mekanisme pencegahan kebocoran informasi sensitif?	Dalam Perencanaan
6.34	IV	3	Apakah teknologi DLP (Data Leakage Prevention) telah diterapkan?	Dalam Perencanaan
6.35	IV	3	Apakah pihak independen dilibatkan untuk mengkaji keandalan keamanan informasi?	Tidak Dilakukan

Tabel B.7. Kuesioner Area Pelindungan Data Pribadi

Bagian VII: Pelindungan Data Pribadi				
Bagian ini mengevaluasi kelengkapan, konsistensi, dan efektivitas penerapan kontrol keamanan terkait Pelindungan Data Pribadi (PDP).				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Pelindungan Data Pribadi**	
7.1	II	1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah, dan dipertukarkan dengan pihak eksternal?	Tidak Dilakukan
7.2	II	1	Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan di mana data pribadi diperoleh?	Dalam Perencanaan
7.3	II	1	Apakah proses terkait penyimpanan, pengolahan, dan pertukaran data pribadi sudah didokumentasikan?	Dalam Perencanaan
7.4	II	1	Apakah instansi/perusahaan sudah memiliki kebijakan Pelindungan Data Pribadi sesuai peraturan perundangan yang berlaku?	Dalam Perencanaan
7.5	II	2	Apakah instansi/perusahaan sudah menunjuk fungsi/unit Pejabat Pelindung Data Pribadi yang bertanggung jawab dan berwenang?	Dalam Penerapan / Diterapkan Sebagian
7.6	II	2	Apakah instansi/perusahaan sudah menganalisis dampak terungkapnya data pribadi secara ilegal atau akibat insiden lain?	Dalam Perencanaan
7.7	III	2	Apakah kajian risiko keamanan sudah memasukkan aspek Pelindungan Data Pribadi?	Dalam Perencanaan
7.8	III	2	Apakah mekanisme pelindungan data pribadi diterapkan sesuai mitigasi risiko dan peraturan perundangan?	Dalam Perencanaan
7.9	III	2	Apakah instansi/perusahaan menjalankan program peningkatan pemahaman pegawai terkait Pelindungan Data Pribadi?	Dalam Perencanaan
7.10	III	2	Apakah instansi/perusahaan sudah memperoleh persetujuan pemilik data pribadi dan menyimpan catatan persetujuan tersebut?	Dalam Perencanaan

Tabel B.7. Kuesioner Area Pelindungan Data Pribadi (Tabel Lanjutan...)

Bagian VII: Pelindungan Data Pribadi (Lanjutan)				
7.11	III	2	Apakah instansi/perusahaan memiliki proses pelaporan insiden terkait kebocoran data pribadi?	Dalam Perencanaan
7.12	III	2	Apakah instansi/perusahaan menerapkan proses yang menjamin hak pemilik data untuk mengakses data pribadinya?	Dalam Perencanaan
7.13	III	2	Apakah instansi/perusahaan menerapkan proses untuk memastikan data pribadi akurat dan mutakhir?	Dalam Perencanaan
7.14	III	2	Apakah instansi/perusahaan menerapkan proses periode penyimpanan dan penghapusan/pemusnahan data pribadi sesuai ketentuan?	Dalam Perencanaan
7.15	III	2	Apakah instansi/perusahaan menerapkan proses penghapusan/pemusnahan data pribadi atas permintaan pemilik data dan menyimpan catatannya?	Dalam Perencanaan
7.16	III	2	Apakah instansi/perusahaan menerapkan proses pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	Dalam Perencanaan

Tabel B.8. Kuesioner Area Suplemen

Bagian VIII: Suplemen				
Bagian ini mengevaluasi kelengkapan, konsistensi, dan efektivitas penerapan mekanisme keamanan terkait risiko keterlibatan pihak ketiga eksternal dalam operasional penyelenggaraan layanan instansi/perusahaan.				
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**	
8.1			**Manajemen Risiko dan Pengelolaan Keamanan Pihak Ketiga**	
8.1.1		1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi terkait kerja sama dengan pihak ketiga atau karyawan kontrak?	Tidak Dilakukan
8.1.2		1	Apakah instansi/perusahaan mengomunikasikan dan mengklarifikasi risiko keamanan informasi kepada pihak ketiga?	Tidak Dilakukan

Tabel B.8. Kuesioner Area Suplemen (Tabel Lanjutan...)

Bagian VIII: Suplemen (Lanjutan)			
8.1.3	1	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko dan ekspektasi yang harus dipatuhi pihak ketiga?	Tidak Dilakukan
8.1.4	1	Apakah rencana mitigasi risiko tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	Tidak Dilakukan
8.1.5	1	Apakah instansi/perusahaan menerapkan kebijakan keamanan informasi bagi pihak ketiga, termasuk pengendalian akses, penghancuran informasi, manajemen risiko, dan NDA?	Dalam Perencanaan
8.1.6	1	Apakah kebijakan tersebut dikomunikasikan kepada pihak ketiga dan disetujui dalam kontrak, SLA, atau dokumen sejenis?	Tidak Dilakukan
8.1.7	1	Apakah hak audit TI terhadap pihak ketiga ditetapkan dalam kontrak, termasuk akses terhadap laporan audit internal/eksternal?	Tidak Dilakukan
8.2		**Pengelolaan Sub-Kontraktor / Alih Daya pada Pihak Ketiga**	
8.2.1	1	Apakah pihak ketiga mengidentifikasi risiko terkait alih daya, subkontraktor, atau penyedia teknologi yang digunakan?	Dalam Perencanaan
8.2.2	1	Apakah pihak ketiga menerapkan pengendalian risiko tersebut dalam perjanjian atau dokumen sejenis?	Dalam Perencanaan
8.2.3	1	Apakah pihak ketiga melakukan pemantauan dan evaluasi kepatuhan subkontraktor terhadap persyaratan keamanan?	Dalam Perencanaan
8.3		**Pengelolaan Layanan dan Keamanan Pihak Ketiga**	
8.3.1	1	Apakah instansi/perusahaan memiliki proses terdokumentasi untuk mengelola dan memantau layanan serta keamanan informasi dalam kerja sama dengan pihak ketiga?	Tidak Dilakukan
8.3.2	1	Apakah peran dan tanggung jawab pemantauan atau audit keamanan informasi pihak ketiga telah ditetapkan?	Dalam Perencanaan
8.3.3	1	Apakah tersedia laporan berkala pencapaian SLA dan aspek keamanan sesuai perjanjian kontrak?	Dalam Perencanaan

Tabel B.8. Kuesioner Area Suplemen (Tabel Lanjutan...)

Bagian VIII: Suplemen (Lanjutan)			
8.3.4	1	Apakah dilakukan rapat berkala untuk memantau dan mengevaluasi pencapaian SLA dan aspek keamanan?	Dalam Perencanaan
8.3.5	1	Apakah hasil pemantauan dan evaluasi tersebut didokumentasikan, dikomunikasikan, dan ditindaklanjuti oleh pihak ketiga?	Dalam Perencanaan
8.3.6	1	Apakah instansi/perusahaan menetapkan rencana dan melakukan audit pemenuhan persyaratan keamanan informasi pihak ketiga?	Dalam Perencanaan
8.3.7	1	Apakah hasil audit ditindaklanjuti pihak ketiga dengan rencana perbaikan dan bukti penerapannya?	Dalam Perencanaan
8.3.8	1	Apakah ketentuan denda atau penalti atas ketidakpatuhan pihak ketiga telah didokumentasikan dan diterapkan?	Dalam Perencanaan
8.4		**Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga**	
8.4.1	1	Apakah instansi/perusahaan mengelola perubahan layanan, kebijakan, prosedur, atau kontrol risiko pihak ketiga?	Dalam Perencanaan
8.4.2	1	Apakah risiko akibat perubahan tersebut dikaji, didokumentasikan, dan ditetapkan rencana mitigasinya?	Dalam Perencanaan
8.5		**Penanganan Aset**	
8.5.1	1	Apakah pihak ketiga memiliki prosedur formal penanganan data sepanjang siklus hidup aset informasi?	Dalam Perencanaan
8.5.2	1	Apakah prosedur penghancuran data secara aman telah disepakati bersama pihak ketiga?	Dalam Perencanaan
8.6		**Pengelolaan Insiden oleh Pihak Ketiga**	
8.6.1	1	Apakah pihak ketiga memiliki prosedur pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	Dalam Perencanaan
8.6.2	1	Apakah pihak ketiga memiliki bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	Dalam Perencanaan
8.7		**Rencana Kelangsungan Layanan Pihak Ketiga**	

Tabel B.8. Kuesioner Area Suplemen (Tabel Lanjutan...)

Bagian VIII: Suplemen (Lanjutan)			
8.7.1	1	Apakah pihak ketiga memiliki kebijakan atau rencana terdokumentasi untuk kelangsungan layanan saat darurat/bencana?	Dalam Perencanaan
8.7.2	1	Apakah rencana kelangsungan layanan tersebut telah diuji coba, didokumentasikan, dan dievaluasi efektivitasnya?	Dalam Perencanaan
8.7.3	1	Apakah pihak ketiga memiliki tim atau organisasi khusus untuk mengelola kelangsungan layanan?	Dalam Perencanaan

LAMPIRAN C
KUESIONER CHECKLIST

Nama Responden : Adinda Fiandini
Jabatan : Koordinator Tim IT
Hari/Tanggal : Jum'at, 10 Oktober 2025

Tabel C.1. Kuesioner *Checklist* Area Tata Kelola Keamanan Informasi

#			Fungsi / Organisasi Keamanan Informasi	Bukti		Keterangan
				Ada	Tidak	
2.1	II	1	Apakah pimpinan instansi/perusahaan secara resmi bertanggung jawab terhadap pelaksanaan program keamanan informasi?		✓	–
2.2	II	1	Apakah instansi/perusahaan memiliki fungsi atau bagian khusus pengelola keamanan informasi?	✓		SK Pengangkatan Staf IT
2.3	II	1	Apakah pejabat pelaksana pengamanan informasi memiliki wewenang yang memadai?	✓		SK Pengangkatan Staf IT
2.4	II	1	Apakah penanggung jawab keamanan informasi memperoleh alokasi sumber daya yang sesuai?	✓		DPA Pengembangan dan Pemeliharaan Layanan
2.5	II	1	Apakah peran pelaksana pengamanan informasi telah dipetakan secara lengkap?		✓	–
2.6	II	1	Apakah telah ditetapkan standar kompetensi pelaksana pengelolaan keamanan informasi?	✓		Pergub Riau No. 53 Tahun
2.7	II	1	Apakah pelaksana pengamanan informasi memiliki kompetensi sesuai standar?	✓		Ijazah dan Sertifikat Kompetensi
2.8	II	1	Apakah telah diterapkan program sosialisasi dan peningkatan pemahaman keamanan informasi?		✓	–
2.9	II	2	Apakah terdapat program peningkatan kompetensi pengelola keamanan informasi?	✓		Sertifikat Kompetensi
2.10	II	2	Apakah persyaratan keamanan informasi telah terintegrasi dalam proses kerja?		✓	–
2.11	II	2	Apakah data pribadi telah diidentifikasi dan diamankan sesuai peraturan?		✓	–

Tabel C.1. Kuesioner *Checklist* Area Tata Kelola Keamanan Informasi (Tabel Lanjutan...)

#			Fungsi / Organisasi Keamanan Informasi	Bukti		Keterangan
				Ada	Tidak	
2.12	II	2	Apakah pengelolaan keamanan informasi mencakup koordinasi dengan pihak internal dan eksternal?		✓	–
2.13	II	2	Apakah pengelola keamanan informasi berkoordinasi dengan unit terkait dan pihak eksternal?		✓	–
2.14	III	2	Apakah tanggung jawab pengelolaan kelangsungan layanan TIK telah didefinisikan?		✓	–
2.15	III	2	Apakah laporan kondisi dan kinerja keamanan informasi disampaikan secara rutin?		✓	–
2.16	III	2	Apakah isu keamanan informasi menjadi bagian pengambilan keputusan strategis?		✓	–
2.17	IV	3	Apakah pimpinan satuan kerja menerapkan program kepatuhan keamanan informasi?		✓	–
2.18	IV	3	Apakah metrik dan proses pengukuran kinerja keamanan informasi telah ditetapkan?		✓	–
2.19	IV	3	Apakah program penilaian kinerja keamanan informasi individu telah diterapkan?		✓	–
2.20	IV	3	Apakah target dan evaluasi pengelolaan keamanan informasi dilakukan secara rutin?		✓	–
2.21	IV	3	Apakah legislasi dan standar keamanan informasi telah diidentifikasi?		✓	–
2.22	IV	3	Apakah kebijakan penanggulangan insiden keamanan informasi telah ditetapkan?		✓	–

Tabel C.2. Kuesioner *Checklist* Kerangka Kerja Pengelolaan Keamanan Informasi

#			Kerangka Kerja Pengelolaan Keamanan Informasi	Bukti		Keterangan
				Ada	Tidak	
Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi						
4.1	II	1	Apakah kebijakan dan prosedur keamanan informasi telah disusun dengan jelas termasuk peran dan tanggung jawabnya?	✓		SOP Back-up, Restore, Exit Server
4.2	II	1	Apakah kebijakan keamanan informasi telah ditetapkan secara formal dan dipublikasikan?		✓	–
4.3	II	1	Apakah tersedia mekanisme pengelolaan dokumen kebijakan keamanan informasi?		✓	–

Tabel C.2. Kuesioner *Checklist* Kerangka Kerja Pengelolaan Keamanan Informasi (Tabel Lanjutan...)

#			Kerangka Kerja Pengelolaan Keamanan Informasi	Bukti		Keterangan
				Ada	Tidak	
4.4	II	1	Apakah tersedia proses komunikasi kebijakan keamanan informasi kepada seluruh pihak terkait?	✓		SK Pengangkatan Staf IT
4.5	II	1	Apakah kebijakan keamanan informasi merefleksikan hasil kajian risiko?		✓	–
4.6	II	1	Apakah tersedia proses identifikasi dan penanganan insiden keamanan informasi?		✓	–
4.7	II	1	Apakah aspek keamanan informasi tercantum dalam kontrak pihak ketiga?		✓	–
4.8	II	2	Apakah konsekuensi pelanggaran kebijakan keamanan informasi telah ditetapkan?		✓	–
4.9	II	2	Apakah tersedia prosedur resmi pengelolaan pengecualian keamanan informasi?		✓	–
4.10	III	2	Apakah terdapat kebijakan pengelolaan *security patch*?		✓	–
4.11	III	2	Apakah aspek keamanan informasi dibahas dalam manajemen proyek?		✓	–
4.12	III	2	Apakah terdapat proses evaluasi risiko dalam pembelian atau implementasi sistem baru?		✓	–
4.13	III	2	Apakah diterapkan proses pengembangan sistem yang aman (*Secure SDLC*)?		✓	–
4.14	III	2	Apakah tersedia proses pengendalian risiko baru akibat penerapan sistem?		✓	–
4.15	III	2	Apakah terdapat fungsi khusus pengelolaan ancaman keamanan informasi?		✓	–
4.16	III	2	Apakah tersedia kerangka kerja perencanaan kelangsungan layanan TIK?		✓	–
4.17	III	3	Apakah kebijakan terkait *threat intelligence* telah disusun?		✓	–
4.18	III	3	Apakah hasil analisis ancaman disampaikan kepada pihak terkait mitigasi risiko?		✓	–
4.19	III	3	Apakah perencanaan pemulihan bencana mendefinisikan peran dan tanggung jawab tim?		✓	–
4.20	III	3	Apakah uji coba *disaster recovery plan* dilakukan secara berkala?		✓	–
4.21	IV	3	Apakah hasil uji coba DRP dievaluasi untuk perbaikan berkelanjutan?		✓	–

Tabel C.2. Kuesioner *Checklist* Kerangka Kerja Pengelolaan Keamanan Informasi (Tabel Lanjutan...)

#			Kerangka Kerja Pengelolaan Keamanan Informasi	Bukti		Keterangan
				Ada	Tidak	
4.22	IV	3	Apakah kebijakan keamanan informasi dievaluasi secara berkala?		✓	–
Pengelolaan Strategi dan Program Keamanan Informasi						
4.23	II	1	Apakah tersedia strategi penerapan keamanan informasi berbasis risiko?		✓	–
4.24	II	1	Apakah tersedia strategi penggunaan teknologi keamanan informasi?		✓	–
4.25	III	1	Apakah strategi keamanan informasi direalisasikan dalam program kerja?	✓		DPA Tahun Anggaran 2025
4.26	III	1	Apakah terdapat program audit internal keamanan informasi?		✓	–
4.27	III	1	Apakah audit internal mengevaluasi kepatuhan dan efektivitas keamanan informasi?		✓	–
4.28	III	2	Apakah hasil audit dikaji untuk perbaikan keamanan informasi?		✓	–
4.29	III	2	Apakah hasil audit dilaporkan kepada pimpinan organisasi?		✓	–
4.30	IV	3	Apakah terdapat analisa dampak biaya dan infrastruktur untuk revisi kebijakan?		✓	–
4.31	V	3	Apakah kepatuhan program keamanan informasi dievaluasi secara periodik?		✓	–
4.32	V	3	Apakah tersedia rencana peningkatan keamanan informasi jangka menengah/panjang?		✓	–

Mengetahui,
Koordinator Tim IT

Adinda Fiandini, S.S.T.
Nip. 19900831 201903 2 001

Nama Responden : Abdul Rohman Wahid
Jabatan : Staf IT
Hari/Tanggal : Senin, 20 Januari 2025

Tabel C.3. Kuesioner *Checklist* Pengelolaan Risiko Keamanan Informasi

#			Pengelolaan Risiko Keamanan Informasi	Bukti		Keterangan
				Ada	Tidak	
Kajian Risiko Keamanan Informasi						
3.1	II	1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?		✓	–
3.2	II	1	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?		✓	–
3.3	II	1	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	✓		SK Pengangkatan Koordinator IT
3.4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman dan dampak kerugian?		✓	–
3.5	II	1	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?		✓	–
3.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada?		✓	–
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?		✓	–
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya atau terganggunya fungsi aset utama sudah ditetapkan?		✓	–
3.9	II	1	Apakah instansi/perusahaan anda sudah menjalankan kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada?		✓	–

Tabel C.3. Kuesioner *Checklist* Pengelolaan Risiko Keamanan Informasi (Tabel Lanjutan...)

#			Pengelolaan Risiko Keamanan Informasi	Bukti Ada	Bukti Tidak	Keterangan
3.10	II	1	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?		✓	–
3.11	III	2	Apakah langkah mitigasi risiko disusun berdasarkan prioritas, target penyelesaian dan penanggung jawabnya?		✓	–
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala?		✓	–
3.13	IV	2	Apakah langkah mitigasi yang telah diterapkan dievaluasi untuk memastikan efektivitasnya?		✓	–
3.14	IV	2	Apakah profil risiko dan mitigasinya dikaji ulang secara berkala?		✓	–
3.15	V	3	Apakah kerangka kerja pengelolaan risiko dikaji secara berkala untuk meningkatkan efektivitasnya?		✓	–
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria penilaian kinerja pengamanan?		✓	–

Tabel C.4. Kuesioner *Checklist* Area Pengelolaan Aset

#			Pengelolaan Aset Informasi	Bukti Ada	Bukti Tidak	Keterangan
Pengelolaan Aset Informasi						
5.1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)	✓		Kartu Inventaris Aset
5.2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	✓		Pergub 35 Tahun 2020 Pasal 3
5.3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?		✓	–

Tabel C.4. Kuesioner *Checklist* Area Pengelolaan Aset (Tabel Lanjutan...)

#			Pengelolaan Aset Informasi	Bukti		Keterangan
				Ada	Tidak	
5.4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut		✓	–
5.5	II	1	Apakah tersedia proses untuk mengidentifikasi dan menginventarisir syarat retensi asset informasi sesuai dengan peraturan perundangan yang ada dan menghapusnya jika sudah melewati batas retensi tersebut		✓	–
5.6	II	1	Apakah tersedia proses untuk mengevaluasi kepatuhan terhadap syarat retensi dan menghapus aset informasi jika sudah melewati batas retensi tersebut		✓	–
5.7	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?		✓	–
5.8	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?		✓	–
5.9	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?		✓	–
			Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?		✓	–
5.10	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda		✓	–

Tabel C.4. Kuesioner *Checklist* Area Pengelolaan Aset (Tabel Lanjutan...)

#			Pengelolaan Aset Informasi	Bukti		Keterangan
				Ada	Tidak	
5.11	II	1	Tata tertib penggunaan komputer, e-mail, internet dan intranet	✓		SOP Penerimaan Nasakah Elektronik Melalui Email
5.12	II	1	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI		✓	–
5.13	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan		✓	–
5.14	II	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi		✓	–
5.15	II	1	Pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya		✓	–
5.16	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi		✓	–
5.17	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data		✓	–
5.18	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya		✓	–
5.19	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi		✓	–
5.20	II	1	Prosedur back-up dan uji coba pengembalian data (restore) secara berkala	✓		SK pengangkatan staf IT
5.21	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya		✓	–
5.22	III	2	Proses pengecekan latar belakang SDM		✓	–

Tabel C.4. Kuesioner *Checklist* Area Pengelolaan Aset (Tabel Lanjutan...)

#			Pengelolaan Aset Informasi	Bukti		Keterangan
				Ada	Tidak	
5.23	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.		✓	–
5.24	III	2	Proses dan metoda untuk penghancuran informasi yang sudah tidak diperlukan dan sesuai dengan klasifikasi informasi (mis: secure delete, jenis/kerapatan shredder dll), Termasuk didalamnya laporan bukti penghancuran informasi ?		✓	–
5.25	III	2	Prosedur kajian penggunaan akses (user access review) dan hak aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidaksesuaian (non-conformity) terhadap kebijakan yang berlaku		✓	–
5.26	III	2	Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.		✓	–
5.27	III	3	Apakah tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya?	✓		DPA Pengembangan dan Pemeliharaan Layanan Perpustakaan Elektronik
5.28	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?		✓	–
5.29	III	3	Apakah telah diterapkan proses dan metoda untuk mengaburkan data (data masking) agar hanya dapat dilihat oleh pihak yang mempunyai otoritas sesuai regulasi atau kebijakan? Mis: pengamanan data pribadi, data sensitif		✓	–

Tabel C.4. Kuesioner *Checklist* Area Pengelolaan Aset (Tabel Lanjutan...)

#			Pengelolaan Aset Informasi	Bukti		Keterangan
				Ada	Tidak	
5.30	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?		✓	–
Pengamanan Layanan Infrastruktur Awan (*Cloud Service*)						
5.31	III	2	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis cloud dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?		✓	–
5.32	III	2	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis cloud?		✓	–
5.33	III	2	Apakah instansi/perusahaan sudah menetapkan kebijakan dan menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan cloud?		✓	–
5.34	III	2	Apakah instansi/perusahaan sudah mengkaji, menetapkan pembagian tanggung jawab keamanan informasi antara perusahaan dan penyelenggara layanan cloud ?		✓	–
5.35	III	2	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis cloud?		✓	–
5.36	III	2	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan cloud terkait reputasi penyelenggaranya?		✓	–
5.37	III	2	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan cloud, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?		✓	–

Tabel C.4. Kuesioner *Checklist* Area Pengelolaan Aset (Tabel Lanjutan...)

#			Pengelolaan Aset Informasi	Bukti		Keterangan
				Ada	Tidak	
5.38	III	2	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan cloud termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?		✓	–
5.39	III	2	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan cloud?		✓	–
5.40	III	3	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan cloud atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?		✓	–
5.41	III	3	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan cloud, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?		✓	–
Pengamanan Fisik						
5.42	II	1	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	✓		Implementasi Kunci fisik, Satpam, CCTV pada ruang server
5.43	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	✓		Implementasi Finger print pada ruang server
5.44	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	✓		Fire Alarm System
5.45	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	✓		Kartu Inventaris Aset

Tabel C.4. Kuesioner *Checklist* Area Pengelolaan Aset (Tabel Lanjutan...)

#			Pengelolaan Aset Informasi	Bukti		Keterangan
				Ada	Tidak	
5.46	II	1	Apakah infrastruktur komputasi yang terpasang dapat dipantau melalui C-CTV ?	✓		Kartu Inventaris Aset
5.47	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?		✓	–
5.48	II	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?		✓	–
5.49	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?		✓	–
5.50	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	✓		DPA Pengembangan dan Pemeliharaan Layanan Perpustakaan Elektronik
5.51	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?		✓	–

Tabel C.4. Kuesioner *Checklist* Area Pengelolaan Aset (Tabel Lanjutan...)

#			Pengelolaan Aset Informasi	Bukti		Keterangan
				Ada	Tidak	
5.52	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya?		✓	–
5.53	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?		✓	–

Tabel C.5. Kuesioner *Checklist* Teknologi dan Keamanan Informasi

#			Teknologi dan Keamanan Informasi	Bukti		Keterangan
				Ada	Tidak	
Pengamanan Teknologi						
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?		✓	–
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?		✓	–
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?		✓	–
6.4	III	2	Apakah tersedia proses pengelolaan konfigurasi perangkat komputasi (server, perangkat jaringan, sistem operasi dan aplikasi) yang diterapkan secara konsisten?		✓	–

Tabel C.5. Kuesioner *Checklist* Teknologi dan Keamanan Informasi (Tabel Lanjutan...)

#			Teknologi dan Keamanan Informasi	Bukti		Keterangan
				Ada	Tidak	
6.5	IV	3	Apakah perangkat komputasi terpasang tersebut sudah dikaji ulang secara berkala sesuai dengan konfigurasi standard untuk keamanan sistem, dipantau efektivitasnya dan dimutakhirkan/disesuaikan konfigurasinya melalui proses Manajemen Perubahan (change management)?		✓	–
6.6	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?		✓	–
6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?		✓	–
6.8	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada dan efektivitas keamanannya?	✓		Aplikasi monitoring Jaringan
6.9	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?		✓	–
6.10	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?		✓	–
6.11	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?		✓	–
Catatan Periksa Logging						

Tabel C.5. Kuesioner *Checklist* Teknologi dan Keamanan Informasi (Tabel Lanjutan...)

#			Teknologi dan Keamanan Informasi	Bukti		Keterangan
				Ada	Tidak	
6.11a			[Catatan Periksa] Minimal yang harus di log adalah: 1. outbound and inbound trafik jaringan; 2. Akses terhadap sistem, server, perangkat jaringan, aplikasi kritis; 3. penggunaan file sistem dan konfigurasi jaringan; 4. dari perangkat keamanan (antivirus, IDS, IPS, web filters, firewalls, DLP); 5. event log yang berhubungan dengan sistem dan aktifitas jaringan;	✓		SOP Penerimaan Nasakah Elektronik Melalui Email
6.12	II	1	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?		✓	–
6.13	III	2	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?		✓	–
6.14	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?		✓	–
6.15	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama?		✓	–
6.16	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?		✓	–

Tabel C.5. Kuesioner *Checklist* Teknologi dan Keamanan Informasi (Tabel Lanjutan...)

#			Teknologi dan Keamanan Informasi	Bukti		Keterangan
				Ada	Tidak	
6.17	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login, dan penarikan akses?		✓	–
6.18	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?		✓	–
6.19	II	1	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	✓		Windows Defender
6.20	II	1	Apakah sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini?	✓		Windows Defender
6.21	II	1	Apakah setiap desktop dan server dilindungi dari penyerangan virus (malware)?	✓		Windows Defender
6.22	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	✓		Windows Defender
6.23	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?		✓	–
6.24	III	2	Apakah instansi/perusahaan anda secara rutin menganalisa dan menetapkan website yang membahayakan perusahaan atau tidak seharusnya diakses karyawan? Untuk selanjutnya website tersebut diblok agar tidak dapat diakses.		✓	–
6.25	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?		✓	–

Tabel C.5. Kuesioner *Checklist* Teknologi dan Keamanan Informasi (Tabel Lanjutan...)

#			Teknologi dan Keamanan Informasi	Bukti		Keterangan
				Ada	Tidak	
6.26	III	2	Apakah instansi/perusahaan anda sudah menetapkan prinsip pengembangan aplikasi yang aman (secure coding) yang digunakan untuk pengembangan aplikasi secara internal (in-house) maupun yang melibatkan pihak eksternal? misal: menggunakan standard OWASP 10		✓	–
6.27	III	2	Apakah instansi/perusahaan anda sudah menerapkan proses perencanaan pengembangan sistem? (Dengan mempertimbangkan hasil pemrograman yang tidak baik/laik pada sistem sebelumnya, konfigurasi software development tool yang aman, kontrol terhadap lingkungan pengembangan, desain arsitektur yang aman)		✓	–
6.28	III	2	Apakah instansi/perusahaan anda menerapkan proses source code review (baik secara manual atau menggunakan piranti lunak) sebelum dijalankan di lingkungan produksi?		✓	–
6.29	II	1	Apakah instansi/perusahaan anda menerapkan kontrol akses untuk source code aplikasi?		✓	–
6.30	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?		✓	–
6.31	III	3	Apakah instansi/perusahaan anda secara rutin menganalisa dan memperbaiki jika ditemukenali ancaman baru yang berdampak pada keamanan sistem aplikasi?		✓	–

Tabel C.5. Kuesioner *Checklist* Teknologi dan Keamanan Informasi (Tabel Lanjutan...)

#			Teknologi dan Keamanan Informasi	Bukti		Keterangan
				Ada	Tidak	
6.32	III	3	Apakah instansi/perusahaan anda menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun?		✓	–
6.33	III	3	Apakah instansi/perusahaan sudah menerapkan proses atau mekanisme untuk mencegah terungkapnya informasi sensitif ke luar dari perusahaan?		✓	–
6.34	IV	3	Apakah instansi/perusahaan sudah menerapkan teknologi (DLP Data Leakage Prevention) untuk mencegah terungkapnya informasi sensitif ke luar dari perusahaan?		✓	–
6.35	IV	3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?		✓	–

Tabel C.6. Kuesioner *Checklist* Pelindungan Data Pribadi

#			Pelindungan Data Pribadi	Bukti		Keterangan
				Ada	Tidak	
Pelindungan Data Pribadi						
7.1	II	1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?		✓	–
7.2	II	1	Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?		✓	–
7.3	II	1	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?		✓	–

Tabel C.6. Kuesioner *Checklist* Pelindungan Data Pribadi (Tabel Lanjutan...)

#			Pelindungan Data Pribadi	Bukti		Keterangan
				Ada	Tidak	
7.4	II	1	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Pelindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?		✓	–
7.5	II	2	Apakah instansi/perusahaan sudah menunjuk fungsi/unit Pejabat Pelindung Data Pribadi yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Pelindungan Data Pribadi?	✓		SK Pengangkatan Staf IT
7.6	II	2	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?		✓	–
7.7	III	2	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Pelindungan Data Pribadi?		✓	–
7.8	III	2	Apakah mekanisme pelindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?		✓	–
7.9	III	2	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?		✓	–
7.10	III	2	Apakah instansi/perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut?		✓	–

Tabel C.6. Kuesioner *Checklist* Pelindungan Data Pribadi (Tabel Lanjutan...)

#			Pelindungan Data Pribadi	Bukti		Keterangan
				Ada	Tidak	
7.11	III	2	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?		✓	–
7.12	III	2	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?		✓	–
7.13	III	2	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?		✓	–
7.14	III	2	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?		✓	–
7.15	III	2	Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?		✓	–
7.16	III	2	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?		✓	–

Tabel C.7. Kuesioner *Checklist* Suplemen

#			Suplemen	Bukti		Keterangan
				Ada	Tidak	
Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan						
8.1 Manajemen Risiko dan Pengelolaan Keamanan Pihak Ketiga						
8.1.1		1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?		✓	–

Tabel C.7. Kuesioner *Checklist* Suplemen (Tabel Lanjutan...)

#		Suplemen	Bukti		Keterangan
			Ada	Tidak	
8.1.2	1	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?		✓	–
8.1.3	1	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?		✓	–
8.1.4	1	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?		✓	–
8.1.5	1	Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?		✓	–
8.1.6	1	Apakah kebijakan tersebut telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?		✓	–
8.1.7	1	Apakah hak audit TI secara berkala ke pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga?		✓	–
8.2 Pengelolaan Sub-Kontraktor / Alih Daya pada Pihak Ketiga					
8.2.1	1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?		✓	–
8.2.2	1	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?		✓	–

Tabel C.7. Kuesioner *Checklist* Suplemen (Tabel Lanjutan...)

#		Suplemen	Bukti		Keterangan
			Ada	Tidak	
8.2.3	1	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?		✓	–
8.3 Pengelolaan Layanan dan Keamanan Pihak Ketiga					
8.3.1	1	Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi dalam hubungan kerjasama dengan pihak ketiga?		✓	–
8.3.2	1	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan?		✓	–
8.3.3	1	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil?		✓	–
8.3.4	1	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?		✓	–
8.3.5	1	Apakah hasil pemantauan dan evaluasi tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuannya?		✓	–
8.3.6	1	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?		✓	–
8.3.7	1	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur?		✓	–

Tabel C.7. Kuesioner *Checklist* Suplemen (Tabel Lanjutan...)

#		Suplemen	Bukti		Keterangan
			Ada	Tidak	
8.3.8	1	Apakah kondisi terkait denda/penalti karena ketidakpatuhan pihak ketiga telah didokumentasikan dan diterapkan?		✓	–
8.4 Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga					
8.4.1	1	Apakah instansi/perusahaan mengelola perubahan layanan, kebijakan, prosedur dan kontrol risiko pihak ketiga?		✓	–
8.4.2	1	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasinya?		✓	–
8.5 Penanganan Aset					
8.5.1	1	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama siklus hidup aset?		✓	–
8.5.2	1	Apakah persyaratan penghancuran data secara aman telah disepakati bersama pihak ketiga?		✓	–
8.6 Pengelolaan Insiden oleh Pihak Ketiga					
8.6.1	1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan dan analisis insiden keamanan informasi?		✓	–
8.6.2	1	Apakah pihak ketiga memiliki bukti penerapan yang memadai dalam menangani insiden keamanan informasi?		✓	–
8.7 Rencana Kelangsungan Layanan Pihak Ketiga					
8.7.1	1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk kelangsungan layanan?		✓	–
8.7.2	1	Apakah rencana tersebut telah diuji, didokumentasikan dan dievaluasi efektivitasnya?		✓	–
8.7.3	1	Apakah pihak ketiga memiliki organisasi atau tim khusus untuk mengelola kelangsungan layanan?		✓	–

Mengetahui Responden

Abdul Rohman Wahid

LAMPIRAN D
BUKTI ATAU DOKUMEN

PEMERINTAH PROVINSI RIAU		Nomor SOP	
		Tanggal Pembuatan	18 April 2022
		Tanggal Revisi	-
		Tanggal Efektif	-
		Disahkan oleh	Kepala Dinas Perpustakaan dan Kearsipan Provinsi Riau
DINAS PERPUSTAKAAN DAN KEARSIPAN			Dra. Mimi Yuliani Nazir, Apt, MM NIP. 19660717 199102 2 001
BIDANG SEKRETARIAT		Judul SOP	Penerimaan Naskah Dinas Elektronik Melalui Email
Dasar Hukum		Kualifikasi pelaksana	
1. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 152, Tambahan Lembaran Negara Republik 2. Peraturan Pemerintah Republik Indonesia Nomor 28 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 43 Tahun 2009 Tentang Kearsipan 3. Peraturan Kepala Arsip Nasional Republik Indonesia Nomor 34 Tahun 2015 tentang Pedoman Pengurusan Surat di Lingkungan Arsip Nasional Republik Indonesia 4. Peraturan Arsip Nasional Republik Indonesia Nomor 19 Tahun 2017 tentang Petunjuk Pelaksanaan Penyusunan, Pemantauan dan Evaluasi Standar Operasional Prosedur 5. Peraturan Arsip Nasional Republik Indonesia Nomor 7 Tahun 2018 tentang Tata Naskah Dinas di Lingkungan Arsip Nasional Republik Indonesia (Berita Negara 6. Peraturan Arsip Nasional Republik Indonesia Nomor 9 Tahun 2018 Tentang Pedoman Pemeliharaan Arsip Dinamis 7. Peraturan Arsip Nasional Republik Indonesia Nomor 4 Tahun 2020 Tentang Organisasi dan Tata Kerja Arsip Nasional Republik Indonesia 8. Peraturan Arsip Nasional Republik Indonesia Nomor 4 Tahun 2021 Tentang Pedoman Penerapan Sistem Informasi Kearsipan Dinamis Terintegrasi		1. Memahami tugas dan fungsi unit kerja sesuai dengan Peraturan Arsip Nasional Republik Indonesia Nomor 4 Tahun 2020 tentang Organisasi dan Tata Kerja Arsip Nasional Republik Indonesia 2. Memiliki pengetahuan dan kemampuan mengoperasikan Komputer 3. Mengetahui aplikasi komputer 4 Memiliki kemampuan menggunakan email	
Keterkaitan		Peralatan/perlengkapan	
1. SOP AP tentang Registrasi Naskah Dinas Masuk Elektronik ke Dalam Aplikasi SRIKANDI		1. File Elektronik Berupa Naskah Dinas Masuk 2. Struktur Organisasi dan Tata Kerja ANRI 3. Tautan Agenda Surat Masuk Melalui Email 4. Komputer 5. Akun Email ANRI 6. Aplikasi SRIKANDI 7. Jaringan Internet	
Peringatan		Pencatatan dan pendataan	
Jika SOP ini tidak dilaksanakan, maka dapat mengakibatkan informasi surat tidak tersampaikan		Disimpan sebagai elektronik dan manual	

Gambar D.1. SOP Penggunaan Email, *Backup, Restore, Exit Server*

PEMERINTAH PROVINSI RIAU
BADAN KEPEGAWAIAN DAERAH
Jln. Cut Nyak Dien Tlp. (0761) 21172, 848593, 28997, 33073 Fax. (0761) 21172, 22513,28997
PEKANBARU – RIAU

PETIKAN
KEPUTUSAN GUBERNUR RIAU
NOMOR: Kpts. 363/IV/2021
TENTANG
PENGANGKATAN DALAM JABATAN FUNGSIONAL PRANATA KOMPUTER PEGAWAI NEGERI SIPIL DI LINGKUNGAN PEMERINTAH PROVINSI RIAU ATAS NAMA ADINDA FIANDINI, S.S.T dkk
GUBERNUR RIAU,

Menimbang :)
Mengingat :))) dan sebagainya

MEMUTUSKAN :

Menetapkan :

KESATU : Pengangkatan dalam Jabatan Fungsional Pranata Komputer Pegawai Negeri Sipil di Lingkungan Pemerintah Provinsi Riau atas nama ADINDA FIANDINI, S.S.T dkk.

KEDUA : Pegawai Negeri Sipil : Nomor Urut **1**
Nama : **ADINDA FIANDINI, S.S.T**
NIP : 19900831 201903 2 001
Tempat, Tanggal Lahir : Pekanbaru, 31 Agustus 1990
Pangkat / Gol. Ruang : Penata Muda (Gol. III/a)
Pendidikan : D-IV Teknik Informatika
Unit Kerja : Dinas Perpustakaan dan Kearsipan Provinsi Riau
diangkat dalam Jabatan Fungsional Pranata Komputer Ahli Pertama dengan angka kredit sebesar 116,815 (TMT PAK: 27-11-2020).

KETIGA : Pegawai Negeri Sipil sebagaimana dimaksud pada Diktum Kedua selama memangku jabatan diberikan tunjangan Jabatan Fungsional Pranata Komputer sesuai dengan peraturan perundang-undangan.

KEEMPAT : Petikan Keputusan Gubernur ini disampaikan kepada Pegawai Negeri Sipil sebagaimana dimaksud pada Diktum Kedua untuk diketahui dan dipergunakan sebagaimana mestinya.

KELIMA : Keputusan ini mulai berlaku pada tanggal ditetapkan.

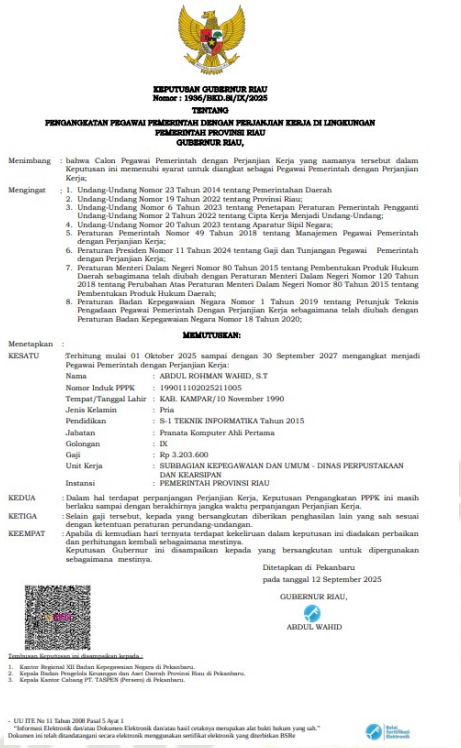
Ditetapkan di Pekanbaru
pada tanggal 1 April 2021

GUBERNUR RIAU
dto
SYAMSUAR

Petikan sesuai dengan aslinya
KEPALA BADAN KEPEGAWAIAN DAERAH PROVINSI RIAU,

IRWAN RIDWAN, SH, M.Si
Pembina Utama Muda
NIP. 19650904 199703 1 001

Gambar D.2. SK Pengangkatan Koordinator IT



KEPUTUSAN GUBERNUR RIAU
Nomor : 1936/BKD.SI/IX/2025
TENTANG
PENGANGKATAN PEGAWAI PEMERINTAH DENGAN PERJANJIAN KERJA DI LINGKUNGAN PEMERINTAH PROVINSI RIAU
GUBERNUR RIAU,

Menimbang : bahwa Calon Pegawai Pemerintah dengan Perjanjian Kerja yang namanya tersebut dalam Keputusan ini memenuhi syarat untuk diangkat sebagai Pegawai Pemerintah dengan Perjanjian Kerja;

Mengingat : 1. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah
2. Undang-Undang Nomor 19 Tahun 2022 tentang Provinsi Riau;
3. Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang;
4. Undang-Undang Nomor 20 Tahun 2023 tentang Aparatur Sipil Negara;
5. Peraturan Pemerintah Nomor 49 Tahun 2018 tentang Manajemen Pegawai Pemerintah dengan Perjanjian Kerja;
6. Peraturan Presiden Nomor 11 Tahun 2024 tentang Gaji dan Tunjangan Pegawai Pemerintah dengan Perjanjian Kerja;
7. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah sebagimana telah diubah dengan Peraturan Menteri Dalam Negeri Nomor 120 Tahun 2018 tentang Perubahan Atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah;
8. Peraturan Badan Kepegawaian Negara Nomor 1 Tahun 2019 tentang Petunjuk Teknis Pengadaan Pegawai Pemerintah Dengan Perjanjian Kerja sebagaimana telah diubah dengan Peraturan Badan Kepegawaian Negara Nomor 18 Tahun 2020;

MEMUTUSKAN:

Menetapkan :

KESATU Terhitung mulai 01 Oktober 2025 sampai dengan 30 September 2027 mengangkat menjadi Pegawai Pemerintah dengan Perjanjian Kerja:

Nama	: ABDUL ROHMAN WAHID, S.T
Nomor Induk PPPK	: 199011102025211005
Tempat/Tanggal Lahir	: KAB. KAMPAR/10 November 1990
Jenis Kelamin	: Pria
Pendidikan	: S-1 TEKNIK INFORMATIKA Tahun 2015
Jabatan	: Pranata Komputer Ahli Pertama
Golongan	: IX
Gaji	: Rp 3.203.600
Unit Kerja	: SUBBAGIAN KEPEGAWAIAN DAN UMUM - DINAS PERPUSTAKAAN DAN KEARSIPAN
Instansi	: PEMERINTAH PROVINSI RIAU

KEDUA : Dalam hal terdapat perpanjangan Perjanjian Kerja, Keputusan Pengangkatan PPPK ini masih berlaku sampai dengan berakhirnya jangka waktu perpanjangan Perjanjian Kerja.

KETIGA : Selain gaji tersebut, kepada yang bersangkutan diberikan penghasilan lain yang sah sesuai dengan ketentuan peraturan perundang-undangan.

KEEMPAT : Apabila di kemudian hari ternyata terdapat kekeliruan dalam keputusan ini diadakan perbaikan dan perhitungan kembali sebagaimana mestinya.
Keputusan Gubernur ini disampaikan kepada yang bersangkutan untuk dipergunakan sebagaimana mestinya.

Ditetapkan di Pekanbaru
pada tanggal 12 September 2025

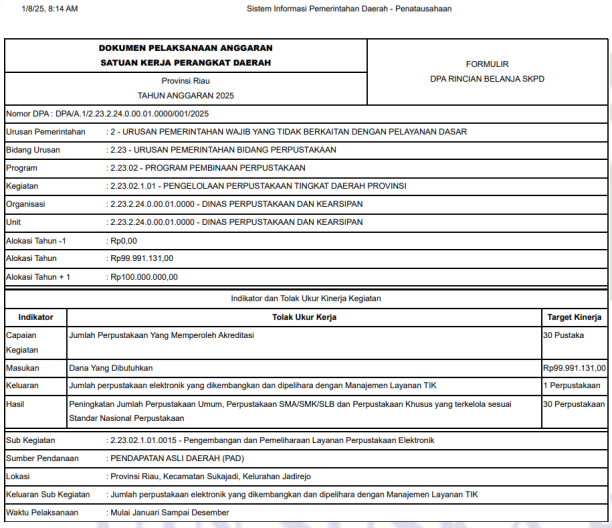
GUBERNUR RIAU,

ABDUL WAHID

Tembusan Keputusan ini disampaikan kepada :
1. Kantor Regional XII Badan Kepegawaian Negara di Pekanbaru.
2. Kepala Badan Pengelola Keuangan dan Aset Daerah Provinsi Riau di Pekanbaru.
3. Kepala Kantor Cabang PT. TASPEN (Persero) di Pekanbaru.

- UU ITE No 11 Tahun 2008 Pasal 5 Ayat 1
"Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan BSRe

Gambar D.3. SK Pengangkatan Staf IT



1/8/25, 8:14 AM Sistem Informasi Pemerintahan Daerah - Penatausahaan

DOKUMEN PELAKSANAAN ANGGARAN SATUAN KERJA PERANGKAT DAERAH	FORMULIR DPA RINCIAN BELANJA SKPD
Provinsi Riau TAHUN ANGGARAN 2025	

Nomor DPA : DPA/A.1/2.23.2.24.0.00.01.0000/001/2025	
Urusan Pemerintahan	: 2 - URUSAN PEMERINTAHAN WAJIB YANG TIDAK BERKAITAN DENGAN PELAYANAN DASAR
Bidang Urusan	: 2.23 - URUSAN PEMERINTAHAN BIDANG PERPUSTAKAAN
Program	: 2.23.02 - PROGRAM PEMBINAAN PERPUSTAKAAN
Kegiatan	: 2.23.02.1.01 - PENGELOLAAN PERPUSTAKAAN TINGKAT DAERAH PROVINSI
Organisasi	: 2.23.2.24.0.00.01.0000 - DINAS PERPUSTAKAAN DAN KEARSIPAN
Unit	: 2.23.2.24.0.00.01.0000 - DINAS PERPUSTAKAAN DAN KEARSIPAN
Alokasi Tahun -1	: Rp0,00
Alokasi Tahun	: Rp99.991.131,00
Alokasi Tahun + 1	: Rp100.000.000,00

Indikator dan Tolak Ukur Kinerja Kegiatan

Indikator	Tolak Ukur Kerja	Target Kinerja
Capaian Kegiatan	Jumlah Perpustakaan Yang Memperoleh Akreditasi	30 Pustaka
Masukan	Dana Yang Dibutuhkan	Rp99.991.131,00
Keluaran	Jumlah perpustakaan elektronik yang dikembangkan dan dipelihara dengan Manajemen Layanan TIK	1 Perpustakaan
Hasil	Peningkatan Jumlah Perpustakaan Umum, Perpustakaan SMA/SMK/SLB dan Perpustakaan Khusus yang terkelola sesuai Standar Nasional Perpustakaan	30 Perpustakaan

Sub Kegiatan	: 2.23.02.1.01.0015 - Pengembangan dan Pemeliharaan Layanan Perpustakaan Elektronik
Sumber Pendanaan	: PENDAPATAN ASLI DAERAH (PAD)
Lokasi	: Provinsi Riau, Kecamatan Sukajadi, Kelurahan Jadirejo
Keluaran Sub Kegiatan	: Jumlah perpustakaan elektronik yang dikembangkan dan dipelihara dengan Manajemen Layanan TIK
Waktu Pelaksanaan	: Mulai Januari Sampai Desember

Gambar D.4. DPA - Pengembangan dan Pemeliharaan Layanan Perpustakaan Elektronik

SALINAN

GUBERNUR RIAU

PERATURAN GUBERNUR RIAU
NOMOR 35 TAHUN 2020

TENTANG

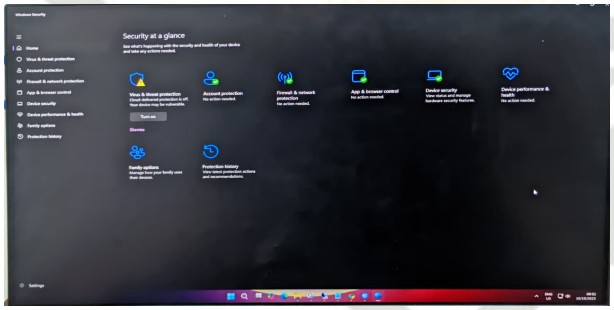
SISTEM KLASIFIKASI KEAMANAN DAN AKSES ARSIP DINAMIS
DI LINGKUNGAN PEMERINTAH PROVINSI RIAU

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR RIAU,

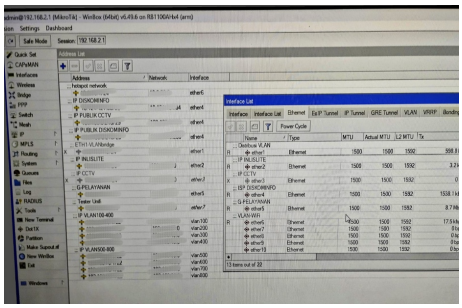
Gambar D.5. Peraturan Gubernur Nomor 35 Tahun 2020

Gambar D.6. Kartu Inventaris Barang (KIB) 2024

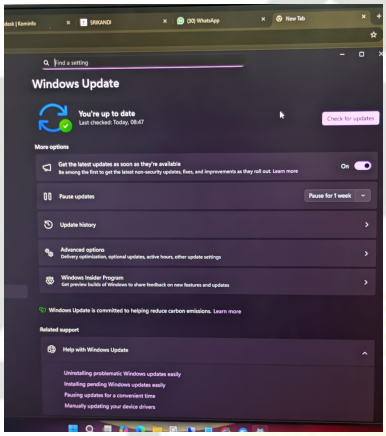


Gambar D.7. Penggunaan Perlindungan *Malware*

Gambar D.8. Finger Print Pengamanan Fasilitas Fisik



Gambar D.9. Aplikasi Monitor Jaringan



Gambar D.10. Perangkat Komputer dengan Sistem Operasi Terbaru

Gambar D.11. Dokumentasi Wawancara

DAFTAR RIWAYAT HIDUP

Ahsan Khoirul Anam lahir pada tanggal 20 Maret 2003 di Bengkalis . merupakan anak ketiga dari tiga bersaudara, putra dari Bapak Sumari Zen dan Ibu Rofikoh. Saat ini bertempat tinggal di Kecamatan Rupat, Kabupaten Bengkalis, Provinsi Riau. Pada tahun 2008, peneliti memulai pendidikan di TK Tunas Harapan Tanjung Kapal, dan lulus pada 2009. Peneliti melanjutkan pendidikan di Sekolah Dasar 19 Tanjung Kapal dan selesai pada tahun 2015. Lalu melanjutkan Sekolah Lanjut Tingkat Pertama (SLTP) di Madrasah Tsanawiyah Negeri 5 Bengkalis dan selesai pada tahun 2018. Peneliti kemudian melanjutkan pendidikan tingkat Sekolah Lanjut Tingkat Atas (SLTA) di Madrasah Aliyah Ar Ridho Batu Panjang, dan lulus pada tahun 2021. Pada tahun yang sama, peneliti diterima sebagai mahasiswa Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau. Dalam Tugas Akhir pada jenjang pendidikan tinggi, peneliti menulis skripsi dengan ”Evaluasi Tata Kelola Keamanan Informasi Pada Dinas Perpustakaan Dan Kearsipan Provinsi Riau Menggunakan Indeks KAMI”.