EVALUASI KEAMANAN INFORMASI PADA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN KEDIRI DENGAN MENGGUNAKAN INDEKS KAMI

SKRIPSI

Untuk memenuhi sebagian persyaratan
Memperoleh gelar Sarjana Komputer

Disusun oleh:
Janet Wulandari
NIM: 175150401111008

PROGRAM STUDI SISTEM INFORMASI
JURUSAN SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
2021

PENGESAHAN

EVALUASI KEAMANAN INFORMASI PADA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN KEDIRI DENGAN MENGGUNAKAN INDEKS KAMI

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun Oleh :
Janet Wulandari
NIM: 175150401111008

Skripsi ini telah diuji dan dinyatakan lulus pada

30 Juni 2021

Telah diperiksa dan disetujui oleh:

Dosen Pembimbing I	Dosen Pembimbing II
digitally signed by Yusi Tyroni Mursityo 08/07/2021	Digitally signed by Widhy H_N_ Putra DN: C=ID, OU=FILKOM, O=UB, CN=Widhy H_N_ Putra, E=widhy@ub.ac.id Reason: I am approving this document Date: 2021-07-13 08:38:43
Yusi Tyroni Mursityo, S.Kom., M.AB.	Widhy Hayuhardhika Nugraha Putra, S.Kom., M.Kom.
NIP: 198002282006041001	NIK: 201712 870409 2 001

Mengetahui
Ketua Jurusan Sistem Informasi

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI UNIVERSITAS BRAWIJAYA FAKULTAS ILMU KOMPUTER JURUSAN SISTEM INFORMASI

Issa Arwani, S.Kom., M.Sc.
NIP: 198309222012121003

PERNYATAAN ORISINALITAS

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, di dalam naskah skripsi ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu perguruan tinggi, dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis disitasi dalam naskah ini dan disebutkan dalam daftar referensi.

Apabila ternyata didalam naskah skripsi ini dapat dibuktikan terdapat unsur-unsur plagiasi, saya bersedia skripsi ini digugurkan dan gelar akademik yang telah saya peroleh (sarjana) dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku (UU No. 20 Tahun 2003, Pasal 25 ayat 2 dan Pasal 70).

Malang, 15 Juni 2021

Janet Wulandari

NIM: 175150401111008

ABSTRAK

Janet Wulandari, Evaluasi Keamanan Informasi Pada Dinas Komunikasi dan Informatika Kabupaten Kediri Dengan Menggunakan Indeks KAMI

Pembimbing: Yusi Tyroni Mursityo, S.Kom., M.AB., dan Widhy Hayuhardhika Nugraha Putra, S.Kom., M.Kom.

Dinas Komunikasi dan Informatika Kabupaten Kediri adalah lembaga pemerintah yang terletak di Kabupaten Kediri yang menjalankan urusan pemerintahan daerah pada bidang persandian, statistik, informatika dan komunikasi di wilayah Kabupaten Kediri. Dalam menjalankan proses kerjanya, Dinas Komunikasi dan Informatika Kabupaten Kediri menerapkan teknologi Informasi sehingga data dan informasi yang dihasilkan semakin banyak dan harus dikelola dan dilindungi dengan baik karena data dan informasi adalah aset yang sangat bernilai dan berharga. Untuk melindungi data dan informasi yang ada, maka diperlukan penerapan pengamanan informasi sesuai Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Belum pernah dilakukan evaluasi keamanan informasi juga mendukung perlunya evaluasi untuk mengetahui kondisi keamanan informasi saat ini. Tujuan evaluasi ini adalah untuk melakukan pengukuran terhadap tingkat kelengkapan dan tingkat kematangan pengamanan menggunakan Indeks KAMI versi 4.1 Hasil dari evaluasi ini dijadikan sebagai acuan dalam penyusunan rekomendasi perbaikan berdasarkan kelengkapan standar ISO/IEC 27001:2013. Skor yang didapatkan dari evaluasi pada tingkat kelengkapan sebesar 163 dan tingkat kelengkapannya dinyatakan belum layak berdasarkan standar yang didefinisikan ISO/IEC 27001:2013. Untuk tingkat kematangan berada pada level I hingga I+ dan. Sehingga terdapat 15 rekomendasi yang diusulkan pada area tata kelola, 17 rekomendasi yang diusulkan pada area pengelolaan risiko, 28 rekomendasi yang diusulkan pada area kerangka kerja, 32 rekomendasi yang diusulkan pada area pengelolaan aset, 15 rekomendasi yang diusulkan pada area teknologi dan 9 rekomendasi yang diusulkan pada area suplemen untuk meningkatkan kualitas keamanan informasi. Rekomendasi yang diberikan yakni seperti menetapkan kebijakan keamanan informasi, dan saran lainnya yang diajukan untuk menerapkan standar ISO/IEC 27001:2013.

Kata Kunci: Indeks KAMI; ISO 27001:2013; Keamanan Informasi; Evaluasi

ABSTRACT

Janet Wulandari, Evaluation of Information Security at the Office of Communication and Informatics of Kediri Regency Using KAMI Index

Supervisors: Yusi Tyroni Mursityo, S.Kom., M.AB., and Widhy Hayuhardhika Nugraha Putra, S.Kom., M.Kom.

Department of Communication and Information of Kediri Regency government agency located in Kediri Regency that carries out government affairs in the fields of communication, informatics, clothing and statistics in the Kediri Regency area. In its work process, Department of Communication and Information of Kediri Regency implements Information technology so that more data and information are produced and must be managed properly because it is a very valuable asset. To protect existing data and information, it is necessary to implement information security based on Regulation of the Minister of Communication and Information of the Republic Indonesia Number 4 of 2016 about Information Security Management System. In addition, the Department of Communication and Information Technology of Kediri Regency is vulnerable to information security disturbances that could pose a threat to information security risks. Never done an evaluation related to information security also supports the need for evaluation to determine the current situation of information security. The purpose of this evaluation is to measure the level of completeness and maturity information security at Department of Communication and Information of Kediri Regency using the KAMI Index 4.1 The results of this evaluation are used as a basic for preparing recommendations for improvement in appropriate to standart equipment the ISO / IEC 27001: 2013. From the evaluation, it is obtained that the completeness is 163 the level of completeness is declared not feasible based on the standard defined by ISO/IEC 27001:2013. For the maturity level is on levels I to I +. Based on the evaluation conducted by the Department of Communication and Informatics Kediri Regency, it was declared unfit to implementation ISO/IEC 27001:2013 standart. So there are 15 recommendations proposed on the governance area, 17 recommendations on risk management area, 28 recommendations on framework area, 32 recommendations on asset management area, 15 recommendations on technology area and 9 recommendations on supplement area to improve the quality of information security. The recommendations such as establishing an information security policy, establish information classification policy and other suggestions submitted for implementation the ISO/IEC 27001:2013 standard.

Keywords: *KAMI Index; ISO 27001:2013; Information Security; Evaluation*

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi pada saat ini sangat pesat. Disamping semakin pesatnya laju teknologi informasi, berpeluang besar untuk memunculkan risiko ancaman yang baru terkait teknologi informasi. Teknologi informasi merupakan alat yang dapat melakukan pekerjaan menggunakan informasi dan melakukan tugas terkait pemrosesan informasi (Haag dan Keen 1996, disitasi dalam Abdul 2014). Definisi informasi merupakan data yang diklasifikasi yang berguna pada proses pengambilan keputusan di sebuah organisasi (Sutabri, 2012). Dengan diterapkannya teknologi informasi, maka data dan informasi yang dihasilkan semakin banyak dan harus dikelola dan dilindungi dengan baik karena data dan informasi adalah aset yang sangat bernilai dan berharga.

Dengan memanfaatkan teknologi informasi, maka semakin banyaknya data dan informasi dan diperlukan pengamanan informasi. Berdasarkan regulasi yang dikeluarkan oleh Menteri Komunikasi dan Informatika yang tertuang dalam Peraturan Menteri Komunikasi dan Informatika nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi dan Peraturan Badan Siber dan Sandi Negara nomor 8 Tahun 2020, dijelaskan bahwa penerapan Sistem Manajemen Pengamanan Informasi wajib dilakukan oleh seluruh pihak instansi pemerintah penyelenggara sistem elektronik untuk pelayanan publik dengan kategori sistem elektronik rendah, tinggi dan strategis yang mana wajib untuk menerapkan standar SNI ISO/IEC 27001:2013. Instansi pemerintah yang memanfaatkan teknologi informasi untuk penyelenggaraan sistem elektronik adalah Dinas Komunikasi dan Informatika Kabupaten Kediri yang merupakan lembaga pemerintah yang terletak di Kabupaten Kediri dan menjalankan urusan pemerintahan pada bidang Komunikasi, Informatika, Persandian dan Statistik di wilayah Kabupaten Kediri. Dengan menjadi sebuah instansi yang memanfaatkan perkembangan teknologi informasi, maka keamanan informasi merupakan hal yang penting agar terhindar dari ancaman risiko keamanan informasi.

Berdasarkan wawancara dilakukan dengan pihak Dinas Komunikasi dan Informatika Kabupaten Kediri, dijelaskan bahwa hingga saat ini Dinas Komunikasi dan Informatika Kabupaten Kediri belum pernah dilakukan evaluasi terkait keamanan informasi untuk mengetahui gambaran terkait penerapan keamanan informasi. Narasumber menyampaikan bahwa Dinas Komunikasi dan Informatika Kabupaten Kediri rentan terhadap gangguan keamanan informasi seperti malware, dan serangan pada website dan aplikasi yang dapat menimbulkan ancaman keamanan informasi, seperti terjadi kebocoran data dan terdapat website yang berhenti operasionalnya. Sehingga hal tersebut menyebabkan kegiatan operasional Dinas Komunikasi dan Informatika Kabupaten Kediri menjadi terganggu.

Berdasarkan permasalahan diatas, maka perlu dilakukan evaluasi keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri untuk mengetahui gambaran kondisi keamanan informasi pada saat ini dan untuk mengidentifikasi penyebab terjadinya permasalahan yang berkaitan dengan keamanan informasi. Evaluasi dilakukan untuk membantu Dinas Komunikasi dan informatika Kabupaten Kediri dalam melakukan pengukuran terhadap tingkat kelengkapan dan tingkat kematangan keamanan informasi dan berupaya untuk meningkatkan kualitas pengamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Evaluasi dilakukan dengan menggunakan alat bantu indeks Keamanan Informasi (KAMI) yang disusun oleh Kementerian Komunikasi dan Informatika Republik Indonesia yang dijadikan sebagai alat untuk melakukan penilaian dalam rangka penerapan SNI ISO/IEC 27001. Indeks Keamanan Informasi (KAMI) merupakan alat ukur yang digunakan untuk mengukur tingkat kesiapan pengamanan informasi pada instansi pemerintahan. Indeks Keamanan Informasi (KAMI) juga digunakan untuk membenahi, membangun dan menerapkan pengamanan informasi. Evaluasi dilakukan pada 6 (enam) area yang dijadikan sebagai target pada penerapan keamanan informasi yang mana ruang lingkup yang dibahas pada Indeks KAMI telah memenuhi seluruh aspek keamanan yang dibahas pada standar SNI ISO/IEC 27001:2013. Evaluasi dilakukan menggunakan Indeks Keamanan Informasi (KAMI) versi 4.1 yang dikeluarkan pada bulan November tahun 2019. Pada revisi versi 4.0 disediakan modul suplemen dan terkait dengan keterlibatan pihak eksternal rantai pasok (*Supply Chain*), layanan berbasis infrastruktur awan dan perlindungan data pribadi.

Evaluasi menggunakan indeks KAMI versi 4.1 dijadikan sebagai target untuk penerapan keamanan informasi yang meliputi Kategori Sistem Elektronik untuk mengevaluasi tingkat atau kategori sistem elektronik yang digunakan pada instansi yang dikelompokkan pada tingkat Rendah, Tinggi, dan Strategis, Tata Kelola Keamanan Informasi untuk mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi. Pengelolaan Risiko Keamanan Informasi untuk mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Kerangka Kerja Keamanan Informasi untuk mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Pengelolaan Aset Informasi untuk mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Teknologi Keamanan Informasi untuk mengevaluasi kelengkapan, konsistensi, dan efektivitas penggunaan teknologi dalam pengamanan aset informasi serta suplemen mengevaluasi aspek pengamanan keterlibatan pihak ketiga sebagai penyedia layanan, Layanan berbasis cloud, dan perlindungan data pribadi. Selanjutnya, berdasarkan hasil evaluasi yang dilakukan, dijadikan sebagai dasar untuk menyusun rekomendasi perbaikan berdasarkan kontrol ISO 27001 yang nantinya dapat digunakan untuk meningkatkan kualitas keamanan informasi kedepannya.

Bertujuan untuk mengukur tingkat kesiapan pengamanan informasi, maka peneliti melakukan penelitian yang berjudul **"Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri Dengan Menggunakan Indeks KAMI".** Penelitian yang dilakukan diharapkan dapat memberikan gambaran kondisi saat ini terkait keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Kemudian rekomendasi-rekomendasi perbaikan yang diusulkan digunakan bahan pertimbangan dalam pengambilan keputusan dalam rangka peningkatan kualitas keamanan informasi.

1.2 Rumusan Masalah

1. Bagaimana hasil evaluasi terhadap tingkat kelengkapan dan tingkat kematangan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri?
2. Bagaimana hasil rekomendasi perbaikan yang diusulkan untuk meningkatkan kualitas keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri?

1.3 Tujuan

1. Mengukur tingkat kelengkapan dan tingkat kematangan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri menggunakan Indeks KAMI.
2. Memberikan rekomendasi perbaikan sebagai upaya peningkatan kualitas keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri.

1.4 Manfaat

1. Bagi Dinas Komunikasi dan Informatika Kabupaten Kediri
   a. Membantu Dinas Komunikasi dan Informatika Kabupaten Kediri melakukan penilaian terhadap tingkat kelengkapan dan tingkat kematangan pengamanan informasi dengan menggunakan Indeks KAMI.
   b. Memberikan rekomendasi perbaikan pada Dinas Komunikasi dan Informatika Kabupaten Kediri yang dapat dijadikan sebagai pertimbangan untuk meningkatkan kualitas pengamanan informasi
2. Bagi Penulis

   Manfaat yang diperoleh oleh penulis adalah dapat menambah wawasan dan meningkatkan pemahaman pada bidang keamanan informasi. Serta meningkatkan kemampuan dan pemahaman penulis terkait dengan cara penelitian dan cara penulisan yang baik.
3. Bagi Pembaca

Manfaat penelitian ini bagi para pembaca untuk menunjang penelitian selanjutnya dengan topik pembahasan yang sama kemudian dapat dijadikan sebagai bahan pembelajaran pada mata kuliah terkait tata kelola keamanan informasi.

1.5 Batasan Masalah

1. Penelitian dilakukan berfokus 7 target area keamanan informasi sesuai penilaian Indeks KAMI yaitu Kategori Sistem Elektronik, Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset Informasi, Teknologi dan Keamanan Informasi dan Suplemen.
2. Penelitian menggunakan alat bantu indeks KAMI dengan rekomendasi perbaikan berdasarkan kontrol ISO 27001:2013.

1.6 Sistematika Pembahasan

Bab I **PENDAHULUAN**

bab ini akan menguraikan mengenai latar belakang permasalahan yang dijadikan sebagai acuan dilaksanakannya penelitian ini, kemudian juga dibahas mengenai rumusan masalah, tujuan penelitian, manfaat penelitian, batasan-batasan masalah serta sistematika pembahasan.

Bab II **LANDASAN KEPUSTAKAAN**

Bab ini memberikan penjabaran singkat tentang penelitian-penelitian terdahulu yang serupa sebagai rujukan dan referensi peneliti serta menjelaskan berbagai teori yang relevan dan berkaitan dengan metode dan objek penelitian yang akan dilakukan.

Bab III **METODOLOGI PENELITIAN**

bab ini menguraikan alur dari penelitian ini serta diuraikan mengenai metode, teknik yang dimanfaatkan agar keluaran yang diharapkan sebelumnya dapat tercapai.

Bab IV **HASIL DAN ANALISIS**

Pada bab ini menjabarkan tentang hasil pengumpulan data yang telah dilakukan sebelumnya dan dijabarkan berdasarkan data yang ada.

Bab V **PEMBAHASAN**

Bab ini dijelaskan mengenai pembahasan hasil pengolahan data yang ada serta temuan penting yang didapatkan. Selain itu, pada bab ini peneliti menyusun saran rekomendasi perbaikan yang dapat bermanfaat terhadap objek penelitian.

Bab VI PENUTUP

Pada bab terakhir kesimpulan berdasar penelitian yang telah dilakukan serta terdapat saran oleh peneliti instansi terkait dan kepada penelitian selanjutnya.

BAB 2 LANDASAN KEPUSTAKAAN

2.1 Kajian Pustaka

Tabel 2. 1 Penelitian Sebelumnya

No	Nama Penelitian	Tujuan Penelitian	Metode Penelitian	Hasil dan Kesimpulan Penelitian
1.	**Nama Peneliti:** (Riswaya et al., 2020). **Judul**: Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks KAMI Untuk Persiapan Standar SNI ISO/IEC 27001 (Studi Kasus: STMIK Mardira Indonesia) **Nama Jurnal:** Jurnal Computech & Bisnis **Tahun** : 2020	- Dibutuhkannya kontrol untuk keamanan teknologi informasi yang bertujuan untuk melindungi keamanan aset informasi pada STMIK Mardira Indonesia - Mengevaluasi kesiapan dan kematangan tata kelola keamanan informasi pada STMIK Mardira Indonesia	- Indeks KAMI 4.0 dan ISO 27001:2013	- Skor yang didapatkan pada penilaian kategori sistem elektronik adalah “21” yang termasuk dalam kategori tinggi. Skor akhir pada 5 (lima) area pengamanan informasi adalah 117 dengan kategori “Tidak Layak” dan pada area suplemen adalah 0% - Salah satu rekomendasi perbaikan yang diajukan adalah sesuai dengan kontrol Annex A.5.1.1 tentang kebijakan keamanan TI dan A.6.1.1 tentang Organisasi dan Keamanan TI dan A.16.1.3 tentang pelaporan kelemahan keamanan TI

		sebagai upaya persiapan standarisasi SNI ISO/IEC 27001:2013		
2.	**Nama Peneliti:** (Ferdiansyah et al., 2019) **Judul:** Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI 4.0 Pada Lembaga UPTD XYZ **Nama Jurnal**: Jurnal Mobile and Forensics (MF) **Tahun**: 2019	- Memperoleh informasi terkait tingkat kesiapan dan tingkat kematangan keamanan informasi sesuai dengan standar ISO/IEC 27001:2013	- Indeks KAMI 4.0 dan ISO/IEC 27001:2013	- Pada penilaian kategori sistem elektronik memperoleh skor 20 termasuk pada kategori tinggi. Total Keseluruhan skor yang diperoleh adalah 245 dengan tingkat kematangan masing-masing area berada pada tingkat I sampai tingkat II dan masuk dalam kategori “Tidak Layak” untuk menerapkan sertifikasi ISO/IEC 27001:2013 - Dari hasil analisis menunjukkan bahwa diperlukannya peningkatan kualitas pengamanan informasi baik pada pihak eksternal serta pihak ketiga yang relevan serta dilakukan evaluasi dan dipantau sesuai interval waktu yang ditetapkan terhadap keamanan informasi untuk mengetahui tingkat pencapaian perbaikan yang diterapkan

Tabel 2. 2 Penelitian Sebelumnya (lanjutan)

3.	**Nama Peneliti:** (Juliharta et al., 2020) **Judul:** Penilaian Keamanan Informasi *E-Government* Menggunakan Index Keamanan Informasi (KAMI) 4.0 **Nama Jurnal:** Jurnal Teknologi Informasi dan Komputer **Tahun:** 2020	- Mengukur kesiapan pengamanan informasi dalam penyelenggaraan *e-government* pada Pemerintah Kota Denpasar untuk melakukan sertifikasi ISO 27001	- Indeks KAMI 4.0	- Penilaian Kategori sistem elektronik memperoleh skor 24 dengan kategori "Tinggi". Pada area pengamanan informasi memperoleh skor 74 dengan kategori "Tidak Layak" untuk melakukan sertifikasi ISO/IEC 27001:2013 dan pencapaian kematangan yakni pada kematangan I sampai I+. Pada area suplemen skor yang didapat adalah 0% - Sebagai upaya untuk meningkatkan kualitas pengamanan informasi, maka rekomendasi yang diberikan pada area tata kelola keamanan informasi adalah perlu menetapkan penanggung jawab pengelola sistem manajemen keamanan informasi - Rekomendasi pada area pengelolaan risiko adalah menyusun kerangka kerja manajemen risiko, penetapan tanggung jawab pengelola risiko dan menetapkan langkah pengembangan pengelolaan risiko - Rekomedasi pada kerangka kerja manajemen risiko adalah perlu pendokumentasian terhadap kerangka kerja sistem manajemen keamanan

				informasi dan proses uji coba sesuai dengan jadwal yang direncanakan dan proses monitoring serta evaluasi secara berkelanjutan - Pada pengelolaan aset informasi, rekomendasi yang diberikan adalah harus melakukan pengelolaan dan pendokumentasian terhadap aset informasi yang digunakan serta menentukan pengelola aset yang bertanggung jawab terhadap aset tersebut dan dilakukan evaluasi serta monitoring secara berkala - Pada area teknologi dan keamanan informasi, rekomendasi yang diajukan adalah harus dilakukan dokumentasi terkait dengan kelengkapan, proses evaluasi efektivitas penggunaan teknologi informasi, melakukan monitoring terhadap teknologi yang diterapkan dalam rangka untuk mendeteksi kelemahan, dan melakukan pemuktahiran - Pada area suplemen, rekomendasi yang diajukan adalah perlu ditetapkan *Memorandum of Understanding* (MoU)

				bersama pihak ketiga untuk melaksanakan pengamanan informasi terhadap layanan yang digunakan
4.	**Nama Peneliti:** (Hambali & Musa, 2020) **Judul:** *Analysis Of Governance Security Management Information System Using Index KAMI in Central Government Institution* **Nama Jurnal:** Angkasa: Jurnal Ilmiah Bidang Teknologi **Tahun:** 2020	- Mengukur tingkat kelengkapan dan tingkat kematangan keamanan informasi berdasarkan standar ISO/IEC 27001:2013 untuk persiapan dalam melakukan sertifikasi Sistem Manajemen Keamanan Informasi (SMKI) sesuai dengan kontrol ISO/IEC 27001:2013	- Indeks KAMI 4.0 dan ISO/IEC 27001:2013	- Skor pada penilaian kategori sistem elektronik adalah 30 dengan kategori "Tinggi". Skor yang diperoleh pada area Tata Kelola adalah 84, Pengelolaan Risiko adalah 35, Kerangka Kerja 61, Pengelolaan Aset 126, Teknologi Informasi 100. Total skor pada area pengamanan informasi adalah 408 dengan tingkat kematangan pada I+ sampai II+ dan termasuk kategori "Perlu Perbaikan" dan berada pada kondisi penerapan kerangka kerja dasar. - Rekomendasi yang diajukan yakni berdasarkan pada ISO/IEC 27001:2013 yang salah satunya adalah kontrol Annex A.12.1.3 tentang *capacity management* - Sebagai upaya peningkatan kualitas keamanan informasi maka rekomendasi yang diberikan yakni diperlukannya pendokumentasikan secara jelas terhadap kebijakan dan prosedur keamanan informasi dengan dilakukan uji coba dan monitoring kebijakan dan prosedur

				keamanan informasi secara berkelanjutan - Perkembangan dari implementasi SMKI harus didokumentasikan dan dikomunikasikan dengan pimpinan instansi dengan tujuan dapat dilakukan pengambilan keputusan yang tepat dan cepat agar dalam setiap permasalahan yang ada dapat terselesaikan dengan baik
5.	**Nama Peneliti:** (Pamungkas & Saputra, 2020) **Judul:** Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013 **Nama Jurnal:** Jurnal Komputer dan Informatika (JSON) **Tahun:** 2017	- Menganalisa kesiapan keamanan informasi pada SMA N 1 Sentolo sebagai sekolah yang telah menerapkan teknologi informasi	- Indeks KAMI 4.0	- Penilaian kategori sistem elektronik memperoleh skor “16” dan termasuk dalam kategori “Tinggi”. Skor Penilaian pada 5 (lima) area pengamanan informasi adalah 512 dan termasuk dalam kategori “Cukup Baik” dengan tingkat kematangan II hingga III+ - Pada area suplemen, pada Pengamanan Keterlibatan Pihak Ketiga memperoleh nilai persentase 91%, Pengamanan Layanan Infrastruktur Awan memperoleh nilai persentase 53%, dan Perlindungan Data Pribadi dengan nilai persentase 92% - Untuk area yang paling baik adalah pengelolaan aset karena mendekati standar penerapan ISO 27001:2013

6.	**Nama Peneliti:** (Thompson et al., 2019) **Judul:** *Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand* **Nama Jurnal:** *Government Information Quarterly* **Tahun:** 2019	- Melakukan audit terhadap keamanan informasi pada *e-government* di Australia dan Thailand	- Analisis konten web kebijakan situs dan audit keamanan informasi	- Penerapan enkripsi sangat rendah pada situs *e-goverment* di Australia hanya 50% dan 35 % di Thailand - Pada situs Australia kebijakan pribadi terdapat pada 20 situs, penolakan 19 situs, kebijakan keamanan sebanyak 17 situs dan syarat penggunaan sebanyak 1 situs. Pada situs Thailand kebijakan pribadi sebanyak 8 situs, penolakan sebanyak 9 situs, kebijakan keamanan sebanyak 8 situs dan syarat penggunaan sebanyak 9 situs. - Dalam hal kerentanan, 45% situs Australia termasuk dalam tingkat kerentanan yang tinggi dan 75% situs berada dalam kerentanan sedang serta keseluruhan situs berada pada kerentanan yang rendah - Pada situd Thailand, 60% situs termasuk dalam tingkat kerentanan yang tinggi dan 65% situs berada dalam kerentanan sedang serta keseluruhan situs berada pada kerentanan yang rendah

Tabel 2. 3 Penelitian Sebelumnya (lanjutan)

7.	**Nama Peneliti:** (Syreyshchikova et al., 2019) **Judul:** *Information Safety Process Development According to ISO 27001 for an Industrial Enterprise* **Nama Jurnal:** *The 12th International Conference Interdisciplinarity in Engineering (Procedia Manufacturing)* **Tahun:** 2019	- Melakukan evaluasi sistem elektronik pada Industri JSC "K" serta merancang, mengembangkan proses keamanan informasi berdasarkan persyaratan ISO/IEC 27001:2013	- ISO 27001:2013	- Melakukan pengembangan proses keamanan informasi yakni kebijakan, tujuan dan prosedur keamanan informasi - Membatasi akses terhadap pemrosesan informasi - Penggunaan kode kriptografi dalam melakukan transfer informasi - Menerapkan penyimpanan informasi yang terenkripsi - Menerapkan proses untuk melakukan pengumpulan informasi yang terjadi dalam sistem dengan log

Terdapat penelitian terdahulu yang serupa terkait dengan evaluasi keamanan informasi yang dijadikan sebagai acuan dalam melakukan penelitian ini. Penelitian-penelitian tersebut dijadikan sebagai bahan referensi dan rujukan yang digunakan untuk menunjang penelitian yang dilakukan. Terdapat 7 (tujuh) referensi yang digunakan oleh peneliti sebagai tambahan informasi pada penelitian yang dipetakan pada tabel 2.1 diatas dengan penjabaran sebagai berikut ini:

Penelitian oleh (Riswaya et al., 2020) menjelaskan bahwa keamanan informasi adalah hal penting pada sebuah organisasi yang memanfaatkan layanan teknologi informasi dalam proses bisnisnya untuk menjaga aset-aset perusahaan yang diantaranya adalah *hardware*, *software*, *database, file server*, dan aset personal untuk menjaga kerahasiaan, keutuhan dan ketersediaan aset-aset tersebut. Sehingga perlu dilakukan evaluasi kesiapan pengamanan informasi pada Pusat Teknologi dan Komputer (PUSKOMTEK) pada STMIK Mardira Indonesia yang bertanggung jawab untuk memelihara aset-aset teknologi informasi di STMIK yang diantaranya adalah perangkat komputer, CCTV, *Access Point*, jaringan internet serta intranet dan laboratorium pembelajaran. Kemudian, pada PUSKOMTEK hingga saat ini belum pernah dilakukan evaluasi keamanan informasi untuk menganalisis penyebab terjadinya gangguan pada teknologi informasi dan belum mengetahui sejauh mana tingkatan pengamanan informasi yang telah diterapkan pada STMIK-MI.

Dari permasalahan diatas diperlukan pengukuran tingkat kesiapan pengamanan informasi dan dilanjutkan dengan menyusun rekomendasi perbaikan. Dari analisis yang telah dilakukan, didapatkan bahwa hasil penilaian pada kategori sistem elektronik pada instansi mendapat skor 21 dan termasuk dalam tingkat tinggi. Pada area pengamanan informasi total skor yang didapat adalah 117 dengan tingkat kematangan I dan masuk dalam level "Tidak Layak" yang berarti tingkat kelengkapan penerapan berdasarkan ISO 27001 tidak terpenuhi dan tidak layak untuk melakukan sertifikasi ISO 27001. Korelasi dengan penelitian ini adalah penggunaan alat evaluasi indeks KAMI untuk mengukur tingkat kesiapan pengamanan informasi. Serta rekomendasi yang ada adalah berdasarkan ISO 27001 dan dapat dijadikan sebagai rujukan oleh penulis sebagai upaya untuk meningkatkan kualitas pengamanan informasi pada objek terkait.

Kemudian penelitian oleh (Ferdiansyah et al., 2019), penelitian ini menjelaskan bahwa seiring semakin pesatnya perkembangan teknologi informasi sebanding terhadap tingkat risiko teknologi informasi. Sehingga pengamanan informasi yang berkualitas sangat diperlukan agar terbebas dari segala aktivitas pada sistem yang tidak berwenang, yakni perubahan data, penghapusan data, dan pencurian data. Sehingga, dengan banyaknya data dan informasi serta aset yang dimiliki, diperlukan evaluasi untuk mengetahui tingkat kelengkapan dan kematangan keamanan informasi dan diharapkan dapat menghasilkan usulan rekomendasi perbaikan keamanan informasi. Skor yang diperoleh pada penilaian

kategori sistem elektronik adalah 10 dengan kategori "Tinggi". Total skor pada area pengamanan informasi adalah 245 dengan tingkat kematangan I+ hingga II dan termasuk dalam kategori "Tidak Layak". Korelasi dengan penelitian ini adalah pengunaan Indeks KAMI 4.0 yang dijadikan acuan oleh peneliti dalam melakukan evaluasi keamanan informasi pada objek terkait.

Referensi selanjutnya adalah penelitian oleh (Juliharta et al., 2020). Dijelaskan bahwa bertujuan untuk meningkatkan layanan kepada masyarakat, pemerintah memanfaatkan *e-government*. Salah satunya adalah Pemerintah Kota Denpasar yang dikelola oleh Dinas Komunikasi dan Informatika Kota Denpasar yang mana saat ini bergabung dalam gerakan menuju 100 *smart city* Indonesia. Untuk menerapkan pengamanan informasi, maka perlu dilakukan evaluasi terhadap kesiapan kerangka kerja keamanan informasi menggunakan instrument yang telah dikembangkan oleh Badan Siber Sandi Negara (BSSN) yaitu Indeks KAMI 4.0. Pengukuran kesiapan pengamanan informasi pada Pemerintah Kota Denpasar dilakukan untuk mempersiapkan penyelenggaran *e-government* dalam melakukan sertifikasi ISO/IEC 27001. Hasil penilaian kategori sistem elektronik memperoleh skor 24 dengan kategori "Tinggi". Total skor pada Area pengamanan informasi adalah 74 dengan tingkat kematangan I hinggan II+ dan termasuk dalam kategori "Tidak Layak" untuk menerapkan sertifikasi ISO/IEC 27001:2013. Berdasarkan diagram *radar chart*, area yang memenuhi kerangka kerja dasar adalah Tata Kelola Keamanan Informasi dan Aspek Teknologi. (Juliharta et al., 2020). Area belum memenuhi kerangka kerja dasar adalah Pengelolaan Risiko, Kerangka Kerja dan Pengelolaan Aset. Korelasi dengan penelitian ini adalah penilaian terhadap kesiapan pengamanan informasi untuk meningkatkan kualitas pengamanan informasi dalam rangka menerapkan sertifikasi ISO 27001.

Pada penelitian selanjutnya oleh (Hambali & Musa, 2020) dijelaskan bahwa teknologi informasi sangat dibutuhkan dalam menjalankan proses bisnis pada organisasi. Sehingga keamanan infomasi menjadi hal yang sangat penting karena keamanan informasi akan berpengaruh terhadap kegiatan operasional suatu instansi. Pada Unit Kerja X di Instansi Pemerintah Pusat saat ini memanfaatkan perkembangan teknologi informasi untuk memberikan kualitas pelayanan yang baik kepada pihak internal dan pihak eksternal. Kemudian keamanan informasi juga diterapkan agar terhindar dari risiko dan ancaman keamanan informasi yang dapat menganggu ketersediaan, kerahasiaan dan keutuhan data dan informasi. Pada Unit Kerja X akan diterapkan Sistem Manajemen Keamanan Informasi berdasar standar ISO/IEC 27001:2013. Sebelum penerapannya, maka akan dilakukan evaluasi terhadap tingkat kesiapan dan tingkat kematangan pengamanan informasi berdasarkan dengan ISO/IEC 27001:2013. Pada area kategori sistem elektronik memperoleh skor 30 dan termasuk dalam kategori "Tinggi". Pada area pengamanan informasi total skor yang diperoleh adalah 408 dan termasuk dalam kategori "Perlu Perbaikan" dengan tingkat kematangan I+ hingga II+. Korelasi dengan penelitian ini adalah

adalah penggunaan alat evaluasi indeks KAMI untuk mengukur tingkat kelengkapan dan kematangan pengamanan informasi. Serta rekomendasi yang ada adalah berdasarkan ISO 27001 dan dapat dijadikan sebagai rujukan oleh penulis sebagai upaya untuk meningkatkan kualitas pengamanan informasi pada objek terkait.

Referensi kelima penelitian yang dilakukan oleh (Pamungkas & Saputra, 2020). Pada penelitian ini dijelaskan bahwa sekolah adalah sarana anak-anak untuk memperoleh ilmu dan pengetahuan sehingga perlu melengkapi fasilitas yang berguna untuk mendukung proses belajar mengajar yang salah satunya adalah SMAN 1 Sentolo. Hal ini disebabkan bahwa infrastruktur teknologi informasi yang diterapkan telah memadai. Dengan diterapkannya teknologi informasi, sudah selayaknya keamanan informasi yang baik diperlukan untuk menjaga kerahasiaan, keutuhan dan ketersediaan data dengan baik. Oleh sebab itu dilakukan analisis terkait keamanan informasi pada SMAN 1 Sentolo untuk mengetahui tingkat kesiapan pengamanan informasi pada sekolah tersebut. Dari hasil analisis yang telah dilakukan diperoleh skor kategori sistem elektronik adalah "16" dan termasuk tingkat tinggi. Pada area pengamanan informasi menghasilkan skor 512 dan berada pada tingkat "Cukup Baik" serta tingkat kematangan berada pada tingkat kematangan II hingga III+. Area yang mendekati standar penerapan ISO 27001 adalah pengelolaan aset. Korelasi dengan penelitian ini adalah penggunaan alat evaluasi indeks KAMI untuk mengukur tingkat kelengkapan dan kematangan pengamanan informasi. Serta rekomendasi yang ada adalah berdasarkan ISO 27001 dan dapat dijadikan sebagai rujukan oleh penulis sebagai upaya untuk meningkatkan kualitas pengamanan informasi pada objek terkait.

Penelitian yang dilakukan oleh (Thompson et al., 2019) mendefinisikan *e-government* adalah sebuah kemampuan pemerintah dalam menyebarkan informasi layanan kepada masyarakat luas untuk mendukung bisnis yang dapat menghemat biaya dan waktu. Penelitian ini melakukan penelitian terhadap keamanan situs web *e-goverment* pada 2 (dua) negara yakni Australia yang memiliki penerapan *e-government* yang tinggi dan Thailand sebagai negara berkembang. Penelitian dilakukan menggunakan metode analisis konten web dari kebijakan situs dan enkripsi dan audit keamanan informasi yang bertujuan untuk mengetahui kerentanan terhadap pelanggaran keamanan informasi yang dilakukan pada 20 halaman situs *e-government* pada 40 domain. Berdasarkan dari penelitian yang dilakukan, diperoleh hasil bahwa keamanan informasi yang baik perlu diterapkan pada instansi pemerintah. Dimana pada situs *e-government* Australia hanya 50% situs yang menerapkan enkripsi serta di Thailad yang menerapkan enkripsi hanya 35%. Korelasi dengan penelitian ini adalah berkaitan dengan keamanan informasi yang dapat dijadikan sebagai rujukan peneliti dalam menyusun rekomendasi perbaikan.

Referensi terakhir oleh (Pimenov et al., 2019). Pada penelitian ini dijelaskan bahwa sebagian besar perusahaan telah menjalankan proses bisnisnya

menggunakan teknologi informasi. Data di proses menggunakan sistem informasi yang memiliki nilai tinggi sehingga data merupakan aset yang sangat bernilai bagi perusahaan. Sehingga, diperlukannya perlindungan informasi yang baik agar informasi dapat dilindungi kerahasiaan, integritas dan keutuhannya dan terhindar dari ancaman risiko keamanan informasi. Perusahaan Industri JSC "K" saat ini memerlukan perlindungan tepat waktu terhadap proses informasi perusahaan. Permasalahan yang teridentifikasi pada perusahaan industri JSC "K" adalah terjadinya pengungkapan informasi kepada pihak ketiga yang tidak memiliki wewenang, terjadinya akses tidak sah ke informasi, rendahnya kualifikasi dalam perlindungan informasi, kurangnya pemahaman pada karyawan tentang pentingnya melindungi informasi. Pada penelitian ini dilakukan perbandingan dalam pemilihan metode keamanan informasi. Metode yang digunakan adalah *logging dan auditing* dengan mengidentifikasi kelemahan dalam keamanan layanan serta melakukan penilaian untuk mengetahui sejauh mana kerusakan yang ditimbulkan pada sistem informasi saat ini. Selanjutnya dilakukan penilaian terhadap risiko dengan mengidentifikasi ancaman, kerentanan serta dampak negatifnya dan dilanjutkan dengan menyusun rekomendasi perbaikan berdasarkan ISO 27001. Korelasi dengan penelitian ini adalah penelitian ini menggunakan kontrol ISO/IEC 27001:2013 sehingga dapat dijadikan sebagai rujukan dalam menyusun rekomendasi perbaikan.

2.2 Evaluasi

Berdasarkan Kamus Besar Bahasa Indonesia (KBBI), Evaluasi adalah sebuah proses penilaian secara ekonomis serta teknis pada objek yang dijadikan sebagai kebutuhan untuk melakukan pengembangan terhadap objek tersebut. Kemudian (Cronholm & Göbel, 2016) mengemukakan pengertian evaluasi adalah sebuah aktivitas untuk ditentukannya seberapa baik kondisi sebuah objek yang ada saat ini (*artifact*). *Artifact* dalam teknologi informasi diartikan sebagai sistem informasi yang diimplementasikan dalam organisasi yang dapat membantu menjalankan suatu proses bisnis. Tujuan dari evaluasi yakni untuk menghasilkan pengetahuan baru sebagai jalan untuk pemecahan masalah yang ada saat ini dan dijadikan acuan untuk perumusan, perbaikan atau penggantian artefak pada saat ini. Evaluasi dapat dilakukan menggunakan pendekatan kuantitatif, kualitatif maupun kuantilatif (campuran). (Cronholm et al., 2003) mengemukakan tentang "*How-Strategies*" atau cara mengevaluasi terbagi menjadi 3 (tiga) yakni sebagai berikut:

1. ***Goal-free evaluation***

Goal-free evaluation adalah cara evaluasi yang mana dilakukan tidak terikat dengan tujuan diadakannya sistem informasi atau tujuan bisnis serta tidak bermaksud untuk membuktikan ketercapaian tujuan organisasi. Evaluasi ini bersifat *interpretative* yang berarti hasilnya membutuhkan suatu penafsiran yang lebih mendalam secara kualitatif terkait keadaan sistem informasi. Dengan menggunakan cara evaluasi ini,

evaluator diharuskan memiliki pengetahuan mendalam terkait sistem informasi yang dievaluasi sebagai gambaran permasalahan apa saja yang dapat ditemukan selama evaluasi berlangsung.

Goal-free evaluation ini termasuk dalam kategori induktif dimana pada proses evaluasinya yaitu mendeskripsikan dan menyimpulkan suatu keadaan atau untuk menemukan suatu permasalahan terkait objek yang dievaluasi berdasarkan dari hasil pengamatan yang dilakukan dan pengamatan yang dilakukan adalah bersifat bebas. Pada evaluasi ini, ruang lingkup sistem informasi dapat bertambah seiring berjalannya evaluasi sesuai dengan kebutuhan saat evaluasi dilakukan. *Goal-free evaluation* cocok digunakan pada penelitian untuk menemukan permasalahan spesifik terkait dengan implementasi sistem informasi.

2. ***Goal-based Evaluation***

Goal-based evaluation adalah evaluasi yang dilaksanakan terikat dengan tujuan organisasi. Evaluasi ini bersifat klarifikasi yang berarti untuk membuktikan apakah tujuan suatu organisasi yang direncanakan telah tercapai atau tidak. Dalam melakukan evaluasi, evaluator perlu memahami secara mendalam tujuan organisasi yang akan dievaluasi. Untuk menggunakan evaluasi ini, perlu pendefinisian tujuan organisasi secara pasti sebelum dilakukan proses evaluasi.

Cara evaluasi ini digunakan bertujuan untuk memahami sistem informasi yang diterapkan apakah telah sesuai dengan tujuan organisasi yang didefinisikan, tujuan organisasi yang mana yang tercapai, serta apabila masih belum memenuhi tujuan organisasi, bagaimana cara mencapai target tujuan organisasi. Evaluasi ini dikategorikan dalam deduktif yang memiliki arti bahwa evaluasi dilakukan dengan memberikan gambaran keadaan sistem informasi berdasarkan permasalahan yang ingin diselesaikan dengan dilakukannya kegiatan evaluasi.

3. ***Criteria-based Evaluation***

Pengertian *Criteria Based Evaluation* adalah evaluasi yang dilaksanakan terikat dengan suatu kriteria atau standar kerangka kerja (*framework*) tertentu yang dijadikan sebagai tolak ukur melakukan evaluasi. Evaluasi ini memiliki tujuan untuk mengungkapkan atau membuktikan keadaan *artifact* sesuai dengan kriteria yang didefinisikan. Untuk menggunakan evaluasi ini, perlu pendefinisian kriteria atau standar yang pasti sebelum dilakukan proses evaluasi.

Criteria-based Evaluation termasuk kategori deduktif yang memiliki arti yakni evaluasi dilakukan dengan memberikan gambaran keadaan sistem informasi saat ini atau objek yang dievaluasi sesuai dengan permasalahan yang ada melalui kegiatan evaluasi untuk mengetahui apakah telah memenuhi standar yang diharapkan. Evaluator

perlu memahami secara mendalam mengenai keilmuan terkait standar atau kriteria yang digunakan.

Selain itu, terdapat dua (2) strategi atau "*what-strategies*" evaluasi yaitu berdasarkan yang apa yang dievaluasi yakni sebagai berikut:

1. ***IT-system as such***

   IT-system as such merupakan evaluasi yang dilakukan tanpa keterlibatan pengguna. Pada evaluasi ini yang terlibat adalah evaluator serta sistem yang sedang dievaluasi dan tidak terdapat kegiatan observasi mengenai bagaimana pengguna berinteraksi dengan sistem TI. Sumber data berasal dari sistem informasi serta dokumentasinya. Tujuan dilakukan evaluasi ini adalah untuk mengetahui seberapa jauh sistem TI mendukung tujuan organisasi. Dengan menggunakan strategi evaluasi ini, evaluator perlu memahami terkait sistem TI yang dievaluasi dan hasilnya berdasarkan pemahaman atau pengalaman evaluator terkait TI.

   Saat evaluator menggunakan strategi ini, yang dilakukan evaluator adalah mengeksplorasi secara mandiri terkait dengan sistem TI yang dievaluasi. Sehingga evaluator perlu memahami fungsionalitas dari sistem TI yang di evaluasi. Hasil dari evaluasi ini adalah murni berdasarkan pengetahuan evaluator berdasarkan sistem TI yang dievaluasi.

2. ***IT-system in use***

   IT-system in use merupakan strategi evaluasi yang dalam pelaksanaannya melibatkan pengguna. Evaluasi ini melibatkan interaksi pengguna dan sistem yang sedang dievaluasi. Sumber data evaluasi ini berasal dari wawancara atau perspektif pengguna terkait sistem, observasi mengenai interaksi pengguna dan sistem TI serta dokumentasinya. Hasil evaluasi ini berdasarkan pada pemahaman evaluator terhadap fungsionalitas sistem TI dan perspektif pengguna terkait manfaat Sistem TI untuk mendukung menyelesaikan tugas mereka.

   Dengan menggunakan strategi ini, data yang akan diperoleh lebih banyak dan evaluasi dilakukan menggunakan beberapa sumber data sehingga dapat digunakan teknik triangulasi data untuk memperoleh data yang akurat.

Selain itu, dengan menggabungkan pendekatan *How-Strategies"* dan *"what-Strategies"* memberikan enam (6) tipe evaluasi yaitu sebagai berikut ini:

Tabel 2.4 Enam Tipe Evaluasi

	IT-systems as such	***IT-systems in use***
Goal-free evaluation	Tipe 1	Tipe 4
Goal-based evaluation	Tipe 2	Tipe 5
Criteria-based evaluation	Tipe 3	Tipe 6

Sumber: Cronholm dan Goldkuhl (2003)

1. ***Tipe 1- Goal-free evaluation of IT-systems as such***

Tipe ini adalah gabungan antara *Goal-free evaluation* dan *IT-systems as such*. Evaluasi tipe 1 ini dilakukan dengan berpikir secara terbuka (*open minded*) dengan objek evaluasinya adalah sistem TI. Tipe ini bertujuan agar evaluator memperoleh pemahaman dan pengetahuan yang lebih luas tentang sistem TI yang dievaluasi dan dilakukan ketika sumber data yang ada sedikit dan tidak ada pengguna yang tersedia.

Evaluasi tipe 1 digunakan untuk meningkatkan pemahaman yang lebih luas mengenai sistem TI. Evaluasi tipe 1 ini sumber data yang digunakan berasal dari sistem TI itu sendiri beserta deskripsi sistem TI. Evaluasi tipe 1 termasuk dalam kategori penelitian induktif dan tipe evaluasi ini digunakan apabila sumber daya yang ada terbatas dan tidak ada pengguna yang tersedia. Dalam menggunakan tipe evaluasi ini, evaluator dianjurkan untuk menjabarkan mengenai fungsionalitas sistem TI yang dilakukan dengan mempelajari sistem TI , dokumentasi sistem TI serta wawancara dengan pemilik sistem TI. Dalam beberapa kasus yang ada, evaluasi tipe 1 ini perlu digabungkan dengan tipe evaluasi lainnya yang mana hasil evaluasi dengan tipe 1 menjadi rekomendasi dilakukannya evaluasi lanjutan dengan tipe evaluasi yang berbeda.

2. ***Tipe 2 Goal-based evaluation of IT-systems as such***

Goal-based evaluation of IT-systems as such merupakan gabungan antara *Goal-based evaluation* dan *IT-systems as such* yang berarti bahwa evaluasi tipe 2 ini dilakukan menyesuaikan terhadap tujuan bisnis yang ditetapkan serta objek evaluasinya adalah sistem TI itu sendiri. Evaluasi dengan tipe ini bertujuan untuk mengetahui apakah sistem TI telah mencapai tujuan bisnis yang diharapkan atau belum. Sumber data tipe evaluasi ini terdiri dari sistem TI, deskripsi tujuan, spesifikasi kebutuhan dan deskripsi sistem TI.

Penggunaan evaluasi tipe 2 apabila sumber daya yang ada terbatas. Evaluasi tipe ini termasuk dalam penelitian deduktif. Dalam menerapkan evaluasi tipe 2 ini, diperlukan penjabaran mengenai tujuan bisnis yang ingin dicapai, tujuan bisnis ini dapat ditemukan pada dokumen-dokumen pendukung yang ada atau dapat di identifikasi

melalui proses wawancara dengan manajer bisnis atau pihak lain yang bertanggung jawab yang dilanjutkan dengan mendeskripsikan fungsionalitas sistem TI.

3. ***Tipe 3- Criteria-based evaluation of IT-systems as such***

Criteria-based evaluation of IT-systems as such merupakan gabungan antara *Criteria-based evaluation* dan *IT-systems as such* yang berarti bahwa evaluasi tipe 3 dilakukan berdasarkan standar atau kriteria (*framework*) tertentu yang mana objek evaluasinya adalah sistem TI itu sendiri. Sumber data tipe evaluasi ini adalah sistem TI, deksripsi standar atau kriteria (*framework*). Evaluasi tipe 3 ini digunakan untuk mengetahui apakah kualitas sistem TI telah memenuhi kriteria yang digunakan. Evaluasi ini termasuk dalam evaluasi deduktif. Evaluasi tipe 3 dimulai dengan memilih kriteria yang sesuai, selanjutnya mendeskripsikan fungsionalitas sistem TI atau mempelajari sistem TI dan melakukan wawancara dengan pemilik sistem atau orang yang bertanggung jawab terhadap sistem TI itu sendiri.

Dalam penelitian yang dilakukan, tipe evaluasi yang digunakan adalah tipe 3. Karena pada tipe 3 ini evaluasi dilakukan menggunakan standar atau kriteria tertentu dan objeknya adalah sistem TI itu sendiri. Evaluasi tipe 3 ini sesuai dengan penelitian yang akan dilakukan yakni evaluasi keamanan informasi dilakukan untuk mengukur tingkat kesiapan pengamanan informasi menggunakan standar keamanan informasi yang dibuat oleh Kementerian Komunikasi dan Informatika yaitu Indeks KAMI yang mana pendefinisian Indeks KAMI ini berdasarkan ISO/IEC 27001:2013 yang mana sumber data berasal yakni deskripsi sistem TI itu sendiri yang diperoleh dari wawancara menggunakan instrumen kuisioner Indeks KAMI kepada pihak yang bertanggung jawab terhadap keamanan informasi.

4. ***Tipe 4- Goal-free evaluation of IT-systems in use***

Goal-free evaluation of IT-systems in use gabungan antara *Goal-free evaluation* dan *IT-systems in use* yang memiliki arti bahwa evaluasi yang dilakukan tanpa terikat pada tujuan organisasi dengan melibatkan pengguna *(user)*, sistem TI dan dokumentasinya serta dilakukan dengan pikiran terbuka (*open minded*). Tujuan evaluasi tipe 4 adalah untuk memperoleh pengetahuan lebih luas tentang sistem TI itu sendiri berdasarkan dengan perspektif pengguna. Data yang diperlukan pada evaluasi tipe ini adalah sistem TI, observasi evaluator terhadap interaksi antara pengguna dengan sistem TI dan wawancara.

Perbedaan tipe 4 dengan tipe 1 adalah tersedianya sumber data lebih banyak. Sumber data pada tipe 4 ini adalah Sistem TI, observasi interaksi pengguna dengan sistem TI, pendapat pengguna tentang sistem TI dan *IT Maturity*. Dalam melakukan evaluasi menggunakan tipe ini,

disarankan kepada evaluator untuk menjabarkan mengenai fungsionalitas sistem TI, dokumentasi serta wawancara dengan pemilik sistem TI atau pihak yang bertanggung jawab. Selain itu, juga dilakukan pengamatan terhadap interaksi pengguna dengan sistem TI.

5. ***Tipe 5- Goal-based evaluation of IT-systems in use***

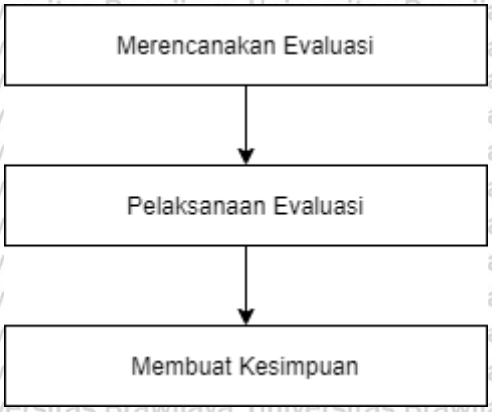
Goal-based evaluation of IT-systems in use merupakan gabungan antara *Goal-based evaluation* dan *IT-systems in use* yang artinya bahwa evaluasi tipe 5 ini dilaksanakan sesuai pada tujuan organisasi yang ditentukan sebelumnya dengan objek evaluasinya berupa sistem TI dan perspektif pengguna. Tujuan evaluasi ini untuk mengetahui apakah tujuan bisnis telah sesuai dengan yang diharapkan. Sumber data yang diperlukan pada tipe evaluasi ini adalah sistem TI, deskripsi tujuan, spesifikasi kebutuhan, deskripsi sistem TI, interaksi pengguna dan sistem TI dan perspektif pengguna terhadap sistem TI dan *IT maturity*.

Jenis penelitian pada evaluasi tipe 5 merupakan penelitian deduktif. Perbedaan paling utama dengan evaluasi tipe 2 yakni sumber data yang tersedia lebih banyak. Selain sistem TI, deskripsi tujuan, deskripsi TI dan spesifikasi kebutuhan dan, terdapat juga interaksi pengguna dengan sistem TI. Interaksi ini bergantung pada sikap dan pemahaman pengguna mengenai sistem TI terkait serta wawancara (perspektif pengguna).

6. ***Tipe 6- Criteria-based evaluation of IT-systems in use***

Criteria-based evaluation of IT-systems in use merupakan gabungan dari *Criteria-based evaluation* dan *IT-systems in use* yang mana evaluasi ini dilaksanakan berdasarkan standar atau kriteria (*framework*) tertentu, dengan objek evaluasinya adalah sistem TI yang digunakan. Tujuan evaluasi ini adalah untuk memutuskan apakah kualitas sistem TI telah sesuai dengan standar yang telah ditentukan serta memperoleh pemahaman yang lebih dalam tentang sistem TI terkait dan perspektif pengguna terhadap sistem TI. Sumber data yang diperlukan pada evaluasi ini adalah sistem TI, deskripsi sistem TI, deskripsi standar atau kriteria (*framework*), pengamatan interaksi, perspektif pengguna terhadap sistem TI dan *IT maturity*.

Evaluasi tipe 6 ini termasuk dalam kategori penelitian deduktif. Perbedaan utama tipe 6 dengan tipe 3 adalah evaluasi tipe 6 memiliki sumber data yang lebih banyak. Dengan evaluasi ini, selain mendapatkan pemahaman mengenai sistem TI dan deskripsi TI, didapatkan juga pemahaman dan sikap pengguna tentang sistem TI dengan melakukan wawancara.



Gambar 2.1 Tahapan Evaluasi

Sumber: Cronholm dan Goldkuhl (2003)

Berdasarkan pada gambar 2.1, tahapan evaluasi terdiri dari tiga (3) tahapan yaitu merencanakan evaluasi, pelaksanaan evaluasi dan membuat kesimpulan (Cronholm et al., 2003). Tahap awal ialah merencanakan evaluasi dengan menentukan ruang lingkup evaluasi, objek yang akan dievaluasi, kedalaman evaluasi, waktu evaluasi, sumber daya yang diperlukan, pengumpulan data dan sumber data serta *pre-knowledge* terkait proses bisnis dan informasi tentang objek yang dievaluasi. Pelaksanaan evaluasi adalah proses penerapan dari perencanaan evaluasi yang dilakukan dengan memilih satu atau gabungan dari beberapa evaluasi. Tahap terakhir ialah membuat kesimpulan yang merupakan hasil analisis dari permasalahan yang ditemukan yang mencakup penyusunan rekomendasi untuk perbaikan atau pengembangan selanjutnya.

2.3 Sistem Informasi

Sistem informasi adalah gabungan beberapa komponen terintegrasi dan berhubungan satu sama lain yang terdiri dari *software*, *hardware*, dan manusia yang bertujuan untuk melakukan pengumpulan dan pengolahan data menjadi informasi yang bernilai (Hasan, 2019). (O'brien, 2005) menyatakan sistem informasi merupakan gabungan yang terstruktur dan teratur antara perangkat lunak, perangkat keras, manusia, sumber daya data, dan jaringan komunikasi yang mengumpulkan, mengubah serta menyalurkan informasi dalam sebuah organisasi. Sistem informasi pada bisnis memiliki 3 (tiga) fungsi mendasar yang diantaranya adalah untuk mendukung pengambilan keputusan dalam konteks bisnis, untuk membuat keputusan yang tepat, untuk mendukung keunggulan yang kompetitif.

Menurut (Alter, 2008), sistem informasi merupakan sistem kerja dimana aktivitasnya secara spesifik bertujuan untuk melakukan pemprosesan informasi yang meliputi menangkap, mentransmisikan, menyimpan, memanipulasi serta menyajikan informasi. Sistem informasi adalah sebuah sistem dimana manusia/atau mesin melakukan aktivitas atau proses menggunakan teknologi informasi dan sumber daya yang lain yang bertujuan untuk menciptakan produk

informasi atau layanan kepada pelanggan internal dan eksternal. Sistem informasi merupakan sebuah sarana kepada organisasi dan orang-orang untuk memanfaatkan teknologi informasi dalam mengumpulkan, memproses, menyimpan, menggunakan serta menyebarkan informasi.

2.4 Keamanan Informasi

Informasi merupakan data yang diinterpretasi dan diklasifikasi sehingga dapat digunakan sebagai pedoman pengambilan keputusan. Informasi yang dimaksud merupakan data tersusun, data mentah, kapasitas sebuah komunikasi dan lain sebagainya (Sutabri, 2012). Kemudian data merupakan kenyataan yang dapat memberikan gambaran terhadap suatu kejadian yang mana data tersebut h masih mentah sehingga perlu diolajsupaya menghasilkan pengetahuan yang bernilai. Untuk menjaga informasi dan data, diperlukan keamanan informasi.

Keamanan informasi dapat diartikan sebagai terjaganya aspek pengamanan informasi yang terdiri dari aspek keutuhan (*integrity*), kerahasiaan (*confidentiality*), dan ketersediaan (*avaliability*) informasi (Kementerian Komunikasi dan Informatika,2016). Menurut G.J Simons, keamanan informasi merupakah sebuah upaya yang dapat mendeteksi adanya penipuan pada sistem informasi serta melakukan pencegahan penipuan (*cheating*) yang mana informasi itu sendiri tidak mempunyai arti fisik (1995 disitasi dalam Budi, 1998).

Tata Sutabri (2012) menyatakan pengertian dari aspek *integrity*, *confidentiality* dan *avalialability* yang dijelaskan berikut ini:

- Keutuhan (*integrity*) berarti validitas dan kepercayaan atau keakuratan data terjaga dan data tidak dapat diganti atau diubah oleh orang-orang yang tidak memiliki kepentingan.
- Kerahasiaan (*Confidentiality*) memiliki arti bahwa orang yang tidak memiliki wewenang, tidak dapat mengakses informasi dan data yang artinya bahwa informasi dan data hanya bisa diakses orang yang memiliki otoritas. Hal ini bertujuan untuk melindungi kerahasiaan data dan informasi dan hanya diperuntukkan untuk orang-orang tertentu. Misalnya, data pribadi nasabah bank yang harus dilindungi.
- Ketersediaan (*avaliability*) yakni kepastian ketersediaan informasi ketika diperlukan oleh orang yang berwenang untuk mengetahui. Dengan tujuan ketika terdapat pengguna membutuhkan sebuah informasi tersebut, informasi dapat digunakan dengan cepat serta dapat diakses dengan mudah.

Keamanan Informasi perlu diterapkan dengan baik dan seimbang diantara ketiga aspek diatas, apabila terjadi gangguan pada keamanan informasi maka aspek keamanan informasi mengalami permasalahan yang akan menghambat aktivitas organisasi itu sendiri.

2.5 ISO/IEC 27001:2013

International Organization for Standardization (ISO) dan *International Electrotechnical Commission* (IEC) mengembangkan sebuah standar tentang Sistem Manajemen Keamanan Informasi (SMKI) yang dijadikan sebagai acuan dan diakui sebagai standar seluruh dunia. Standar ini dirancang berbentuk panduan ataupun persyaratan. Sejak tahun 2005, telah dikembangkan standar 27000 hingga kemudian mengembangkan standar 27001:2013. Dalam membangun Sistem Manajemen Keamanan Informasi (SMKI), diharuskan untuk memenuhi spesifikasi atau persyaratan pada standar ISO 27001:2013 (Kementerian Komunikasi dan Informatika Republik Indonesia,2017). ISO/IEC 27001:2013 dirancang untuk menjaga aset informasi dari ancaman dan risiko.

ISO/IEC 27001:2013 bertujuan untuk penetapan, menerapkan, mengoperasikan, melakukan pemantauan, peninjauan, memelihara serta peningkatan untuk Sistem Manajemen Keamanan Informasi. Pengembangan ISO/IEC 27001:2013 berguna untuk menekankan pentingnya untuk memahami syarat-syarat keamanan informasi dan keperluan terhadap kebijakan dan sasaran keamanan informasi, menerapkan dan mengoperasikan kontrol keamanan untuk mengelola risiko secara keseluruhan pada konteks risiko bisnis, pentingnya memantau dan meninjau ulang terhadap kinerja dan keefektivitasan penerapan Sistem Manajemen Keamanan Informasi (SMKI) dan menekankan pentingnya berkelanjutan pada pengukuran tingkat ketercapaian sasaran. Standar ISO/IEC:27001:2013 bersifat independen pada produk teknologi informasi, standar disusun dengan tujuan untuk memberikan jaminan terhadap kontrol keamanan yang diterapkan dan dipilih untuk menjaga dan melindungi kerahasiaan aset informasi dari ancaman risiko serta untuk memberikan keyakinan keamanan kepada pemangku kepentingan.

ISO/IEC 27001:2013 terbagi menjadi 2 bagian yakni klausul utama atau *mandatory process* yang memiliki 11 klausul serta lampiran Annex A atau *security control* yang berjumlah 14 domain area yang akan dijabarkan sebagai berikut ini:

- **Klausul Utama atau Mandatory Process**

1. Klausul 0 - Pendahuluan (*Introduction*)
2. Klausul 1 - Ruang Lingkup (*Scope*)
3. Kalusul 2 - Rujukan Normatif (*Normative References*)
4. Klausul 3 - Istilah dan Definisi (*Terms and definition*)
5. Klausul 4 - Konteks Organisasi (*Context of the organization*)
6. Klausul 5 – Kepemimpinan (*Leadership*)
7. Klausul 6 - Perencanaan (*Planning*)
8. Klausul 7 - Dukungan (*Support*)
9. Klausul 8 - Operasi (*Operation*)

10. Klausul 9 - Evaluasi Kinerja (*Performance evaluation*)
11. Klausul 10 – Peningkatan (*Improvement*)

- **Lampiran A (Annex A)**

A.5 Security Policies

A.6 Organisation of Information Security

A.7 Human Resource Security

A.8 Asset Management

A.9 Access Control

A.10 Cryptography

A.11 Physical and Enviromental Security

A.12 Operations Security

A.13 Communications Security

A.14 Systems Acquisition, Development and Maintenance

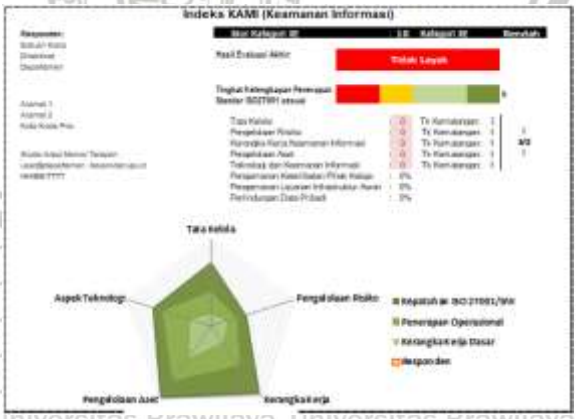
A.15 Supplier Relationships

A.16 Information Security Incident Management

A.17 Information Security Aspects of Business Continuity Management

A.18 Compliance

2.6 Indeks Keamanan Informasi (KAMI) 4.1



Gambar 2.2 Tampilan Dashboard Hasil Evaluasi Indeks KAMI

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.1 (2019)

Indeks Keamanan Informasi (KAMI) adalah *tools* atau alat ukur yang dipergunakan pada instansi pemerintah untuk mengukur tingkat kesiapan (tingkat kelengkapan dan tingkat kematangan) pengamanan informasi.

Penggunaan alat ukur ini bertujuan untuk memberikan gambaran atau kondisi terkait kondisi keamanan informasi pada saat ini pada pimpinan instansi. Indeks KAMI tidak digunakan untuk menganalisa efektivitas atau kelayakan pengamanan yang diterapkan. Evaluasi ini dilaksanakan pada area yang dijadikan sebagai target dalam penerapan keamanan informasi yang mana ruang lingkup yang dibahas pada Indeks KAMI telah memenuhi seluruh aspek yang dibahas pada SNI ISO/IEC 27001:2013 (KOMINFO, 2017).

Data yang dipakai pada evaluasi yang dilakukan akan menghasilkan indeks terkait kesiapan dari tingkat kematangan ataupun kelengkapan penerapan kerangka kerja keamanan informasi. Yang mana dalam menyusun perbaikan serta penetapan prioritas, indeks yang dihasikan dapat dipergunakan untuk pembanding. Evaluasi dengan menggunakan indeks KAMI ini disusun untuk dapat diterapkan pada organisasi dari berbagai tingkat kepentingan, ukuran, serta kepentingan pemanfaatan TIK untuk mendukung proses yang ada.

Evaluasi dengan menggunakan indeks KAMI sebaiknya dilakukan secara berkala atau 2 (dua) kali dalam setahun sebagai peninjauan ulang terhadap kesiapan keamanan informasi dan mengukur ketercapaian terhadap perbaikan yang diterapkan, berdasarkan pencapaian tingkat kematangan atau kelengkapan tertentu. Evaluasi keamanan informasi menggunakan indeks KAMI dilakukan dengan menjawab sejumlah pertanyaan yang terbagi dalam area yang menjadi fokus keamanan informasi yakni sebagai berikut:

1. Kategori Sistem Elektronik : digunakan untuk mengevaluasi tingkat atau kategori sistem elektronik yang digunakan pada instansi yang dikelompokkan pada tingkat Rendah, Tinggi, dan Strategis.
2. Tata Kelola Keamanan Informasi: untuk mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.
3. Pengelolaan Risiko Keamanan Informasi: untuk mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
4. Kerangka Kerja Pengelolaan Keamanan Informasi: untuk mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
7. Pengelolaan Aset Informasi: untuk mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.
8. Teknologi dan Keamanan Informasi: untuk mengevaluasi kelengkapan, konsistensi, dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

9. Suplemen : mengevaluasi aspek pengamanan keterlibatan pihak ketiga sebagai penyedia layanan, layanan berbasis cloud, dan perlindungan data pribadi.

2.6.1 Kuisioner Indeks KAMI 4.1

Alat evaluasi Indeks KAMI memanfaatkan *Microsoft Excel* yang berisi lembar kerja untuk melakukan evaluasi terkait keamanan informasi yang terdiri dari dua (2) area yaitu sebagai berikut ini:

1. **Bagian I - Kategori Sistem Elektronik**

   Langkah awal yang dilakukan pada evaluasi ini adalah mendefinisikan kategori sistem elektronik di instansinya. Tujuan kegiatan ini yakni untuk mengklasifikasikan sistem elektronik yang dipakai instansi pada tingkatan tertentu, yakni Rendah, Tinggi, dan Strategis yang menghasilkan suatu pemetaan terhadap instansi yang memiliki karakteristik sistem elektronik yang sama. Dalam pendefinisian kategori sistem elektronik ini, dilakukan dengan menjawab 10 pertanyaan yang diantaranya adalah sebagai berikut ini:

   1. Nilai investasi sistem elektronik yang terpasang
   2. Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Elektronik
   3. Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu
   4. Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam sistem elektronik
   5. Jumlah pengguna sistem elektronik
   6. Data pribadi yang dikelola sistem elektronik
   7. Tingkat klasifikasi/kekritisan data yang ada dalam sistem elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi
   8. Tingkat kekritisan proses yang ada dalam sistem elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi
   9. Dampak kegagalan sistem elektronik
   10. Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem elektronik (sabotase, terorisme)

Untuk menjawab pertanyaan diatas, responden diminta memilih satu (1) dari tiga (3) jawaban yang tersedia yaitu A atau B atau C dan untuk setiap jawaban memiliki bobot nilai tertentu yaitu untuk jawaban A memiliki bobot nilai 5, jawaban B memiliki bobot nilai 2 dan jawaban C memiliki bobot nilai 1. Dan kemudian nilai dari seluruh pertanyaan dijumlahkan untuk menentukan sistem elektronik instansi terkait berada pada tingkatan tertentu yaitu sebagai berikut:

- Rendah : artinya bahwa sistem elektronik dalam organisasi terkait mendukung proses kerja yang berjalan walaupun tidak pada tingkat yang signifikan.
- Tinggi : artinya bahwa sistem elektronik merupakan bagian yang tidak terpisahkan dari proses kerja yang berjalan pada organisasi.
- Strategis: artinya bahwa sistem elektronik merupakan satu-satunya cara untuk menjalankan proses kerja yang berskala nasional dan bersifat strategis.

Tabel 2.5 Klasifikasi Kategori Sistem Elektronik

Tingkat Kategori Sistem Elektronik	Total Skor
Rendah	10-15
Tinggi	16-34
Strategis	35-50

Sumber: Indeks Keamanan Informasi (Indeks KAMI) Versi 4.1 (2019)

Tabel 2.3 merepresentasikan klasifikasi kategori sistem elektronik yang terbagi menjadi 3 (tiga) kategori yakni rendah, tinggi serta strategis. Sistem elektronik termasuk dalam kategori rendah apabila total skor penilaian sistem elektronik adalah 10 sampai dengan 15. Sistem elektronik termasuk dalam kategori tinggi apabila total skor penilaian sistem elektronik adalah 16-34. Dan sistem elektronik termasuk dalam kategori strategis apabila total skor penilaian sistem elektronik adalah 35 sampai 50.

Bagian I: Kategori Sistem Elektronik			
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan			
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis		Status	Skor
#	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	C	1
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
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional	C	1

Gambar 2.3 Kuisioner Kategori Sistem Elektronik

Sumber: Indeks Keamanan Informasi (Indeks KAMI) Versi 4.1 (2019)

2. Area Pengamanan Informasi

Pada area pengamanan informasi, dilakukan evaluasi dengan tujuan memberikan gambaran atau kondisi atau keadaan terkait keamanan informasi sebagai hasil dari program kerja yang telah dilaksanakan. Pengamanan informasi memiliki 6 area yaitu Tata Kelola Keamanan Informasi (Bagian II), Pengelolaan Risiko Keamanan Informasi (Bagian III), Kerangka Kerja Keamanan Informasi (Bagian IV), Pengelolaan Aset Informasi (Bagian V), Teknologi dan Keamanan Informasi (Bagian VI) dan Suplemen (Bagian VII). Setiap pertanyaan pada area ini dikelompokkan menjadi 3 (tiga) kategori pengamanan yang akan dijelaskan sebagai berikut ini:

1. **Kategori 1**

   Pertanyaan pada kategori ini berkaitan dengan kerangka kerja dasar keamanan informasi.

2. **Kategori 2:**

   Pertanyaan pada kategori ini berkaitan dengan efektivitas serta konsistensi penerapan keamanan informasi.

3. **Kategori 3**

   Pertanyaan pada kategori ini berkaitan dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi. Pada kategori 3 ini merupakan kesiapan minimum untuk proses sertifikasi standar ISO/IEC 27001:2013.

Selanjutnya responden menjawab setiap pertanyaan pada setiap area dengan memilih 1 (satu) jawaban status pengamanan dari 4 (empat) jawaban yang disediakan yaitu:

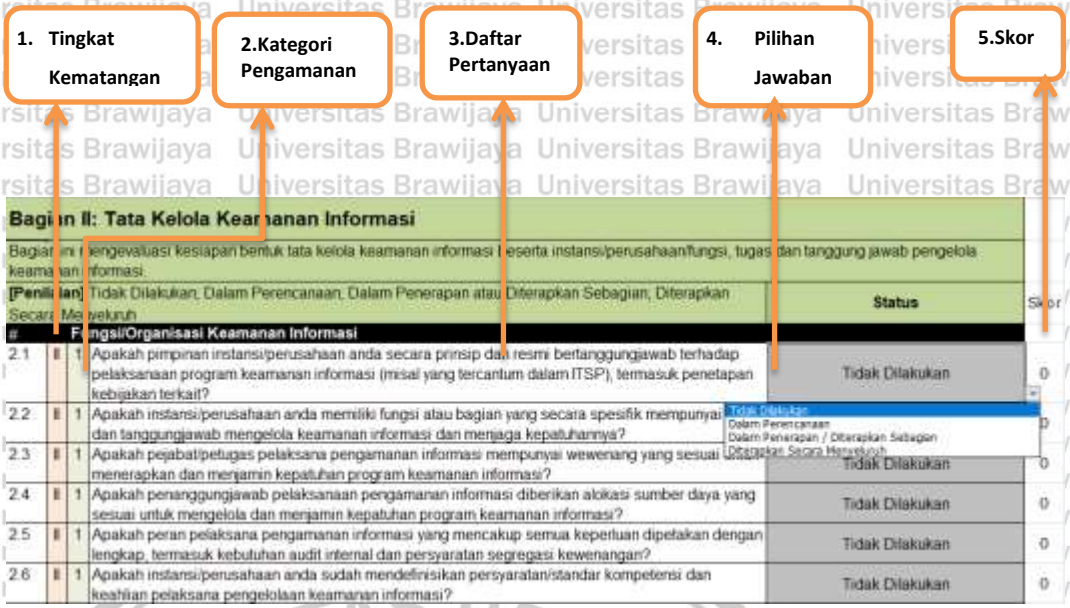
- Tidak Dilakukan
- Dalam Perencanaan
- Dalam Penerapan atau Diterapkan Sebagian
- Diterapkan secara Menyeluruh

Setiap status jawaban diatas mempunyai skor tertentu berdasarkan kategori bentuk pengamanan (kategori 1 sampai kategori 3). Dengan ketentuan untuk tahapan awal memiliki skor nilai lebih rendah daripada tahapan berikutnya. Untuk status penerapan pengamanan, penerapan yang telah diterapkan secara menyeluruh menghasilkan nilai yang lebih tinggi daripada bentuk penerapan lainnya. Tabel 2.4 menyajikan seluruh jawaban penilaian status pengamanan dan membentuk matriks antara status keamanan dan kategori pengamanan.

Tabel 2.6 Pemetaan Skor Pengamanan

	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

Sumber: Indeks Keamanan Informasi versi 4.1 (2019)



Gambar 2. 4 Tampilan Kuisioner Pengamanan Informasi

Sumber: Indeks Keamanan Informasi versi 4.1 (2019)

Gambar 2.4 ditunjukkan contoh tampilan kuisioner pada area pengamanan informasi dengan atribut dan kolom yang sama di semua area (bagian II sampai bagian VII) dengan penjelasan atribut sebagai berikut ini:

1. Tingkat Kematangan: ditunjukkan kategori kematangan berkaitan dengan pertanyaan yang dibahas yang mencakup 5 (lima) tingkat yakni, Tingkat I (Kondisi Awal), Tingkat II (Penerapan Kerangka Kerja Dasar), Tingkat III (Terdefinisi dan Konsisten), Tingkat IV (Terkelola dan Terukur) dan Tingkat 5 (Optimal).
2. Kategori Pengamanan: Kolom yang menunjukkan kategori tahap penerapan yang memiliki 3 (tiga) kategori.
3. Daftar Pertanyaan: daftar pertanyaan yang perlu dijawab responden.
4. Pilihan Jawaban: adalah opsi jawabahan yang tersedia untuk menggambarkan kondisi setiap pertanyaan dan terdiri dari 4 pilihan jawaban.
5. Skor : merupakan nilai dari setiap pertanyaan berdasarkan pilihan jawaban yang dipilih dan kategori pengamanannya.

2.6.2 Mekanisme Penilaian Indeks KAMI

Dalam penilaian menggunakan indeks KAMI, terbagi menjadi 2 (dua) yakni penilaian kelengkapan dan penilaian kematangan menggunakan peraturan yang ditentukan. Berikut pada tabel 2.5 merupakan rangkuman jumlah pertanyaan penilaian kelengkapan dan kematangan.

Tabel 2.7 Matriks Jumlah Pertanyaan Indeks KAMI 4.1

	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi
Kategori 1	8	10	12	24	14
Kategori 2	8	4	10	10	10
Kategori 3	6	2	7	4	2
Total Pertanyaan	**22**	**16**	**29**	**38**	**26**
Skor Maksimal	126	72	159	168	120
Batas Skor Minimal untuk Skor Kategori 3	48	36	64	88	68
Jumlah Pertanyaan Tk Kematangan II	13	10	11	29	14
Jumlah pertanyaan kategori 1	8	10	9	24	14
Jumlah Pertanyaan Kategori 2	5	0	2	5	0
Jumlah Pertanyaan Tk Kematangan III	**3**	**2**	**13**	**9**	**11**
Jumlah Pertanyaan Kategori 1	0	0	3	0	0
Jumlah Pertanyaan Kategori 2	3	2	8	5	10
Jumlah Pertanyaan	0	0	2	4	1

Kategori 3					
Jumlah Pertanyaan Tk Kematangan IV	**6**	**2**	**3**	**0**	**1**
Jumlah Pertanyaan Kategori 2	0	2	0	0	0
Jumlah Pertanyaan Kategori 3	6	0	3	0	1
Jumlah Pertanyaan Tk Kematangan V	**0**	**2**	**2**	**0**	**0**
Jumlah Pertanyaan Kategori 3	0	2	2	0	0

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.1 (2019)

Matrik jumlah pertanyaan Indeks KAMI direpresentasikan pada tabel 2.5 Dapat diketahui bahwa jumlah pertanyaan pada Indeks KAMI 4.1 di 5 area evaluasi adalah 131 pertanyaan dengan skor maksimal adalah 645. Dalam tabel 2.5 diketahui bahwa untuk area tata kelola memiliki 22 pertanyaan yang terdiri dari 8 pertanyaan dalam kategori 1, 8 pertanyaan dalam kategori 2 dan 6 pertanyaan dalam kategori 3 dengan skor maksimal adalah 126. Pada area pengelolaan risiko memiliki 16 pertanyaan yang terdiri dari 10 pertanyaan dalam kategori 1, 4 pertanyaan dalam kategori 2 dan 2 pertanyaan pada kategori 3 yang memiliki skor maksimal adalah 72. Pada area kerangka kerja total jumlah pertanyaan adalah 29 yang terbagi dalam kategori 1 yakni 12 pertanyaan, kategori 2 yakni 10 pertanyaan dan kategori 3 yakni 7 pertanyaan dan memiliki skor maksimal 159. Pada area pengelolaan aset memiliki total pertanyaan yakni 38 pertanyaan yang terbagi dalam kategori 1 yakni 24 pertanyaan, kategori 2 yakni 10 pertanyaan dan kategori 3 yakni 4 pertanyaan dengan skor maksimal adalah 168. Dan yang terakhir adalah area teknologi memiliki total pertanyaan yakni 26 pertanyaan yang terdiri dari 14 pertanyaan dalam kategori 1, 10 pertanyaan dalam kategori 2 dan 2 pertanyaan dalam kategori 3. Pada 5 area tersebut, memiliki skor minimal untuk Tahapan Kategori 3 yang berarti bahwa pertanyaan dalam kategori 3 akan menghasilkan nilai apabila skor minimum yang ditentukan pada setiap area tercapai atau pertanyaan pada kategori 1 dan kategori 2 telah diisi dengan status minimal “Dalam Penerapan atau Diterapkan Sebagian”.

Penilaian kematangan dalam indeks KAMI merujuk pada tingkat kematangan yang diterapkan oleh kerangka kerja (*framework*) COBIT (*Control Objective for Information and Related Technology*) atau CMMI (*Capability Maturity Model Integration*) (KOMINFO,2017)). Perolehan ketercapaian tingkat kematangan dihasilkan kemudian dapat dijadikan sebagai sebuah alat untuk melaporkan pemeringkatan tingkat kematangan dan pemetaan pemetaan dan pemeringkatan tingkat kematangan, tingkat kelengkapan keamanan informasi di Lembaga atau Kementerian. Tingkat kematangan dalam Indeks KAMI didefinisikan sebagai berikut ini:

Tabel 2. 8 Definisi Tingkat Kematangan

Tingkat Kematangan	Definisi
Tingkat 0 – Tidak Diketahui (PASIF)	Status kesiapan keamanan informasi tidak diketahui
	Pihak yang terlibat tidak mengikuti atau tidak melaporkan pemeringkatan indeks KAMI.
Tingkat I – Kondisi Awal (REAKTIF)	Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi
	Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu pada keseluruhan risiko yang ada, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan.
	Kelemahan teknis dan non-teknis tidak terindentifikasi dengan baik.
	Pihak yang terlibat tidak menyadari tanggung jawab mereka.
Tingkat II – Penerapan Kerangka Kerja Dasar (AKTIF)	Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
	Proses pengamanan berjalan tanpa dokumentasi atau rekaman resmi.
	Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana.
	Bentuk pengamanan secara keseluruhan belum dapat dibuktikan efektivitasnya.
	Kelemahan dalam manajemen pengamanan masih banyak ditemukan dan tidak dapat diselesaikan dengan tuntas oleh pelaksana maupun pimpinan sehingga

	menyebabkan dampak yang sangat signifikan.
	Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten.
	Pihak yang terlibat kemungkinan besar masih belum memahami tanggung jawab mereka.
Tingkat III- Terdefinisi dan Konsisten (PRO AKTIF)	Bentuk dokumentasi yang baku sudah diterapkan secara konsisten dan terdokumentasi secara resmi.
	Efektivitas pengamanan evaluasi secara berkala, walaupun belum melalui proses yang terstruktur.
	Pihak pelaksana dan pimpinan secara umum dapat menangani permasalahan terkait pengelolaan keamanan pengendalian dengan tepat, akan tetapi beberapa kelemahan dalam sistem manajemen masih ditemukan sehingga dapat mengakibatkan dampak yang sangat signifikan.
	Kerangka kerja pengamanan sudah mematuhi ambang batas minimum standar atau persyaratan hukum yang terkait.
	Secara umum semua pihak yang terlibat menyadari tanggung jawab mereka dalam pengamanan informasi.
Tingkat IV- Terkelola dan Terukur (TERKENDALI)	Pengamanan diterapkan secara efektif sesuai dengan strategi manajemen risiko.
	Evaluasi (pengukuran) pencapaian sasaran secara konsisten dievaluasi efektivitasnya.
	Kelemahan manajemen pengamanan teridentifikasi dengan baik dan secara konsisten ditindaklanjuti pembenahannya.
	Manajemen pengamanan bersifat pro-aktif dan menerapkan pembenahan untuk mencapai bentuk pengelolaan yang efisien.
	Insiden dan ketidakpatuhan (*non-confirmity*) diselesaikan melalui proses formal dengan pembelajaran akar permasalahan.
	Karyawan merupakan bagian yang tidak terpisahkan dari pelaksana pengamanan informasi.
Tingkat V- Optimal (OPTIMAL)	Pengamanan menyeluruh diterapkan secara berkelanjutan dan efektif melalui program pengelolaan risiko yang terstruktur.

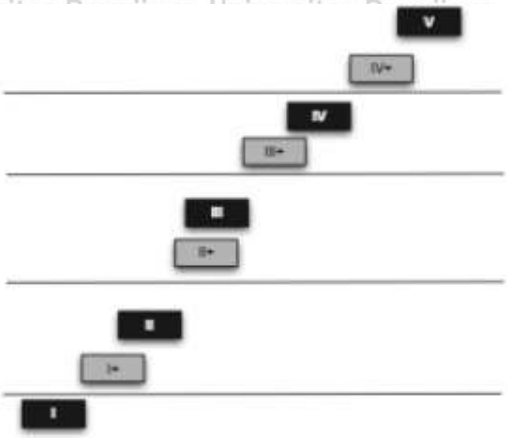
	Pengamanan informasi dievaluasi secara kontinyu, dengan analisis parameter efektivitas kontrol, kajian permasalahan dan penerapan langkah untuk optimasi peningkatan kinerja.
	Target pencapaian program pengamanan informasi selalu dipantau, dievaluasi dan diperbaiki.
	Karyawan secara pro-aktif terlibat dalam peningkatan efektivitas pengamanan.

Sumber: Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik (2011)

Penilaian kematangan dilaksanakan dengan menganalisa jumlah skor pada area yang tersedia apakah telah mencapai batas kematangan tertentu atau telah melebihi yang mana proses perhitungannya adalah sebagai berikut:

- Pencapaian tingkat kematangan di berdasarkan kelengkapan, konsistensi dan efektivitas penerapannya.
- Tingkat kematangan yang lebih tinggi memiliki persyaratan kelengkapan, konsistensi dan efektivitas pengamanan di level bawahnya yang mana pencapaian pada tingkat kematangan II dan III hanya dapat diterapkan apabila sebagian besar pertanyaan pada tingkat kematangan sebelumnya [x-1] telah "Diterapkan Secara Menyeluruh".
- Pada pencapaian tingkat kematangan IV dan tingkat kematangan V mengharuskan seluruh pengamanan pada tingkat sebelumnya sudah "Diterapkan Secara Menyeluruh".

Sebagai upaya membantu memberikan definisi dan uraian yang lebih rinci, tingkatan kematangan pada indeks KAMI memiliki tambahan 4 (empat) tingkat kematangan yang diantaranya adalah I+, II+, III+, dan IV+ sehingga seluruh tingkatannya berjumlah 9 (sembilan) tingkat kematangan. Gambaran ambang batas pencapaian tingkat kematangan tertentu didefinisikan pada gambar 2.5 berikut ini.



Gambar 2. 5 Definisi Tingkat Kematangan

Sumber: Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik (2011)

(KOMINFO,2011) menentukan ambang batas ketercapaian suatu tingkat tertentu ditentukan berdasarkan perumusan yang dijabarkan dibawah ini:

- **Tingkat Kematangan I**
  - Tidak memiliki ambang batas minimal.
  - Ketika memulai evaluasi, seluruh responden diasumsikan berada pada tingkat kematangan I
- **Tingkat Kematangan I+ - Mencapai Minimal**
  - 4 (empat) pengamanan TKII-Kategori 1 berada dalam status "Dalam Penerapan/Diterapkan Sebagian".
  - Sisa jumlah pengamanan TKII- Kategori 1 berada dalam status "Dalam Perencanaan".
- **Tingkat Kematangan II – Mencapai Minimal**
  - Keseluruhan pengamanan TKII- Kategori 1 berada dalam status "Dalam Penerapan atau Diterapkan Sebagian".
  - Keseluruhan pengamanan TKII- Kategori 2 berada dalam status "Dalam Penerapan/Diterapkan Sebagian".
- **Tingkat Kematangan II+ - Mencapai Minimal**
  - Syarat TKII+ yakni 80% TKII- Kategori 1 dan Kategori 2 berada dalam status "Diterapkan Secara Menyeluruh
  - Keseluruhan pengamanan TKIII-Kategori 1 berada dalam status "Diterapkan Secara Menyeluruh".
  - 2 (dua) pengamanan TKIII-Kategori 2 berada dalam status "Dalam Perencanaan".

- Sisa jumlah pengamanan TKIII-Kategori 2 berada dalam status "Dalam Penerapan atau Diterapkan Sebagian".
- 1 (satu) pengamanan TKIII-Kategori 2 berada dalam status "Dalam Perencanaan".
- Sisa jumlah pengamanan TKIII-Kategori 3 berada dalam status "Dalam Penerapan atau Diterapkan Sebagian".

- **Tingkat Kematangan III: Mencapai Minimal**
  - Memiliki persyaratan tingkat kematangan II+ telah terpenuhi
  - Keseluruhan bentuk pengamanan TKIII-Kategori 1 berada dalam status "Diterapkan secara menyeluruh".
  - Sisa jumlah pengamanan TKIII-Kategori 2 berada dalam status "Dalam Penerapan atau Diterapkan Sebagian".
  - 2 (dua) bentuk pengamanan TKIII-Kategori 3 berada dalam status "Dalam Penerapan atau Diterapkan Sebagian.
- **Tingkat Kematangan III+: Mencapai minimal**
  - Keseluruhan bentuk pengamanan TKIII-Kategori 1 berada dalam status "Diterapkan Secara Menyeluruh".
  - 1 (satu) bentuk pengamanan TKIII-Kategori 2 berada dalam status "Dalam Penerapan atau Diterapkan Sebagian".
  - Sisa jumlah pengamanan TKIII-Kategori 2 yang ada berada dalam status "Diterapkan secara menyeluruh".
  - 1 (satu) bentuk pengamanan TKIII-Kategori 3 berada dalam status "Dalam Penerapan atau Diterapkan Sebagian".
  - Sisa jumlah pengamanan TKIII-Kategori 3 berada dalam status "Dalam Penerapan atau Diterapkan Sebagian".
  - 2 (dua) pengamanan TKIV-kategori 3 berada dalam status "Diterapkan Secara Menyeluruh".
  - Sisa bentuk jumlah pengamanan TKIV-Kategori 3 berada dalam status "Dalam Perencanaan".
- **Tingkat Kematangan IV**
  - Memiliki persyaratan tingkat kematangan III+ telah terpenuhi
  - Keseluruhan bentuk pengamanan TKIV-Kategori 3 berada dalam "Diterapkan Secara Menyeluruh".
- **Tingkat Kematangan IV+**
  - Telah terpenuhinya seluruh persyaratan pada tingkat kematangan IV

- Satu bentuk pengamanan TKV-Kategori 3 berada dalam status "Dalam Penerapan atau Diterapkan Sebagian".

- **Tingkat Kematangan V**
- Telah terpenuhinya seluruh persyaratan pada tingkat kematangan IV.
- Keseluruhan pengamanan TKV-Kategori 3 dengan status "Diterapkan Secara Menyeluruh".

2.6.3 Pengkajian Hasil Kuisioner Indeks KAMI

Hasil pada seluruh penjumlahan skor yang didapat pada setiap area selanjutnya akan ditampilkan pada 2 (dua) instrumen yang terdiri dari:

1. Tabel nilai masing-masing area

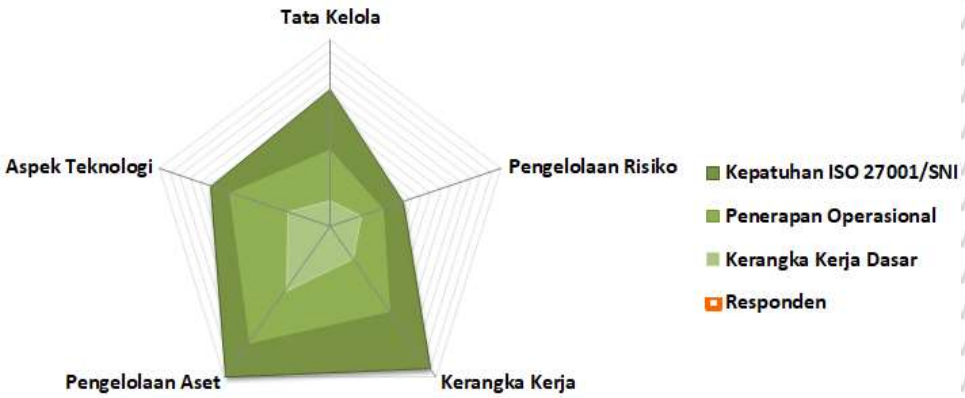
Tata Kelola	:	0
Pengelolaan Risiko	:	0
Kerangka Kerja Keamanan Informasi	:	0
Pengelolaan Aset	:	0
Teknologi dan Keamanan Informasi	:	0
Pengamanan Keterlibatan Pihak Ketiga	:	0%
Pengamanan Layanan Infrastruktur Awar	:	0%
Perlindungan Data Pribadi	:	0%

Gambar 2.6 Rangkuman Nilai Area Pengamanan Informasi

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.1 (2019)

Gambar 2.6 menampilkan contoh rangkuman nilai masing-masing area Indeks KAMI. Dengan menggunakan rangkuman ini, dapat memudahkan instansi atau organisasi untuk melihat seberapa besar tingkat kelengkapan yang telah tercapai di setiap masing-masing area.

2. Radar Chart 5 (lima) sumbu area pengamanan informasi



Gambar 2.7 Diagram Radar Kematangan

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.1 (2019)

Gambar 2.7 menunjukkan diagram radar tingkat kelengkapan untuk 5 (lima) area pengamanan informasi dengan latar belakang berwarna hijau muda hingga hijau tua yang menyajikan batas tingkat kelengkapan pada kategori 1, kategori 2 dan kategori 3. Untuk setiap nilai dari jawaban responden disajikan pada area berwarna oranye. Pada diagram radar tersebut, memperlihatkan perbandingan antara kondisi kesiapan dari pengamanan informasi yang merupakan hasil evaluasi tingkat kelengkapan serta untuk menunjukkan seberapa jauh tingkat kelengkapan pengamanan informasi yang diterapkan sudah mencapai tingkat kelengkapan yang diinginkan.

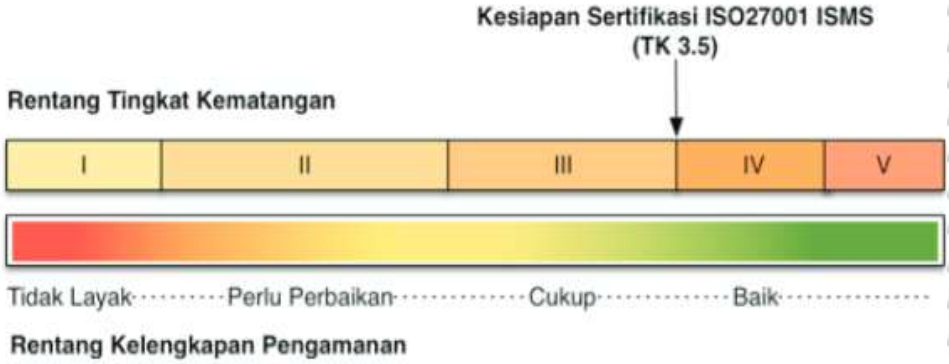
Tabel 2.9 Hubungan Antara Kategori Sistem Elektronik dengan Status Kesiapan Pengamanan

KATEGORI SISTEM ELEKTRONIK				
Rendah		**Skor Akhir**		**Status Kesiapan**
10	15	0	174	Tidak Layak
		175	312	Penerapan Kerangka Kerja Dasar
		313	535	Cukup Baik
		536	645	Baik
Tinggi		**Skor Akhir**		**Status Kesiapan**
16	34	0	272	Tidak Layak
		273	455	Penerapan Kerangka Kerja Dasar
		456	583	Cukup Baik
		584	645	Baik
Strategis		**Skor Akhir**		**Status Kesiapan**
35	50	0	333	Tidak Layak
		334	535	Penerapan Kerangka Kerja Dasar
		536	609	Cukup Baik
		610	645	Baik

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.1 (2019)

Nilai yang telah diperoleh dari proses evaluasi selanjutnya dipetakan pada tingkatan kategori sistem elektronik yang ada terhadap cakupan instansi tersebut. pemetaan tersebut digambarkan pada tabel 2.7. Dari tabel 2.7, disimpulkan bahwa semakin tinggi ketergantungan

suatu instansi pada sistem elektronik diperlukan banyaknya bentuk pengamanan yang perlu diterapkan sampai pada tahapan tertinggi.



Gambar 2.8 *Bar Chart* Hubungan Tingkat Kelengkapan dan Tingkat Kematangan

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.1 (2019)

2.7 Hubungan Indeks KAMI dengan ISO 27001:2013

Penilaian dilakukan pada area pengamanan informasi yang ruang lingkup pembahasannya telah memenuhi aspek keamanan informasi yang didefinisikan oleh standar SNI ISO/IEC 27001:2013. Dalam Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Publik (2011), dijabarkan mengenai hubungan antara aspek-aspek pertanyaan indeks KAMI versi terhadap domain-domain area Annex A ISO/IEC 27001:2013. 14 domain area pada kontrol Annex A ISO/IEC 27001:2013 dirangkum dalam 6 area evaluasi pada Indeks KAMI yakni ditunjukkan pada gambar 2.9 berikut ini.

	tata kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi	Suplemen
Security Policies	✓	✓	✓			✓
Organisation of Information Security	✓	✓	✓			✓
Human Resource Security	✓		✓	✓		✓
Asset Management		✓		✓		✓
Access Control				✓	✓	✓
Cryptography				✓	✓	✓
Physical and Enviromental Security				✓		
Operations Security			✓	✓	✓	✓
Communication Security	✓		✓	✓	✓	✓
Systems acquisition, Development and Maintenance			✓	✓	✓	
Supplier Relationships				✓		
Information Security Incident Management	✓	✓	✓	✓	✓	✓
information Security Aspects of BCM	✓	✓	✓		✓	✓
Compliance	✓	✓	✓	✓	✓	✓

Gambar 2.9 Hubungan Antara Indeks KAMI 4.1 Dengan ISO 27001

2.8 Profil Dinas Komunikasi dan Informatika Kabupaten Kediri

Menurut Peraturan Bupati Kediri Nomor 51 Tahun 2016 Tentang Kedudukan, Susunan Organisasi, Uraian Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi

dan Informatik Kabupaten Kediri, Dinas Komunikasi dan Informatika Kabupaten Kediri adalah unsur pelaksana urusan Pemerintahan Daerah di bidang Komunikasi dan Informatika, urusan Pemerintahan Daerah di bidang Persandian dan urusan Pemerintahan Daerah di bidang Statistik. Dinas Komunikasi dan Informatika Kabupaten Kediri beralamat di Jalan Sekartaji Nomor 2, Doko, Kecamatan Ngasem, Kabupaten Kediri, Jawa Timur.

2.8.1 Tugas dan Fungsi

Tertuang pada Peraturan Bupati Kediri Nomor 51 Tahun 2016 Tentang Kedudukan, Susunan Organisasi, Uraian Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi dan Informatik Kabupaten Kediri pada BAB II Pasal 2 Dinas Komunikasi dan Informatika Kabupaten Kediri memiliki tugas membantu Bupati melaksanakan urusan pemerintahan yang menjadi kewenangan daerah di bidang Komunikasi, Informatika, Persandian dan Statistik. Untuk melaksanakan tugas sebagaimana yang telah dijabarkan diatas, maka Dinas Komunikasi dan Informatika Kabupaten Kediri menyelenggarakan fungsi sebagai berikut ini:

1. Perumusan kebijakan teknis di bidang komunikasi, informatika, persandian dan statistik.
2. Penyusunan perencanaan program dan anggaran di bidang komunikasi, informatika, persandian, dan statistik.
3. Pelaksanaan di bidang komunikasi, informatika, persandian dan statistik.
4. Pemantauan, evaluasi dan pelaporan atas pelaksanaan di bidang komunikasi, informatika, persandian dan statistik.
5. Koordinasi dan sinkronisasi pelaksanaan di bidang komunikasi, informatika, persandian, dan statistik.
6. Pembinaan penyelenggaraan di bidang komunikasi, informatika, persandian dan statistik.
7. Pelaksanaan administrasi di bidang komunikasi, informatika, persandian dan statistik.
8. Pelaksanaan administrasi di bidang komunikasi, informatika, persandian, dan statistik.
9. Penyusunan dan perumusan laporan kinerja secara periodik kepada Bupati.
10. Pelaksanaan tugas lain yang diberikan oleh Bupati sesuai dengan peraturan perundang-undangan.

2.8.2 Visi dan Misi

Visi dari Dinas Komunikasi dan Informatika Kabupaten Kediri adalah Terwujudnya Masyarakat Kabupaten Kediri yang sejahtera berbasis teknologi Komunikasi dan Informatika yang Efektif dan Efisien. Adapun misi Dinas

Komunikasi dan Informatika Kabupaten Kediri untuk mencapai visi yang diharapkan adalah sebagai berikut ini:

1. Meningkatkan kapasitas layanan informasi dan pemberdayaan potensi masyarakat dalam rangka mewujudkan masyarakat berbudaya informasi
2. Meningkatkan daya jangkau infrastruktur Komunikasi dan Informasi untuk memperluas aksesbilitas masyarakat terhadap infomasi dalam rangka mengurangi kesenjangan informasi.
3. Mendorong peningkatan aplikasi layanan publik dan industri aplikasi telematika dalam rangka meningkatkan nilai tambah layanan dan industri aplikasi.
4. Meningkatkan kerjasama dan kemitraan serta Pemberdayaan Lembaga Komunikasi dan Informatika Pemerintah dan masyarakat.
5. Meningkatkan kapasitas Sumber Daya Manusia (SDM) bidang Komunikasi dan Informatika dalam rangka meningkatkan Literasi dan Profesionalisme.

2.8.3 Struktur Organisasi Dinas Komunikasi dan Informatika Kabupaten Kediri

Adapun struktur organisasi pada Diskominfo Kabupaten Kediri yakni sebagai berikut:

Gambar 2. 10 Struktur Organisasi Dinas Komunikasi dan Informatika Kabupaten Kediri

Sumber: Peraturan Bupati Kediri Nomor 51 Tahun 2016

2.8.4 Seksi Sandi dan Keamanan Teknologi Informasi dan Komunikasi

Seksi Sandi dan Keamanan Teknologi Informasi dan Komunikasi memiliki tugas sebagai berikut ini:

- Penyiapan bahan perumusan dan pelaksanaan kebijakan, penyusunan norma, standar, prosedur dan kriteria, dan pemberian bimbingan teknis dan supervisi, serta pemantauan, evaluasi dan pelaporan terkait fungsi layanan monitoring trafik elektronik layanan penanganan insiden keamanan teknologi informasi dan komunikasi, mengelola berita sandi yang diterima dari Pusat, Provinsi dan Daerah lain.

2.9 Gambaran Pengelolaan Infrastruktur Teknologi Informasi Dinas Komunikasi dan Informatika Kabupaten Kediri

Infrastruktur Teknologi Informasi dan Komunikasi (TIK) dikelola pada Dinas Komunikasi dan Informatika Kabupaten Kediri yang digunakan untuk mendukung jalannya sistem TIK. Berikut merupakan infrastruktur TIK pada Dinas Komunikasi dan Informatika Kabupaten Kediri.

1. Jaringan Fiber Optik

   Jaringan Kabel Fiber Optik (FO) merupakan jaringan TI yang menggunakan kabel serat *optic* sebagai media komunikasi datanya. Jaringan FO terbagi menjadi 2 :

   a. Jaringan FO Milik Pemerintah Kabupaten Kediri
      Jaringan FO ini menjangkau seluruh Kantor SKPD (DPMPTSP, Pos Satpol, Disdag, Dinkop, Dukcapil, Dinkes, Balitbangda, Bapenda, Ruang Bupati, Bappeda, LPSE, BKD, dan Gedung baru Dinkes) dengan kantor dinas Komunikasi dan Informatika Kabupaten Kediri sebagai Backbone. Jaringan FO yang menghubungkan SKPD merupakan milik Pemerintah Kabupaten Kediri.

   b. Jaringan FO Sewa PT TELKOM (Metro)
      Jaringan FO yang menyebar ke Kantor Kecamatan menggunakan Jaringan Metro milik PT. TELKOM. Layanan tersebut merupakan bentuk kerjasama dan penguatan jaringan Dinas komunikasi dan Informatika. Jaringan FO ini merupakan jaringan utama dalam koneksi data di Pemerintah Kabupaten Kediri.

2. Jaringan Wireless Radio

   Jaringan Wireless Radio adalah jaringan TI yang memakai gelombang radio sebagai media dan inter koneksi datanya. Seluruh Kantor Kecamatan pada wilayah Kabupaten Kediri sudah terjangkau secara jaringan. Jaringan ini secara fisik berupa antenna dan Jaringan Radio yang dipasang pada menara yang dibangun di setiap Kantor Kecamatan di Wilayah Kabupaten Kediri. Fungsi utama jaringan wireless ini adalah sebagai jaringan Utama. Jaringan ini membawa Bandwidth local yang besar rata-rata 100 Mbps.

3. Tower

Sebagai upaya dalam mendukung Jaringan *Wireless* radio, maka diperlukan tower untuk memasang Radio agar dapat dihubungkan dengan jaringan Internet dan Internal Dinas Komunikasi dan Informatika Kabupaten Kediri.

Pada Wilayah Kabupaten Kediri terdapat 31 Tower yakni sebagai berikut:

Tabel 2.10 Tower Pemerintah Kabupaten Kediri

No	Lokasi	Jenis	Tinggi (m)	Tahun pembuatan
1	Diskominfo	SST	52	2017
2	Purwoasri	Triangle	32	2016
3	Kunjang	Triangle	40	2018
4	Papar	Triangle	32	2016
5	Plemahan	Triangle	40	2018
6	Kayen Kidul	Triangle	40	2018
7	Pagu	Triangle	32	2016
8	Pare	Triangle	32	2016
9	Badas	Triangle	32	2016
10	Kepung	Triangle	32	2016
11	Puncu	Triangle	40	2018
12	Gurah	Triangle	32	2016
13	Plosoklaten	Triangle	40	2018
14	Kandangan	Triangle	32	2016
15	Ngadiluwih	Triangle	32	2016
16	Kras	Triangle	40	2018
17	Kandat	Triangle	32	2016
18	Ringinrejo	Triangle	32	2016
19	Wates	Triangle	40	2018
20	Ngancar	Triangle	40	2018
21	Grogol	Triangle	32	2016
22	Tarokan	Triangle	40	2018
23	Banyakan	Triangle	40	2018
24	Semen	Triangle	32	2016
25	Mojo	Triangle	40	2018
26	Gampengrejo	Triangle	32	2016
27	Ngasem	Triangle	32	2016
28	Ubalan	Triangle	32	2017
29	Kelud	Triangle	32	2016
30	Pasar Induk	Triangle	32	2016
31	Pemkab	Triangle	40	2009

Sumber: Laporan Pengelolaan Infrastruktur TIK Dinas Komunikasi dan Informatika Kabupaten Kediri (2019)

4. Mesin Absensi

Mesin absensi merupakan sebuah perangkat yang digunakan untuk mengetahui dan melacak kehadiran pegawai pada Pemerintah Kabupaten Kediri. Mesin absensi pada Pemerintah Kabupaten Kediri dikelola oleh Dinas Komunikasi dan Informatika Kabupaten Kediri dan terbagi menjadi 2 (dua) yaitu Mesin Absensi *Finger Print* dan Mesin absensi Wajah.

5. *Network Operation Center* (NOC)

Network Operation Center (NOC) merupakan sebuah tempat untuk meletakkan sistem komputer serta komponen lainnya yang berhubungan secara terpusat dan mencakup sistem komunikasi dan penyimpanan data. Pada *data center* terdapat komputer server yang memiliki fungsi menyediakan layanan teknologi indormasi dalam sebuah jaringan komputer yang dapat diakses dengan mudah oleh komputer klien pada jaringan komputer Pemerintah Kabupaten Kediri. Dinas Komunikasi dan Informatika Kabupaten Kediri saat ini mengelola 15 server. Berikut pada tabel 2.9 merupakann spesifikasi server *data center* pada Dinas Komunikasi dan Informatika Kabupaten Kediri.

Tabel 2.11 Spesifikasi Server *Data Center* Dinas Komunikasi dan Informatika Kabupaten Kediri

No	Nama Server	Merk	Type	CPU	RAM	HDD
1	Server 1	IBM	x3650 M4	XEON F5-2697v2	16 GB	2x1 TB
2	Server 2	IBM	x3650 M5	XEON F5-2697v2	16 GB	2x1 TB
3	Server 3	IBM	x3650 M6	XEON F5-2697v2	16 GB	2x1 TB
4	Server 4	IBM	x3650 M7	XEON F5-2697v2	16 GB	2x1 TB
5	Server 5	IBM	x3650 M8	XEON F5-2697v2	32 GB	3x1 TB
6	Server 6	IBM	x3650 M9	XEON F5-2697v2	16 GB	1x1 TB
7	Server 7	IBM	x3650 M10	XEON F5-2697v2	8 GB	2x300 MB
8	Server 8	IBM	x3650 M11	XEON F5-2697v2	16 GB	2x1 TB
9	Server 9	IBM	x3650 M12	XEON F5-2697v2	16 GB	2x1 TB
10	Server 10	IBM	x3650 M13	XEON F5-2697v2	16 GB	2x1 TB
11	Server 11	HPE	DL380 GEN9	XEON F5-2697v4	96 GB	2x1,2 TB
12	Server 12	HPE	DL380 GEN10	XEON F5-2697v4	96 GB	2x1,2 TB
13	Server 13	HPE	DL380 GEN11	XEON F5-2697v4	96 GB	2x1,2 TB
14	Server 14	HPE	DL380 GEN10	Xeon® Silver 4114 (2.2GHz/10-core/85W	128 GB	2,4x1 TB

Tabel 2.12 Spesifikasi Server *Data Center* Dinas Komunikasi dan Informatika Kabupaten Kediri (lanjutan)

15	Server 15	HPE	DL380 GEN10	Xeon® Silver 4114 (2.2GHz/10-core/85W	128 GB	2,4x1 TB

Sumber: Laporan Pengelolaan Infrastruktur TIK Dinas Komunikasi dan Informatika Kabupaten Kediri (2019)

Pada server-server tersebut diatas, terdapat aplikasi teknologi informasi dan komunikasi yang digunakan untuk mengirimkan pesan yang diperlukan oleh pengguna. Selain itu, aplikasi-aplikasi tersebut juga digunakan untuk mendukung proses kerja pada pemerintahan agar berjalan lebih efektif dan efisien sebagai sarana untuk memproses informasi. Berikut merupakan aplikasi-aplikasi yang tertanam pada server akan ditunjukkan pada tabel 2.10.

Tabel 2.13 Aplikasi-aplikasi Pada Server *Data Center* Dinas Komunikasi dan Informatika Kabupaten Kediri

No	Nama Aplikasi	Link Alamat
1	BKD Single window	bsw.kedirikab.go.id
2	Sistem Managemen Kearsipan Terpadu (SMKT)	smkt.kedirikab.go.id
3	Sistem Absensi Jari Online (SIABJO)	siabjo.kedirikab.go.id
4	Sistem PPDB	ppdb.kedirikab.go.id
5	Sistem Informasi Pengelolaan Keuangan Sekolah (SIPKS)	sipks.kedirikab.go.id
6	Sistem Informasi Profil Sekolah (SIMPROSEK)	simprosek.kedirikab.go.id
7	Sistem Informasi Perizinan Satu Pintu Kab. Kediri (SIMPATIK)	simpatik.kedirikab.go.id
8	Web Hosting Machine (WHM) - Cpanel	panel.kedirikab.go.id
9	Website Disarpus	arsip.kedirikab.go.id
10	Website Bakesbangpol	bakesbangpol.kedirikab.go.id
11	Website Bapenda	bapenda.kedirikab.go.id
12	Website Bappeda	bappeda.kedirikab.go.id
13	Website BKD	bkd.kedirikab.go.id
14	Website BPBD	bpbd.kedirikab.go.id
15	Website Disdukcapil	dukcapil.kedirikab.go.id
16	Website Desa	desa.kedirikab.go.id
17	Website DPMPD	dinaspmpd.kedirikab.go.id
18	Website Dinkes	dinkes.kedirikab.go.id
19	Website Dinsos	dinsos.kedirikab.go.id
20	Website Disdikpora	disdik.kedirikab.go.id

Tabel 2.14 Aplikasi-aplikasi Pada Server *Data Center* Dinas Komunikasi dan Informatika Kabupaten Kediri (lanjutan)

21	Website Dishub	dishub.kedirikab.go.id
22	Website Diskopum	diskopum.kedirikab.go.id
23	Website Disnaker	disnaker.kedirikab.go.id
24	Website DPMPTSP	dpmptsp.kedirikab.go.id
25	Aplikasi e-audit	e-audit.kedirikab.go.id
26	Aplikasi e-planning	e-planning.kedirikab.go.id
27	Aplikasi e-sakip	e-sakip.kedirikab.go.id
28	Aplikasi e-surat	esurat.kedirikab.go.id
29	Website Inspektorat	inspektorat.kedirikab.go.id
30	Website DP2KBP3A	dp2kbp3a.kedirikab.go.id
31	Aplikasi MPA-DPRD	mpa-dprd.kedirikab.go.id
32	Website Dinas Perikanan	perikanan.kedirikab.go.id
33	Website PPID Pemkab Kediri	ppid.kedirikab.go.id
34	Website RSUD Pare	rsud.kedirikab.go.id
35	Aplikasi SIMPUS	simpus.kedirikab.go.id
36	Website TPID	tpid.kedirikab.go.id
37	Website Resmi Pemkab Kediri	kedirikab.go.id
38	Ekinerja	ekinerja.kedirikab.go.id
39	TV Kedirilagi	kediritvlagi.kedirikab.go.id
40	Simoti	simoti.kedirikab.go.id
41	Sistem Informasi data Pembangunan	sidp.kedirikab.go.id
42	LPSE	lpse.kedirikab.go.id
43	Website Dinas Komunikasi dan informatika	diskominfo.kedirikab.go.id
44	Website bagian hukum	jdih.kedirikab.go.id
45	Website Dinas Arsip	disarpus.kedirikab.go.id
46	Website aplikasi milik bapenda	e-sptpd.kedirikab.go.id
47	Website Diskpusmik	diskopusmik.kedirikab.go.id
48	Website bagian organisasi	bagianorganisasi.kedirikab.go.id
49	Website aplikasi milik diskominfo	sippol.kedirikab.go.id
50	Website aplikasi milik bapenda	e-bphtb.kedirikab.go.id
51	Website aplikasi milik diskominfo	sibuton.kedirikab.go.id
52	Website aplikasi milik diskominfo	silab.kedirikab.go.id
53	Website aplikasi milik diskominfo	berita.kedirikab.go.id
54	Website aplikasi milik diskominfo	portal.kedirikab.go.id
55	Website aplikasi milik diskominfo	sincan.kedirikab.go.id
56	Website aplikasi milik bappeda	silandakbappeda.kedirikab.go.id
57	Website Disnaker	e-daflatker.kedirikab.go.id

Tabel 2.15 Aplikasi-aplikasi Pada Server *Data Center* Dinas Komunikasi dan Informatika Kabupaten Kediri (lanjutan)

58	Website Disnaker	e-pmi.kedirikab.go.id
59	Website RSUD SLG	rsudslg.kedirikab.go.id
60	Website Dispertabun	pertabun.kedirikab.go.id
61	Website BPKAD	bpkad.kedirikab.go.id
62	Website aplikasi inspektorat	itkab.kedirikab.go.id
63	Website kecamatan plosoklaten	sepawonkecplosoklaten.kedirikab.go.id
64	Website kecamatan Puncu	puncukecpuncu.kedirikab.go.id
65	Website kecamatan kepung	besowokeckepung.kedirikab.go.id

Sumber: Laporan Pengelolaan Infrastruktur TIK Dinas Komunikasi dan Informatika Kabupaten Kediri (2019)

Pada Dinas Komunikasi dan Informatika Kabupaten Kediri saat ini menggunakan 2 (dua) provider untuk mendukung jaringan internet yang antara lain adalah sebaga berikut ini.

- *Bandwidth* Global dan *Bandwidth* Domestik menggunakan jaringan Telkom dengan kapasitas Bandwidth 550 Mbps.
- *Bandwidth* Global dan *Bandwidth* Domestik backup menggunakan Icon plus dengan kapasita 60 Mbps

Dinas Komunikasi dan Infornatika juga memiliki fasilitas pendukung yang diantaranya ialah sebagai berikut ini:

1. Ruang AC

   Pada Dinas Komunikasi dan Informatika Kabupaten Kediri memiliki ruang AC untuk *data center* dengan ukuran 4x4 meter. Ruangan ini dilengkapi 2x2 berjenis AC 2PK. AC tersebut bekerja bergantian menyala yakni setiap 4 jam sekali untuk menjaga kestabilan suhu pada ruangan tersebut selalu berada pada 16 derajat celcius.

2. Sistem Keamanan

   Sistem keamanan terdiri dari 2 (dua) jenis yakni keamanan fisik dan non fisik. Pada keamanan fisik digunakan mesin finger lock pada pintu ruangan server. Sedangkan untuk keamanan non fisik, menggunakan firewall pada setiap *software* dan *hardware*.

3. Layanan 7 X 24 Jam

   Sebagai upaya untuk melayani masyarakat dengan baik, data center pada Dinas Komunikasi dan Informatika Kabupaten Kediri tidak pernah mati dan beroperasi secara penuh.

4. Sistem Pemadam Kebakaran

Ruang *data center* dilengkapi tabung pemadam kebakaran tipe C yang berfungsi untuk memadamkan api yang bersumber dari listrik.

5. Listrik

Listrik pada *data center* Dinas Komunikasi dan Informatika Kabupaten Kediri didukung dari 2 sumber yang diantaranya adalah sebagai berikut ini.

1) UPS

Uninteruptible Power Supply atau UPS merupakan sebuah perangkat *hardware* yang memiliki fungsi untuk memberikan suplai listrik apabila suplai listrik utama sedang tidak berfungsi. jumlah UPS yang tersedia adalah 5 unit. Berikut merupakan spesifikasi UPS pada data center:

- BM 6000 VA LCD 4U Rack UPS
- Tipe IBM 5395 KX
- Memiliki ketahanan 5 jam saat listrik utama tidak berfungsi

2) Genset

Generator Set atau Genset merupakan sebuah perangkat yang terdiri dari 2 (dua) perangkat yang berbeda yakni *generator* dan *engine* yang berfungsi untuk menghasilkan daya listrik. *Generator* berfungsi sebagai perangkat untuk pembangkit listrik. Sedangkan engine atau mesin berfungsi sebagai alat pemutar yang berbahan bakar bensin atau solar. Berikut merupakan spesifikasi genset pada Dinas Komunikasi dan Informatika Kabupaten Kediri

- Perkins 45 KVA tipe 1103A-33TG1
- Sistem ATS (*Automatic Transfer Switch*) *on-off*. Sistem ini memiliki arti bahwa genset akan secara otomatis menyala ketika listrik utama sedang tidak berfungsi.

6. Komputer

Pada ruang infrastruktur dan *e-government* Dinas Komunikasi dan Informatika Kabupaten Kabupaten Kediri terdapat komputer yang berfungsi untuk melakukan monitoring terhadap jaringan FO, Metro Telkom, Jaringan Radio, Router, CCTV, Mesin Absensi, dan juga untuk membuat program yang dibutuhkan SKPD dan Kecamatan pada Kabupaten Kediri.

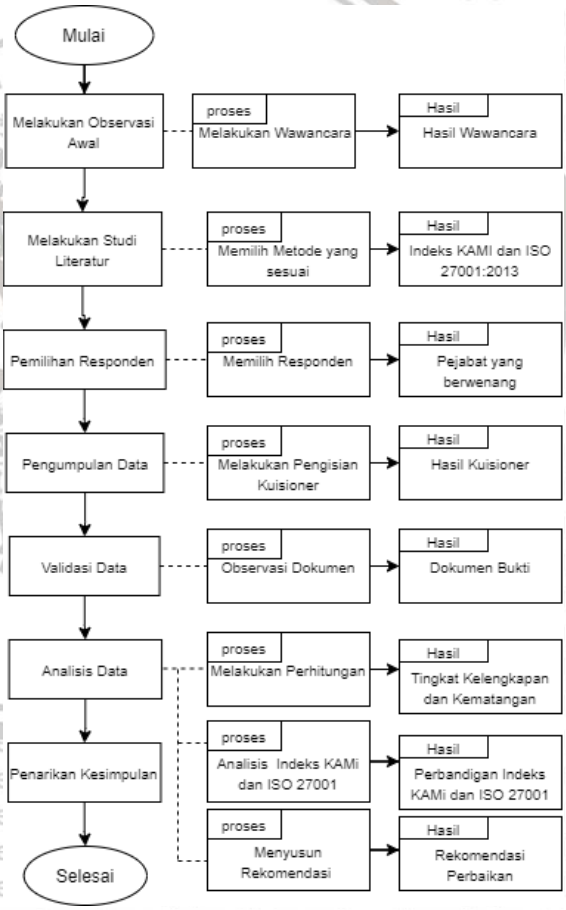
7. CCTV

Closed Circuit Television atau CCTV merupakan sebuah kamera video digital yang memiliki fungsi untuk melakukan pemantauan untuk pengiriman sinyal video dalam suatu ruang yang mana sinyal tersebut kemudian akan diteruskan pada sebuah layar monitor. CCTV berfungsi untuk melakukan pemantauan terkait dengan kondisi pada sebuah tempat dan berkaitan dengan keamanan atau aktivitas di sebuah instansi Seluruh SKPD dan kecamatan pada Pemerintah kabupaten kediri saat ini telah terpasang kamera CCTV yang dapat diakses secara *realtime* dan online oleh pejabat atau orang yang diberi kewenangan untuk mengaksesnya. Dinas Komunikasi dan Informatika Kabupaten Kediri memiliki kewenangan untuk melakukan instalasi dan pemeliharaan CCTV di pemerintah kabupaten kediri sesuai dengan permintaan SKPD dan kecamatan yang membutuhkan.

BAB 3 METODOLOGI PENELITIAN

3.1 Metode Penelitian

Penelitian dengan judul "Evaluasi Keamanan Informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri dengan Menggunakan Indeks KAMI" merupakan evaluasi tipe 3 yang merupakan gabungan antara *Criteria-based evaluation* dan *IT-systems as such* yang berarti bahwa evaluasi dilakukan sesuai dengan standar atau kriteria (*framework*) tertentu yang mana objek evaluasinya adalah sistem TI itu sendiri tanpa melibatkan pengguna. Standar yang digunakan pada evaluasi ini adalah Indeks KAMI dan kontrol ISO 27001:2013. Dalam penelitian ini terdapat beberapa proses yang akan dilakukan dalam metode penelitian, berikut pada gambar 3.1 ditunjukkan diagram alir penelitian ini.



Gambar 3.1 Diagram Alir Penelitian

3.1.1 Penjelasan Alur Penelitian

Pada Gambar 3.1 menunjukkan diagram alir penelitian yang akan dilakukan yang dijelaskan sebagai berikut:

1. Melakukan observasi awal untuk mengidentifikasi permasalahan terkait keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Observasi dilakukan dengan melakukan wawancara kepada pejabat yang memiliki wewenang pada Dinas Komunikasi dan Informatika Kabupaten Kediri.
2. Melakukan studi literatur dengan membaca penelitan terdahulu, paper, dan jurnal untuk mengetahui metode yang sesuai untuk dilakukan evaluasi terhadap keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri sehingga didapatkan alat bantu Indeks KAMI.
3. Melakukan pemilihan responden yang sesuai dengan panduan Indeks KAMI yaitu pejabat berwenang yang bertanggung jawab terhadap keamanan informasi.
4. Melakukan pengumpulan data dengan melakukan wawancara menggunakan instrument kuisioner indeks KAMI.
5. Melakukan validasi data dengan melakukan observasi dokumen untuk memverifikasi data yang diperoleh dari kuisioner sesuai dengan keadaan yang sebenarnya.
6. Melakukan analisis data kuisioner yang diperoleh sesuai dengan panduan indeks KAMI. Selanjutnya membandingkan hasil yang diperoleh dari evaluasi menggunakan Indeks KAMI dengan kontrol ISO 27001:2013 dan dilanjutkan dengan menyusun rekomendasi perbaikan.
7. penyusunan kesimpulan terhadap evaluasi yang telah dilakukan serta penyusunan saran kepada Dinas Komunikasi dan Informatika Kabupaten Kediri dan penelitian selanjutnya.

3.2 Melakukan Observasi Awal

Tahap awal yang dilakukan adalah melakukan observasi awal. Observasi dilakukan bertujuan untuk menggali informasi yang akurat terkait kondisi keamanan informasi serta permasalahan yang dihadapi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Observasi dilakukan dengan melakukan wawancara kepada pejabat yang memiliki wewenang pada Dinas Komunikasi dan Informatika Kabupaten Kediri yang sesuai dengan pedoman indeks KAMI.

3.3 Melakukan Studi Literatur

Melakukan studi literatur dengan membaca penelitan terdahulu, paper, dan jurnal untuk mengetahui metode yang sesuai untuk dilakukan evaluasi terhadap keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri sehingga didapatkan alat bantu Indeks Keamanan Informasi (KAMI) yang sesuai untuk melaksanakan evaluasi.

3.4 Pemilihan Responden

Tahap selanjutnya adalah melakukan pemilihan responden sesuai dengan panduan Keamanan Informasi (KAMI) untuk melakukan pengumpulan data yang dibutuhkan. Pada pemilihan responden kali ini, tidak diperlukan melakukan pemetaan peran dan tugas menggunakan RACI CHART. Hasil ini disebabkan karena proses pemilihan responden adalah berdasarkan pada panduan karakteristik Indeks KAMI yang mana responden terpilih merupakan pejabat berwenang yang bertanggung jawab terhadap keamanan informasi.

3.5 Pengumpulan Data

Tahap ini dilakukan pengumpulan data untuk memperoleh informasi yang diharapkan agar tujuan penelitian dapat tercapai. Pengumpulan data ini dilakukan dengan wawancara terstruktur yang berpedoman pada pertanyaan dan pilihan jawaban yang telah ada yang sesuai kuisioner pertanyaan yang mengacu pada Indeks KAMI 4.1 yang terdiri dari 2 (dua) kategori yaitu Kategori Sistem Elektronik dan area pengamanan informasi.

3.6 Validasi Data

Setelah dilakukaannya pengumpulan data, selajutnya dilakukan validasi data untuk memverifikasi keadaan sebenarnya berdasarkan dengan data yang diperoleh saat pengisian kuisioner. Validasi data dilakukan dengan menggunakan teknik triangulasi data. Triangulasi data adalah teknik yang digunakan untuk mendapatkan data yang akurat dan absah untuk meningkatkan derajat kepercayaan (Siregar & Harahap, 2019). Triangulasi yang digunakan pada penelitian ini merupakan triangulasi metode. Triangulasi metode merupakan teknik mencari keabsahan data dengan digunakannya lebih dari satu metode pengumpulan data (Bachri, 2010). Penelitian kali ini dilakukan dengan 2 (dua) metode yakni wawancara dan *checklist*. *Checklist* dilaksanakan dengan melakukan observasi dokumen dan dilakukan dengan bertatap muka secara langsung dengan responden. Setiap pertanyaan yang telah dijawab dibuktikan dengan dokumen pendukung untuk memverifikasi jawaban yang diberikan oleh responden. Setiap jawaban dengan status "Dalam Penerapan atau Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh" membutuhkan dokumen pendukung untuk mendukung jawaban kuisioner yang diberikan.

3.7 Analisis Data

Data yang pakai pada penelitian merupakan data primer. Definisi data primer merupakan data yang mana sumbernya diperoleh dari sumber pertama atau sumber asli. Analisis data penelitian ini dilakukan menggunakan formula *excel* sesuai dengan panduan Indeks KAMI yang tersedia. Peneliti memasukkan jawaban-jawaban dari responden yang telah didapatkan dari pengumpulan data ke formula *excel* tersebut yang nantinya akan menghasilkan skor nilai yaitu tingkat kesiapan pengamanan informasi (kelengkapan dan kematangan)

berbentuk tabel pada masing-masing area pengamanan informasi dan diagram radar 5 (lima) sumbu area. Selanjuntnya dilakukan analisis kontrol pada Indeks KAMI dengan ISO 27001 berdasarkan hasil evaluasi untuk menganalisis *gap* yang terjadi pada instansi terkait dengan dokumen yang disyaratkan pada standar ISO 27001:2013. Dan dilanjutkan dengan menyusun rekomendasi perbaikan sesuai dengan kontrol ISO/IEC 27001:2013.

3.8 Penarikan Kesimpulan

Tahap terakhir adalah penyusunan kesimpulan berdasarkan rumusan masalah yang telah dijabarkan serta berisi mengenai penjabaran terhadap analisis data serta hasil dari pembahasan yang telah dilaksanakan. Serta penulis juga memberikan saran kepada Dinas Komunikasi dan Informatika Kabupaten Kediri dan penelitian selanjutnya.

BAB 4 HASIL DAN ANALISIS

Berdasarkan yang dijelaskan pada sub bab 3.3 yaitu pada tahapan pemilihan responden, yang mana responden yang dipilih berdasarkan panduan Indeks KAMI yaitu pejabat berwenang yang bertanggung jawab terhadap keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Berikut merupakan data responden pada penelitian ini.

4.1 Karakteristik Responden

No	Nama	Jabatan	Tugas
1	Arik Fefriyono A.Md	Pengelola Keamanan Sistem Informasi / Staff Seksi Sandi dan Keamanan Teknologi Informasi	- Penyiapan bahan perumusan dan pelaksanaan kebijakan, penyusunan norma, standar, prosedur dan kriteria, dan pemberian bimbingan teknis dan supervisi - Pemantauan, evaluasi dan pelaporan terkait fungsi layanan monitoring trafik elektronik Layanan penanganan insiden keamanan teknologi informasi dan komunikasi - Mengelola berita sandi yang diterima dari Pusat, Provinsi dan Daerah lain - Koordinasi terkait layanan sandi dan keamanan TIK - Monitoring terkait layanan Sumberdaya TIK, Monitoring Firewall, Penggunaan Sertifikat SSL domain dan subdomain

4.2 Kategori Sistem Elektronik

Pada kategori sistem elektronik dilakukan penilaian yang bertujuan untuk mengevaluasi tingkat atau kategori sistem elektronik yang digunakan oleh Dinas Komunikasi dan Informatika Kabupaten Kediri. Sebelum responden melakukan pengisian kuisioner, diawali dengan mendefinisikan ruang lingkup yang terdiri dari:

- Pengelolaan infrastruktur TIK (termasuk 15 server) yang ada dilakukan oleh Diskominfo Kabupaten Kediri.
- Tanggung jawab Diskominfo Kabupaten Kediri dalam mengelola infrastruktur TIK hanya sebatas pada SKPD induk dan kantor kecamatan.

Berikut pada tabel 4.1 ditampilkan hasil dari penilaian kategori sistem elektronik

Tabel 4.1 Data Penilaian Kategori Sistem Elektronik

Bagian I: Kategori Sistem Elektronik		
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan		
Total Pertanyaan	**10**	
Pilihan Jawaban	**Hasil**	**Skor**
A	1	5
B	4	2
C	5	1
Total Skor		**18**

Tabel 4.1 merupakan hasil pengumpulan data penilaian kategori sistem elektronik. Pada penilaian kategori sistem elektronik tersedia 10 pertanyaan untuk dijawab responden berdasarkan pilihan jawaban yang tersedia yaitu A,B dan C. Pertanyaan dengan pilihan jawaban "A" memperoleh hasil sebanyak 1 pertanyaan dengan skor total yaitu 5. Pertanyaan dengan pilihan jawaban "B" memperoleh hasil sebanyak 4 pertanyaan dengan skor total 8. Pertanyaan dengan pilihan jawaban "C" memperoleh hasil sebanyak 5 pertanyaan dengan skor total 5. Skor total yang diperoleh pada kategori sistem elektronik ini adalah 18 yang termasuk pada kategori "**Tinggi"** yang memiliki arti bahwa proses kerja yang dijalankan Dinas Komunikasi dan Informatika Kabupaten Kediri tidak dapat terpisahkan dengan sistem elektronik.

4.3 Tata Kelola Keamanan Informasi

Tabel 4.2 Data Penilaian Area Tata Kelola Keamanan Informasi

Bagian II: Tata Kelola Keamanan Informasi							
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi							
Jumlah Pertanyaan	**KP1**		**KP2**		**KP3**		**Total**
	8		8		6		22
Hasil Jawaban							
Kategori Pengamanan	**KP1**	**Skor KP1**	**KP2**	**Skor KP2**	**KP3**	**Skor KP3**	**Total**
Tidak Dilakukan	1	0	0	0	3	0	0
Dalam Perencanaan	2	2	8	16	3	0	18
Dalam Penerapan/Diterapkan Sebagian	0	0	0	0	0	0	0
Diterapkan Secara Menyeluruh	5	15	0	0	0	0	15
Total Nilai Evaluasi Tata Kelola							**33**

Tabel 4.2 merupakan data penilaian area tata kelola keamanan informasi. Dalam area ini memiliki jumlah pertanyaan sebanyak 22 pertanyaan. Pertanyaan terbagi dalam 3 (tiga) kategori yakni terdiri dari 8 pertanyaan dengan kategori pengamanan 1, 8 pertanyaan dengan kategori pengamanan 2 dan 6 pertanyaan pada kategori pengamanan 3.

Responden menjawab pertanyaan-pertanyaan yang ada dengan memilih salah satu opsi jawaban yang ada yaitu “Tidak Dilakukan”, “Dalam Perencanaan”, “Dalam Penerapan/Diterapkan Sebagian” dan “Diterapkan Secara Menyeluruh” sesuai kondisi sebenarnya. Setelah dilakukan validasi dokumen, Terdapat 1 (satu) pertanyaan yang tidak dapat dibuktikan yaitu pada pertanyaan no 2.7 tentang keahlian serta kompetensi memadai yang harus dimiliki seluruh pelaksana keamanan informasi yang ada sehingga status jawaban diturunkan pada status “Dalam Perencanaan”. *Checklist* validasi dokumen dilampirkan pada poin 4.16.

Untuk pertanyaan dengan jawaban “Tidak Dilakukan” pada kategori pengamanan 1 berjumlah 0, Kategori pengamanan 2 berjumlah 0, dan kategori pengamanan 3 berjumlah 3 pertanyaan. Selanjutnya pertanyaan dengan status “Dalam Perencanaan” pada kategori pengamanan 1 berjumlah 2, kategori pengamanan 2 berjumlah 8, dan kategori pengamanan 3 berjumlah 3

pertanyaan. Selanjutnya pertanyaan dengan jawaban "Dalam Penerapan/Diterapkan Sebagian" pada kategori pengamanan 1 berjumlah 0, kategori pengamanan 2 berjumlah 0, dan kategori pengamanan 3 berjumlah 0 pertanyaan. Untuk pertanyaan dengan jawaban "Diterapkan Secara Menyeluruh" pada kategori pengamanan 1 berjumlah 5, kategori pengamanan 2 sebanyak 0, dan kategori pengamanan 3 berjumlah 0 pertanyaan. adalah 33. Total skor yang diperoleh pada area ini adalah 33.

Tabel 4.3 Data Tingkat Kematangan Area Tata Kelola Keamanan Informasi

Jumlah Pertanyaan Tingkat Kematangan	**II**	**III**	**IV**	**V**	**Total**
	13	3	6	0	22
Hasil Jawaban					
Status Pengamanan	**II**	**III**	**IV**	**V**	**Total**
Tidak Dilakukan	1	0	3	0	4
Dalam Perencanaan	7	3	3	0	13
Dalam Penerapan/Diterapkan Sebagian	0	0	0	0	0
Diterapkan Secara Menyeluruh	5	0	0	0	5
Total	**13**	**3**	**6**	**0**	**22**

Tabel 4.3 menyajikan data penilaian tingkat kematangan area tata kelola keamanan informasi. Dalam area ini, jumlah pertanyaan pada tingkat kematangan II sebanyak 13 pertanyaan dengan memperoleh hasil yakni 1 pertanyaan dengan status "Tidak Dilakukan", 7 pertanyaan dengan status "Dalam Perencanaan",0 pertanyaan dengan status "Dalam Penerapan/Diterapkan Sebagian", dan 5 pertanyaan dengan status "Diterapkan Secara Menyeluruh.

Jumlah pertanyaan tingkat kematangan III yaitu 3, dengan memperoleh hasil 0 pertanyaan dengan status "Tidak Dilakukan", 3 pertanyaan dengan status "Dalam Perencanaan", 0 pertanyaan dengan status "Dalam Penerapan/ Diterapkan Sebagian" dan 0 pertanyaan dengan status "Diterapkan Secara Menyeluruh". Tingkat kematangan IV terdapat 6 pertanyaan yang memperoleh hasil 3 pertanyaan dengan status "Tidak Dilakukan" , 3 pertanyaan dengan status "Dalam Perencanaan", 0 pertanyaan dengan status "Dalam Penerapan/Diterapkan Sebagian" dan 0 pertanyaan dengan status "Diterapkan Secara Menyeluruh". Berdasarkan dari data penilaian yang diperoleh, tingkat kematangan tata kelola keamanan informasi mencapai tingkat I+ (Reaktif/kondisi awal).

4.4 Pengelolaan Risiko Keamanan Informasi

Tabel 4.4 Data Penilaian Area 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.							
Jumlah Pertanyaan	**KP1**		**KP2**		**KP3**		**Total**
	10		4		2		16
Hasil Jawaban							
Kategori Pengamanan	**KP1**	**Skor KP1**	**KP2**	**Skor KP2**	**KP3**	**Skor KP3**	**Total**
Tidak Dilakukan	7	0	1	0	2	0	**0**
Dalam Perencanaan	3	3	3	6	0	0	**9**
Dalam Penerapan/Diterapkan Sebagian	0	0	0	0	0	0	**0**
Diterapkan Secara Menyeluruh	0	0	0	0	0	0	**0**
Total Nilai Evaluasi Pengelolaan Risiko							**9**

Data penilaian pada area pengelolaan risiko keamanan informasi ditampilkan pada tabel 4.4. Pada area ini memiliki jumlah pertanyaan sebanyak 16 pertanyaan. Pertanyaan terbagi dalam 3 (tiga) kategori yakni terdiri dari 10 pertanyaan dengan kategori pengamanan 1, 4 pertanyaan dengan kategori pengamanan 2 dan 2 pertanyaan dengan kategori pengamanan 3.

Responden menjawab pertanyaan dengan memilih opsi jawaban yang tersedia antara lain "Tidak Dilakukan", "Dalam Perencanaan", "Dalam Penerapan/ Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh" sesuai dengan kondisi sebenarnya. Pada area ini, diperoleh 1 (satu) pertanyaan yang memiliki status jawaban "Dalam Penerapan/ Diterapkan Sebagian" yakni pada no 3.2. Pertanyaan tersebut yaitu no 3.2 tentang penanggung jawab pengelolaan manajemen risiko keamanan informasi serta tanggung jawab untuk melaporkan status pengelolaan risiko keamanan informasi pada pimpinan tidak dapat dibuktikan dokumen pendukungnya sehingga status jawaban diturunkan pada status "Dalam Perencanaan". *Checklist* validasi dokumen dilampirkan pada poin 4.16.

Pertanyaan dengan status jawaban "Tidak Dilakukan" pada kategori pengamanan 1 sebanyak 7 pertanyaan, 1 pertanyaan pada kategori pengamanan 2 dan 2 pertanyaan pada kategori pengamanan 3 yang masing-masing kategori

pengamanan memperoleh skor 0. Pertanyaan dengan status jawaban "Dalam Perencanaan" pada kategori pengamanan 1 sebanyak 3 pertanyaan dengan total skor yaitu 3, 3 pertanyaan pada kategori pengamanan 2 dengan total skor yaitu 6 dan 0 pertanyaan pada kategori pengamanan 3 dengan total skor yaitu 0. Pertanyaan dengan status jawaban "Dalam Penerapan/Diterapkan Sebagian" pada kategori pengamanan 1 sebanyak 0 pertanyaan dengan skor 0, 0 pertanyaan pada kategori pengamanan 2 dan kategori pengamanan 3 dengan total skor yaitu 0. Total skor yang diperoleh pada area ini adalah 9.

Tabel 4.5 Data Tingkat Kematangan Area Pengelolaan Risiko Keamanan Informasi

Jumlah Pertanyaan Tingkat Kematangan	**II**	**III**	**IV**	**V**	**Total**
	10	2	2	2	16
Hasil Jawaban					
Status Pengamanan	**II**	**III**	**IV**	**V**	**Total**
Tidak Dilakukan	7	0	1	2	10
Dalam Perencanaan	3	2	1	0	6
Dalam Penerapan/ Diterapkan Sebagian	0	0	0	0	0
Diterapkan Secara Menyeluruh	0	0	0	0	0
Total	**10**	**2**	**2**	**2**	**16**

Dijabarkan pada Tabel 4.5 merupakan data tingkat kematangan area pengelolaan risiko kemanan informasi. Jumlah pertanyaan pada tingkat kematangan II sebanyak 10 pertanyaan, jumlah pertanyaan pada tingkat kematangan III sebanyak 2 pertanyaan, jumlah pertanyaan pada tingkat kematangan IV sebanyak 2 pertanyaan dan jumlah pertanyaan pada tingkat kematangan V sebanyak 2 pertanyaan.

Pertanyaan tingkat kematangan II memperoleh status jawaban "Tidak Dilakukan" sebanyak 7 pertanyaan, 3 pertanyaan dengan status jawaban "Dalam Perencanaan", 0 pertanyaan dengan status jawaban "Dalam Penerapan/Diterapkan Sebagian" dan 0 pertanyaan dengan status jawaban "Diterapkan Secara Menyeluruh". Pada pertanyaan tingkat kematangan III, pertanyaan dengan status jawaban "Tidak Dilakukan" sebanyak 0 pertanyaan, 2 pertanyaan dengan status jawaban "Dalam Perencanaan" serta 0 pertanyaan untuk status jawaban "Dalam Penerapan/ Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh". Pada pertanyaan tingkat kematangan IV, pertanyaan dengan status jawaban "Tidak Dilakukan" sebanyak 1 pertanyaan dan 1 pertanyaan dengan status jawaban "Dalam Perencanaan". Pada pertanyaan tingkat kematangan V, 2 pertanyaan dengan status jawaban "Tidak

Dilakukan". Berdasarkan dari data yang telah diperoleh, tingkat kematangan yang diperoleh pada area ini mencapai pada tingkat I.

4.5 Kerangka Kerja Pengelolaan Keamanan Informasi

Tabel 4.6 Data Penilaian Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi							
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya							
Jumlah Pertanyaan	**KP1**		**KP2**		**KP3**		**Total**
	12		10		7		29
Hasil Jawaban							
Kategori Pengamanan	**KP1**	**Skor KP1**	**KP2**	**Skor KP2**	**KP3**	**Skor KP3**	**Total**
Tidak Dilakukan	3	0	5	0	3	0	0
Dalam Perencanaan	9	9	5	10	3	0	19
Dalam Penerapan/Diterapkan Sebagian	0	0	0	0	0	0	0
Diterapkan Secara Menyeluruh	0	0	0	0	0	0	0
Total Nilai Evaluasi Kerangka Kerja							**19**

Data penilaian area kerangka kerja pengelolaan keamanan informasi ditampilkan pada tabel 4.6. Pada area ini memiliki jumlah pertanyaan sebanyak 29 pertanyaan. Pertanyaan terbagi dalam 3 (tiga) kategori yakni terdiri dari 12 pertanyaan dengan kategori pengamanan 10 pertanyaan dengan kategori pengamanan 2 serta 7 pertanyaan pada kategori pengamanan 3.

Responden menjawab pertanyaan dengan memilih opsi jawaban yang tersedia antara lain "Tidak Dilakukan", "Dalam Perencanaan", "Dalam Penerapan/ Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh" sesuai dengan kondisi sebenarnya. Pada area ini, terdapat 6 (enam) pertanyaan yang tidak dapat ditunjukkan bukti pendukungnya yaitu pertanyaan pada no 4.12 terkait diterapkannya mekanisme untuk melakukan evaluasi padarisiko berkaitan dengan pembelian sistem atau pengimplementasian sistem baru, no 4.13 tentang penerapan proses mengembangkan sistem informasi yang aman (*Secure SDLC*), no 4.20 terkait ketersediaan strategi dalam menerapkan keamanan informasi yang disesuaikan dengan hasil analisa risiko, 4.21 tentang ketersediaan strategi pemanfaatan teknologi keamanan informasi yang mana

penerapan dan pemuktahirannya berdasarkan dengan kebutuhan serta profil risiko, pertanyaan no 4.22 terkait dengan ketersediaan strategi penerapan keamanan informasi yang dilaksanakan sebagai bagian dalam melaksanakan program kerja dan pertanyaan no 4.27 tentang melakukan analisis untuk menilai aspek finansial yakni mencakup kebutuhan anggaran dan dampak biaya untuk keperluan revisi kebijakan dan prosedur keamanan informasi . Sehingga 6 (enam) pertanyaan diatas status jawabannya diturunkan menjadi "Dalam Perencanaan". *Checklist* validasi dokumen dilampirkan pada poin 4.16.

Pertanyaan dengan status jawaban "Tidak Dilakukan" pada kategori pengamanan 1 berjumlah 3 pertanyaan, 5 pertanyaan pada kategori pengamanan 2 dan 3 pertanyaan pada kategori pengamanan 3 yang masing-masing kategori pengamanan memperoleh skor 0. Pertanyaan dengan status jawaban "Dalam Perencanaan" pada kategori pengamanan 1 sebanyak 6 pertanyaan dengan total skor yaitu 1, 3 pertanyaan pada kategori pengamanan 2 dengan total skor yaitu 6 dan 2 pertanyaan pada kategori pengamanan 3 dengan total skor yaitu 0. Pertanyaan dengan status jawaban "Dalam Penerapan/Diterapkan Sebagian" pada kategori pengamanan 1 sebanyak 1 pertanyaan dengan skor 2, 2 pertanyaan pada kategori pengamanan 2 dengan skor 8 dan 2 pertanyaan pada kategori pengamanan 3 dengan total skor yaitu 0. Total skor yang diperoleh pada area ini adalah 19.

Tabel 4.7 Data Tingkat Kematangan Kerangka Kerja Pengelolaan Keamanan Informasi

Jumlah Pertanyaan Tingkat Kematangan	**II**	**III**	**IV**	**V**	**Total**
	11	13	3	2	29
Hasil Jawaban					
Status Pengamanan	**II**	**III**	**IV**	**V**	**Total**
Tidak Dilakukan	4	4	2	1	11
Dalam Perencanaan	6	9	0	1	16
Dalam Penerapan/Diterapkan Sebagian	0	0	1	0	1
Diterapkan Secara Menyeluruh	1	0	0	0	1
Total	**11**	**13**	**3**	**2**	**29**

Data tingkat kematangan kerangka kerja pengelolaan keamanan informasi ditunjukkan pada tabel 4.7. Jumlah pertanyaan dengan tingkat kematangan II adalah 11 pertanyaan, tingkat kematangan III sebanyak 13 pertanyaan, tingkat kematangan IV sebanyak 3 pertanyaan dan tingkat kematangan V sebanyak 2 pertanyaan dengan total pertanyaan berjumlah 29 pertanyaan.

Pada pertanyaan tingkat kematangan II, pertanyaan dengan status jawaban "Tidak Dilakukan" sebanyak 4 pertanyaan, 6 pertanyaan dengan status jawaban "Dalam Perencanaan", 0 pertanyaan dengan status jawaban "Dalam Penerapan/Diterapkan Sebagian" dan 1 pertanyaan dengan status jawaban "Diterapkan Secara Menyeluruh". Pada pertanyaan tingkat kematangan III, pertanyaan dengan status jawaban "Tidak Dilakukan" sebanyak 4 pertanyaan, 9 pertanyaan dengan status jawaban "Dalam Perencanaan" serta 0 pertanyaan untuk status jawaban "Dalam Penerapan/ Diterapkan Sebagian" dan 0 pertanyaan dengan status jawaban "Diterapkan Secara Menyeluruh". Pada pertanyaan tingkat kematangan IV, pertanyaan dengan status jawaban "Tidak Dilakukan" sebanyak 1 pertanyaan dan 1 pertanyaan dengan status jawaban "Dalam Perencanaan". 0 pertanyaan dengan status jawaban "Dalam Penerapan/ Diterapkan Sebagian" dan 0 pertanyaan dengan status jawaban "Diterapkan Secara Menyeluruh".Berdasarkan dari data yang telah diperoleh, tingkat kematangan yang diperoleh pada area ini mencapai pada tingkat I.

4.6 Pengelolaan Aset Informasi

Tabel 4.8 Data Penilaian Pengelolaan Aset Informasi

Bagian V: Pengelolaan Aset Informasi							
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.							
Jumlah Pertanyaan	**KP1**		**KP2**		**KP3**		**Total**
	24		10		4		38
Hasil Jawaban							
Kategori Pengamanan	**KP1**	**Skor KP1**	**KP2**	**Skor KP2**	**KP3**	**Skor KP3**	**Total**
Tidak Dilakukan	7	0	1	0	1	0	0
Dalam Perencanaan	13	13	7	14	3	0	27
Dalam Penerapan/Diterapkan Sebagian	0	0	1	4	0	0	4
Diterapkan Secara Menyeluruh	4	12	1	6	0	0	18
Total Nilai Evaluasi Pengelolaan Aset							**49**

Hasil penilaian pada area pengelolaan informasi ditampilkan pada tabel 4.8. Area ini memiliki jumlah pertanyaan sebanyak 38 pertanyaan. Pertanyaan terbagi dalam 3 (tiga) kategori yakni terdiri dengan dari kategori pengamanan

berjumlah 24 pertanyan, kategori pengamanan 2 berjumlah 10 pertanyaan 2 dan 4 pertanyaan pada kategori pengamanan 3.

Responden menjawab pertanyaan dengan memilih opsi jawaban yang tersedia antara lain "Tidak Dilakukan", "Dalam Perencanaan", "Dalam Penerapan/ Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh" sesuai dengan kondisi sebenarnya. Pada area ini, terdapat 10 (sepuluh) pertanyaan yang tidak dapat dibuktikan dokumen pendukungnya yaitu pada pertanyaan no 5.1 tentang ketersediaan daftar inventaris aset secara lengkap, terpelihara dan akurat termasuk kepemilikan asetnya. Pertanyaan no 5.9 tentang peraturan dalam penggunaan komputer ,internet, intranet dan email, pertanyaan no 5.11 tentang peraturan penginstallan perangkat lunak pada aset milik instansi. Pertanyaan no 5.13 tentang proses mengelola identitas elektronik dan proses otentikasi pada username dan kata sandi mencakup kebijakan terhadap pelanggarannya. Pertanyaan no 5.14 tentang prosedur dan persyaratan pengelolaan sertapemberian hak akses, otorisasi dan otentikasi untuk menggunakan aset informasi. Pertanyaan no 5.19 tentang ketentuan dalam mengamankan fisik berdasarkan definisi klasifikasi aset dan zona. Pertanyaan no 5.20 tentang proses pengecekan latar belakang SDM. Pertanyaan no 5.23 tentang mekanisme untuk mengkaji pemakaian akses (*user access review*) dan hak akses (*access rights*) yang diikuti dengan penyusunan langkah perbaikan apabila terjadi ketidaksesuaian berdasarkan kebijakan yang berlaku. Pertanyaan no 5.37 tentang peraturan untuk melakukan pengamanan pada lokasi kerja penting atau utama yang meliputi ruangan server dan ruangan arsip dari bahan dan perangkat yang membahayakan aset informasi. Pertanyaan no 5.38 tentang mekanisme pengamanan lokasi kerja utama dari kehadiran pihak ketiga yang bekerja pada instansi sehingga 10 (Sepuluh) pertanyaan diatas yang tidak dapat ditunjukkan dokumen pendukungnya diturunkan status jawabannya menjadi "Dalam Perencanaan". *Checklist* validasi dokumen dilampirkan pada poin 4.16.

Pertanyaan dengan status jawaban "Tidak Dilakukan" pada kategori pengamanan 1 sebanyak 7 pertanyaan, 1 pertanyaan pada kategori pengamanan 2 dan 1 pertanyaan pada kategori pengamanan 3 yang masing-masing kategori pengamanan memperoleh skor 0. Pertanyaan dengan status jawaban "Dalam Perencanaan" pada kategori pengamanan 1 sebanyak 13 pertanyaan dengan total skor yaitu 13, 7 pertanyaan pada kategori pengamanan 2 dengan total skor yaitu 14 dan 3 pertanyaan pada kategori pengamanan 3 dengan total skor yaitu 0. Pertanyaan dengan status jawaban "Dalam Penerapan/Diterapkan Sebagian" pada kategori pengamanan 1 sebanyak 0 pertanyaan dengan skor 0, 1 pertanyaan pada kategori pengamanan 2 dengan skor 4 dan 0 pertanyaan pada kategori pengamanan 3 dengan total skor yaitu 0. Pertanyaan dengan status jawaban "Diterapkan Secara Menyeluruh" pada kategori pengamanan 1 sebanyak 4 pertanyaan dengan total skor yaitu 12, 1 pertanyaan pada kategori pengamanan 2 dengan total skor yaitu 6 dan 0 pertanyaan pada kategori pengamanan 3 dengan total skor yaitu 0. Total skor yang diperoleh ini adalah 49.

Tabel 4.9 Data Tingkat Kematangan Pengelolaan Aset Informasi

Jumlah Pertanyaan Tingkat Kematangan	II	III	IV	V	Total
	29	9	0	0	38
Hasil Jawaban					
Status Pengamanan	**II**	**III**	**IV**	**V**	**Total**
Tidak Dilakukan	8	1	0	0	9
Dalam Perencanaan	15	8	0	0	23
Dalam Penerapan/Diterapkan Sebagian	1	0	0	0	1
Diterapkan Secara Menyeluruh	5	0	0	0	5
Total	**29**	**9**	**0**	**0**	**38**

Pencapaian tingkat kematangan pada area pengelolaan aset informasi ditunjukkan pada tabel 4.9. Jumlah pertanyaan pada tingkat kematangan II adalah 29 pertanyaan, pada tingkat kematangan III adalah 9 pertanyaan dan untuk tingkat kematangan IV dan tingkat kematangan V adalah 0 pertanyaan dengan total seluruh pertanyaan pada area ini adalah 38 pertanyaan.

Pada pertanyaan tingkat kematangan II, pertanyaan dengan status jawaban "Tidak Dilakukan" sebanyak 8 pertanyaan, 15 pertanyaan dengan status jawaban "Dalam Perencanaan", 1 pertanyaan dengan status jawaban "Dalam Penerapan/Diterapkan Sebagian" dan 5 pertanyaan dengan status jawaban "Diterapkan Secara Menyeluruh". Pada pertanyaan tingkat kematangan III, pertanyaan dengan status jawaban "Tidak Dilakukan" sebanyak 1 pertanyaan, 8 pertanyaan dengan status jawaban "Dalam Perencanaan" serta 0 pertanyaan untuk status jawaban "Dalam Penerapan/ Diterapkan Sebagian" dan 0 pertanyaan untuk jawaban "Diterapkan Secara Menyeluruh". Dalam area ini tidak terdapat pertanyaan yang memiliki tingkat kematangan IV dan tingkat kematangan V sehingga pada tingkat kematangan IV dan tingkat kematangan V berjumlah 0 pertanyaan pada setiap status jawaban yang ada. Berdasarkan dari data yang telah diperoleh, tingkat kematangan yang diperoleh pada area ini mencapai pada tingkat I+.

4.7 Teknologi dan Keamanan Informasi

Tabel 4.10 Data penilaian Teknologi dan Keamanan Informasi

Bagian VI: Teknologi dan Keamanan Informasi							
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.							
Jumlah Pertanyaan	**KP1**		**KP2**		**KP3**		**Total**
	14		10		2		26
Hasil Jawaban							
Kategori Pengamanan	**KP1**	**Skor KP1**	**KP2**	**Skor KP2**	**KP3**	**Skor KP3**	**Total**
Tidak Dilakukan	1	0	2	0	0	0	0
Dalam Perencanaan	5	5	5	10	2	3	18
Dalam Penerapan/ Diterapkan Sebagian	5	10	1	4	0	0	14
Diterapkan Secara Menyeluruh	3	9	2	12	0	0	21
Total Nilai Evaluasi Teknologi dan Keamanan Informasi							**53**

Tabel 4.10 menampilkan data penilaian pada area teknologi dan keamanan informasi. Pada area ini memiliki jumlah pertanyaan sebanyak 26 pertanyaan yang terdiri dari 14 pertanyaan dengan kategori pengamanan 1, 10 pertanyaan dengan kategori pengamanan 2 dan 2 pertanyaan dengan kategori pengamanan 3.

Responden menjawab pertanyaan yang ada dengan memilih opsi jawaban yang tersedia antara lain “Tidak Dilakukan”, “Dalam Perencanaan”, “Dalam Penerapan/ Diterapkan Sebagian” dan “Diterapkan Secara Menyeluruh” sesuai dengan kondisi sebenarnya. Pada area ini terdapat pada area ini, terdapat 7 (tujuh) pertanyaan yang tidak dapat dibuktikan dokumen pendukungnya yang diantaranya adalah pertanyaan no 6.3 tentang ketersediaan konfigurasi untuk keamanan sistem untuk seluruh aplikasi, aset jaringan, dan sistem. pertanyaan no 6.4 tentang menganalisa kepatuhan penerapan konfigurasi standar secara rutin. Pertanyaan no 6.5 tentang kerutinan melakukan pemindaian terhadap aplikasi, sistem, dan jaringan yang dipakai untuk melakukan identifikasi kemungkinan adanya kelemahan, perubahan dankeutuhan konfigurasi. Pertanyaan 6.10 tentang analisa log secara rutin untuk memastikan keakuratan, kevalidan, dan kelengkapan isinya yang berguna dalam pelaksanaan jejak audit dan forensik. Pertanyaan no 6.14 tentang penerapan pada aplikasi dan sistem belum didukung dan diterapkan perubahan *password* secara sistematis dan

pengaturan panjang atau kompleksitasnya *password*. Pertanyaan no 6.21 tentang dokumen rekaman serta hasil analisis jejak audit atau untuk mengkonfirmasikan bahwa antivirus atau antimalware telah termutakhir secara berkala dan sistematis. Pertanyaan no 6.22 tentang laporan terkait penyerangan *malware* atau virus yang gagal atau sukses ditindaklanjuti dan diselesaikan. Sehingga pada 7 (tujuh) pertanyaan diatas diturunkan status jawabannya menjadi "Dalam Perencanaan". *Checklist* validasi dokumen dilampirkan pada poin 4.16.

Pertanyaan dengan status jawaban "Tidak Dilakukan" pada kategori pengamanan 1 sebanyak 1 pertanyaan, 2 pertanyaan pada kategori pengamanan 2 dan 0 pertanyaan pada kategori pengamanan 3 yang masing-masing kategori pengamanan memperoleh skor 0. Pertanyaan dengan status jawaban "Dalam Perencanaan" pada kategori pengamanan 1 sebanyak 5 pertanyaan dengan total skor yaitu 5, 5 pertanyaan pada kategori pengamanan 2 dengan total skor yaitu 10 dan 2 pertanyaan pada kategori pengamanan 3 dengan total skor yaitu 3. Pertanyaan dengan status jawaban "Dalam Penerapan/Diterapkan Sebagian" pada kategori pengamanan 1 sebanyak 5 pertanyaan dengan skor 10, 1 pertanyaan pada kategori pengamanan 2 dengan skor 4 dan 0 pertanyaan pada kategori pengamanan 3 dengan total skor yaitu 0. Pertanyaan dengan status jawaban "Diterapkan Secara Menyeluruh" pada kategori pengamanan 1 sebanyak 3 pertanyaan dengan skor 9, 2 pertanyaan pada kategori pengamanan 2 dengan skor 12 dan 0 pertanyaan pada kategori pengamanan 3 dengan total skor yaitu 0. Total skor yang didapatkan pada area ini adalah 53.

Tabel 4.11 Data Tingkat Kematangan Teknologi dan Keamanan Informasi

Jumlah Pertanyaan Tingkat Kematangan	**II**	**III**	**IV**	**V**	**Total**
	14	11	1	0	26
Hasil Jawaban					
Status Pengamanan	**II**	**III**	**IV**	**V**	**Total**
Tidak Dilakukan	1	2	0	0	3
Dalam Perencanaan	5	6	1	0	12
Dalam Penerapan/ Diterapkan Sebagian	5	1	0	0	6
Diterapkan Secara Menyeluruh	3	2	0	0	5
Total	**14**	**11**	**1**	**0**	**26**

Pencapaian tingkat kematangan area teknologi dan keamanan informasi ditunjukkan pada tabel 4.11. Jumlah pertanyaan pada tingkat kematangan II adalah 14 pertanyaan, pada tingkat kematangan III adalah 11 pertanyaan dan untuk tingkat kematangan IV ialah 1 pertanyaan serta jumlah pertanyaan tingkat

kematangan V adalah 0 pertanyaan dengan total seluruh pertanyaan pada area ini adalah 26 pertanyaan.

Pada pertanyaan tingkat kematangan II, pertanyaan dengan status jawaban "Tidak Dilakukan" sebanyak 1 pertanyaan, 5 pertanyaan dengan status jawaban "Dalam Perencanaan", 5 pertanyaan dengan status jawaban "Dalam Penerapan/Diterapkan Sebagian" dan 3 pertanyaan dengan status jawaban "Diterapkan Secara Menyeluruh". Pada pertanyaan tingkat kematangan III, pertanyaan dengan status jawaban "Tidak Dilakukan" sebanyak 2 pertanyaan, 6 pertanyaan dengan status jawaban "Dalam Perencanaan" serta 1 pertanyaan untuk status jawaban "Dalam Penerapan/ Diterapkan Sebagian" dan 2 pertanyaan untuk jawaban "Diterapkan Secara Menyeluruh". Pada pertanyaan tingkat kematangan IV yakni 0 pertanyaan dengan status jawaban "Tidak Dilakukan", 1 pertanyaan dengan status jawaban "Dalam Perencanaan" dan 0 pertanyaan dengan status "Dalam Penerapan/ Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh". Berdasarkan dari data yang telah diperoleh pada area ini mencapai tingkat kematangan I+.

4.8 Suplemen

Tabel 4.12 Data Penilaian Area Suplemen

Bagian VII: Suplemen		
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi yang mencakup aspek pengamanan keterlibatan pihak ketiga penyedia layanan, layanan berbasis cloud, dan perlindungan data pribadi.		
Jumlah Pertanyaan (KP1)	53	
Hasil Jawaban		
Kategori Pengamanan	**KP1**	**Skor**
Tidak Dilakukan	53	0
Dalam Perencanaan	0	0
Dalam Penerapan/ Diterapkan Sebagian	0	0
Diterapkan Secara Menyeluruh	0	0
Total	**53**	**0**

Berikut pada 4.12 merupakan data penilaian area suplemen. Seluruh pertanyaan pada area suplemen merupakan pertanyaan dengan kategori pengamanan 1 dengan total pertanyaan sebanyak 53 pertanyaan dimana seluruh pertanyaan tersebut didapatkan jawaban dengan status "Tidak Dilakukan" yang berarti bahwa Dinas Komunikasi dan Informatika Kabupaten Kediri belum

menerapkan pengamanan keterlibatan pihak ketiga penyedia layanan, layanan berbasis cloud, dan perlindungan data pribadi.

4.9 Validasi Data

Untuk mendukung jawaban atau hasil kuisioner yang telah ada, maka dilakukan validasi menggunakan *checklist* untuk membuktikan hasil jawaban pada kuisioner sesuai dengan keadaan sebenarnya berdasarkan dokumen atau bukti yang tersedia. *Checklist* ini dilakukan pada pertanyaan dengan hasil jawaban "Dalam Penerapan/ Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh". Untuk pertanyaan dengan status jawaban "Tidak Dilakukan" dan "Dalam Perencanaan" tidak dilakukan *checklist*. Berikut merupakan *checklist* pada area yang dievaluasi pada area Indeks KAMI.

Tabel 4. 13 *Checklist* Area Tata Kelola Keamanan Informasi

No Pertanyaan	Bukti		Keterangan
	ada	Tidak	
2.1	√		- Peraturan Bupati Kabupaten Kediri Nomor 51 Tahun 2016 pada pasal 13
2.2	√		- Peraturan Bupati Nomor 51 Tahun 2016 pada bagian tugas Seksi Sandi dan Keamanan Teknologi Informasi
2.3	√		- Peraturan Bupati No 51 Tahun 2016 pada bagian tugas Seksi Sandi dan Keamanan Teknologi Informasi
2.4	√		- Rencana Strategis (RENSTRA) Dinas Komunikasi dan Informatika Kabupaten Kediri Tahun 2016-2021
2.7		√	- Tidak ada bukti
2.8	√		- Foto Kegiatan Sosialiasi

Tabel 4.13 merupakan hasil validasi data kuisioner yang telah dilakukan dengan metode *checklist* pada area tata kelola kemanan informasi. Bukti yang dilampirkan yakni berupa dokumen serta foto kegiatan. Salah satunya yakni pada pertanyaan 2.1 yang memiliki bukti yakni Peraturan Bupati Kabupaten Kediri No 51 Tahun 2016 pada pasal 13.

Tabel 4. 14 *Checklist* Area Pengelolaan Risiko Keamanan Informasi

No Pertanyaan	Bukti		Keterangan
	ada	Tidak	
3.2		√	- Tidak ada bukti

Validasi data kuisioner yang telah dilakukan ditunjukkan pada tabel 4.14. validasi dilakukan dengan metode *checklist* pada area pengelolaan risiko keamanan informasi. Pada area ini tidak ada satupun dokumen bukti yang terlampir karena pada pertanyaan 3.2 dokumen bukti tidak valid. No pertayaan 3.2 memuat tentang penetapan tanggung jawab manajemen risiko dan eskalasi pelaporannya.

Tabel 4. 15 *Checklist* Area Kerangka Kerja Pengelolaan Keamanan Informasi

No Pertanyaan	Bukti		Keterangan
	ada	Tidak	
4.12		√	- Tidak ada bukti
4.13		√	- Tidak ada bukti
4.20		√	- Tidak ada bukti
4.21		√	- Tidak ada bukti
4.22		√	- Tidak ada bukti
4.27		√	- Tidak ada bukti
4.29	√		- Dokumen Kerangka Acuan Kerja Belanja Antivirus Tahun Anggaran 2020 - Dokumen Rencana Strategis (RENSTRA) Dinas Komunikasi dan Informatika Kabupaten Kediri Tahun 2016-2021

Berikut ditunjukkan pada tabel 4.15 merupakan hasil validasi data kuisioner yang telah dilakukan dengan metode *checklist* pada area kerangka kerja pengelolaan keamanan informasi. Bukti yang dilampirkan yakni berupa dokumen serta foto kegiatan. Salah satunya yakni pertanyaan no 4.29 yang memiliki dokumen bukti yakni Dokumen Kerangka Acuan Kerja Belanja Antivirus Tahun Anggaran 2020.

Tabel 4. 16 *Checklist* Area Pengelolaan Aset Informasi

No Pertanyaan	Bukti		Keterangan
	ada	Tidak	
5.1		√	- Tidak ada bukti
5.9		√	- Tidak ada bukti
5.11		√	- Tidak ada bukti
5.13		√	- Tidak ada bukti
5.14		√	- Tidak ada bukti
5.19		√	- Tidak ada bukti
5.20		√	- Tidak ada bukti
5.23		√	- Tidak ada bukti
5.28	√		- Laporan Pengelolaan Infrastuktur TIK - Foto
5.29	√		- Laporan Pengelolaan Infrastuktur TIK - *Standart Operational Procedur* (SOP) cara Memasuki Ruang Server - Penggunaan *Firewall*
5.30	√		- Laporan Pengelolaan Infrastuktur TIK - Foto
5.31	√		- Laporan Pengelolaan Infrastuktur TIK - Foto
5.34	√		- Laporan Pengelolaan Infrastuktur TIK - Foto
5.35	√		- *Standart Operational Procedur* (SOP) Pemeliharaan CCTV, Pemeliharaan mesin absensi, perbaikan CCTV, perbaikan mesin absensi
5.37		√	- Tidak ada bukti
5.38		√	- Tidak ada bukti

Hasil validasi data kuisioner yang telah dilakukan dengan metode *checklist* pada area pengelolaan aset informasi ditujukkan Pada Tabel 4.16. Bukti yang dilampirkan yakni berupa dokumen serta foto kegiatan. Salah satunya yakni

pertanyaan no 5.28 yang memiliki bukti Dokumen Laporan Pengelolaan Infrastruktur TIK.

Tabel 4. 17 *Checklist* Area Teknologi dan Keamanan Informasi

No Pertanyaan	Bukti		Keterangan
	ada	Tidak	
6.1	√		- *Screenshot* Penggunaan Firewall
6.2	√		- *Screenshot* Penggunaan Virtual LAN
6.3		√	- Tidak ada bukti
6.4		√	- Tidak ada bukti
6.5		√	- Tidak ada bukti
6.6	√		- Laporan Pengelolaan Infrastruktur TIK
6.7	√		- *Screenshot* monitoring menggunakan Zabbix dan Sophos
6.8	√		- *Screenshot* Log perubahan sistem informasi otomatis
6.9	√		- *Screenshot* Rekaman aktivitas di log
6.10		√	- Tidak ada bukti
6.14		√	- Tidak ada bukti
6.16	√		- Foto
6.17	√		- *Screenshot* Penggunaan Firewall
6.18	√		- *Screenshot* Penggunaan VPN
6.19	√		- *Screenshot* penggunaan sistem operasi versi terkini pada desktop
6.21		√	- Tidak ada bukti
6.22		√	- Tidak ada bukti
6.23	√		- *Screenshot* penggunaan NTP (*Network Time Protocol*)

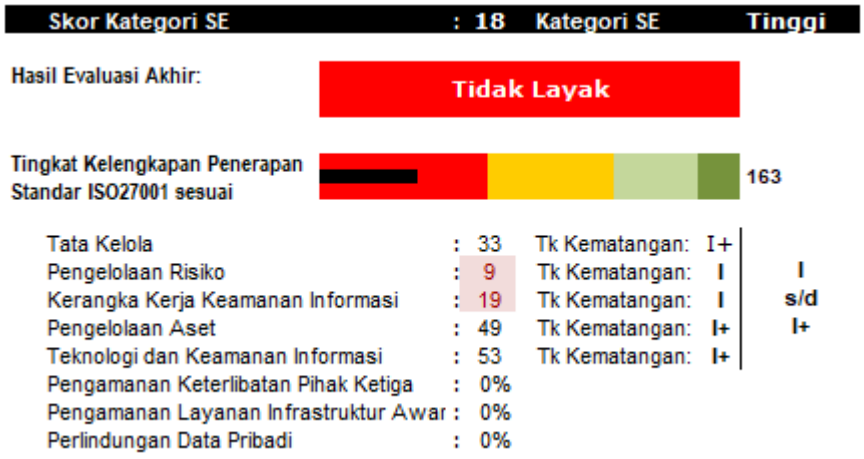
Ditunjukkan tabel 4.17 merupakan hasil validasi data kuisioner yang telah dilakukan dengan metode *checklist* pada area teknologi dan keamanan informasi. Bukti yang dilampirkan yakni berupa dokumen serta foto kegiatan. Salah satunya yakni pertanyaan 6.1 yang memiliki bukti *Screenshot* Penggunaan Firewall Sophos.

Area suplemen tidak dilakukan validasi terhadap dokumen bukti pada jawaban kuisioner yang telah didapatkan karena pada area suplemen seluruh pertanyaan memiliki status jawaban "Tidak Dilakukan". Sehingga pada area ini tidak dilampirkan dokumen bukti. Seluruh dokumen bukti dilampirkan pada akhir penelitian ini.

4.10 Hasil Akhir Penilaian Indeks KAMI

Penyajian hasil akhir penilaian tingkat pengamanan informasi dan tingkat kematangan yang telah dilakukan disajikan dalam 2 (dua) bentuk yaitu penyajian nilai masing-masing area yang menunjukkan tingkat kematangan dan nilai setiap area yang dievaluasi serta penyajian dalam bentuk diagram radar

4.10.1 Penyajian Hasil Akhir Setiap Area



Gambar 4. 1 Tingkat Kelengkapan dan Tingkat Kematangan Dinas Komunikasi dan Informatika Kabupaten Kediri

Gambar 4.1 disajikan hasil akhir penilaian tingkat kelengkapan dan tingkat kematangan terhadap masing-masing area yang telah dievaluasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Berdasar penilaian Tingkat Kelengkapan dan Tingkat Kematangan pada gambar 4.1 disimpulkan bahwa:

a. Skor yang diperoleh pada penilaian kategori sistem elektronik di Dinas Komunikasi dan Informatika Kabupaten Kediri adalah 18 yang termasuk pada kategori **"Tinggi"** dengan arti yakni sistem elektronik adalah hal yang tidak dapat dipisahkan dari proses kerja yang dilaksanakan pada Dinas Komunikasi dan Informatika Kabupaten Kediri.
b. Hasil akhir terhadap penilaian tingkat kelengkapan penerapan standar ISO 27001 memperoleh skor 163 yang berada dalam area berwarna **"Merah"** dan dikategorikan sebagai **"Tidak Layak"**.

Tabel 4. 18 Persentase Tingkat Kematangan Keamanan Informasi

Keterangan	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Teknologi
Skor Kuisioner	33	9	19	49	53
Skor Maksimal	126	72	159	168	120
Persentase	26,1%	12,5%	11,9%	29,1%	44,1%
Tingkat Kematangan	I+	I	I	I+	I+

Persentase pencapaian tingkat kematangan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri ditunjukkan pada tabel 4.18 yang masing-masing areanya akan dijabarkan pada berikut ini:

1. Tata Kelola Keamanan Informasi

Area tata kelola keamanan informasi memperoleh skor berdasarkan hasil kuisioner adalah 33 dari skor maksimal sebesar 126. Persentase pencapaian tingkat kematangan pada area ini adalah 26,1% dengan rincian skor tingkat kematangan sebagai berikut ini:

- Skor Tingkat Kematangan II : 27
- Skor Tingkat Kematangan III : 6
- Skor Tingkat Kematangan IV : 0
- Skor Tingkat Kematangan V : 0

Dari hasil jawaban yang telah diperoleh, pada area ini mencapai tingkat kematangan I+ yang berarti bahwa Dinas Komunikasi dan Informatika Kabupaten Kediri mulai memahami mengenai perlunya mengelola keamanan informasi, untuk penerapan langkah pengamanan yang telah dilaksanakan saat ini bersifat reaktif, tidak teratur, serta tidak berpacu pada seluruh risiko yang ada, tidak memiliki alur komunikasi dan kewenangan yang jelas dan tidak dilakukan pengawasan, kelemahan terakit teknis serta non-teknis belum diidentifikasi dengan baik serta pihak-pihak yang terlibat belum paham dan menyadari akan tanggung jawab mereka (KOMINFO, 2011).

2. Pengelolaan Risiko Keamanan Informasi

Pengelolaan risiko keamanan informasi memperoleh skor berdasarkan hasil kuisioner adalah 9 dari skor maksimal sebesar 72. Persentase pencapaian tingkat kematangan pada area ini adalah 12,5% dengan rincian skor tingkat kematangan sebagai berikut ini:

- Skor Tingkat Kematangan II : 3
- Skor Tingkat Kematangan III : 4

- Skor Tingkat Kematangan IV : 2
- Skor Tingkat Kematangan V : 0

Berdasarkan dari hasil jawaban yang telah diperoleh, pada area ini mencapai tingkat kematangan I yang berarti bahwa Dinas Komunikasi dan Informatika Kabupaten Kediri mulai memahami mengenai perlunya mengelola keamanan informasi, untuk penerapan langkah pengamanan yang telah dilaksanakan saat ini bersifat reaktif, tidak teratur, serta tidak berpacu pada seluruh risiko yang ada, tidak memiliki alur komunikasi dan kewenangan yang jelas dan tidak dilakukan pengawasan, kelemahan terakit teknis serta non-teknis belum diidentifikasi dengan baik serta pihak-pihak yang terlibat belum paham dan menyadari akan tanggung jawab mereka (KOMINFO, 2011).

3. Kerangka Kerja Pengelolaan Keamanan Informasi

Kerangka kerja pengelolaan risiko keamanan informasi memperoleh skor berdasarkan hasil kuisioner adalah 19 dari skor maksimal sebesar 159. Persentase pencapaian tingkat kematangan pada area ini adalah 11,9% dengan rincian skor tingkat kematangan sebagai berikut ini:

- Skor Tingkat Kematangan II : 8
- Skor Tingkat Kematangan III : 11
- Skor Tingkat Kematangan IV : 0
- Skor Tingkat Kematangan V : 0

Dari hasil jawaban yang telah didapatkan, pada area ini mencapai tingkat kematangan I yang berarti bahwa Dinas Komunikasi dan Informatika Kabupaten Kediri mulai memahami mengenai perlunya mengelola keamanan informasi, untuk penerapan langkah pengamanan yang telah dilaksanakan saat ini bersifat reaktif, tidak teratur, serta tidak berpacu pada seluruh risiko yang ada, tidak memiliki alur komunikasi dan kewenangan yang jelas dan tidak dilakukan pengawasan, kelemahan terakit teknis serta non-teknis belum diidentifikasi dengan baik serta pihak-pihak yang terlibat belum paham dan menyadari akan tanggung jawab mereka (KOMINFO, 2011).

4. Pengelolaan Aset Informasi

Pengelolaan aset informasi memperoleh skor berdasarkan hasil kuisioner adalah 49 dari skor maksimal sebesar 168. Persentase pencapaian tingkat kematangan pada area ini adalah 29,1% dengan rincian skor tingkat kematangan sebagai berikut ini:

- Skor Tingkat Kematangan II : 39
- Skor Tingkat Kematangan III : 10
- Skor Tingkat Kematangan IV : 0

- Skor Tingkat Kematangan V : 0

Berdasarkan dari hasil jawaban yang telah diperoleh, pada area ini mencapai tingkat kematangan I+ yang berarti bahwa Dinas Komunikasi dan Informatika Kabupaten Kediri mulai memahami mengenai perlunya mengelola keamanan informasi, untuk penerapan langkah pengamanan yang telah dilaksanakan saat ini bersifat reaktif, tidak teratur, serta tidak berpacu pada seluruh risiko yang ada, tidak memiliki alur komunikasi dan kewenangan yang jelas dan tidak dilakukan pengawasan, kelemahan terakit teknis serta non-teknis belum diidentifikasi dengan baik serta pihak-pihak yang terlibat belum paham dan menyadari akan tanggung jawab mereka (KOMINFO, 2011).

5. Teknologi dan Keamanan Informasi

Area teknologi dan keamanan informasi memperoleh skor berdasarkan hasil kuisioner adalah 53 dari skor maksimal sebesar 120. Persentase pencapaian tingkat kematangan pada area ini 54,1% dengan rincian skor tingkat kematangan sebagai berikut ini:

- Skor Tingkat Kematangan II : 24
- Skor Tingkat Kematangan III : 29
- Skor Tingkat Kematangan IV : 0
- Skor Tingkat Kematangan V : 0

Dari hasil jawaban yang telah diperoleh, pada area ini mencapai tingkat kematangan I+ yang berarti bahwa Dinas Komunikasi dan Informatika Kabupaten Kediri mulai memahami mengenai perlunya mengelola keamanan informasi, untuk penerapan langkah pengamanan yang telah dilaksanakan saat ini bersifat reaktif, tidak teratur, serta tidak berpacu pada seluruh risiko yang ada, tidak memiliki alur komunikasi dan kewenangan yang jelas dan tidak dilakukan pengawasan, kelemahan terakit teknis serta non-teknis belum diidentifikasi dengan baik serta pihak-pihak yang terlibat belum paham dan menyadari akan tanggung jawab mereka (KOMINFO, 2011).

6. Suplemen

Area suplemen memperoleh skor untuk setiap aspek adalah 0 karena pada saat ini Dinas Komunikasi dan Informatika Kabupaten Kediri belum menerapkan pengamanan keterlibatan pihak ketiga, pengamanan layanan infrastruktur awan dan perlindungan data pribadi sehingga hasil akhir yang didapatkan pada ketiga area tersebut adalah 0%.

4.10.2 Diagram Radar Pengamanan Informasi

Gambar 4. 2 Diagram Radar Tingkat Kelengkapan Pengamanan Informasi

Gambar 4.2 ditunjukkan diagram radar tingkat kelengkapan pengamanan informasi yang memiliki 5 sumbu area pengamanan dengan berlatar belakang berwarna hijau yang terdiri dari kerangka kerja dasar, penerapan operasional serta kepatuhan SNI ISO/IEC 27001:2013. Area berwarna oren menggambarkan hasil jawaban responden yang telah didapatkan. berdasarkan dari gambar 4.2 diatas, dapat disimpulkan bahwa:

1. Area yang belum memenuhi kerangka kerja dasar, penerapan operasinal dan kepatuhan ISO 27001 adalah pengelolaan risiko, kerangka kerja dan pengelolaan aset.
2. Area yang paling baik dan mendekati standar kepatuhan ISO 27001 adalah aspek teknologi.

4.11 Analisis Kontrol Area Tata Kelola Keamanan Informasi

Berdasarkan pengumpulan data yang telah dilakukan, selanjutnya dilakukan analisis kontrol pada setiap jawaban yang diberikan responden dengan kontrol ISO/IEC 27001:2013. Hal ini bertujuan untuk mengetahui bentuk pengamanan yang belum diterapkan pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Berikut hasil analisis kontrol pada are tata kelola keamanan informasi dengan kontrol ISO/IEC 27001:2013.

Tabel 4.19 Hasil Analisis Area Tata Kelola Keamanan Informasi

No Pertanyaan	Status Pengamanan	Kontrol ISO 27001	Keterangan
2.5	Tidak Dilakukan	A.6.1.1	Tentang peran dan tanggung jawab keamanan informasi

Tabel 4.20 Hasil Analisis Area Tata Kelola Keamanan Informasi (lanjutan)

2.6	Dalam Perencanaan	A.7.1.2	Tentang syarat dan ketentuan pekerjaan
2.7	Dalam Perencanaan	A.7.2.1	Tentang tanggung jawab manajemen
2.9	Dalam Perencanaan	A.7.2.2	Tentang kesadaran keamanan informasi, pendidikan dan pelatihan
2.10	Dalam Perencanaan	A.17.1.1	Tentang merencakan keberlanjutan keamanan informasi
2.11	Dalam Perencanaan	A.18.1.4	Tentang privasi dan perlindungan informasi identitas pribadi
2.12	Dalam Perencanaan	A.13.2.2	Tentang kesepakatan transfer informasi
2.13	Dalam Perencanaan	A.7.1.2	Tentang tanggung jawab manajemen
2.14	Dalam Perencanaan	A.17.1.1	Tentang merencakan keberlanjutan keamanan informasi
2.15	Dalam Perencanaan	A.18.2.2	Tentang kepatuhan dengan kebijakan dan standar keamanan
2.16	Dalam Perencanaan	A.7.2.1	Tentang tanggung jawab manajemen
2.17	Dalam Perencanaan	A.6.1.5	Tentang keamanan informasi dalam proyek
2.18	Tidak Dilakukan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
2.19	Tidak Dilakukan	A.7.2.3	Tentang proses pendisiplinan
2.20	Dalam Perencanaan	A.5.1.1	Tentang kebijakan untuk keamanan informasi

Tabel 4.21 Hasil Analisis Area Tata Kelola Keamanan Informasi (lanjutan)

2.21	Dalam Perencanaan	A.18.1.1	Tentang identifikasi peraturan perundangan yang berlaku dan persyaratan kontrak
2.22	Tidak Dilakukan	A.16.1.1	Tentang tanggung jawab dan prosedur

4.12 Analisis Kontrol Area Pengelolaan Risiko Keamanan Informasi

Setelah pengumpulan data dilakukan, selanjutnya dilakukan analisis kontrol pada setiap jawaban yang diberikan responden dengan kontrol ISO/IEC 27001:2013. Hal ini bertujuan untuk mengetahui bentuk pengamanan yang belum diterapkan pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Berikut hasil analisis kontrol pada areq pengelolaan risiko dan keamanan informasi dengan kontrol ISO/IEC 27001:2013.

Tabel 4. 22 Hasil Analisis Area Pengelolaan Risiko Keamanan Informasi

No Pertanyaan	Status Pengamanan	Kontrol ISO 27001	Keterangan
3.1	Tidak Dilakukan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
3.2	Dalam Perencanaan	A.6.1.1	Tentang peran dan tanggung jawab keamanan informasi
3.3	Tidak Dilakukan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
3.4	Tidak Dilakukan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
3.5	Tidak Dilakukan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
3.6	Tidak Dilakukan	A.8.1.2	Tentang kepemilikan aset
3.7	Tidak Dilakukan	A.16.1.3	Tentang melaporkan kelemahan keamanan informasi
3.8	Tidak Dilakukan	A.16.1.6	Tentang penilaian dan keputusan tentang kejadian keamanan informasi

Tabel 4. 23 Hasil Analisis Area Pengelolaan Risiko Keamanan Informasi (lanjutan)

3.9	Tidak Dilakukan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
3.10	Dalam Perencanaan	A.8.2.3	Tentang penanganan aset
3.11	Dalam Perencanaan	A.12.1.3	Tentang manajemen kapasitas
3.12	Dalam Perencanaan	A.12.1.3	Tentang manajemen kapasitas
3.13	Dalam Perencanaan	A.18.2.1	Tentang tinjau independen keamanan informasi
3.14	Dalam Perencanaan	A.18.2.1	Tentang tinjau independen keamanan informasi
3.15	Tidak Dilakukan	A.18.2.1	Tentang tinjau independen keamanan informasi
3.16	Tidak Dilakukan	A.5.1.2	Tentang tinjau kebijakan untuk keamanan informasi

4.13 Analisis Kontrol Area Kerangka Kerja Keamanan Informasi

Selanjutnya dilakukan analisis kontrol pada setiap jawaban yang diberikan responden dengan kontrol ISO/IEC 27001:2013. Hal ini bertujuan untuk mengetahui bentuk pengamanan yang belum diterapkan pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Berikut hasil analisis kontrol pada area kerangka kerja keamanan informasi dengan kontrol ISO/IEC 27001:2013.

Tabel 4. 24 Hasil analisis Area Kerangka Kerja Keamanan Informasi

No Pertanyaan	Status Pengamanan	Kontrol ISO 27001	Keterangan
4.1	Dalam Perencanaan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
4.2	Dalam Perencanaan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
4.3	Tidak Dilakukan	A.5.1.2	Tentang tinjau kebijakan untuk keamanan informasi

Tabel 4. 25 Hasil analisis Area Kerangka Kerja Keamanan Informasi (lanjutan)

4.4	Tidak Dilakukan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
4.5	Dalam Perencanaan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
4.6	Dalam Perencanaan	A.16.1.4	Tentang penilaian dan keputusan tentang kejadian keamanan informasi
4.7	Tidak Dilakukan	A.7.1.2	Tentang syarat dan ketentuan pekerjaan
4.8	Tidak Dilakukan	A.7.2.3	Tentang proses pendisiplinan
4.9	Dalam Perencanaan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
4.10	Tidak Dilakukan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
4.11	Tidak Dilakukan	A.6.1.5	Tentang keamanan informasi untuk manajemen proyek
4.12	Dalam Perencanaan	A.14.1.1	Tentang analisis dan spesifikteasi kebutuhan keamanan informasi
4.13	Dalam Perencanaan	A.14.2.1	Tentang kebijakan pembangunan yang aman
4.14	Tidak Dilakukan	A.14.2.3	Tentang prosedur kontrol perubahan sistem
4.15	Tidak Dilakukan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
4.16	Dalam Perencanaan	A.17.1.2	Tentang merencakan keberlanjutan keamanan informasi
4.17	Dalam Perencanaan	A.17.1.2	Tentang merencakan keberlanjutan keamanan informasi
4.18	Tidak Dilakukan	A.17.1.3	Tentang verifikasi, tinjau, dan evaluasi keberlanjutan keamanan informasi

Tabel 4. 26 Hasil analisis Area Kerangka Kerja Keamanan Informasi (lanjutan)

4.19	Tidak Dilakukan	A.5.1.2	Tentang tinjau kebijakan untuk keamanan informasi
4.20	Dalam Perencanaan	A.16.1.6	Tentang belajar dari insiden keamanan informasi
4.21	Dalam Perencanaan	A.17.1.2	Tentang menerapkan kontinuitas keamanan informasi
4.22	Dalam Perencanaan	A.16.1.5	Tentang tanggapan terhadap insiden keamanan informasi
4.23	Dalam Perencanaan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
4.24	Dalam Perencanaan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
4.25	Dalam Perencanaan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
4.26	Dalam Perencanaan	A.5.1.1	Tentang kebijakan untuk keamanan informasi
4.27	Tidak Dilakukan	A.5.1.2	Tentang tinjau kebijakan untuk keamanan informasi
4.28	Tidak Dilakukan	A.7.2.3	Tentang proses pendisiplinan

4.14 Analisis kontrol area Pengelolaan Aset Informasi

Berdasarkan pengumpulan data yang telah dilakukan, selanjutnya dilakukan analisis kontrol pada setiap jawaban yang diberikan responden dengan kontrol ISO/IEC 27001:2013. Hal ini bertujuan untuk mengetahui bentuk pengamanan yang belum diterapkan pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Berikut hasil analisis kontrol pada area pengelolaan aset informasi dengan kontrol ISO/IEC 27001:2013.

Tabel 4. 27 Hasil Analisis Area Pengelolaan Aset Informasi

No Pertanyaan	Status Pengamanan	Kontrol ISO 27001	Keterangan
5.1	Dalam Perencanaan	A.8.1.1 A.8.1.2	Tentang invetarisasi aset dan kepemilikan aset

Tabel 4. 28 Hasil Analisis Area Pengelolaan Aset Informasi (lanjutan)

5.2	Tidak Dilakukan	A.8.2.1	Tentang klasifikasi informasi
5.3	Dalam Perencanaan	A.8.2.1	Tentang klasifikasi informasi
5.4	Dalam Perencanaan	A.9.1.1	Tentang kebijakan kontrol akses
5.5	Dalam Perencanaan	A.12.1.1	Tentang prosedur operasi terdokumentasi
5.6	Dalam Perencanaan	A.12.5.1	Tentang pemasangan perangkat lunak pada sistem operasional
5.7	Tidak Dilakukan	A.8.2.3	Tentang penanganan aset
5.8	Dalam Perencanaan	A.6.1.1	Tentang organisasi dan keamanan informasi
5.9	Dalam Perencanaan	A.8.1.3	Tentang penggunana aset yang dapat diterima
5.10	Dalam Perencanaan	A.18.1.2	Tentang Hak Kekayaan Intelektual
5.11	Dalam Perencanaan	A.12.6.2	Tentang pembatasan pada instalasi perangkat lunak
5.12	Tidak Dilakukan	A.18.1.4	Tentang privasi dan perlindungan informasi identitas pribadi
5.13	Dalam Perencanaan	A.9.3.1	Tentang penggunaan informasi otentikasi rahasia
5.14	Dalam Perencanaan	A.9.1.1	Tentang kebijakan kontrol akses
5.15	Tidak Dilakukan	A.8.3.2	Tentang pembuangan media
5.16	Tidak Dilakukan	A.13.2.2	Tentang kesepakatan transfer informasi
5.17	Dalam Perencanaan	A.16.1.3	Tentang melaporkan kelemahan keamanan informasi

Tabel 4. 29 Hasil Analisis Area Pengelolaan Aset Informasi (lanjutan)

5.18	Dalam Perencanaan	A.12.3.1	Tentang pencadangan informasi
5.19	Dalam Perencanaan	A.11.1.1	Tentang perimeter keamanan fisik
5.20	Dalam Perencanaan	A.7.1.1	Tentang penyaringan
5.21	Dalam Perencanaan	A.16.1.2	Tentang pelaporan kejadian keamanan informasi
5.22	Dalam Perencanaan	A.8.3.2	Tentang pembuangan media
5.23	Dalam Perencanaan	A.9.2.2	Tentang provisioning akses pengguna
5.24	Dalam Perencanaan	A.7.3.1	Tentang penghentian dan perubahan tanggung jawab pekerjaan
5.25	Dalam Perencanaan	A.12.3.1	Tentang pencadangan informasi
5.26	Dalam Perencanaan	A.12.4.1	Tentang pencatatan kejadian
5.27	Dalam Perencanaan	A.18.1.2	Tentang Hak Kekayaaan Intelektual
5.32	Tidak Dilakukan	A.11.2.6	Tentang keamanan peralatan dan aset di luar lokasi
5.33	Tidak Dilakukan	A.11.1.6 A.13.1.2	Tentang area pengiriman yang aman
5.36	Tidak Dilakukan	A.13.2.2	Tentang kesepakatan transfer informasi
5.37	Dalam Perencanaan	A.11.1.5	Tentang bekerja di area yang aman
5.38	Dalam Perencanaan	A.11.1.2	Tentang kontrol entri fisik

4.15 Analisis Pada Teknologi dan Keamanan Informasi

Berdasarkan pengumpulan data yang telah dilakukan, selanjutnya dilakukan analisis kontrol pada setiap jawaban yang diberikan responden dengan kontrol ISO/IEC 27001:2013. Hal ini bertujuan untuk mengetahui bentuk pengamanan yang belum diterapkan pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Berikut hasil analisis kontrol pada area teknlogi dan keamanan informasi dengan kontrol ISO/IEC 27001:2013.

Tabel 4. 30 Hasil Analisis Area Teknologi dan Keamanan Informasi

No Pertanyaan	Status Pengamanan	Kontrol ISO 27001	Keterangan
6.3	Dalam Perencanaan	A.13.1.1 A.13.1.2	Tentang kontrol jaringan dan keamanan layanan jaringan
6.4	Dalam Perencanaan	A.13.1.1	Tentang kontrol jaringan
6.5	Dalam Perencanaan	A.13.1.1	Tentang kontrol jaringan
6.10	Dalam Perencanaan	A.12.4.1	Tentang pencatatan kejadian
6.11	Tidak Dilakukan	A.10.1.1	Tentang pengunaan kontrol kriptografi
6.12	Dalam Perencanaan	A.10.1.1	Tentang pengunaan kontrol kriptografi
6.13	Tidak Dilakukan	A.10.1.2	Tentang pengelolaan kunci
6.14	Dalam Perencanaan	A.9.4.3	Tentang sistem manajemen kata sandi
6.15	Tidak Dilakukan	A.9.4.5	Tentang kontrol akses ke kode sumber
6.20	Dalam Perencanaan	A.12.2.1	Tentang prosedur operasi terdokumentasi
6.21	Dalam Perencanaan	A.12.2.1	Tentang prosedur operasi terdokumentasi
6.22	Dalam Perencanaan	A.12.2.1	Tentang prosedur operasi terdokumentasi
6.24	Dalam Perencanaan	A.14.2.1	Tentang kebijakan pembangunan yang aman

Tabel 4. 31 Hasil Analisis Area Teknologi dan Keamanan Informasi (lanjutan)

6.25	Dalam Perencanaan	A.14.2.6	Tentang lingkungan pengembangan yang aman
6.26	Dalam Perencanaan	A.18.2.1	Tentang tinjau independen atas keamanan informasi

4.16 Analisis Kontrol Pada Area Suplemen

Berdasarkan pengumpulan data yang telah dilakukan, selanjutnya dilakukan analisis kontrol pada setiap jawaban yang diberikan responden dengan kontrol ISO/IEC 27001:2013. Hal ini bertujuan untuk mengetahui bentuk pengamanan yang belum diterapkan pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Berikut hasil analisis kontrol pada area suplemen dengan kontrol ISO/IEC 27001:2013.

Tabel 4. 32 Hasil Analisis Area Suplemen

No Pertanyaan	Status Pengamanan	Kontrol ISO 27001	Keterangan
7.1.1	Tidak Dilakukan	A.5.1.1 A.12.7.1 A.16.1.3 A.16.1.6 A.17.1.1 A.17.1.2 A.17.1.3 A.18.2.1	Tentang kebijakan untuk keamanan informasi, kontrol audit sistem informasi, tentang melaporkan kelemahan keamanan informasi, tentang belajar insiden keamanan informasi, tentang merencanakan keberlanjutan keamanan informasi, tentang menerapkan kontinuitas keamanan informasi, tentang verifikasi, tinjau dan evaluasi keberlanjutan keamanan informasi dan tentang tinjauan independen atas keamanan informasi.

Tabel 4. 33 Hasil Analisis Area Suplemen (lanjutan)

7.1.2	Tidak Dilakukan	A.5.1.1 14.2.7	Tentang kebijakan untuk keamanan informasi dan tentang pengembangan yang dialih dayakan.
7.1.3	Tidak Dilakukan	A.5.1.1 A.6.1.1 A.12.7.1	Tentang kebijakan untuk keamanan informasi, tentang peran dan tanggung jawab keamanan informasi dan tentang kontrol audit sistem informasi.
7.1.4	Tidak Dilakukan	A.15.2.2	Tentang mengelola perubahan pada layanan pemasok
7.1.5	Tidak Dilakukan	A.5.1.1 A.8.3.1 A.8.3.2	Tentang kebijakan untuk keamanan informasi, tentang pengelolaan media yang dapat dilepas, dan tentang pembuangan media.
7.1.6	Tidak Dilakukan	A.16.1.2 A.16.1.4 A.16.1.5 A.16.1.7	Tentang pelaporan kejadian keamanan informasi, tentang penilaian dan keputusan tentang kejadian keamanan informasi, tentang tanggapan terhadap insiden keamanan informasi, tentang belajar dari insiden keamanan informasi dan tentang pengumpulan bukti.

Tabel 4. 34 Hasil Analisis Area Suplemen (lanjutan)

7.1.7	Tidak Dilakukan	A.5.1.1 A.17.1.1 A.17.1.2 A.17.1.3	Tentang kebijakan untuk keamanan informasi, tentang merencanajan keberlanjutan keamanan informasi, tentang menerapkan kontinuitas keamanan informasi dan tentang verifikasi, tinjau, dan evaluasi keberlanjutan keamanan informasi
7.2	Tidak Dilakukan	A.5.1.1 A.8.2.3 A.18.1.4 A.18.1.1 A.16.12	Tentang kebijakan untuk keamanan informasi, Tentang penanganan aset, tentang privasi dan perlindungan informasi identitas pribadi, tentang identifikasi peraturan perundangan yang berlaku dan persyaratan kontrak dan tentang pelaporan kejadian keamanan informasi
7.3	Tidak Dilakukan	A.5.1.1 A.6.1.1 A.8.3.2 A.18.1.1 A.18.1.2 A.18.1.4	Tentang kebijakan untuk keamanan informasi, Tentang peran dan tanggung jawab keamanan informasi, Tentang pembuangan media, Tentang identifikasi peraturan perundangan yang berlaku dan persyaratan kontrak, Tentang hak kekayaan intelektual dan tentang privasi dan perlindungan informasi identitas pribadi.

BAB 5 PEMBAHASAN

Berdasarkan dari hasil akhir penilaian indeks KAMI pada gambar 4.1, diperoleh hasil bahwa tingkat kelengkapan penerapan standar ISO/IEC 27001:2013 berdasarkan kategori sistem elektronik memperoleh skor 163 yang berada pada area berwarna "Merah" dan termasuk dalam status "Tidak Layak". Hal tersebut menunjukkan bahwa bentuk pengamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri yang sudah diterapkan belum memenuhi tingkat kelengkapan sesuai standar ISO 27001 dan banyak diperlukan perbaikan untuk meningkatkan keamanan informasi.

5.1 Tata Kelola Keamanan Informasi

Penerapan tata kelola keamanan informasi memperoleh skor pencapaian penerapan pengamanan informasi sebesar 33 dan tingkat kematangan I+ serta persentase tingkat kematangan yang dicapai adalah 26,1%. Berdasarkan penilaian yang telah dilakukan, diperoleh informasi bahwa pada area ini dengan cakupan evaluasi pada fungsi/organisasi keamanan informasi pada saat ini belum diterapkan sepenuhnya. Saat ini pimpinan instansi telah secara formal bertanggung jawab penuh atas pelaksanaan program keamanan informasi, telah mempunyai fungsi/tugas atau bagian yang spesifik yang bertanggung jawab penuh pada pengelolaan keamanan informasi serta menjaga kepatuhannya. Berdasarkan penilaian yang telah dilakukan, didapatkan beberapa aspek yang belum dilakukan atau sedang dalam perencanaan pada penilaian Indeks KAMI sehingga pertanyaan pada Indeks KAMI yang belum terpenuhi diajukan sebagai rekomendasi berdasarkan pemetaan pada kontrol Annex A ISO 27001 dan *Information Security Management Documentation Checklist*. Pada tabel 5.1 merupakan pemetaan 17 rekomendasi pada area tata kelola keamanan informasi dengan kontrol Annex A ISO 27001 yang terbagi dalam 3 (tiga) tahap penerapannya. Rekomendasi diajukan secara bertahap dilakukan per tahun sesuai dengan kategori pengamanan pada Indeks KAMI. Berikut merupakan 3 (tiga) rekomendasi perbaikan pada kategori pengamanan 1 terkait dengan penerapan kerangka kerja dasar pada tahun pertama yang diusulkan.

Tabel 5. 1 Rekomendasi Perbaikan Area Tata Kelola Keamanan Informasi Kategori Pengamanan 1

No Pertanyaan	Area Tata Kelola Keamanan Informasi (*as-is*)	Rekomendasi (*to-be*)	Kontrol ISO 27001
2.5	Belum ditetapkannya tugas dan peran pengelola pengamanan informasi yang	Menetapkan peran pelaksana pengamanan informasi pada masing-masing individu yang mencakup kewenangan	A.6.1.1

	meliputi seluruh keperluan secara lengkap	masing-masing pelaksana pengamanan informasi yang didokumentasikan dalam uraian tugas, pemberitahuan lowongan, kebijakan keamanan informasi, buku pegangan karyawan, kontrak kerja, kontrak layanan	
2.6	Belum mendefinisikan persyaratan atau standar-standar keahlian serta kompetensi yang perlu dimiliki oleh setiap individu pelaksana pengelola keamanan informasi	Menetapkan persyaratan atau kompetensi, lmu keahlian yang perlu dimiliki oleh setiap individu pelaksana pengelolaan keamanan informasi yang tercantum dalam perjanjian kontrak dengan karyawan	A.7.1.2
2.7	Belum memadainya kompetensi serta keahlian yang dimiliki pengelola keamanan informasi berdasarkan persyaratan/standar yang berlaku	Menetapkan program kerja terkait penilaian kompetensi dan keahlian pelaksana keamanan informasi dengan melakukan penilaian terhadap komitmen dan motivasi para karyawan untuk selalu meningkatkan pengamanan informasi serta kewaspadaan karyawan untuk selalu menghindari kegiatan yang menyebabkan insiden kegagalan keamanan informasi, peran serta tanggung jawab setiap pelaksana pengamanan informasi pada instansi	A.7.2.1

Kondisi saat ini belum ditetapkannya tugas serta peran pengamanan informasi yang meliputi seluruh keperluan mencakup kebutuhan terhadap audit internal dan syarat segregasi kewenangan sesuai dengan kontrol ISO A.6.1.1

tentang peran dan tanggung jawab keamanan informasi. Rekomendasi yang diberikan adalah perlu mengalokasikan dan menentukan peran dan tanggung jawab pelaksana pengamanan informasi meliputi seluruh keperluan termasuk pada kebutuhan internal serta persyaratan segregasi kewenangan harus ditetapkan. Peran serta tanggung jawab pelaksana pengamanan informasi perlu didokumentasi dalam uraian tugas, pemberitahuan lowongan, kebijakan keamanan informasi, buku pegangan karyawan, kontrak kerja, kontrak layanan dan lain-lain.

Keadaan saat ini yakni belum mendefinisikan persyaratan atau standar-standar terkait keahlian serta kompetensi yang perlu dimiliki oleh setiap pelaksana pengelolaan keamanan informasi berdasarkan kontrol Annex A A.7.1.2 tentang syarat dan ketentuan pekerjaan. Rekomendasi yang perlu dilakukan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan syarat-syarat dan kriteria keahlian yang perlu dimiliki setiap pelaksana pengelolaan keamanan informasi yang tercantum dalam perjanjian kontrak dengan karyawan.

Kondisi saat ini yakni kompetensi, ilmu dan keahlian yang dimiliki pelaksana pengamanan informasi belum memadai. Kondisi ini berdasarkan persyaratan/standar yang sedang berlaku. Kondisi tersebut sesuai dengan kontrol Annex A A.7.2.1 tentang tanggung jawab manajemen. Rekomendasi yang diberikan adalah perlu menetapkan program kerja terkait penilaian kompetensi dan keahlian pelaksana pengamanan informasi pada instansi dengan melakukan penilaian terhadap komitmen dan motivasi para karyawan untuk selalu meningkatkan pengamanan informasi serta kewaspadaan karyawan untuk selalu menghindari kegiatan yang menyebabkan insiden keamanan informasi.

Berikutnya merupakan rekomendasi yang diusulkan untuk tahun ke 2 (dua) dalam penerapan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Kategori pengamanan 2 yakni terkait dengan efektivitas serta konsistensi penerapan keamanan informasi atau penerapan operasional. Rekomendasi berikut diusulkan dilaksanakan sebagai lanjutan dari penerapan rekomendasi pada kategori pengamanan 1 sebelumnya. Berikut terdapat 8 (delapan) rekomendasi perbaikan yang diusulkan pada kategori pengamanan 2.

Tabel 5. 2 Rekomendasi Perbaikan Area Tata Kelola Keamanan Informasi Kategori Pengamanan 2

No Pertanyaan	Area Tata Kelola Keamanan Informasi (*as-is*)	Rekomendasi (*to-be*)	Kontrol ISO 27001
2.9	Belum diterapkannya program sebagai upaya untuk meningkatkan kompetensi dan	Menetapkan program kerja yang bertujuan untuk meningkatkan kompetensi dan keahlian pelaksana pengelola keamanan	A.7.2.2

	keahlian pada setiap petugas dan pejabat pelaksana pengelolaan keamanan informasi	informasi. Program kerja ini dapat berupa poster kesadaran untuk memenuhi tanggung jawab, pendidikan, pelatihan atau seminar, dan pembaruan rutin, pelaksanaan tes dan kuis	
2.10	Belum mengintegrasikan keperluan atau persyaratan keamanan informasi	Mendefinisikan strategi kesinambungan bisnis, kebijakan, rencana, syarat terhadap keamanan informasi serta kelanjutan manajemen keamanan informasi	A.17.1.1
2.11	Belum mengidentifikasikan data pribadi yang berdasarkan dengan peraturan perundangan yang berlaku	Menetapkan kebijakan, prosedur serta proses terkait dengan privasi dan perlindungan informasi pribadi sesuai dalam peraturan yang berlaku dan harus dikomunikasikan kepada seluruh pihak yang terlibat	A.18.1.4
2.12	Tanggung jawab dan tugas pengelola keamanan informasi belum termasuk berkoordinasi bersama pihak pengguna/pengelola aset informasi meliputi pihak internal dan eksternal ataupun pihak lain yang berkepentingan (misal: pertukaran informasi)	Menetapkan sebuah prosedur dan kebjiakan terkait transfer informasi pihak internal dan eksternal yang meliputi analisis risiko, kontrak, pengamatan, identifikasi dan otentikasi, enkripsi, logging dan peringatan, konfirmasi pengiriman atau tanda terima, kontak darurat, peringatan tentang kegagalan tautan	A.13.2.2
2.13	Tanggung jawab pengelola keamanan informasi belum termasuk koordinasi bersama satuan kerja	Perjanjian kontrak dengan karyawan harus mencakup peran dan tanggung jawab pengelola keamanan terkait penerapan	A.7.1.2

	terkait dan pihak eksternal	pengamanan informasi yang melibatkan berbagai pihak	
2.14	Belum menentukan serta mengalokasikan tanggung jawab dalam pemutusan, perancangan, melaksanakan dan mengelola langkah keberlangsungan layanan teknologi informasi dan komunikasi atau *business continuity* dan *disaster recovery plans*	Menentukan dan menetapkan dokumen terkait dengan syarat untuk keamanan informasi serta kelanjutan untuk keamanan informasi meliputi dokumen strategi kesinambungan bisnis,rencana, kebijakan, prosedur, laporan pengujian atau pelatihan	A.17.1.1
2.15	Belum terdapat penanggung jawab yang mengelola keamanan informasi yang bertugas terhadap pelaporan eketivitas, kinerja atau kinerja dan kepatuhan terhadap program keamanan informasi pada pimpinan	Menetapkan penanggung jawab dan tugas keamanan informasi untuk menyampaikan pelaporan terkait efektivitas, pelaporan, dan kepatuhan pada program keamanan informasi pada pimpinan yang didokumentasikan dalam uraian tugas, pemberitahuan lowongan, kebijakan keamanan informasi, buku pegangan karyawan, kontrak kerja, kontrak layanan	A.18.2.2
2.16	Permasalahan dan serta kondisi terkait keamanan informasi tidak dijadikan bagian pertimbangan dalam pengambilan keputusan yang strategis di instansi	Menetapkan karyawan serta kontraktor pada instansi untuk melakukan penerapan keamanan informasi berdasarkan kebijakan dan prosedur yang berlaku untuk mengidentifikasi permasalahan-permasalahan keamanan informasi pada instansi	A.7.2.1

Kemudian saat ini belum diterapkannya program khusus yang bertujuan untuk meningkatkan kompetensi keahlian pada setiap petugas dan pejabat pelaksana pengelolaan keamanan informasi adalah salah satu aspek indeks KAMI yang belum dilakukan. Kondisi tersebut sesuai dengan kontrol Annex A A.7.2.2 tentang kesadaran keamanan informasi, pendidikan dan pelatihan. Rekomendasi yang diberikan adalah perlu ditetapkan program kerja yang bertujuan untuk mengembangkan kompetensi, ilmu dan keahlian pelaksana pengelola keamanan informasi. Program kerja ini dapat berupa poster kesadaran untuk memenuhi tanggung jawab, pendidikan, pelatihan atau seminar, dan pembaruan rutin, pelaksanaan tes dan kuis.

Kondisi saat ini belum terintegrasinya kebutuhan atau persyaratan-persyaratan keamanan informasi pada proses kerja yang ada. Kondisi tersebut sesuai dengan kontrol Annex A 17.1.1 tentang merencanakan keberlanjutan keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu mendefinisikan strategi kelangsungan bisnis, kebijakan, rencana, persyaratan keamanan informasi serta kelangsungan manajemen keamanan informasi pada kondisi merugikan yang bertujuan untuk memastikan kesinambungan aktivitas dan kontrol keamanan informasi selama terjadi insiden.

Belum mengidentifikasi data pribadi sesuai berdasarkan peraturan perundangan yang berlaku merupakan salah satu aspek yang belum diterapkan pada area ini. Kondisi ini sesuai dengan kontrol Annex A A.18.1.4 tentang privasi dan perlindungan informasi identitas pribadi. Rekomendasi yang diusulkan adalah perlu menetapkan serangkaian kebijakan, prosedur, dan proses terkait dengan privasi dan serta untuk melindungi informasi data pribadi sesuai dengan yang disyaratkan pada peraturan perundang-undangandan dan harus dikomunikasikan kepada seluruh pihak yang terlibat. Kemudian perlu menetapkan pengelola tim yang memiliki peran dan tanggung jawab terhadap pengelolaan data pribadi yang dijalankan.

Tugas pengelolaan keamanan informasi belum meliputi berkoordinasi bersama pihak pengelola aset dan pengguna aset informasi yang meliputi pihak internal dan pihak eksternal ataupun pihak lain yang memiliki kepentingan untuk menerapkan serta menjamin kepatuhan pengamanan informasi, misalnya pertukaran informasi. Kondisi tersebut sesuai dengan kontrol Annex A A.13.2.2 tentang kesepakatan tentang transfer informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan prosedur dan kebijakan terkait transfer informasi pihak internal dan pihak eksternal. Prosedur dan kebijakan tersebut meliputi analisis risiko, kontrak, pengamatan, identifikasi dan otentikasi, enkripsi, logging dan peringatan, konfirmasi pengiriman atau tanda terima, kontak darurat, peringatan tentang kegagalan tautan dan lain-lain.

Kondisi pada saat ini adalah tanggungjawab pengelola keamanan informasi belum termasuk koordinasi yang secara proaktif berkoordinasi bersama satuan kerja instansi pemerintah dan pihak luar yang memliki kepentingan untuk penerapan dan memastikan terjaminnya kepatuhan pengamanan informasi yang berkaitan proses kerja yang melibatkan banyak pihak. Kondisi tersebut sesuai dengan kontrol Annex A A.7.1.2 tentang syarat dan ketentuan pekerjaan. Rekomendasi yang harus dilakukan adalah pada setiap perjanjian kontrak dengan karyawan atau pengelola keamanan informasi harus terdapat peran serta tanggung jawab pengelola keamanan informasi yang mencakup penerapan serta menjamin kepatuhan pada pengamanan informasi yang berkaitan dengan proses kerja yang melibatkan banyak pihak.

Belum didefinisikan dan dialokasikan tanggung jawab untuk pemutusan, perancangan, pelaksanaan serta mengelola langkah keberlangsungan layanan TIK dan komunikasi atau *business continuity* dan *disaster recovery plans*. Kondisi ini sesuai dengan kontrol A.17.1.1 pada Annex A tentang merencanakan keberlanjutan keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu mendefinisikan dan menetapkan dokumen terkait dengan syarat untuk keamanan informasi dan kelanjutan untuk manajemen keamanan informasi. Rekomendasi tersebut mencakup strategi kesinambungan bisnis,rencana, kebijakan, prosedur, laporan pengujian atau pelatihan dan lain sebagainya.

Kondisi saat ini yakni belum terdapat penanggung jawab yang mengelola keamanan informasi yang bertugas terhadap pelaporan eketivitas, kinerja atau kinerja dan kepatuhan program keamanan informasi pada pimpinan Kondisi tersebut sesuai dengan kontrol Annex A A.18.2.2 tentang kepatuhan dengan kebijakan dan standar keamanan. Sehingga diajukan rekomendasi yakni adalah perlu menetapkan penanggung jawab dan tugas keamanan informasi untuk menyampaikan pelaporan terkait efektivitas, pelaporan, dan kepatuhan pada program keamanan informasi pada pimpinan instansi yang didokumentasikan dalam uraian tugas, pemberitahuan lowongan, kebijakan keamanan informasi, buku pegangan karyawan, kontrak kerja, kontrak layanan.

Permasalahan dan serta kondisi terkait keamanan informasi tidak dijadikan bagian pertimbangan dalam pengambilan keputusan yang strategis di instansi. Kondisi tersebut sesuai dengan kontrol Annex A A.7.2.1 tentang tanggung jawab manajemen. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu mengharuskan karyawan serta kontraktor pada instansi untuk melakukan penerapan keamanan informasi berdasarkan kebijakan dan prosedur yang berlaku untuk mengidentifikasi permasalahan-permasalahan keamanan informasi pada instansi kemudian harus dicatat, dianalisis, ditindaklanjuti kemudian diselesaikan untuk dijadikan sebagai bukti terhadap kepatuhan organisasi untuk menetapkan langkah-langkah perbaikan untuk dijadikan dasar untuk pengambilan keputusan strategis pada instansi meningkatkan kualitas pengamanan informasi.

Berikutnya merupakan rekomendasi yang diusulkan untuk tahun ke 3 (tiga) dalam penerapan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Kategori pengamanan 3 yakni terkait dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi. Pada kategori pengamanan 3 memiliki persyaratan bahwa seluruh bentuk pengamanan pada kategori 1 dan 2 telah diterapkan. Sehingga rekomendasi berikut diusulkan dilaksanakan sebagai lanjutan dari penerapan rekomendasi pada kategori pengamanan 1 dan 2 sebelumnya. Berikut terdapat 6 (enam) rekomendasi perbaikan yang diusulkan pada kategori pengamanan 3.

Tabel 5. 3 Rekomendasi Perbaikan Area Tata Kelola Keamanan Informasi Kategori Pengamanan 3

No Pertanyaan	Area Tata Kelola Keamanan Informasi (*as-is*)	Rekomendasi (*to-be*)	Kontrol ISO 27001
2.17	Belum diterapkannya program yang bertujuan untuk patuh terhadap sasaran dan tujuan kepatuhan pengamanan informasi	Menetapkan program khusus yang bertujuan untuk patuh terhadap sasaran dan tujuan kepatuhan pengamanan informasi yang diimplementasikan dalam manajemen proyek yang mencakup pengidentifikasian dan penilaian terhadap risiko keamanan informasi yang relevan dan aktivitas keamanan informasi untuk menetapkan langkah yang harus dilakukan, dan tujuan keamanan informasi harus diimplementasikan pada tujuan proyek terkait	A.6.1.5

Tabel 5. 3 Rekomendasi Perbaikan Area Tata Kelola Keamanan Informasi Kategori Pengamanan 3 (lanjutan)

2.18	Belum didefinisikan parameter, metrik , jadwal dan proses untuk mengukur performa pengelolaan keamanan informasi	Mendefinisikan kebijakan keamanan informasi yang mencakup parameter, metrik , jadwal dan proses untuk mengukur terhadap performa pengelola keamanan informasi	A.5.1.1
2.19	Belum diterapkannnya program terkait penilaian terhadap terhadap performa pengelolaan keamanan informasi pada setiap pejabat dan petugas	Menetapkan proses disiplin formal dengan menyusun prosedur dan program penilaian peforma terhadap pengelola keamanan informasi serta dapat digunakan sebagai pertimbangan dalam melakukan tindakan yang sesuai pada karyawan melanggar keamanan informasi	A.7.2.3
2.20	Belum diterapkannya sasaran dan target untuk mengelola keamanan informasi pada berbagai area yang relevan	Menetapkan kebijakan terkait sasaran dan target keamanan informasi pada area yang relevan mencakup aspek penetapan sasaran dan target mengelola keamanan informasi, evaluasi ketercapaian, penerapan langkah pembenahan serta melaporkannya kepada pimpinan instansi yang terdokumentasi.	A.5.1.1

Tabel 5. 3 Rekomendasi Perbaikan Area Tata Kelola Keamanan Informasi Kategori Pengamanan 3 (lanjutan)

2.21	belum mengidentifikasi legislasi standar keamanan informasi, perundang-undangan serta perangkat hukum	Mengidentifikasi dan memelihara seluruh persyaratan kepatuhan atau kewajiban atau harapan pihak eksternal pada instansi yang meliputi undang-undangan yang berkaitan, persyaratan kontrak, legislasi, misalnya lisensi perangkat lunak, hak paten, dan hak cipta	A.18.1.1
2.22	Belum didefinisikan langkah langkah untuk menanggulangi insiden keamanan informasi dan kebijakannya	Mendefinisikan kebijakan, prosedur, pedoman keamanan informasi terkait dengan penangulangan insiden yang mencakup catatan atau bukti tentang insiden atau peristiwa yang dilaporkan dan menetapkan peran penanggulang insiden keamanan informasi	A.16.1.1

Saat ini sebagai upaya dalam patuh terhadap sasaran dan tujuan kepatuhan pengamanan informasi, instansi terkait belum menerapkan sebuah program khusus. khususnya meliputi aset informasi yang menjadi tanggung jawabnya. Kondisi tersebut sesuai dengan kontrol Annex A A.6.1.5 tentang keamanan informasi dalam manajemen proyek. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu diterapkan program untuk patuh terhadap sasaran dan tujuan kepatuhan pengamanan informasi yang diimplementasikan dalam manajemen proyek. Dalam pelaksanaanya, harus mencakup pengidentifikasian dan penilaian terhadap risiko keamanan informasi yang relevan dan aktivitas keamanan informasi untuk menetapkan langkah yang harus dilakukan, dan tujuan keamanan informasi harus diimplementasikan dalam tujuan proyek terkait.

Aspek pada Indeks KAMI yang belum diterapkan yaitu belum didefinisikan parameter, metrik dan proses mengukur performa pengelolaan keamanan informasi yang meliputi jadwal pengukuran, mekanisme, penanggung jawabnya, pemantauan dan eskalasi pelaporan. Kondisi ini sesuai dengan kontrol Annex A

A.5.1.1 tentang kebijakan untuk keamanan informasi. Rekomendasi yang diajukan yakni perlu menetapkan kebijakan keamanan informasi tertulis yang mencakup parameter, metrik dan proses untuk mengukur performa pengelolaan keamanan informasi yang meliputi jadwal pengukuran, mekanisme, penanggung jawabnya, pemantauan dan pelaporannya. Pimpinan instansi harus menetapkan dan menyetujui kebijakan tersebut secara resmi kemudian harus diterbitkan dan dikomunikasikan pada karyawan serta pihak eksternal relevan.

Program kerja terkait penilaian terhadap performa pengelolaan keamanan informasi bagi setiap pejabat dan petugas masih belum ditetapkan pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Kondisi ini sesuai dengan kontrol Annex A A.7.2.3 tentang proses pendisiplinan. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan proses disipliner formal dengan menyusun prosedur dan program terkait penilaian performa pengelola kemanan informasi serta dapat digunakan untuk melakukan tindakan yang sesuai dan tepat pada karyawan yang melanggar keamanan informasi.

Pengelolaan keamanan informasi pada area yang relevan belum mencakup sasaran dan target yang ditetapkan. Kondisi ini sesuai dengan kontrol Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan keamanan informasi yang didalamnya mencakup aspek penetapan sasaran dan target pengelolaan keamanan informasi, evaluasi ketercapaian, penerapan langkah pembenahan dan melaporkannya pada pimpinan yang terdokumentas resmi. Pimpinan instansi harus menetapkan, menyetujui, menerbitkan serta mengkomunikasikan kebijakan pada karyawan dan pihak eksternal yang bersangkutan.

standar, legilasi dan perangkat hukum terkait keamanan informasi saat ini belum diterapkan yaitu belum mengidentifikasi Kondisi tersebut sesuai dengan kontrol Annex A A.18.1.1 tentang identifikasi peraturan perundangan yang berlaku dan pesyaratan kontrak. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu mengidentifikasi, dan memelihara seluruh persyaratan kepatuhan atau kewajiban atau harapan pihak eksternal pada instansi yang meliputi undang-udang yang berkaitan, peraturan persyaratan kontrak, legislasi, misalnya lisensi perangkat lunak, hak paten, dan hak cipta.

Kebijakan serta langkah untuk menanggulangi insiden yang berkaitan dengan pelanggaran hukum perdata dan pidana masih belum didefinisikan. Kondisi ini sesuai dengan kontrol Annex A A.16.1.1 tentang tanggung jawab dan prosedur manajemen insiden keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu mendefinisikan dan menetapkan kebijakan, prosedur, pedoman keamanan informasi dan menetapkan tanggung jawab untuk mengelola insiden keamanan informasi. prosedur, kebijakan dan pedoman tersebut harus mencakup catatan atau bukti

tentang insiden yang dilaporkan, melakukan pencatatan dan analisis, diatasi serta dharus diselesaikan sebagai bukti kepatuhan terhadap kebijakan yang berlaku.

Berdasarkan dari penjabaran diatas, secara garis besar diperlukannya penetapan peran pelaksana pengamanan informasi. Menetapkan persyaratan atau kompetensi keahlian pelaksana pengamanan informasi. Menetapkan program kerja terkait penilaian keahlian dan kompetensi pelaksana pengamanan informasi. Menetapkan program kerja untuk meningkatkan keahlian, ilmu kompetensi pengelola keamanan informasi. Kemudian perlu mendefinisikan strategi kesinambungan bisnis, kebijakan dan rencana bisnis dalam situasi yang merugikan. Mendefinisikan kebijakan dan prosedur terkait dengan privasi dan perlindungan informasi pribadi. Menetapkan kebijakan dan prosedur transfer informasi terhadap pihak internal dan pihak eksternal. Menetapkan syarat-syarat dan ketentuan untuk keamanan informasi dan keberlanjutan manajemen keamanan informasi. Menetapkan pnanggung jawab pengelola manajemen insiden keamanan informasi. Menetapkan tujuan, sasaran dan target kepatuhan pengamanan informasi pada manajemen proyek. Menetapkan kebijakan terkait dengan parameter, metrik dan proses untuk mengukur kinerja pengelolaan keamanan informasi. Menetapkan proses disipliner formal dengan menyusun prosedur dan program terkait penilaian kinerja pengelola kemanan informasi. Menetapkan kebijakan keamanan informasi yang didalamnya mencakup aspek penetapan sasaran dan target pengelolaan keamanan informasi, evaluasi pencapaian, penerapan langkah perbaikan dan pelaporannya. Mengidentifikasi persyaratan kepatuhan atau kewajiban pihak eksternal pada instansi.

5.2 Pengelolaan Risiko Keamanan Informasi

Skor ketercapaian penerapan pengelolaan risiko keamanan informasi adalah 9 dengan tingkat kematangan I serta persentase tingkat kematangan yang dicapai adalah 12,5%. Berdasarkan penilaian yang telah dilakukan, diperoleh informasi bahwa penerapan langkah untuk mengelola risiko keamanan informasi tidak dilakukan. Dinas Komunikasi dan Informatika Kabupaten Kediri saat ini belum mendefinisikan dan menetapkan kerangka kerja pengeloaan risiko keamanan informasi secara terperinci terkait penetapan penanggung jawab/ pengelola manajemen risiko, proses identifikasi dan pengkajian risiko serta langkah mitigasinya. Berdasarkan penilaian yang telah dilakukan, dapat diketahui bahwa seluruh aspek pengelolaan risiko keamanan informasi belum diterapkan seluruhnya. Sehingga aspek tersebut diajukan sebagai rekomendasi perbaikan yang perlu dilakukan berdasarkan pemetaan pertanyaan pada Indeks KAMI dengan kontrol ISO Annex A dan *Information Security Management Documentation Checklist*. Berikut pada tabel 5.2 merupakan pemetaan 16 rekomendasi perbaikan pada area pengelolaan risiko keamanan informasi yang terbagi dalam 3 (tiga) tahap penerapannya. Rekomendasi diajukan secara bertahap dilakukan per tahun sesuai dengan kategori pengamanan pada Indeks KAMI. Berikut merupakan 10 (sepuluh) rekomendasi perbaikan pada kategori

pengamanan 1 terkait dengan penerapan kerangka kerja dasar pada tahun pertama yang diusulkan.

Tabel 5. 4 Rekomendasi Perbaikan Area Pengelolaan Risiko Keamanan Informasi Kategori Pengamanan 1

No Pertanyaan	Area Pengelolaan Risiko Keamanan Informasi (*as-is*)	Rekomendasi (*to-be*)	Kontrol ISO 27001
3.1	Belum memiliki program kerja untuk mengelola risiko keamanan informasi	Menetapkan program kerja untuk mengelola risiko keamanan informasi yang tertulis dan ditetapkan secara formal dan resmi oleh pimpinan	A.5.1.1
3.2	Tanggung jawab untuk mengelola manajemen risiko serta melapokannya pada pimpinan belum ditetapkan	Mendefinisikan dan menetapkan peran serta tanggung jawab pengelola manajemen risiko dan eskalasi pelaporannya yang terdokumentasi dalam kebijakan risiko keamanan informasi, uraian tugas, pemberitahuan lowongan, buku pegangan karyawan, kontrak kerja dan kontrak layanan yang telah ditetapkan dan disetujui, kemudian diterbitkan serta harus dikomunikasikan pada karyawan serta pihak eksternal berkaitan	A.6.1.1
3.3	Belum memiliki kerangka kerja untuk mengelola risiko keamanan informasi yang didokumentasikan secara resmi	Mendefinisikan dan kerangka kerja untuk mengelola risiko terkait keamanan informasi yang terdokumentasi dan ditetapkan oleh pimpinan instansi	A.5.1.1

Tabel 5. 5 Rekomendasi Perbaikan Area Pengelolaan Risiko Keamanan Informasi Kategori Pengamanan 1 (lanjutan)

3.4	Belum terdapat kerangka kerja untuk mengelola risiko yang meliputi hubungan dan definisi tingakatan klasifikasi aset informasi serta tingkatan ancamannya	Mendefinisikan kerangka kerja, kebijakan mengelola risiko meliputi meliputi hubungan dan definisi tingakatan klasifikasi aset informasi serta tingkatan ancamannya	A.5.1.1
3.5	Belum ditetapkannya ambang batasan tingkatan risiko yang dapat diterima	Menetapkan ambang batas risiko keamanan informasi yang dapat diterima organisasi pada kerangka kerja	A.5.1.1
3.6	Pihak pengelola aset dan kemepilikannya belum didefinisikan	Menetapkan dokumen terkait kepemilikan dan pengelola aset informasi informasi secara resmi	A.8.1.2
3.7	Kelemahan dan ancaman pada aset informasi belum teridentifikasi	Mengidentifikasi secara tertulis dan spesifik terkait jenis kelemahan (*vulnerability*) dan ancaman (*threat*)n dari aset infomasi yang ada yang tertulis dalam catatan/ bukti/ kelemahan yang dilaporkan. Kemudian dianalisis, ditangani dan diselesaikan untuk menetapkan langkah-langkah penerapan pengamanan informasi	A.16.1.3
3.8	Belum menetapkan dampak kerugian terkait hilanganya/terganggunya fungsi aset utama	mengidentifikasi dampak kerugian terkait hilang/terganggunya fungsi aset informasi yang ada yang dapat dibuktikan dalam bentuk catatan/ bukti peristiwa	A.16.1.6

Tabel 5. 6 Rekomendasi Perbaikan Area Pengelolaan Risiko Keamanan Informasi Kategori Pengamanan 1 (lanjutan)

3.9	Belum menerapkan analisa/kajian risiko keamanan informasi secara terstruktur	Menetapkan proses pengelolaan risiko keamanan informasi berkaitan dengan analisi dan pengkajian risiko keamanan informasi secara terstruktur dan sistematis pada aset informasi	A.5.1.1
3.10	Belum menyusun langkah mitigasi dan penanggulangan risiko	Menetapkan kebijakan klasifikasi informasi, prosedur terkait penanggulangan risiko yang ada serta langkah mitigasinya sesuai dengan klasifikasi aset informasi	A.8.2.3

Program kerja formal dan resmi berkaitan dengan proses mengelola risiko keamanan informasi saat ini belum dimiliki. Rekomendasi perbaikan yang diajukan bedasarkan dengan kontrol A.5.1.1 tentang kebijakan untuk keamanan informasi pada ISO Annex A. Rekomendasi untuk Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan program kerja untuk mengelola risiko keamanan informasi yang mana pimpinan instansi harus menyetujui dan menetapkan secara resmi kemudian harus menerbitkan dan mengkomunikasikan pada karyawan dan pihak eksternal. Pengelolaan risiko keamanan informasi tersebut dapat mencakup persiapan perencanaan respon terhadap insiden, perencanaan manajemen risiko, perencanaan *risk analysis*, prosedur pemantauan, pendeteksian dan analisis serta pelaporan insiden, prosedur penangangan bukti forensik, prosedur insiden logging serta menyusun langkah-langkah yang harus diterapkan serta mengontrol insiden keamanan informasi.

Penanggung jawab terkait untuk mengelola risiko dan melakukan pelaporan pada pimpinan saat ini belum ditetapkan. Rekomendasi perbaikan diajukan sesuai dengan kontrol A.6.1.1 tentang peran dan tanggung jawab keamanan informasi pada ISO Annex A. Rekomendasi yang diajukan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu mendefinisikan atau menguraikan peran dan tanggung jawab penanggung jawab manajemen risiko yang terdokumentasi dalam kebijakan risiko keamanan informasi, uraian tugas, pemberitahuan lowongan, buku pegangan karyawan, kontrak kerja dan kontrak layanan yang ditetapkan dan disetujui, diterbitkan serta dikomunikasikan pada

seluruh karyawan serta pihak eksternal yang relevan. Misalnya, tugas pengelola manajemen risiko yakni harus mendefinisikan dan menentukan apa saja yang perlu dilindungi dan diberi kontrol keamanan yang baik pada organisasi, menetapkan apa saja yang dibutuhkan untuk melindungi, bagaimana langkah untuk melindunginya dan menentukan prioritas apa saja yang diberikan pengamanan yang tinggi dan rendah.

Kerangka kerja mengelola risiko keamanan informasi yang ditetapkan secara resmi dan terdokumentasi saat ini belum dimiliki. Selanjutnya, kerangka kerja belum mencakup hubungan dan definisi tingkatan klasifikasi aset informasi dan tingkat ancamannya serta dampak yang mungkin dapat merugikan instansi, kemudian belum ditetapkannya ambang batasan risiko yang dapat diterima dan serta menerapkan kajian dan analisis risiko keamanan informasi yang dilakukan pada aset yang ada. Rekomendasi yang diajukan sesuai dengan kontrol A.5.1.1 pada ISO Annex A. Sehingga, perlu mendefinisikan dan menetapkan kerangka kerja untuk mengelola risiko yang terdokumentasi dan ditetapkan oleh pimpinan instansi. Kerangka kerja tersebut meliputi hubungan dan definisi tingkatan klasifikasi aset informasi, identifikasi tingkatan ancamanya, kemungkinan terjadinya ancaman atau risiko serta identifikasi dampak kelemahan dari aset informasi yang ada. Kemudian, perlu mengklasifikasikan risiko yang kemungkinan terjadi dan ditetapkannya ambang batas risiko yang dapat diterima oleh instansi, waktu, metrik, kategori risiko, peran dan tanggung jawab manajemen insiden keamanan informasi serta proses penanggulangan risiko tertulis sesuai dengan sesuai ketetapan pimpinan instansi. Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan proses mengelola risiko keamanan informasi untuk mengkaji dan menganalisis risiko keamanan informasi secara sistematis pada aset informasi yang ada.

Belum ditetapkannya pihak pengelola aset serta kepemilikannya merupakan aspek Indeks KAMI yang belum dilaksanakan. Kondisi ini sesuai dengan kontrol A.8.1.2 tentang kepemilikan aset pada Annex A. Rekomendasi yang perlu dilakukan adalah perlu mendefinisikan dan mendokumentasikan secara tertulis berbentuk dokumen terkait Pihak pengelola aset serta kepemilikan aset informasi yang ada secara detail, misalnya mencantumkan nama dan peran pemilik aset. Aset informasi merupakan pengetahuan/ data bernilai yang dimiliki oleh suatu organisasi (Kementrian Komunikasi dan Informatika, 2017). Pemilik aset memiliki kewenangan besar dalam pemakaiannya serta bertanggung jawab dalam menjaga keutuhan fungsional aset yang dimiliki. Aset informasi meliputi dan tidak terbatas pada informasi/data , *software*, *hardware*, layanan, sumber daya manusia yang mencakup pengalaman, kualifikasi dan keterampilannya, fasilitas pendukung, barang yang tidak terwujud.

Ancaman dan kelemahan terkait aset informasi yang ada saat ini belum masih teridentifikasi dengan baik. Permasalahan tersebut sesuai dengan kontrol Annex A A.16.1.3 tentang melaporkan kelemahan keamanan informasi. Rekomendasi yang perlu dilakukan adalah mengidentifikasi secara tertulis dan

spesifik terkait jenis ancaman, dan kelemahan dari aset infomasi yang ada dalam bentuk bukti peristia/ catatan kelemahan yang dilaporkan. Kemudian dianalisis, ditangani dan diselesaikan untuk menetapkan langkah-langkah penerapan pengamanan informasi untuk dengan tujuan menghindari dampak yang kemungkinan terjadi di masa depan. Identifikasi ancaman/kelemahan ini dapat dilakukan dengan teknik SWOT analisis. SWOT analisis merupakan proses menganalisis risiko yang terstruktur dan dirancang untuk mengidenfikasi risiko dan peluang yang mungkin terjadi dalam konteks organisasi (Pritchard, 2015). SWOT analisis dilakukan dengan mengidentifikasi/ menjabarkan 4 komponen yang terdiri dari kekuatan (*strength*) yang dimiliki oleh aset informasi, kelemahan (*weakness*) yang dimiliki oleh aset informasi , peluang (*opportunity*) yang mungkin dapat terjadi, dan ancaman (*threats*) terkait aset informasi yang ada kemudian melakukan penyusunan strategi berdasarkan risiko atau ancaman yang telah teridentifikasi.

Kondisi saat ini belum ditetapkannya dampak kerugian yang mungkin terjadi ketika fungsi aset utama hilang dan terganggu. Permasalahan tersebut sesuai dengan kontrol Annex A A.16.1.6 tentang belajar dari insiden keamanan informasi. Rekomendasi yang diajukan pada Dinas Komunikasi dan Informatika Kabupaten Kediri adalah mengidentifikasi dampak/kerugian terkait hilang/terganggunya fungsi aset informasi yang dapat dibuktikan dengan catatan/ bukti peristiwa. Kemudian insiden tersebut harus dianalisis, ditangani dan harus diselesaikan sebagai bukti kepatuhan instansi yang dapat dijadikan sebagai dasar untuk menetapkan langkah untuk menghilangkan/ mengurangi dampak yang kemungkinan terjadi atau menyusun langkah-langkah yang harus dilakukan apabila pada masa yang akan datang terjadi gangguan atau hilangnya fungsi aset utama.

Belum menyusun langkah mitigasi dan penanggulangan risiko merupakan salah satu aspek yang belum diterapkan oleh Dinas Komunikasi dan Informatika. Permasalahan tersebut sesuai dengan kontrol Annex A A.8.2.3 tentang penanganan aset. Rekomendasi yang diajukan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan, prosedur dan panduan klasifikasi informasi bertujuan untuk menangani aset informasi sesuai dengan klasifikasi risiko termasuk untuk mengidentifikasi dampak kerugian terkait hilangnya/tergangunya fungsi aset utama berdasarkan identifikasi risiko yang kemungkinan dapat terjadi di masa depan.

Selanjutnya merupakan rekomendasi yang diusulkan untuk tahun ke 2 (dua) dalam penerapan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Kategori pengamanan 2 yakni terkait dengan efektivitas serta konsistensi penerapan keamanan informasi atau penerapan operasional pada area pengelolaan risiko. Rekomendasi berikut diusulkan dilaksanakan sebagai lanjutan dari penerapan rekomendasi pada kategori pengamanan 1 sebelumnya. Berikut terdapat 4 (empat) rekomendasi perbaikan yang diusulkan pada kategori pengamanan 2.

Tabel 5. 7 Rekomendasi Perbaikan Area Pengelolaan Risiko Keamanan Informasi Kategori Pengamanan 2

No Pertanyaan	Area Pengelolaan Risiko Keamanan Informasi (*as-is*)	Rekomendasi (*to-be*)	Kontrol ISO 27001
3.11	Tahapan untuk mengurangi dampak risiko belum tersusun berdasarkan prioritas target penyelesaian serta penanggung jawabnya	Tahapan untuk mengurangi dampak risiko yang dilakukan harus memperhatikan efektivitas sumber daya yang tersedia serta harus dilakukan pemantauan, disesuaikan dan proyeksi yang dibuat berdasarkan kebutuhan kapasitas yang dibutuhkan	A.12.1.3
3.12	Belum melakukan pemantauan penyelesaian langkah mitigasi risiko secara berkala	Pada langkah mitigasi risiko, harus tersedia status penyelesaian risiko secara rutin untuk memastikand status penyelesaian atau performa kerjanya dengan tujuan menurunkan tingkatan risiko ke ambang batas risiko dapat diterima instansi dengan mengurangi dampak terhadap operasional layanan teknologi informasi yang sedang berlangsung	A.12.1.3
3.13	Penyelesaian langkah mitigasi risiko belum di evaluasi	Menetapkan prosedur kajian terkait dengan kepatuhan instansi terhadap risiko keamanan informasi dan kewajiban keamanan informasi	A.18.2.1

Tabel 5. 8 Rekomendasi Perbaikan Area Pengelolaan Risiko Keamanan Informasi Kategori Pengamanan 2 (lanjutan)

3.14	Belum melakukan kajian ulang terhadap profil risiko dan mitigasinya secara berkala termasuk merevisi profil risiko	Profil risiko harus dikaji ulang dan ditinjau melalui pemeriksaan, pengujian, dan audit termasuk langkah mitigasi yang ditetapkan untuk memastikan efektivitas, akurasi dan validitasnya yang kemudian hasil kajian dan tinjauan dilakukan revisi terhadap profil risiko dan menghasilkan penerapan bentuk pengamanan informasi baru	A.18.2.1

Belum dilakukan pemantauan secara berkala terhadap langkah-langkah untuk mengurangi dampak risiko yang disesuaikan dengan prioritas serta target penyelesaian dan penanggung jawabnya dengan memperhatikan efektivitas sumber daya yang ada serta penyelesaian mitigas risiko. Permasalahan ini sesuai dengan kontrol Annex A A.12.1.3 tentang manajemen kapasitas. Rekomendasi yang diajukan adalah instansi perlu menetapkan strategi mitigasi risiko yang disesuaikan dengan tingkatan prioritas dan target penyelesaiannya dalam memperhatikan sumber daya yang tersedia dan perlu dilakukan pemantauan dan disesuaikan, kemudian proyeksi yang telah disusun berdasarkan keperluan di masa depan untuk memastikan performa sistem yang dibutuhkan. Kemudian dalam penyusunan langkah mitigasi risiko harus tersedia status penyelesaian risiko tersebut untuk mengetahui status penyelesaian langkah mitigasi risiko yang dilakukan dengan tujuan dapat menurunkan tingkatan risiko ke ambang batas risiko yang dapat diterima oleh instansi dengan mengurangi dampak pada operasional layanan teknologi informasi yang berlangsung.

Penyelesaian langkah mitigasi yang sudah diterapkan belum di evaluasi melalui prosedur terukur dan obyektif untuk memastikan efektivitas dan konsistensinya. Kemudian profil risiko dan bentuk mitigasinya belum dikaji secara berkala termasuk merevisi profil risiko apabila ada perubahan. Permasalahan ini sesuai dengan kontrol Annex A A.18.2.1 tentang tinjauan independen atas keamanan informasi. Rekomendasi yang diajukan pada Dinas Komunikasi dan Informatika Kabupaten Kediri adalah instansi perlu melakukan kajian terkait dengan kepatuhan instansi terhadap risiko keamanan informasi dan kewajiban keamanan informasi. Kemudian profil risiko harus dikaji ulang dan ditinjau melalui pemeriksaan, pengujian, dan audit termasuk langkah mitigasi yang

ditetapkan untuk memastikan keefektivitasan, keakuratan dan kevalidannya yang kemudian hasil kajian dan tinjauan dilakukan revisi terhadap profil risiko dan memunculkan penerapan bentuk pengamanan informasi baru.

Berikutnya merupakan rekomendasi yang diusulkan untuk tahun ke 3 (tiga) dalam penerapan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Kategori pengamanan 3 yakni terkait dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi pada area pengelolaan risiko. Pada kategori pengamanan 3 memiliki persyaratan bahwa seluruh bentuk pengamanan pada kategori 1 dan 2 telah diterapkan. Sehingga rekomendasi berikut diusulkan dilaksanakan sebagai lanjutan dari penerapan rekomendasi pada kategori pengamanan 1 dan 2 sebelumnya. Berikut terdapat 2 (dua) rekomendasi perbaikan yang diusulkan pada kategori pengamanan 3.

Tabel 5. 6 Rekomendasi Perbaikan Area Pengelolaan Risiko Keamanan Informasi Kategori Pengamanan 3

No Pertanyaan	Area Pengelolaan Risiko Keamanan Informasi (*as-is*)	Rekomendasi (*to-be*)	Kontrol ISO 27001
3.15	Belum melakukan kajian terhadap kerangka kerja untuk mengelola risiko secara rutin	Kebijakan dan kerangka kerja mengelola risiko yang timbul harus dilakukan peninjauan secara rutin pada jadwal yang ditentukan atau apabila terdapat perubahan agar dapat dipastikan kesesuaian, kecukupan dan efektivitas keberlanjutan instansi kemudian tinjau kerangka kerja pengelolaan risiko perlu dibuktikan dengan melakukan dokumentasi yang dapat berupa buku harian yang menunjukkan tinjauan atau tanggal peninjauan yang dilakukan, uraian perubahan (apabila terjadi perubahan) dengan persetujuan penganggung jawab atau pimpinan instansi sesuai yang telah ditetapkan	A.5.1.2

Tabel 5. 6 Rekomendasi Perbaikan Area Pengelolaan Risiko Keamanan Informasi Kategori Pengamanan 3 (lanjutan)

3.16	Pengelolaan risiko yanng dilakukan belum dijadikan bagian kriteria proses penilaian obyektif kinerja efektivitas pengamanan	Proses mengelola risiko harus menghasilkan wawasan yang baru sebagai upaya untuk meminimalisir dampak risiko di masa depan	A.16.1.6

Belum melakukan pengujian secara rutin terhadap kerangka kerja untuk mengelola risiko. Permasalahan ini sesuai dengan Kontrol Annex A A.5.1.2 tentang tinjau kebijakan keamanan informasi. Rekomendasi yang perlu dilakukan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri harus melakukan peninjauan terhadap kerangka kerja untuk mengelola risiko yang ada pada jadwal yang ditentukan oleh instansi atau apabila terdapat perubahan untuk agar dapat dipastikan kesesuaian, kecukupan dan efektivitas keberlanjutan instansi. Tinjau kerangka kerja pengelolaan risiko perlu dibuktikan dengan melakukan dokumentasi yang dapat berupa buku harian yang menunjukkan tinjauan atau tanggal peninjauan yang dilakukan, uraian perubahan (apabila terjadi perubahan) dengan persetujuan penganggung jawab atau pimpinan instansi sesuai yang telah ditetapkan.

Pengelolaan risiko saat ini belum dijadikan penilaian obyektif kinerja efektivitas pengamanan informasi. Permasalahan ini sesuai dengan kontrol Annex A A.16.1.6 tentang belajar dari insiden keamanan informasi. Rekomendasi untuk Dinas Komunikasi dan Informatika Kabupaten Kediri adalah pada proses pengelolaan risiko dan penilaian risiko yang dilakukan oleh Dinas Komunikasi dan Informatika Kabupaten Kediri harus dapat menghasilkan wawasan baru yang didapat daru menyelesasikan insiden kegagalan keamanan informasi dan analisanya yang kemudian dapat digunakan sebagai dasar untuk menyusun langkah-langkah strategis yang bertujuan untuk mengurangi dampak insiden keamanan informasi di masa depan.

Berdasarkan dari penjabaran diatas, secara keseluruhan Dinas Komunikasi dan Informatika Kabupaten Kediri perlu ditetapkannya program kerja pengelolaan risiko terdokumentasi. Menetapkan penanggung jawab manajemen risiko. Menetapkan kebijakan, prosedur dan pedoman pengelolaan risiko terdokumentasi meliputi meliputi hubungan dan definisi tingakatan klasifikasi aset informasi, identifikasi tingkat ancaman, kemungkinan terjadinya ancaman atau risiko serta identifikasi dampak kelemahan dari aset informasi yang ada. Harus ditetapkannya ambang batas risiko yang dapat diterima oleh instansi. Menetapkan kepemilikan dan pengelola aset informasi. Mengidentifikasi ancaman dan kelemahan aset informasi, dampak kerugian hilangnya atau

terganggunya aset utama. Menetapkan kebijakan klasifikasi infromasi, prosedur dan panduan untuk menangani aset informasi sesuai dengan klasifikasi risiko. Menyusun langkah mitigasi risiko dan melakukan evaluasi terhadapnya. Melakukan peninjauan terhadap kerangka kerja pengelolaan risiko yang ada pada jadwal yang ditetapkan, prosedur pengelolaan risiko, dan kepatuhan pengelolaan risiko.

5.3 Kerangka Kerja Pengelolaan Keamanan Informasi

Penerapan Kerangka Kerja Pengelolaan Keamanan Informasi memperoleh skor 19 dengan tingkat kematangan I dan persentase ketercapaian tingkat kematangan yang diperoleh adalah 11,9%. Berdasarkan penilaian yang telah dilakukan, didapatkan bahwa saat ini mendefinisikan dan menetapkan kebijakan dan prosedur terkait keamanan informasi. Selain itu, saat ini belum melakukan pengelolaan strategi dan program keamanan informasi. Sehingga terdapat aspek yang tidak dilakukan atau dalam perencanaan yang diajukan sebagai rekomendasi perbaikan. Rekomendasi perbaikan yang diajukan berdasarkan pemetaan pada pertanyaan Indeks KAMI yang belum dilakukan atau dalam perencanaan dengan kontrol Annex A dan *Information Security Management Documentation Checklist*. Terdapat 28 rekomendasi perbaikan pada area kerangka kerja pengelolaan keamanan informasi yang terbagi dalam 3 (tiga) tahap penerapannya. Rekomendasi diajukan secara bertahap dilakukan per tahun sesuai dengan kategori pengamanan pada Indeks KAMI. Berikut merupakan 12 (dua belas) rekomendasi perbaikan pada kategori pengamanan 1 terkait dengan penerapan kerangka kerja dasar pada tahun pertama yang diusulkan.

Tabel 5. 9 Rekomendasi Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi Kategori Pengamanan 1

No Pertanyaan	Area Kerangka Kerja Pengelolaan Keamanan Informasi (*as-is*)	Rekomendasi (*to-be*)	Kontrol ISO 27001
4.1	Belum memiliki prosedur serta kebijakan terkait keamanan informasi yang tertulis jelas	Mendefinisikan dan menetapkan kebijakan serta prosedur keamanan informasi terdokumentasi secara resmi dan dilindungi agar terhindar dari kerusakan, kesalahan penggunaan atau akses oleh pihak yang tidak berhak	A.5.1.1

Tabel 5. 10 Rekomendasi Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi Kategori Pengamanan 1 (lanjutan)

4.2	Belum ditetapkannya kebijakan keamanan informasi secara resmi serta mempublikasikan pada karyawan dan staf yang terlibat	Kebijakan keamanan informasi harus ditetapkan oleh pimpinan instansi secara resmi, disimpan dalam media penyimpanan yang tersedia, dan dipublikasikan kepada seluruh karyawan agar mudah diakses berbagai pihak yang membutuhkan	A.5.1.1
4.3	Belum tersedianya prosedur untuk pengelolaan prosedur dan keamanan informasi	Menetapkan prosedur pengelolaan prosedur dan kebijakan keamanan informasi secara resmi dan terdokumentasi untuk melakukan peninjauan pada jadwal yang ditetapkan atau apabila terjadi perubahan yang signifikan pada prosedur dan kebijakan keamanan informasi untuk dapat dipastikan kecukupan efektivitas, dan kesesuaian keberlanjutan mereka. Kemudian apabila terjadi ketidakpatuhan maka perlu mengidentifikasi penyebab ketidakpatuhan, melakukan evaluasi sebagai upaya untuk mencapai kepatuhan yang diharapkan, menerapkan tindak koreksi yang tepat serta melakukan peninjauan terhadap tindakan korektif untuk verifikasi keefektifan pada setiap kelemahan dan kekurangan yang ada	A.5.1.2

Tabel 5. 11 Rekomendasi Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi Kategori Pengamanan 1 (lanjutan)

4.4	Belum tersedianya proses untuk mengkomunikasikan kebijakan keamanan informasi dan perubahannya	Menetapkan kebijakan, proses dan prosedur mengkomunikasikan kebijakan keamanan informasi pada pihak terkait agar dipatuhi dan mudah dipahami yang dapat berupa mengkomunikasikan kebijakan keamanan informasi dan perubahannya menggunakan teknologi komunikasi, dicetak serta melakukan sosialiasi tentang kebijakan keamanan informasi kepada pihak terkait	A.5.1.1
4.5	Prosedur dan kebijakan keamanan belum direfleksikan dari kebutuhan untuk memitigasi risiko dari proses mengkaji hasil risiko	Mengidentifikasi mitigasi dari hasil kajian risiko yang didefinisikan pada prosedur dan kebijakan yang ditetapkan sehingga dapat dijadikan sebagai dasar penetapan kebijakan keamanan dan informasi berdasarkan hasil kajian risiko keamanan informasi yang ada	A.5.1.1
4.6	Belum tersedianya mekanisme melakukan identifikasi terhadap keadaan yang dapat berbahaya bagi keamanan informasi serta penetapannya sebagai insiden keamanan informasi untuk diselesaikan	Menetapkan proses, prosedur untuk pengidentifikasian terhadap keadaan yang membahayakan keamanan informasi terdokumentasi meliputi pencatatan, penilaian dan analisis apakah ditetapkan sebagai insiden keamanan informasi yang kemudian harus ditangani dan	A.16.1.4

		diselesaikan sebagai bentuk kepatuhan	
4.7	Belum terdapat dokumen kontrak dengan pihak ketiga meliputi peraturan penggunaan serta perlindangan pada aset, pelaporan insiden, HAKI dan menjaga kerahasiaan	Menetapkan dokumen perjanjian kontrak dengan pihak ketiga yang meliputi pelaporan insiden, melindungi kerahasiaan, Hak Keyaan Intelektual (HAKI), dan tata tertib dalam menggunakan dan mengamankan aset kemudian setiap pihak yang terlibat harus menerapkan serta menjamin kepatuhan pengamanan informasi	A.7.1.2
4.20	Belum memiliki strategi menerapkan keamanan informasi yang disesuaikan dengan hasil analisa risiko	Menetapkan strategi penerapan keamanan informasi yang didapatkan dari pengetahuan dari menganalisis dan menyelesaikan insiden keamanan informasi	A.16.1.6
4.21	Belum memiliki strategi pemakaian teknologi keamanan informasi berdasarkan profil risiko	Menetapkan strategi dan rencana penggunaan teknologi informasi yang terdokumentasi dengan mempertimbangkan dan disesuaikan dengan profil risiko	A.17.1.2
4.22	Strategi untuk menerapkan keamanan informasi belum terealisasi sebagai bagian dari penerapan program kerja	menetapkan sebuah program kerja terkait dengan penerapan strategi keamanan informasi dengan memperhatikan profil risiko yang ada	A.16.1.5

Tabel 5. 12 Rekomendasi Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi Kategori Pengamanan 1 (lanjutan)

4.23	belum memiliki dan melakukan program audit internal	Menetapkan kebijakan dan prosedur keamanan informasi terkait pelaksanaan audit internal yang dilaksanakan pihak independen yang mencakup seluruh aset informasi, kebijakan serta prosedur keamanan informasi yang tersedia	A.5.1.1
4.24	Belum dilakukan evaluasi terhadap tingkat konsistensi, efektivitas dan kepatuhan penerapan keamanan informasi pada pelaksaaan audit internal	Menetapkan kebijakan dan prosedur terdokumentasi terkait pelaksanaan audit internal terkait tingkat konsistensi, efektivitas dan kepatuhan penerapan keamanan informasi	A.5.1.1

Aspek yang belum diterapkan yaitu saat ini belum memiliki prosedur serta kebijakan terkait keamanan informasi yang tertulis jelas. Kemudian belum menetapkan kebijakan keamanan informasi secara resmi serta mempublikasikan kepada pada karyawan dan staf yang terlibat sehingga dengan mudah diakses pihak yang membutuhkan. Kondisi ini sesuai dengan kontrol Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi. Rekomendasi yang diusulkan adalah perlu mendefinisikan dan menetapkan serangkaian kebijakan, pedoman, dan prosedur untuk keamanan informasi secara resmi dan terdokumentasi, disimpan dalam media penyimpanan yang tersedia yang ditetapkan, disetujui oleh pimpinan instansi kemudian dilindungi agar terhindar dari kerusakan, kesalahan penggunaan atau akses oleh pihak yang tidak berhak. Kemudian pimpinan harus menerbitkan dan mengokumunikasikan pada karyawan atau pihak lain yang relevan melalui saluran media komunikasi yang tersedia agar dipatuhi dan dipahami. Kebijakan merupakan rangkaian ketetapan, prinsip, dan pedoman yang menjadi dasar landasan kerja pada suatu organisasi dan memvisualkan komitmen, tekad dan rencana manajemen yang dirancang secara formal terhadap suatu masalah tertentu. Prosedur merupakan serangkaian kegiatan/aktivitas/aksi dari serangkaian proses yang harus dijalankan dan melibatkan satu/beberapa unit kerja pada organisasi.

Saat ini belum tersedia prosedur untuk pengelolaan prosedur dan kebijakan keamanan informasi mencakup distribusi, penarikan dan peredaran, serta pemakaian daftar induk. Kondisi ini sesuai dengan kontrol Annex A A.5.1.2 tentang tinjau kebijakan untuk keamanan informasi. Rekomendasi yang diberikan adalah harus menetapkan prosedur untuk pengelolaan kebijakan dan prosedur keamanan informasi secara resmi dan terdokumentasi untuk melakukan peninjauan pada jadwal yang ditetapkan atau apabila terjadi perubahan yang signifikan pada kebijakan dan prosedur keamanan informasi untuk dipastikan kesesuaiannya, kecukupan dan efektivitas keberlanjutan mereka. Kemudian apabila terjadi ketidakpatuhan maka perlu mengidentifikasi penyebab ketidakpatuhan, melakukan evaluasi sebagai upaya untuk mencapai kepatuhan yang diharapkan, menerapkan tindak koreksi yang tepat serta melakukan peninjauan terhadap tindakan korektif untuk verifikasi efektivitas pada setiap kelemahan dan kekurangan yang terdeteksi.

Saat ini belum memiliki proses mengkomunikasikan kebijakan keamanan informasi dan serta perubahannya pada pihak terkait. Kondisi ini sesuai dengan kontrol A Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi. Rekomendasi yang diusulkan adalah diperlukannya penetapan kebijakan, proses, dan prosedur untuk untuk menyebarkan dan mengokumunikasaikan seluruh kebijakan keamanan informasi yang ada kepada pihak terkait agar dipatuhi dan mudah dipahami. Sebagai contoh, mengkomunikasikan kebijakan keamanan informasi dan perubahannya menggunakan teknologi komunikasi, dicetak serta melakukan sosialiasi tentang kebijakan keamanan informasi kepada pihak terkait.

Seluruh Prosedur dan kebijakan keamanan belum direfleksikan dari kebutuhan untuk memitigasi risiko dari proses mengkaji hasil risiko maupun sasaram atau obyektif tertentu yang ditetapkan pimpinan. Kondisi ini sesuai dengan kontrol Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi. Rekomendasi yang berikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri dalam penyusunan kebijakan dan prosedur keamanan informasi perlu melakukan analisis risiko terlebih dahulu dengan mengidentifikasi sumber daya apa saja yang dimiliki oleh instansi, menetapkan sumber daya mana yang harus dilindungi serta menetapkan sumber daya mana yang memiliki pengamanan lebih ketat dari pada yang lainnya kemudian mendefinisikan mitigasi dari hasil analisis risiko dan hasil kajian perlu didefinisikan atau dimasukkan pada kebijakan dan prosedur keamanan informasi yang ditetapkan sehingga dapat dijadikan sebagai dasar penetapan kebijakan keamanan dan informasi berdasarkan hasil kajian risiko keamanan informasi yang ada.

Keadaan saat ini belum memiliki mekanisme melakukan identifikasi terhadap keadaan yang berbahaya terhadap keamanan informasi serta penetapannya sebagai insiden keamanan informasi untuk diselesaikan. Kondisi tersebut berdasarkan kontrol Annex A A.16.1.4 tentang penilaian dan keputusan tentang kejadian keamanan informasi. Rekomendasi untuk Dinas Komunikasi dan

Informatika Kabupaten Kediri adalah perlu ditetapkannya proses, prosedur atau mekanisme untuk mengidentifikasi situasi yang membahayakan dan merugikan keamanan informasi yang meliputi dilakukan pencatatan, penilaian dan analisis apakah ditetapkan sebagai insiden keamanan informasi yang kemudian harus ditangani dan diselesaikan sebagai bentuk kepatuhan.

Belum memiliki dokumen kontrak dengan pihak ketiga meliputi peraturan penggunaan serta perlindangan pada aset, pelaporan insiden, HAKI dan menjaga kerahasiaan adalah salah satu aspek pada Indeks KAMI yang belum diterapkan. Kondisi ini sesuai dengan kontrol Annex A A.7.1.2 tentang syarat dan ketentuan pekerjaan. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan dokumen perjanjian kontrak bersama karyawan atau pihak ketiga yang meliputi pelaporan insiden, melindungi kerahasiaan, Hak Keyaan Intelektual (HAKI), dan tata tertib dalam menggunakan dan mengamankan aset kemudian setiap pihak yang terlibat harus menerapkan serta menjamin kepatuhan pengamanan informasi.

Pada saat ini belum memiliki strategi menerapkan keamanan informasi yang disesuaikan dengan hasil analisa risiko. Kondisi tersebut sesuai dengan kontrol Annex A A.16.1.6 tentang belajar dari insiden keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan strategi penerapan keamanan informasi yang diperoleh dari pengetahuan dari hasil analisis risiko dan harus menindaklnajuti dan menyelesaikan insiden keamanan informasi yang bertujuan untuk mengurangi dampak insiden yang terjadi di masa depan.

Pada saat ini belum memiliki strategi pemakaian teknologi keamanan informasi yang sesuai kebutuhan profil risiko. Kondisi tersebut sesuai dengan kontrol Annex A A.17.1.2 tentang menerapkan kontinuitas keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kediri perlu menetapkan strategi dan rencana penggunaan teknologi informasi yang terdokumentasi dengan mempertimbangkan dan menyesuaikan profil risiko yang ada untuk agar dapat dipastikan tingkat keberlanjutan yang dibutuhkan untuk keamanan informasi pada situasi merugikan.

Strategi untuk menerapkan keamanan informasi belum terealisasi sebagai bagian dari pelaksanaan program kerja. Kondisi tersebut sesuai dengan kontrol Annex A A.16.1.5 tentang kebijakan untuk keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan sebuah program kerja terkait dengan penerapan strategi keamanan informasi pada instansi yang mana program kerja tersebut harus memperhatikan dan disesuaikan dengan perubahan profil risiko yang telah ditetapkan.

Kondisi saat ini belum dimilikinya dan belum melakukan program audit internal yang dilaksanakan pihak independen. Kemudian program audit internal belum mencakup atau mengevaluasi tingat kepatuhan, konsistensi, dan efektivitas penerapan keamanan informasi. Kondisi tersebut berdasarkan kontrol

Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi. Sehingga diajukan rekomendasi yakni perlu menetapkan kebijakan serta prosedur terkait keamanan informasi terkait dengan penerapan audit internal yang dilaksanakan pihak independen yang mencakup seluruh aset informasi, kebijakan serta prosedur keamanan informasi. Kebijakan dan prosedur tersebut mencakup syarat-syarat serta aktivitas audit yang melibatkan verifkasi sistem operasional untuk meminimalkan dampak terhadap proses bisnis. Program audit internal yang dilakukan harus mencakup evaluasi terhadap konsistensi, efektivitas, dan tingkat kepatuhan penerapan keamanan informasi. Kemudian hasil program audit harus ditinjau, dievaluasi dan dikaji untuk menetapkan langkah perbaikan serta untuk mencegah terhadap kemungkinan munculnya dampak di masa depan serta inisiatif untuk peningkatan performa keamanan informasi. Kemudian harus melaporkan hasil audit kepada pimpinan instansi untuk dijadikan dasar terhadap strategi penerapan keamanan informasi kedepannya dan dijadikan acuan untuk dalam penetapan langkah perbaikan atau peningkatan performa keamanan informasi.

Berikutnya merupakan rekomendasi yang diusulkan untuk tahun ke 2 (dua) dalam penerapan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Kategori pengamanan 2 yakni terkait dengan efektivitas serta konsistensi penerapan keamanan informasi atau penerapan operasional. Rekomendasi berikut diusulkan dilaksanakan sebagai lanjutan dari penerapan rekomendasi pada kategori pengamanan 1 sebelumnya. Berikut terdapat 10 (sepuluh) rekomendasi perbaikan yang diusulkan pada kategori pengamanan 2.

Tabel 5. 13 Rekomendasi Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi Kategori Pengamanan 2

No Pertanyaan	Area Kerangka Kerja Pengelolaan Keamanan Informasi (*as-is*)	Rekomendasi (*to-be*)	Kontrol ISO 27001
4.8	Belum terdapat konsekuensi dari pelanggaran kebijakan keamanan informasi	Menetapkan proses disipliner formal terkait konsekuensi terhadap pelaksana keamanan informasi yang melakukan pelanggaran yang terdokumentasi yaitu sanksi administratif atau tindakan disiplin lain yang ditetapkan secara resmi dan dikomunikasikan kepada seluruh pihak yang	A.7.2.3

		terlibat agar dipahami	
4.9	Belum tersedia nya prosedur yang secara resmi dalam pengelolaan suatu pengecualian	Menetapkan kebijakan keamanan informasi yang mencakup pengelolaan suatu pengecualian dan proses untuk menindaklankjuti konsekuensi kondisi tersebut serta kebijakan harus ditetapkan dan disetujui secara resmi oleh pimpinan serta diterbitkan dan dikomunikasian pada karyawan dan pihak eksternal yang terkait agar dipahami dan dipatuhi	A.5.1.1
4.10	Belum diterapkannya prosedur operasional dan dan kebijakan untuk pengelolaan dan implementasi *security patch*, mengalokasikan tangung jawab dan tugas, monitor *security patch* baru	Mendefinisikan dan menetapkan kebijakan keamanan informasi terkait peran dan tanggung jawab pengelola implementasi *security patch* meliputi monitoring apabila ada perilisan *security patch* baru dan pemasangan dan pelaporannya	A.5.1.1
4.11	Dalam manajemen proyek belum dibahas mengenai aspek keamanan informasi terkait ruang lingkup	Menetapkan kebijakan dan prosedur keamanan informasi meliputi aspek keamanan informasi pada manajemen proyek	A.6.1.5
4.12	Belum diterapkannya mekanisme untuk melakukan evaluasi risiko terhadap rencana implementasi dan pembelian sistem baru serta untuk menanggulangi permasalahan yang muncul	Menetapkan persyaratan berkaitan keamanan informasi dalam persyaratan untuk implenetasi sistem baru yang meliputi persyaratan kepatuhan berdasarkan kebijakan terkait dan mengidentifikasi kemungkinan ancaman yang dapat terjadi yang	A.14.1.1

		terdokumentasi dan ditinjau secara resmi oleh pihak terkait yang berkepentingan	
4.13	Belum diterapkannya mekanisme mengembangkan sistem yang aman (*Secure SDLC*)	Menetapkan strategi, kebijakan, prosedur,aturan dan pedoman untuk mengembangkan perangkat lunak yang aman dalam instansi. Yang misalnya ialah menetapkan teknik pengembangan sistem terstruktur sesuai dengan analisis risiko terdokumentasi, desain dan penentuan keamanan yang tepat, platform yang aman, layanan atau fungsi atau proses keamanan, pengembangan atau pengkodean yang aman, pengujian keamanan dan kinerja, implementasi atau konfigurasi, verifikasi pasca pemasangan perangkat lunak, pengujian keamanan dan kinerja dan pemeliharaan sistem	A.14.2.1
4.14	Belum terdapat proses untuk menganggulangi risiko pada penerapan sistem baru	Menetapkan proses, pedoman perubahan dan prosedur kontrol formal terkait sistem untuk meninjau dan menanggulangi risiko yang timbul atau ketika terjadi ketidakpatuhan pada kebijakan yang ditetapkan pada penerapan suatu sistem. Hal tersebut mencakup kebijakan, pedoman perubahan, prosedur, rencana perubahan dan otorisasi,	A.14.2.3

		catatan perubahan pada log, penilaian risiko, koordinasi dan prioritas	
4.15	Belum tersedianya kerangka kerja untuk mengelola layanan teknologi informasi dan komunikasi atau *business continuity planning*) yang memuat definisi syarat atau konsiderans keamanan informasi	Menetapkan kebijakan dan pedoman keamanan informasi terkait mengelola perencanaan kelangsungan layanan teknologi informasi dan komunikasi (*business continuity planning*) dan mencakup pendefinisian persyaratan atau konsiderans keamanan informasi dan jadwal uji coba berdasarkan jangka waktu yang telah direncanakan	A.5.1.1
4.25	Belum menetapkan untuk mengevaluasi hasil audit internal untuk mengidentifikasi langkah perbaikan atau inisiatif untuk meningkatkan performa keamanan informasi	Menetapkan kebijakan dan prosedur terkait peraturan hasil audit internal yang harus dikaji atau evaluasi untuk mengidentifikasi langkah perbaikan di masa depan	A.5.1.1
4.26	Belum menetapkan kebijakan untuk melaporkan hasil audit internal kepada pimpinan instansi	Mendefinisikan dan menetapkan kebijakan terkait hasil audit internal yang mencakup pelaporan hasil audit internal pada pimpinan instansi untuk dijadikan dasar terhadap penyusunan strategi penerapan keamanan informasi kedepannya	A.5.1.1

Konsekuensi dari pelanggaran kebijakan keamanan informasi saat ini belum didefinisikan. Kondisi ini sesuai dengan kontrol Annex A A.7.2.3 tentang proses pendisiplinan. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan proses disipliner formal terkait konsekuensi terhadap pelaksana pengamanan informasi yang melakukan pelanggaran keamanan informasi yaitu sanksi administratif atau tindakan disiplin lain yang ditetapkan secara resmi dan dikomunikasikan kepada seluruh pihak yang terlibat agar dipahami dan ditaati.

Prosedur resmi untuk pengelolaan suatu pengecualian dalam menerapkan keamanan informasi merupakan salah satu aspek Indeks KAMI yang belum diterapkan. Kondisi tersebut sesuai dengan kontrol Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi. Rekomendasi perbaikan yang diajukan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu mendefinisikan dan menetapkan kebijakan keamanan informasi yang mencakup pengelolaan suatu pengecualian dalam menerapkan keamanan informasi dan mencakup proses untuk menindaklankjuti konsekuensi kondisi tersebut. selanjutnya guna agar kebijakan dipahami dan dipatahui oleh karyawan dan pihak eksternal maka pimpinan harus menetaojab dan menyetujui secara resmi kemudian diterbitkan.

Prosedur operasional dan kebijakan untuk untuk pengelolaan dan pengimplementasian *security patch*, pengalokasian penanggung jawabnya, monitoring *security patch* baru masih belum diterapkan. Kondisi tersebut sesuai dengan kontrol Annex A.5.1.1 tentang kebijakan untuk keamanan informasi. Rekomendasi yang diajukan adalah perlu mendefinisikan dan menetapkan kebijakan keamanan informasi terkait peran dan tanggung jawab pengelola implementasi *security patch* meliputi monitoring apabila ada perilisan *security patch* baru, pemasangannya serta pelaporannya kepada pimpinan yang bertanggung jawab atau pimpinan instansi. Kebijakan dan prosedur tersebut harus ditetapkan,disetujui dan diterbitkan secara resmi oleh pimpinan instansi serta dikomunikasikan pada karyawan dan pihak eksternal yang terkait.

Dalam manajemen proyek belum dibahas mengenai aspek keamanan informasi terkait ruang lingkup. Kondisi ini sesuai dengan kontrol Annex A A.6.1.5 tentang keamanan informasi dalam manajemen proyek. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri menetapkan kebijakan, prosedur, pedoman terkait dengan keamanan informasi pada manajemen proyek yang mencakup pendefinisian ruang lingkup terlepas dari jenis proyek tersebut.

Kondisi saat ini yakni Belum diterapkannya mekanisme untuk melakukan evaluasi risiko terhadap rencana implementasi dan pembelian sistem baru serta untuk menanggulangi permasalahan yang muncul. Kondisi tersebut sesuai dengan kontrol Annex A A.14.1.1 tentang analisis dan spesifikasi kebutuhan keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan persyaratan terkait keamanan

informasi untuk sistem baru yang meliputi persyaratan kepatuhan berdasarkan kebijakan terkait dan mengidentifikasi kemungkinan ancaman yang dapat terjadi yang terdokumentasi dan ditinjau secara resmi oleh pihak terkait yang berkepentingan.

Keadaan saat ini Belum diterapkannya mekanisme untuk mengembangkan sistem yang aman atau *Secure SDLC* sesuai metode, prinsip dan sesuai standar platform teknologi yang digunakan. Kondisi tersebut sesuai dengan kontrol Annex A A.14.2.1 tentang kebijakan pembangunan yang aman. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan, strategi, prosedur, aturan serta pedoman untuk pengembangan perangkat lunak yang aman dalam instansi. Yang misalnya adalah menetapkan teknik pengembangan sistem yang sistematis berdasarkan analisa risiko yang tertulis, desain atau pemilihan keamanan yang sesuai, *platform* yang aman, layanan atau fungsi atau proses keamanan, pengembangan atau pengkodean yang aman, pengujian keamanan dan kinerja, implementasi atau konfigurasi, verifikasi pasca pemasangan perangkat lunak, pengujian keamanan dan kinerja dan pemeliharaan sistem.

Proses untuk menanggulangi risiko pada penerapan sistem baru atau aapabila terjadi ketidakpatuhan pada kebijakan yang ada saat ini masih belum dimiliki dan ditetapkan. Kondisi tersebut sesuai dengan kontrol Annex A A.14.2.3 tentang tinjau teknis aplikasi setelah perubahan platform operasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan proses, pedoman perubahan dan prosedur kontrol formal terkait sistem untuk meninjau dan menanggulangi risiko yang timbul atau ketika terjadi ketidakpatuhan pada kebijakan yang ditetapkan pada penerapan suatu sistem. Hal tersebut mencakup kebijakan, pedoman perubahan, prosedur, otorisasi dan rencana perubahan, catatan perubahan dalam log, menilai risiko, dan prioritas.

Kerangka kerja terkait untuk mengelola kelangsungan layanan TIK (*business continuity planning*) saat ini masih belum dimiliki dan ditetapkan. Kondisi tersebut sesuai dengan kontrol Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi. Sehingga diajukan rekomendasi untuk Dinas Komunikasi dan Informatika Kabupaten Kediri yaitu perlu menetapkan kebijakan dan pedoman keamanan informasi untuk mengelola kelangsungan layanan TIK (*business continuity planning*) dan mencakup pendefinisian persyaratan keamanan informasi dan jadwal uji coba berdasarkan jangka waktu yang telah direncanakan. Kebijakan dan pedoman keamanan informasi tersebut harus ditetapkan dan disetujui oleh pimpinan instansi serta diterbitkan secara resmi dan dikomunikasikan pada pihak eksternal dan karyawan agar dapat dipahami dan dengan mudah dipatuhi.

Berikutnya merupakan rekomendasi yang diusulkan untuk tahun ke 3 (tiga) dalam penerapan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Kategori pengamanan 3 yakni terkait dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi. Pada

kategori pengamanan 3 memiliki persyaratan bahwa seluruh bentuk pengamanan pada kategori 1 dan 2 telah diterapkan. Sehingga rekomendasi berikut diusulkan dilaksanakan sebagai lanjutan dari penerapan rekomendasi pada kategori pengamanan 1 dan 2 sebelumnya. Berikut terdapat 6 (enam) rekomendasi perbaikan yang diusulkan pada kategori pengamanan 3.

Tabel 5. 14 Rekomendasi Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi Kategori Pengamanan 3

No Pertanyaan	Area Kerangka Kerja Pengelolaan Keamanan Informasi (*as-is*)	Rekomendasi (*to-be*)	Kontrol ISO 27001
4.16	Belum didefinisikan tanggung jawab, komposisi, peran dan wewenang tim dalam merencankan pemulihan bencana terhadap layanan teknologi informasi dan komunikasi (*disaster recovery plan*)	Mendefinisikan dan menetapkan tanggung jawab, komposisi, peran dan wewenang tim dalam merencankan pemulihan bencana terhadap layanan teknologi informasi dan komunikasi terdokumentasi dalam uraian tugas, pemberitahuan lowongan, kebijakan keamanan informasi, buku pegangan karyawan, kontrak kerja, kontrak layanan dan memastikan bahwa tim yang menangani memiliki kemampuan, pengetahuan, keahlian, kompetensi yang memadai dalam mempersiapkan, dan memitigasi risiko yang kemungkinan dapat terjadi dan mengelola insiden dan menjaga keamanan informasi	A.17.1.2

Tabel 5. 15 Rekomendasi Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi Kategori Pengamanan 3 (lanjutan)

4.17	Belum dilakukan uji coba merencanakan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*)	Menetapkan kebijakan dan prosedur terkait uji coba perencanaan terhadap pemulihan bencana terhadap layanan teknologi informasi secara berkala yang dilakukan berdasarkan jadwal dan mekanisme yang telah ditentukan	A.17.1.2
4.18	Belum melakukan evaluasi pada perencanaan pemulihan bencana terhadap layanan teknologi informasi dan komunikasi (*disaster recovery plan*) untuk penerapan langkah perbaikan	Melakukan verifikasi, tinjau dan evaluasi terhadap perencanaan pemulihan bencana terhadap layanan TIK secara berkala untuk memastikan bahwa kontrol yang ditetapkan telah valid dan efektif pada situasi yang merugikan serta melakukan peninjauan terhadap validitas dan efektivitas terkait mekanisme penilaian keberlanjutan pada keamanan informasi, kontrol dan prosedur manajemen pemulihan bencana serta proses keamanan informasi	A.17.1.3
4.19	Belum melakukan evaluasi terhadap kelayakan prosedur dan kebijakan keamanan informasi secara berkala	Menetapkan kebijakan untuk mengevaluasi prosedur dan kebijakan informasi secara rutin pada interval yang ditetapkan apabila terjadi perubahan yang signifikan pada kebijakan dan prosedur yang berlaku	A.5.1.2

Tabel 5. 16 Rekomendasi Perbaikan Area Kerangka Kerja Pengelolaan Keamanan Informasi Kategori Pengamanan 3 (lanjutan)

4.27	Belum melakukan analisis untuk menilai aspek finansial yakni mencakup kebutuhan anggaran dan dampak biaya untuk keperluan revisi kebijakan dan prosedur keamanan informasi	Melakukan tinjau pada kebijakan serta prosedur keamanan informasi yang berlaku yang meliputi melakukan analisa untuk menilai aspek finansial	A.5.1.2
4.28	Belum dilakukan pengujian dan melakukan evaluasi terhadap tingkat kepatuhan program keamanan informasi secara periodik	Menetapkan proses disipliner formal terkait pengujian dan evaluasi terjadwal terkait status atau tingkat kepatuhan program keamanan informasi yang meliputi kondisi ketidakpatuhan atau pengecualian untuk membuktikan bahwa semua inisiatif perbaikan dan langkah pembenahan di diterapkan secara efisien dan efektif	A.7.2.3

Tanggung jawab, wewenang, komposisi dan peran tim dalam merencanakan pemulihan bencana pada layanan TIK (*disaster recovery plan*) saat ini masih belum didefinisikan. Kondisi tersebut sesuai dengan kontrol Annex A A.17.1.2 tentang menerapkan kontinuitas keamanan informasi. Rekomendasi yang diberikan adalah perlu mendefinisikan Tanggung jawab, wewenang, komposisi dan peran pengelola dalam merencanakan penanggulangan bencana terhadap layanan TIK (*business continuity planning*) yang terdokumentasi yang mana tim yang bertanggung jawab memiliki tugas untuk mengumpulkan informasi pada instansi yang berkaitan dengan komputerisasi, penentuan prioritas terhadap apa saja yang memiliki risiko yang tinggi pada instansi dan sangat sensitif, melakukan evaluasi terhadap alternatif yang ada, melakukan uji coba, mendokumentasikan serta bertugas dalam *maintance* dan *review*. Peran dan tanggung jawab dijabarkan pada uraian tugas, pemberitahuan lowongan, kebijakan keamanan informasi, buku pegangan karyawan, kontrak kerja, kontrak layanan dan lain-lain dan memastikan bahwa tim yang menangani memiliki kemampuan, pengetahuan, keahlian, kompetensi yang memadai dalam mempersiapkan, dan memitigasi risiko yang kemungkinan dapat terjadi dan

melakukan pengelolaan insiden dan melindungi keamanan informasi. Kemudian dilakukan pengembangan rencana pemulihan, respon serta mekanisme pemulihan secara detail sebagai upaya untuk menangani dan mengelola peristiwa keamanan informasi dan menjaga keamanan informasi sesuai dengan tujuan keamanan informasi yang ditetapkan.

Keadaan saat ini yakni belum dilakukan uji coba untuk merencanakan pemulihan terhadap terhadap bencana pada layanan TIK (*disaster recovery plan*). Kondisi tersebut berdasarkan kontrol Annex A A.17.1.2 tentang menerapkan kontinuitas keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan dan prosedur terkait uji coba merencanakan pemulihan terhadap bencana pada layanan TIK *(disaster recovery plan)* secara berkala yang dilaksanakan sesuai dengan jadwal dan mekanisme yang telah ditentukan pada kebijakan yang telah ada yang dan didokumentasikan dan dibuktikan menggunakan laporan pengujian perencaan pemulihan layanan TIK dan menunjukkan efektivitasnya. Uji coba disini dapat dilakukan dengan melakukan tes secara mendadak untuk mengetahui tingkah laku serta kesiapan personil, kemudian dapat dilakukan dengan tes yang direncanakan, kemudian uji coba dilakukan dengan global tes yakni seluruh kantor dilakukan uji cob serta dapat juga dilakukan dengan partial tes yakni uji coba yang dilakukan tidak menyeluruh dan tidak melibatkan banyak unit.

Evaluasi terhadap perencanaan pemulihan bencana terhadap layanan TIK (*business continuity planning*) untuk menerapkan langkah perbaikan dan pembenahan yang diperlukan masih belum dilaksanakan. Kondisi tersebut sesuai dengan kontrol Annex A A.17.1.3 tentang verifikasi, tinjau, dan evaluasi keberlanjutan keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu memverifikasi, meninjau dan melakukan evaluasi terhadap kontrol keberlanjutan keamanan informasi yang telah ditetapkan untuk memastikan bahwa kontrol yang ditetapkan telah valid dan efektif pada situasi yang merugikan. Kemudian dilakukan proses peninjauan terhadap validitas dan efektivitas terkait mekanisme penilaian keberlanjutan keamanan informasi, kontrol dan mekanisme manajemen pemulihan bencana serta proses keamanan informasi.

Evaluasi secara rutin pada seluruh prosedur dan kebijakan keamanan informasi saat ini masih belum diterapkan. Kondisi tersebut sesuai dengan kontrol Annex A A.5.1.2 tentang kebijakan untuk keamanan informasi. Rekomendasi yang diberikan adalah ketika terjadi perubahan yang signidikan pada kebijakan dan prosedur yang ada, dalam rangka untuk memastikan memastikan kesesuaian, kecukupan dan efetivitas penerapan kebijakan pada seluruh unit kerja terkait maka perlu dilakukan evaluasi dan pemantauan secara rutin pada kebijakan dan prosedur keamanan informasi. Kemudian hasil tinjauan didokumentasikan pada catatan perubahan yang menunjukkan tinjauan dan/tanggal tinjauan dan persetujuan atas perubahan kebijakan tersebut.

Keadaan saat ini adalah Belum melakukan analisis untuk menilai aspek finansial yakni mencakup kebutuhan anggaran dan dampak biaya untuk keperluan revisi kebijakan dan prosedur keamanan informasi atau perubahan pada dan untuk mengelola perubahannya. Kondisi tersebut sesuai dengan kontrol Annex A A.5.1.2 tentang tinjau kebijakan untuk keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri dalam melakukan peninjauan kebijakan dan prosedur keamanan informasi perlu dilakukan analisis untuk melakukan penilaian pada aspek finansial yang mencakup dampak biaya dan keperluan anggaran tertulis yang diperlukan paa infrastruktur dan pengelolaan perubahan yang terjadi.

Dinas Komunikasi dan Informatika Kabupaten Kediri saat ini belum dilakukan pengujian dan proses untuk mengevaluasi status dan tingkat kepatuhan terhadap program keamanan informasi yang ada secara periodik mencakup kondisi ketidakpatuhan atau pengecualian. Kondisi tersebut sesuai dengan kontrol Annex A A.7.2.3 tentang proses pendisplinan. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu dilakukan proses disipliner formal untuk melakukan pengujian dan evaluasi secara periodik berdasarkan jadwal yang telah ditetapkan yang mencakup status atau tingkat kepatuhan program keamanan informasi dan mencakup kondisi ketidakpatuhan atau pengecualian untuk dapat dipastikan bahwa seluruh inisiatif dan langkah pembenahanannya diterapkan secara efektif. Keseluruhan proses tersebut harus didokumentasikan sebagai bukti bahwa proses pengujian dan evaluasi telah dilaksanakan.

Berdasarkan dari penjabaran diatas, secara garis besar Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan dan prosedur keamanan informasi. Menetapkan proses mengkomunikasikan dan mempublikasikan kebijakan keamanan informasi. Menetapkan prosedur untuk pengelolaan kebijakan dan prosedur keamanan informasi . Mengidentifikasi kondisi yang membahayakan keamanan informasi. Menetapkan dokumen kontrak dengan pihak ketiga yang mencakup peraturan penggunaan serta perlindangan pada aset, pelaporan isiden, HAKI dan menjaga kerahasiaan. Menetapkan konsekuensi terhadap pelanggaran kebijakan keamanan informasi. Menetapkan kebijakan dan prosedur terkait terkait peran dan tanggung jawab untuk mengelola implementasi *security patch* mencakup monitoring apabila ada perilisan *security patch* baru, pemasangannya dan eskalasi pelaporannya. Menetapkan kebijakan, prosedur, pedoman terkait dengan keamanan informasi pada manajemen proyek. Menetapkan persyaratan terkait keamanan informasi untuk penerapan sistem baru. Menetapkan prosedur, pedoman dan kebijakan untuk mengembangkan perangkat lunak yang aman dan proses untuk menanggulangi risiko terhadap sistem baru. Menetapkan kebijakan dan pedoman keamanan informasi untuk mengelola perencanaan kelangsungan layanan TIK (*business continuity planning*) dan menetapkan peran dan tanggung jawab pengelolanya, uji coba pemulihan bencanan layanan TIK. Melakukan verifikasi, meninjau dan melakukan evaluasi terhadap kontrol keberlanjutan

keamanan informasi. Menetapkan proses untuk mengevaluasi kebijakan dan prosedur keamanan informasi. Menetapkan program kerja penerapan strategi keamanan informasi. Menetapkan kebijakan audit internal. Menetapkan proses disipliner formal pengujian dan evaluasi tingkat/status kepatuhan program keamanan informasi.

5.4 Pengelolaan Aset Informasi

Pengelolaan Aset Informasi memperoleh skor 49 dengan tingkat kematangan I+ dan persentase pencapaian tingkat kematangan adalah 29,1%. Berdasarkan penilaian yang telah dilakukan, diperoleh informasi bahwa saat ini pengelolaan aset informasi belum dilakukan dengan baik dan tidak terdokumentasi terkait dengan ketersediaan inventaris aset informasi dan kepemilikan aset, proses mengklasifikasi infromasi dan evaluasinya. Pada bagian pengamanan fisik, sebagian telah diterapkan seluruhnya yang mencakup pengamanan lokasi kerja dan ruang server. Sehingga terdapat aspek dalam indeks KAMI yang tidak terpenuhi karena belum dilakukan atau sedang dalam perencanaan. Aspek pada Indeks KAMI yang belum dilakukan atau dalam perencanaan tersebut diajukan sebagai rekomendasi perbaikan pada Dinas Komunikasi dan Informatika Kabupaten Kediri dengan melakukan pemetaan terhadap kontrol Annex A pada ISO 27001 dan *Information Security Management Documentation Checklist*. Berikut pada tabel 5.4 merupakan 32 rekomendasi perbaikan pada area pengelolaan aset informasi yang terbagi dalam 3 (tiga) tahap penerapannya. Rekomendasi diajukan secara bertahap dilakukan per tahun sesuai dengan kategori pengamanan pada Indeks KAMI. Berikut merupakan 20 (dua puluh) rekomendasi perbaikan pada kategori pengamanan 1 terkait dengan penerapan kerangka kerja dasar pada tahun pertama yang diusulkan.

Tabel 5. 17 Rekomendasi Perbaikan Area Pengelolaan Aset Informasi Kategori Pengamanan 1

No Pertanyaan	Area Pengelolaan Aset Informasi (*as-is*)	Rekomendasi (*to-be*)	Kontrol ISO 27001
5.1	Belum tersedia dokumen yang memuat daftar inventaris aset informasi dan aset yang bekaitan dengan proses teknologi informasi	Mengidentifikasi, mencatat, mengelola seluruh aset informasi dan menetapkan kepemilikan aset informasi meliputi nama atau peran pemilik aset yang bertanggung jawab pada aset tersebut yang berkaitan dengan proses teknologi informasi	A.8.1.1 A.8.1.2

		aset	
5.2	Belum tersedianya klasifikasi aset informasi yang disesuaikan peraturan perundangan yang berlaku	Menetapkan kebijakan, prosedur dan skema klasifikasi informasi dengan tingkatan tertentu yang harus diterapkan pada organisasi secara konsisten serta mekanisme penanganannya sesuai dengan klasifikasinya. Misalnya, skema klasifikasi aset informasi berdasarkan kekrititas data yakni rahasia, internal, dan publik.	A.8.2.1
5.3	Belum tersedianya mekanisme untuk melakukan evaluasi dan mengklasifikasikan aset informasi kepentingannya	Menetapkan kebijakan dan mekanisme untuk melakukan evaluasi dan mekanisme klasifikasi aset informasi berdasar tingkat kepentingannya	A.8.2.1
5.4	Belum tersedianya definisi yang memuat tingkatan akses yang definisi tingkatan dari setiap klasifikasi aset yang ada	Menetapkan kebijakan kontrol tingkatan akses pada setiap klasifikasi aset informasi. Contohnya adalah panduan tentang kata sandi, firewall, dan VPN *(Virtual Private Network)*.	A.9.1.1
5.5	Belum tersedianya mekanisme untuk mengelola perubahan pada proses bisnis, sistem dan proses teknologi informasi yang mencakup perubahan konfigurasi	Menetapkan proses operasi tertulis terkait perubahan pada proses bisnis, sistem dan proses teknologi informasi mencakup perubahan konfigurasi, *back-up*, penjadwalan pekerjaan, logging dan pemantauan, perbaikan, identifikasi kesalahan, kapasitas dan manajemen kinerja, manajemen perubahan	A.12.1.1

Tabel 5. 18 Rekomendasi Perbaikan Area Pengelolaan Aset Informasi Kategori Pengamanan 1 (lanjutan)

5.6	Belum tersedianya mekanisme untuk mengelola konfigurasi secara rutin	Menetapkan proses terkait pengelolaan konfigurasi yang dilaksanakan secara berkala yang mencakup proses untuk pengujian perangkat lunak, persetujuan perubahan, daftar aplikasi yang disetujui atau disahkan, cadangan aplikasi sebelum dan setelah pemasangan, hak tebatas dalam memperbarui perangkat lunak	A.12.5.1
5.7	Belum tersedianya mekanisme perilisan aset baru dan pemuktahiran inventaris aset	Menetapkan kebijakan klasifikasi informasi, proses serta panduan untuk menangani aset terkait proses merilis aset baru yang disesuaikan berdasar skema klasifikasi informasi yang diterapkan dan pemuktahirannya	A.8.2.3
5.8	Belum mendefinisikan tanggung jawab pengamanan informasi secara individual	Mendefinisikan peran dan tanggung jawab pengamanan informasi secara individual yang terdokumentasi resmi dalam uraian tugas, kebijakan, pemberitahuan lowongan, buku pegangan karyawan, kontrak kerja, kontrak layanan	A.6.1.1

Tabel 5. 19 Rekomendasi Perbaikan Area Pengelolaan Aset Informasi Kategori Pengamanan 1 (lanjutan)

5.9	Belum memiliki peraturan dalam menggunakan email intranet, komputer, email dan internet	Menetapkan kebijakan penggunaan komputer, email, internet dan intranet yang terdokumentasi untuk memberika panduan tentang tata cara dalam menggunakan email intranet, komputer, email dan internet yang diijinkan dan menjelaskan berbagai hal yang dilarang untuk mencegah timbulnya risiko yang dapat menganggu operasional proses kerja dan tata tertib tersebut harus dikomunikasikan kepada seluruh karyawan	A.8.1.3
5.10	Belum memiliki peraturan untuk mengamankan dan menggunakan aset intansi sesuai HAKI	Menetapkan peraturan untuk mengamankan dan menggunakan aset instansi sesuai HAKI sesuai peraturan perundangan yang berlaku yang mencakup hak paten, merk dagang dan hak cipta dan pengguna wajib bertanggung jawab terhadapnya	A.18.1.2
5.11	Belum memiliki tata terbit untuk penginstallan perangkat lunak pada aset instansi	Menetapkan peraturan terkait pembatasan instalasi perangkat lunak aset TI instansi, misalnya mendefinisikan daftar software atau aplikasi yang tidak diizinkan di untuk di *install*	A.12.6.2

Tabel 5. 20 Rekomendasi Perbaikan Area Pengelolaan Aset Informasi Kategori Pengamanan 1 (lanjutan)

5.12	Belum dimilikinya peraturan dalam menggunakan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemiliknya	Menetapkan kebijakan dan peraturan berkaitan dengan privasi dan perlindungan penggunaan data pribadi secara tertulis dan ditetapkan secara resmi oleh pimpinan instansi serta dikomunikasikan kepada karyawan	A.18.1.4
5.13	Belum memiliki proses untuk mengelola identitas elektronik serta proses otentikasi yang mencakup *username* dan *password*	Menetapkan prosedur formal terkait pengelolaan identitas elektronik dan proses otentikasi yang mencakup mengontrol hak akses pengguna, penyediaan data yang dapat diakses.	A.9.3.1
5.14	Belum memiliki syarat dan mekanisme untuk mengelola atau memberikan otentikasi, hak akses dan otorisasi untuk menggunakan aset informasi	Menetapkan kebijakan dan mekanisme mengelola atau memberikan otentikasi, hak akses dan otorisasi kepada pihak yang berwenang dan harus memperhatikan peraturan terkait pembatasan hak akses, kebijakan klasifikasi informasi dan konsistensi hak akses serta persyaratan keamanan informasi pada aplikasi	A.9.1.1
5.15	Belum ditetapkan persyaratan untuk menghancurkan data dan waktu penyimpanan klasifikasi data	Menetapkan kebijakan dan prosedur waktu untuk menyimpan klasifikasi data dan persyaratan penghancuran data untuk menghancurkan data yang dilakukan, harus terdapat laporan serta catatan kejadian	A.8.3.2

Tabel 5. 21 Rekomendasi Perbaikan Area Pengelolaan Aset Informasi Kategori Pengamanan 1 (lanjutan)

5.16	Belum menetapkan aturan pertukaran data dengan pihak eksternal	Menetapkan kebijakan, prosedur dan aturan terkait pertukaran data dengan pihak eksternal yang mencakup kontrol pengalamatan, analisis risiko, identifikasi dan otentikasi, logging, enkripsi, konfirmasi pengiriman atau tanda terima	A.13.2.2
5.17	Belum memiliki mekanisme investigasi atau penyidikan utuk menindaklanjuti dan menyelesaikan insiden keamanan informasi	Meningkatkan peran serta tanggung jawab manajemen insiden keamanan informasi dalam menangani insiden keamanan informasi kemudian manajemen insiden keamanan informasi perlu mencatat, menganalisis, meningkatkan, menangani dan menyelesaikan insiden keamanan informasi dan mengelola insiden secara terukur	A.16.1.3
5.18	Belum memiliki mekanisme untuk *back-up* atau mencadangkan dan uji coba untuk mengembalikan data (*restore*) secara rutin	Menetapkan kebijakan, strategi, arsitektur, prosedur, pedoman, sistem manajemen cadangan, jadwal pecadangan serta catatan terkait dengan log, laporan pengujian terhadap pengembalian data *(restore)*	A.12.3.1

Tabel 5. 22 Rekomendasi Perbaikan Area Pengelolaan Aset Informasi Kategori Pengamanan 1 (lanjutan)

5.32	Belum tersedia peraturan untuk mengamankan perangkat milik instansi ketika dipakai diluar kantor	Menetapkan peraturan terkait pengamanan perangkat komputasi di luar lokasi kerja dengan memperhatikan risiko di luar instansi misalnya perlindungan pada laptop, tablet, USB, dokumen dan lain sebagainya saat melakukan konferensi atau rapat di luar kantor	A.11.2.6
5.33	Belum tersedianya mekanisme untuk melakukan pemindahan aset TIK dari lokasi yang telah ditentukan	Menetapkan pedoman dan proses untuk pemindahan aset TIK dari lokasi yang telah ditentukan dengan aman untuk melindungi aset TIK dari akses pihak yang berhak	A.11.1.6 A.13.2.1

Saat ini tidak tersedianya dokumen yang memuat data-data inventaris aset informasi serta aset yang bekaitan dengan pemrosesan teknologi informasi secara terpelihara, lengkap dan akurat yang mencakup pemiliknya. Kondisi tersebut sesuai dengan kontrol Annex A A.8.1.1 tentang invetarisasi aset dan A.8.1.2 tentang kepemilikan aset. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu mengidentifikasi, mencatat, mengelola seluruh aset informasi terkait dengan teknologi informasi secara terpelihara, lengkap dan akurat serta menetapkan pemilik aset yang meliputi nama atau peran pemilik aset yang bertanggung jawab terhadap aset tersebut. misalnya mengidentifikasi nama barang, tipe, merk, spesifikasi, jumlah dan pemilik aset serta peran pemilik aset informasi tersebut. misalnya adalah data karyawan, data pengguna, *hardware*, *software*, sarana pendukung yang digunakan untuk menjaga layanan TIK CCTV, Generator, UPS, dan AC secara lengkap.

Saat ini belum tersedianya klasifikasi informasi yang disesuaikan dengan peraturan perundangan yang berlaku. Kondisi tersebut sesuai dengan kontrol Annex A A.8.2.1 tentang klasifikasi informasi. Rekomendasi yang diberikan adalah harus menetapkan kebijakan, prosedur dan skema klasifikasi informasi dengan tingkatan tertentu yang harus diterapkan pada organisasi secara konsisten serta mekanisme penanganannya sesuai dengan klasifikasinya. Klasifikasi informasi dilakukan untuk dapat memberikan pengamanan yang

efektif dan tepat terhadap informasi yang ada berdasarkan tingkat klasifikasinya. Misalnya, skema klasifikasi aset informasi berdasarkan kekrititas data yakni rahasia, internal, dan publik.

Keadaan saat ini belum memiliki proses untuk mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingannya. Kondisi tersebut sesuai dengan kontrol Annex A A.8.2.1 tentang klasifikasi informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan dan prosedur terkait klasifikasi informasi yang mencakup proses atau mekanisme untuk melakukan evaluasi dan melakukan klasifikasi terhadap aset informasi yang disesuaikan dengan tingkat kepentingan aset bagi instansi serta mendefinisikan keperluan pengamanan yang perlu dilakukan terhadap setiap klasifikasi aset yang ditentukan untuk menjaga keamanan informasi.

Saat ini belum memiliki definisi yang memuat tingkatan akses yang definisi tingkatan dari setiap klasifikasi aset yang ada dan matriks untuk melakukan perekaman alokasi akses. Kondisi tersebut sesuai dengan kontrol Annex A A.9.1.1 tentang kebijakan kontrol Akses. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu ditetapkannya kebijakan terkait kontrol akses yang mencakup mendefinisikan tingkat akses yang beda pada setiap klasifikasi aset informasi. Misalnya adalah matriks akses yang diizinkan dan mencakup mengontrol aset yang ada dengan level pengaksesan yang berbeda-beda pada pengguna yakni no acces artinya pengguna tidak diperbolehkan menggunakan sistem, execute berarti bahwa pengguna hanya diperbeolehkan untuk menjalankan sistemnya, read artinya pengguna hanya diperbolehkan untuk mencetak dan mebaca file, modify/update memiliki hak untuk mengakses, menajalankan dan memodifikasi, delete artinya bahwa diperbolehkan untuk menghapus file, add/write artinya memungkinkan pengguna menambahkan file, owner yang artinya diberikan hak akses oleh pemakai kepada pihak lain yang sama kewenangannya dengan pemilik sistem, kemudian menetapkan prosedur log-on yang aman serta panduan lain mengenai akses terkontrol ke jaringan, sistem, aplikasi, data, database, kontrak, dokumen, pengetahuan. Contohnya adalah panduan tentang kata sandi, *firewall*, dan VPN *(Virtual Private Network)*.

Aspek pada Indeks KAMI yang belum diterapkan yaitu saat ini belum tersedianya mekanisme untuk mengelola perubahan pada proses bisnis, sistem dan proses teknologi informasi yang mencakup perubahan konfigurasi. Kondisi tersebut sesuai dengan kontrol Annex A A.12.1.1 tentang prosedur operasi terdokumentasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan proses atau prosedur operasi terdokumentasi untuk mengelola perubahan pada proses bisnis, sistem dan proses teknologi informasi dan tersedia kepada seluruh pengguna yang membutuhkan yang mana perubahan tersebut harus disetujui dan ditinjau ulang oleh pemilik sistem dan pimpinan, selanjutnya harus mengontrol pengaksesan

pada program secara rutin dan hasil perubahan program harud ditinjau serta diverifikasi oleh pemilik sistem da pimpinan. Misalnya adalah prosedur instalasi dan konfigurasi sistem TI, back-up dan arsip, penjadwalan pekerjaan, logging dan pemantauan, perbaikan, identifikasi kesalahan, kapasitas dan manajemen kinerja serta manajemen perubahan.

Kondisi saat ini yakni belum memiliki proses pengelolaan konfigurasi secara konsisten. Kondisi tersebut sesuai dengan kontrol Annex A A.12.5.1 tentang pemasangan perangkat lunak pada sistem operasional. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan prosedur terkait pengelolaan konfigurasi yang dilakukan dalam jangka waktu yang telah dilakukan secara konsisten. Misalnya adalah proses untuk pengujian perangkat lunak, persetujuan perubahan, daftar aplikasi yang disetujui atau disahkan, cadangan aplikasi sebelum dan setelah pemasangan, hak tebatas dalam memperbarui perangkat lunak.

Dinas Komunikasi dan Informatika Kabupaten Kediri saat ini belum memiliki mekanisme perilisan aset baru dan pemuktahiran inventaris aset. Kondisi tersebut sesuai dengan kontrol Annex A A.8.2.3 tentang penanganan aset. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan klasifikasi informasi, proses serta panduan untuk menangani aset terkait proses merilis aset baru sesuai dengan skema klasifikasi informasi yang diterapkan pada instansi serta proses memuktahirkan inventaris aset informasi.

Seluruh personil pada instansi masih belum memiliki tanggung jawab secara individual. Kondisi tersebut sesuai dengan Annex A A.6.1.1 tentang peran dan tanggung jawab keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menentukan, mendefinisikan tanggung jawab dan peran pengamanan informasi dengan rinci secara individual. Peran dan tanggung jawab pengamanan informasi tersebut didokumentasikan dalam uraian tugas, kebijakan, pemberitahuan lowongan, buku pegangan karyawan, kontrak kerja, kontrak layanan.

Tata tertib terkait penggunaan internet, intranet, email dan komputer saat ini belum dimiliki dan ditetapkan. Kondisi tersebut sesuai dengan kontrol Annex A A.8.1.3 tentang penggunaan aset yang dapat diterima. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan penggunaan internet, intranet, email dan komputer tertulis untuk memberikan panduan tentang tata cara penggunaan komputer, email, internet dan intranet yang diijinkan dan menjelaskan berbagai hal yang dilarang untuk mencegah timbulnya risiko yang dapat menganggu operasional proses kerja. Misalnya, pelarangan memberikan pinjaman user ID dan kata sandi pada orang lain, menjalankan software yang dapat menganggu kinerja jaringan, pelaporan kelemahan atau gangguan layanan TI, larangan terhadap penggunaan internet untuk mengakses situs terlarang atau berbahaya, larangan penggunaan email yang melanggar etika ber-email, panduan pencantuman identifitas

pengirim dalam email, panduan *attachment* pada email. Kebijakan penggunaan internet, intranet, email dan komputer tersebut harus ditetapkan dan disetujui oleh pimpinan instansi kemudian intansi perlu menerbitkan serta mengkomunikasika pada pihak eksternal dan karyawan yang relevan.

Belum memiliki peraturan untuk mengamankan dan menggunakan aset intansi sesuai HAKI merupakan salah satu aspek Indeks KAMI yang belum diterapkan. Kondisi tersebut sesuai dengan kontrol Annex A A.18.1.2 tentang Hak kekayaan intelektual. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan peraturan untuk mengamankan dan menggunakan aset instansi terkait Hak Kekayaaan Intelektual (HAKI) sesuai dengan peraturan perundangan yang berlaku. Sehingga instansi harus mengidentifikasi dan memelihara semua persyaratan atau kepatuhan keamanan informasi yang mencakup hak paten, merk dagang dan hak cipta dan pengguna wajib bertanggung jawab terhadap penggunaan teknologi informasi yang ada.

Peraturan terkait instalasi perangkat lunak pada aset teknologi informasi milik instansi masih belum dimiliki dan ditetapkan. Kondisi tersebut sesuai dengan kontrol Annex A A.12.6.2 tentang pembatasan pada instalasi perangkat lunak. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu mendefinisikan dan menetapkan peraturan terkait pembatasan atas pemasangan perangkat lunak pada aset teknologi informasi milik instasi. Misalnya, mendefinisikan daftar *software* atau aplikasi yang tidak diizinkan di untuk di *install*. Peraturan tersebut harus ditetapkan dan disetujui oleh pimpinan instansi kemudian pimpinan harus menerbitkan peraturannya dan dikomunikasikan [ada seluruh karyawan dan pihak lain yang terkait.

Dinas Komunikasi dan Informatika Kabupaten Kediri saat ini belum memiliki peraturan dalam menggunakan data pribadi yang disyaratkan pemberian ijin yang tertulis oleh pemilik data pribadi. Kondisi tersebut sesuai dengan kontrol Annex A A.18.1.4 tentang privasi dan perlindungan informasi identitas pribadi. Rekomendasi yang diberikan adalah perlu mendefinisikan kebijakan dan peraturan terkait dengan perlindungan penggunaan data pribadi secara tertulis yang disetujui dan ditetapkan secara resmi oleh pimpinan instansi serta diterbitkan dan dikomunikasan kepada seluruh karyawan atau pihak yang terlibat dalam pengolaan informasi pribadi. Kemudian tanggung jawab dalam menangani penggunaan data pribadi terkait harus sesuai dengan peraturan perundangan yang berlaku.

Kondisi Dinas Komunikasi dan Informatika Kabupaten Kediri saat ini yakni belum memiliki proses untuk mengelola identitas elektronik dan proses otentikasi yang mencakup *username* dan *password*. Kondisi tersebut sesuai dengan kontrol Annex A A.9.3.1 tentang penggunaan informasi otentikasi rahasia. Rekomendasi yang diberikan adalah perlu menetapkan kebijakan dan prosedur tertulis untuk mengelola identitas elektronik dan proses otentikasi yang mencakup *username* dan *password* serta pengguna diharuskan untuk mengikuti praktik instansi dalam menggunakan otentikasi rahasia. Kebijakan

tersebut dapat mencakup mengontrol hak akses pengguna, penyediaan data yang dapat diakses. Selain itu, pengguna juga harus menyimpan informasi terkait otentikasi serta tidak diperkenankan untuk memberikan kode otentikasi kepada pihak lain, menggunakan *password* yang berkualitas dan melakukan penggantian secara berkala setiap 3 bulan sekali pada *password*.

Selanjutnya, Belum memiliki syarat dan mekanisme untuk mengelola atau memberikan otentikasi, hak akses dan otorisasi untuk menggunakan aset informasi. Kondisi tersebut sesuai dengan kontrol Annex A A.9.1.1 tentang kebijakan kontrol akses. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan dan prosedur kontrol akses, yang mencakup pengelolaan atau pemberian akses, otentikasi dan otorisasi kepada pihak yang berwenang. Kebijakan dan prosedur kontrol akses harus memperhatikan peraturan terkait pembatasan hak akses, kebijakan klasifikasi informasi dan konsistensi hak akses serta persyaratan keamanan informasi pada aplikasi. kemudian kebijakan dan prosedur mencakup pemberian hak akses sesuai dengan wewenang dan tugas/pekerjaan, pembatasan hak akses pada tingkatan yang tinggi (*root* atau *administrator*), penghapusan hak akses untuk pengguna yang telah tidak bekerja pada instansi tersebut atau telah mutasi.

Aturan terkait persyaratan untuk menghancurkan data dan waktu penyimpanan klasifikasi data belum ditetapkan. Kondisi tersebut sesuai dengan kontrol Annex A A.8.3.2 tentang pembuangan media. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan dan prosedur terkait waktu untuk menyimpan klasifikasi data serta menetapkan syarat penghancuran data yang aman ketika data terkait tidak lagi dibutuhkan. Dalam setiap penghacuran data yang dilakukan, harus terdapat laporan serta catatan kejadian.

Saat ini belum menetapkan aturan pertukaran data dengan pihak eksternal dan pengamanannya. Kondisi tersebut sesuai dengan kontrol Annex A A.13.2.2 tentang kesepakatan tentang transfer informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan, strategi, dan prosedur aman terkait dengan transfer informasi yang berharga, sensitif atau penting dengan pihak lain. kebijakan, strategi, dan prosedur aman tersebut harus mencakup kontrol pengalamatan, analisis risiko, identifikasi dan otentikasi, logging, enkripsi, konfirmasi pengiriman atau tanda terima.

Kemudian saat ini belum proses untuk menyelidiki, menindaklanjuti dan menyelesaikan insiden keamanan informasi. Kondisi tersebut sesuai dengan kontrol Annex A.16.1.3 tentang melaporkan kelemahan keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan proses penyidikan atau invesitgasi untuk menyelesaikan insiden kegagalan keamanan informasi. Sehingga instansi perlu meningkatkan peran serta tanggung jawab manajemen insiden keamanan

informasi untuk melakukan penanganan insiden keamanan informasi. Selanjutnya manajemen insiden keamanan informasi harus mencatat, menganalisis, meningkatkan, menangani dan menyelesaikan insiden keamanan informasi atas bukti kepatuhan terhadap keamanan informasi. Kemudian insiden kegagalan keamanan informasi harus dikelola secara terukur, rasional, sistematis dan efektif untuk menangani insiden kegagalan keamanan informasi dan mencakup pembersihan pasca insiden keamanan informasi.

Pada Dinas Komunikasi dan Informatika Kabupaten Kediri saat ini belum memiliki prosedur *back-up* dan uji coba pengembalian *data (restore)* secara rutin. Kondisi tersebut sesuai dengan kontrol Annex A A.12.3.1 tentang pencadangan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan, strategi, arsitektur, prosedur, pedoman, sistem manajemen cadangan, jadwal pecadangan serta catatan terkait dengan log, laporan pengujian terhadap pengembalian data *(restore)* yang telah dilakukan.

Saat ini belum tersedianya peraturan untuk mengamankan perangkat instansi jika dipakai di luar lokasi kantor. Kondisi tersebut sesuai dengan kontrol Annex A A.11.2.6 tentang keamanan peralatan dan aset di luar lokasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan peraturan terkait pengamanan perangkat komputasi di luar lokasi kerja dengan memperhatikan risiko di luar instansi. Misalnya perlindungan pada laptop, tablet, USB, dokumen dan lain sebagainya saat melakukan konferensi atau rapat di luar kantor, di rumah, di kendaraan dan lain-lain. misalnya setiap aset instansi yang keluar harus menggunakan surat jalan yang berisikan merek, jenis perangkat, nomor seri, tanggal keluar, alasan dan harus disetujui dan ditandatangi staff yang bertanggung jawab. Kemudian apabila perangkat tersebut telah kembali, maka dilakukan pencatatan kembali dan mengecek kelengkapan barang.

Saat ini belum tersedia mekanisme untuk melakukan pemindahan aset TIK dari lokasi yang telah ditentukan. Kondisi tersebut sesuai dengan kontrol Annex A A 11.1.6 tentang area pengiriman dan pemuatan dan A.13.2.1 tentang kebijakan dan prosedur pengalihan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu ditetapkannya pedoman dan proses untuk pemindahan aset TIK dari lokasi yang ditentukan dengan aman untuk melindungi aset TIK dari akses pihak yang tidak berwenang. Kemudian pimpinan haru menetapkan, menyetujui, menerbitkan dan mengkomunikasikan pada karyawan.

Berikutnya merupakan rekomendasi yang diusulkan untuk tahun ke 2 (dua) dalam penerapan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Kategori pengamanan 2 yakni terkait dengan efektivitas serta konsistensi penerapan keamanan informasi atau penerapan operasional. Rekomendasi berikut diusulkan dilaksanakan sebagai lanjutan dari penerapan rekomendasi pada kategori pengamanan 1 sebelumnya. Berikut

terdapat 8 (delapan) rekomendasi perbaikan yang diusulkan pada kategori pengamanan 2.

Tabel 5. 23 Rekomendasi Perbaikan Area Pengelolaan Aset Informasi Kategori Pengamanan 2

No Pertanyaan	Area Pengelolaan Aset Informasi (*as-is*)	Rekomendasi (*to-be*)	Kontrol ISO 27001
5.19	Belum memiliki ketentuan dalam mengamankan fisik berdasarkan definisi klasifikasi aset dan zona	Menetapkan batasan-batasan pengamanan fasilitas pemrosesan informasi sebagai upaya agar area yang memiliki informasi sensitif atau penting untuk terlindungi dan mencegah akses fisik yang tidak sah sesuai klasifikasi aset	A.11.1.1
5.20	Belum tersedia proses pengecekan latar belakang SDM	Melakukan pemeriksaan terdokumentasi secara rutin terkait identitas dan latar belakang sumber daya manusia yang disesuaikan dengan etika, hukum, dan peraturan, proposional sesuai syarat bisnis, klasifikasi informasi serta risiko yang dirasakan	A.7.1.1
5.21	Belum tersedianya mekanisme untuk melaporkan insiden keamanan informasi pada pihak berwajib dan pihak eksternal	Menetapkan mekanisme tertulis untuk melaporkan insiden keamanan informasi pada pihak eksternal atau pihak berwajib	A.16.1.2
5.22	Belum tersedianya mekanisme untuk menghancurkan data atau aset yang tidak dibutuhkan	Menetapkan kebijakan dan prosedur terkait penghacuran data dan aset yang tidak diperlukan dan dibuktikan dengan dilakukan pencatatan terhadap data dan aset yang telah di hancurkan	A.8.3.2

Tabel 5. 24 Rekomendasi Perbaikan Area Pengelolaan Aset Informasi Kategori Pengamanan 2 (lanjutan)

5.23	Belum tersedia mekanisme untuk mengkaji pemakaian akses (*user access review*) dan hak akses (*access rights*)	Menetapkan mekanisme untuk mengkaji pengunaan akses (*user access review*) dan hak aksesnya(*user access rights*) ke setiap sistem, database, aplikasi dan layanan serta mendefinisikan persyaratan pencabutan hak akses untuk semua jenis pengguna	A.9.2.2
5.24	Belum tersedianya mekanisme untuk pengguna atau tenaga kerja/kontrak yang telah habis kontrak/masa kerjanya	Menetapkan kebijakan dan prosedur terkait penghentian atau perubahan pekerjaan terhadap karyawan yang keluar atau yang habis masa kerjanya, misalnya adalah mengambil aset instansi yang dimiliki mereka, dokumen, pencabutan hak akses, penggantian atau penghapusan kunci	A.7.3.1
5.36	Belum tersedianya proses untuk mengamankan dan proses mengirim aset informasi yang melibatkan pihak ketiga	Menetapkan strategi, kebijakan dan prosedur keamanan terkait dengan pengamanan dalam pengiriman aset informasi yang aman mencakup pengiriman dokumen dan perangkat berharga, sensitif dan penting dengan pihak ketiga untuk melindungi transfer informasi yang dilakukan pada semua jenis alat komunikasi	A.13.2.2

Tabel 5. 25 Rekomendasi Perbaikan Area Pengelolaan Aset Informasi Kategori Pengamanan 2 (lanjutan)

5.37	Belum tersedianya peraturan terhadap pengamanan pada lokasi kerja penting dari risiko bahan atau perangkat yang berbahaya bagi aset informasi	Menetapkan kebijakan, prosedur, pedoman untuk mengamankan lokasi kerja penting (kantor, ruangan, fasilitas) sebagai kontrol untuk karyawan serta pihak ketiga, seperti pemasangan CCTV, buku dan catatan pengunjung	A.11.1.5

Kondisi saat ini belum memiliki ketentuan dalam mengamankan fisik berdasarkan definisi klasifikasi aset dan zona. Kondisi tersebut sesuai dengan kontrol Annex A A.11.1.1 tentang perimeter keamanan fisik. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menentukan dan menetapkan batas keamanan agar area yang mengandung informasi sensitif dapat terlindungi dan melakukan pencegahan apabila terjadi kerusakan atau akses yang tidak sah serta ganggungan pada fasilitas informasi dan penetapan batasan keamanan sesuai dengan klasifikasi aset yang ada untuk melindungi aset informasi tersebut sesuai klasifikasi yang ditetapkan.

Dinas Komunikasi dan Informatika Kabupaten Kediri saat ini belum memiliki proses pengecekan latar belakang dari sumber daya manusia. Kondisi tersebut sesuai dengan kontrol Annex A A.7.1.1 tentang penyaringan. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu melakukan pemeriksaan tertulis pada semua kandidat untuk pekerjaan terkait dengan identitas dan latar belakang sumber daya manusia yang dilakukan sesuai dengan etika, hukum, dan peraturan serta harus proporsional sesuai persyaratan bisnis, klasifikasi informasi yang akan diakses serta risiko yang dapat dirasakan. Pemeriksaan ini dapat dilakukan secara rutin sebelum dipekerjaan dengan menyalin tanda pengenal resmi saat melakukan wawancara secara berkala.

Saat ini belum memiliki mekanisme untuk melaporkan insiden keamanan informasi pada pihak berwajib dan pihak eksternal. Kondisi tersebut sesuai dengan kontrol Annex A A.16.1.2 tentang pelaporan kejadian keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu mekanisme tertulis untuk melaporkan insiden keamanan informasi kepada pihak berwajib atau pihak eksternal. Sehingga peran dan tanggung jawab manajemen insiden keamanan informasi harus mencakup pelaporan insiden keamanan informasi padda pihak eksternal atau pihak berwajib. Insiden keamanan informasi tersebut harus dicatat, dianalisis, diselesaikan sebagai bukti kepatuhan.

Saat ini belum memiliki prosedur penghancuran data atau aset yang tidak diperlukan. Kondisi tersebut sesuai dengan kontrol Annex A A.8.3.2 tentang pembuangan media. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan prosedur untuk menghancurkan data dan aset yang aman ketika tidak dibutuhkan. Penghancuran data yang dilakukan harus dibuktikan dengan dilakukan pencatatan terhadap data dan aset yang telah di hancurkan.

Kondisi saat ini adalah belum mekanisme untuk mengkaji pemakaian akses (*user access review*) dan hak akses (*access rights*) yang meliputi langkah pembenahan jika terjadi ketidaksesuaian pada kebijakan yang berlaku. Kondisi tersebut sesuai dengan kontrol Annex A A.9.2.2 tentang provisioning akses pengguna. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan mekanisme terkait kajian penggunaan dan penyediaan akses ke setiap sistem, database, aplikasi dan layanan serta mendefinisikan persyaratan pencabutan hak akses untuk semua jenis pengguna . kemudian perlu melakukan peninjauan dan verifikasi secara berkala terhadap kompetensi pengguna terhadap hak akses yang diberikan untuk memastikan pengguna telah menjalankan tugas sebagaimana mestinya.

Belum mekanisme untuk pengguna atau tenaga kerja/kontrak yang habis kontrak/masa bekerjanya. Kondisi tersebut sesuai dengan kontrol Annex A A.7.3.1 tentang penghentian atau perubahan tanggung jawab pekerjaan. Rekomendasi yang diberikan adalah perlu menetapkan kebijakan, prosedur, pedoman dan formulir yang terkait dengan penghentian atau perubahan pekerjaan terhadap karyawan yang mutasi atau keluar atau habis masa kerjanya. kebijakan, prosedur, pedoman dan formulir terkait harus memasukkan elemen keamanan informasi misalnya adalah mengambil aset instansi yang dimiliki mereka, dokumen, pencabutan hak akses, penggantian atau penghapusan kunci. Kebijakan, prosedur dan pedoman tersebut harus ditetapkan, dijalankan dan dikomunikasikan kepada seluruh karyawan atau pihak ketiga yang terkait.

Kondisi saat ini belum tersedia proses untuk mengamankan dan proses mengirim aset informasi yang melibatkan pihak ketiga. Kondisi tersebut sesuai dengan kontrol Annex A A.13.2.2 tentang kesepakatan tentang transfer informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan strategi, kebijakan dan prosedur keamanan terkait dengan pengamanan dalam pengiriman aset informasi yang aman mencakup pengiriman dokumen dan perangkat berharga, sensitif dan penting dengan pihak ketiga untuk melindungi transfer nformasi yang dilakukan melaui semua jenis fasilitas komunikasi. Kemudian harus memperhatikan kontrol analisis risiko, kontrak, oengiriman yang aman, konfirmasi pengiriman, peringatan tentang kegagalan pengiriman, kontak darurat dan lain-lain.

Peraturan peraturan pengamanan lokasi kerja penting dari risiko bahan atau perangkat yang berbahaya pada aset informasi belum dimiliki dan ditetapkan. Kondisi tersebut sesuai dengan kontrol A.11.1.5 tentang bekerja di area yang

aman. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan, prosedur, pedoman untuk mengamankan lokasi kerja penting (kantor, ruangan, fasilitas) sebagai kontrol untuk karyawan serta pihak ketiga. Seperti pemasangan CCTV, buku dan catatan pengunjung. Kemudian juga dilakukan pengawasan kerja untuk mencegah kegiatan yang berbahaya dan tidak melakukan pemotretan, pengambilan video seperti penggunaan kamera, handphone, dan perangkat elektronik lainnya.

Berikutnya merupakan rekomendasi yang diusulkan untuk tahun ke 3 (tiga) dalam penerapan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Kategori pengamanan 3 yakni terkait dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi. Pada kategori pengamanan 3 memiliki persyaratan bahwa seluruh bentuk pengamanan pada kategori 1 dan 2 telah diterapkan. Sehingga rekomendasi berikut diusulkan dilaksanakan sebagai lanjutan dari penerapan rekomendasi pada kategori pengamanan 1 dan 2 sebelumnya. Berikut terdapat 4 (empat) rekomendasi perbaikan yang diusulkan pada kategori pengamanan 3.

Tabel 5. 26 Tabel Rekomendasi Perbaikan Area Pengelolaan Aset Informasi Kategori Pengamanan 3

No Pertanyaan	Area Pengelolaan Aset Informasi (*as-is*)	Rekomendasi (*to-be*)	Kontrol ISO 27001
5.25	Belum tersedianya daftar-daftar informasi atau data yang perlu di *back-up* atau dicadangkan dan dokumen laporan analisis kepatuhan terhadap prosedur *back-up*	Mengidentifikasi dan melakukan pencatatan terhadap data atau informasi yang perlu di *back-up* serta proses *back-up* yang dilakukan harus dianalisa secara berkala berdasarkan waktu yang ditetapkan sebagai bentuk kepatuhan terhadap kebijakan, strategi, arsitektur, prosedur, pedoman *back-up* yang telah ditetapkan	A.12.3.1

Tabel 5. 27 Tabel Rekomendasi Perbaikan Area Pengelolaan Aset Informasi Kategori Pengamanan 3 (lanjutan)

5.26	Belum tersedianya daftar perekaman dalam melaksanakan keamanan informasi dan bentuk keamanan informasi berdasarkan klasifikasinya	Melakukan perekaman atau pencatatan dalam pelaksanaan keamanan informasi dan bentuk keamanan informasi sesuai klasifikasinya. Pencatatan pelaksanaan keamanan informasi dapat meliputi ID pengguna, kegiatan, tanggal dan waktu, lokasi dan identitas perangkat (apabila diperluan), perubahan terhadap konfigurasi, penggunaaan sistem dan hak akses, file yang diakses, jenis akses yang digunakan, alamat IP, serta catatan transaksi dan eksekusi yang dilakukan oleh pengguna	A.12.4.1
5.27	Belum tersedianya mekanisme untuk menggunakan perangkat untuk mengolah informasi milik pihak ketiga	Menetapkan kebijakan dan prosedur untuk menggunakan perangkat untuk mengolah informasi milik pihak ketiga yang memperhatikan kepatuhan pada persyaratan legislatif, peraturan dan kontrak sesuai HAKI, misalnya hak paten, merk dagang dan lisensi perangkat lunak	A.18.1.2

Tabel 5. 28 Tabel Rekomendasi Perbaikan Area Pengelolaan Aset Informasi Kategori Pengamanan 3 (lanjutan)

5.38	Belum tersedianya mekanisme pengamanan lokasi kerja utama dari kehadiran pihak ketiga yang bekerja pada instansi	Menetapkan pedoman dan kontrol entri fisik yang aman pengamanan lokasi kerja dari pihak ketiga yang bekerja untuk instansi seperti ruang server harus dibatasi hanya untuk orang yang memiliki wewenang, memelihara dan memantau buku harian, log fisik dan jejak audit secara aman	A.11.1.2

Belum memiliki daftar-daftar informasi atau data yang perlu di *back-up* dan belum memiliki dokumen laporan analisis kepatuhan prosedur *back-up*. Kondisi tersebut sesuai dengan kontrol Annex A A.12.3.1 tentang pencandangan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu mengidentifikasi dan melakukan pencatatan secara berkala terhadap data dan informasi yang harus di *back*-up dan disimpan dengan aman dan terjamin serta harus dapat dipulihkan saat data dan informasi tersebut diperlukan. Kemudian proses *back-up* yang dilakukan harus dianalisa secara berkala berdasarkan waktu yang ditetapkan sebagai bentuk kepatuhan terhadap kebijakan, strategi, arsitektur, prosedur, pedoman *back-up* yang telah ditetapkan. Analisa kepatuhan terhadap prosedur *back-up* harus terdokumentasi dan di laporkan kepada pimpinan instansi.

Belum tersedia daftar perekaman dalam melaksanakan keamanan informasi dan bentuk keamanan informasi berdasarkan klasifikasinya saat ini. Kondisi tersebut sesuai dengan kontrol Annex A A.12.4.1. tentang pencatatan kejadian. Rekomendasi yang diberikan perlu melakukan pencatatan dan perekaman terkait dengan aktivitas dan peristiwa terkait pelaksanaan keamanan informasi secara rutin dalam log, peringatan dalam bentuk catatan historis atau bukti sebagai tindak lanjut apabila terjadi insiden keamanan informasi. Pencatatan pelaksanaan keamanan informasi dapat meliputi ID pengguna, kegiatan, tanggal dan waktu, lokasi dan identitas perangkat (apabila diperluan), perubahan terhadap konfigurasi, penggunaaan utilitas sistem dan hak ases, file yang diakses, jenis akses yang digunakan, alamat jaringan, serta catatan transaksi dan eksekusi yang dilakukan oleh pengguna.

Pada saat ini belum tersedia mekanisme untuk menggunakan perangkat untuk mengolah informasi milik pihak ketiga mencakup perangkat milik

mitra/vendor dan milik pribadi yang memastikan aspek HAKI dan pengamanan akses yang dipakai. Kondisi tersebut sesuai dengan kontrol Annex A A.18.1.2 tentang Hak Kekayaan Intelektual. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu mengidentifikasi dan menetapkan prosedur terkait penggunaan perangkat pengolahan informasi milik pihak ketiga dengan memperhatikan kepatuhan pada peraturan dan kontrak terkait hak kekayaan intelektual, persyaratan legislatif, Misalnya hak paten, merk dagang dan lisensi perangkat lunak.

Saat ini belum tersedia mekanisme pengamanan lokasi kerja utama dari kehadiran pihak ketiga yang bekerja pada instansi. Kondisi tersebut sesuai dengan kontrol Annex A.11.1.2 tentang kontrol entri fisik. Rekomendasi yang diberikan adalah perlu menetapkan pedoman dan kontrol entri fisik yang aman untuk melakukan pengamanan pada lokasi kerja utama dari pihak ketiga yang bekerja untuk instansi untuk dapat dipastikan bahwa hanya orang yang berkepentingan yang dapat mengakses. pedoman dan kontrol entri fisik tersebut harus memastikan dan mencatat waktu dan tanggal masuk pengunjung atau pihak ketiga dan memastikan seluruh pengunjung atau pihak ketiga diawas dan hanya diberikan akse terbatas hanya saat diperlukan, akses ke ruangan penting (misalnya: ruang server) harus dibatasi hanya untuk orang yang memiliki wewenang, memelihara dan memantau buku harian, log fisik dan jejak audit secara aman.

Berdasarkan dari penjabaran diatas, secara garis besar Dinas Komunikasi dan Informatika Kabupaten Kediri mengidentifikasi, mencatat, mengelola seluruh aset informasi serta menetapkan kepemilikan aset tersebut. Menetapkan kebijakan klasifikasi informasi dan proses untuk mengevaluasi dan mengklasifikasikan aset informasi. Menetapkan kebijakan kontrol akses. Menetapkan pedoman untuk mengelola perubahan pada proses bisnis, sistem dan proses teknologi informasi. Menetapkan pedoman pengelolaan konfigurasi. Menetapkan proses untuk merilis aset baru. Mendefinisikan dan menetapkan peran dan tanggung jawab pengamanan informasi dengan rinci secara individual. Menetapkan kebijakan dalam menggunakan komputer, email, internet dan intranet. Menetapkan peraturan pengamanan dan penggunaan aset. Menetapkan peraturan pembatasan atas pemasangan perangkat lunak pada aset teknologi informasi. Menetapkan kebijakan dan peraturan terkait dengan perlindungan penggunaan data pribadi. Menetapkan kebijakan dan prosedur tertulis terkait untuk mengelola identitas elektronik dan proses otentikasi. Menetapkan kebijakan dan prosedur terkait waktu penyimpanan klasifikasi data. Menetapkan proses untuk menyelidiki menindaklanjuti dan menyelesaikan insiden keamanan informasi. Menetapkan prosedur *back-up* dan uji coba pengembalian *data (restore)*, menetapkan ketentuan pengamanan fisik sesuai klasifikasi aset. Menetapkan proses pengecekan latar belakang sumber daya manusia. Menetapkan prosedur pelaporan insiden keamanan informasi. Menetapkan prosedur penghancuran data. Menetapkan prosedur kajian penggunaan dan penyediaan akses ke setiap sistem, database, aplikasi dan

layanan. Menetapkan kebijakan penghentian atau perubahan pekerjaan terhadap karyawan yang mutasi atau keluar atau habis masa bekerjanya. Mendefinisikan daftar data yang harus di *back-up* dan menyusun dokumen terkait analisa kepatuhan prosedur *back-up*. Melakukan pencatatan aktivitas dan peritiwa pelaksanaan keamanan informasi. Menetapkan prosedur menggunakan perangkat pengolahan informasi milik pihak ketiga. Menetapkan peraturan pengamanan perangkat komputasi di luar lokasi kerja. Menetapkan proses pemindahan aset TIK. Menetapkan prosedur pengiriman aset informasi yang aman dan menetapkan kebijakan keamanan lokasi kerja dari perangkat berbahaya dan pihak ketiga.

5.5 Teknologi dan Keamanan Informasi

Skor tingkat kelengkapan yang diperoleh adalah 53 dengan tingkat kematangan I+ dan persentase tingkat kematangan adalah 44,1%. Berdasarkan penilaian yang dilakukan, didapatkan bahwa penerapan area teknologi dan keamanan informasi sebagian aspek telah terpenuhi. Pengamanan dilakukan dengan *firewall* sebagai pengamanan, jaringan komunikasi telah di segmentasi, infrastruktur aplikasi, sistem dan jaringan disusun untuk memastikan ketersediaan redundan dan dimonitor, perubahan sistem dan upaya akses sistem oleh pihak yang tidak berhak terekam dalam log. Area teknologi dan keamanan informasi terdapat sebagian aspek pada Indeks KAMI yang belum dilakukan atau dalam perencanaan sehingga diajukan sebagai rekomendasi perbaikan dengan dilakukan pemetaan terhadap kontrol Annex A dan *Information Security Management Documentation Checklist*. Berikut pada tabel 5.3 merupakan 15 rekomendasi perbaikan pada area teknologi dan keamanan informasi yang terbagi dalam 3 (tiga) tahap penerapannya. Rekomendasi diajukan secara bertahap dilakukan per tahun sesuai dengan kategori pengamanan pada Indeks KAMI. Berikut merupakan 6 (enam) rekomendasi perbaikan pada kategori pengamanan 1 terkait dengan penerapan kerangka kerja dasar pada tahun pertama yang diusulkan.

Tabel 5. 29 Rekomendasi Perbaikan Area Teknologi dan Keamanan Informasi Kategori Pengamanan 1

No Pertanyaan	Area teknologi dan keamanan informasi (*as-is*)	Rekomendasi (to-be)	Kontrol ISO 27001
6.3	Belum memiliki konfigurasi untuk mengamankan aplikasi, aset jaringan dan sistem	Menetapkan kebijakan terkait konfigurasi standar yang digunakan untuk mengamankan sistem bagi seluruh aplikasi,aset jaringan dan aplikasi	A.13.1.1 A.13.1.2

Tabel 5. 30 Rekomendasi Perbaikan Area Teknologi dan Keamanan Informasi Kategori Pengamanan 1 (lanjutan)

6.4	Instansi belum menganalisa kepatuhan penerapan konfigurasi secara rutin	Instansi melakukan analisis terkait kepatuhan dalam menerapkan konfigurasi secara konsisten berdasarkan jadwal yang direncanakan dan sesuai dengan kebijakan yang berlaku apabila terjadi ketidakpatuhan kemudian mengidentifikasi penyebab ketidakpatuhan dan melakukan evaluasi sebagai upaya untuk mencapai kepatuhan yang diharapkan dan dikaji untuk menetapkan langkah perbaikan sesuai yang diharapkan yang terdokumentasi	A.13.1.1
6.5	Belum melakukan pemindaian pada sistem, aplikasi dan jaringan yang dipakai secara berkala	Menetapkan strategi, kebijakan dan prosedur untuk melakukan pemindaian terhadap sistem, aplikasi dan jaringan sesuai dengan jadwal yang ditetapkan	A.13.1.1
6.10	Belum menganalisa catatan log secara berkala untuk dipastikan kelengkapan, kevalidan dan keakuratan isinya	Melakukan peninjauan dan menganalisa log secara berkala yang mencakup merekam seluruh aktivitas pengguna, kesalahan kejadian keamanan informasi, pengecualian, dan peristiwa lainnya, misalnya catatan historis/ bukti/ forensik	A.12.4.1

Tabel 5. 31 Rekomendasi Perbaikan Area Teknologi dan Keamanan Informasi Kategori Pengamanan 1 (lanjutan)

6.11	Instansi belum diterapkan enksirpsi untuk melindungi aset informasi	Menetapkan kebijakan, standar, pedoman yang tepat terkait dengan kriptografi, algoritma dan kunci untuk enkripsi, dan otentikasi untuk melindungi kerahasiaan dan keaslian informasi seperti penerapan HTTPS untuk melindungi website instansi	A.10.1.1
6.20	Desktop dan server belum terlindungi dari penyerangan virus (*malware*)	Menerapkan perlindungan terhadap setiap desktop dan server dari serangan virus atau *malware* dengan melakukan penginstallan antivirus termutakhir	A.12.2.1

Saat ini belum memiliki konfigurasi berdasarkan standar yang berlaku untuk keamanan sistem bagi seluruh aplikasi, aset jaringan, dan sistem yang dimutakhirkan berdasarkan perkembangan standar industri yang berlaku serta kebutuhan. Kondisi tersebut sesuai dengan kontrol Annex A A.13.1.1 tentang kontrol jaringan A.13.1.2 tentang keamanan layanan dalam jaringan. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu Menetapkan kebijakan terkait konfigurasi standar yang digunakan untuk keamanan sistem seluruh aplikasi, aset jaringan, dan sistem.

Analisa secara rutin terkait dengan kepatuhan terhadap penerapan konfigurasi standar yang ada masih belum dilakukan. Kondisi tersebut sesuai dengan kontrol Annex A A.13.1.1 tentang kontrol jaringan. Rekomendasi yang diberikan adalah perlu menetapkan strategi, prosedur dan kebijakan untuk menganalisa kepatuhan penerapan konfigurasi pada instansi secara berkala sesuai dengan jadwal yang direncanakan untuk memastikan kesesuaian dan efektivitas penerapan konfigurasi telah sesuai kebijakan dan standar yang berlaku. Kemudian apabila terjadi ketidakpatuhan, maka perlu mengidentifikasi penyebab ketidakpatuhan dan melakukan evaluasi sebagai upaya untuk mencapai kepatuhan yang diharapkan dan dikaji untuk menetapkan langkah perbaikan sesuai yang diharapkan. Kemudian hasil analisa tersebut harus dilaporkan kepada pimpinan instansi terkait.

Sistem, aplikasi dan jaringan yang digunakan saat ini belum dipindai secara konsisten sebagai upaya untuk identifikasi terhadap kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi. Kondisi tersebut sesuai dengan kontrol Annex A A.13.1.1 tentang kontrol jaringan. Rekomendasi yang diberikan adalah perlu ditetapkannya strategi, prosedur dan kebijakan berkaitan dengan proses untuk melakukan pemindaian secara berkala terhadap sistem, aplikasi dan jaringan pada instansi untuk melakukan identifikasi adanya celah kelemahan atau perubahan/keutuhan konfigurasi pada aplikasi,sistem dan jaringan tersebut. kemudian hasil pemindaian tersebut harus dicatat, dianalisis dan diselesaikan kemudian dikaji untuk menetapkan langkah-langkah penerapan keamanan informasi sebagai langkah perbaikan untuk menghilangkan/mengurangi kelemahan atau perubahan konfigurasi yang terjadi sebagai bukti kepatuhan instansi terhadap organisasi.

Saat ini belum menganalisa log secara berkala untuk untuk dipastikan kelengkapan, kevalidan dan keakuratan isinya. Kondisi tersebut sesuai dengan kontrol Annex A A.12.4.1 tentang pencatatan kejadian. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu melakukan pencatatan, peninjauan dan menganalisa log secara berkala yang merekam merekam seluruh aktivitas pengguna, kesalahan kejadian keamanan informasi, pengecualian, dan peristiwa lainnya, misalnya catatan historis/ bukti/ forensik yang dapat dijadikan sebagai dasar untuk melakukan tindakan lebih lanjut terhadap insiden keamanan informasi yang ada serta untuk memastikan akurasi, validitas, dan kelengkapan dari isi log.

Dinas Komunikasi dan Informatika Kabupaten Kediri saat ini belum menerapkan enkripsi untuk melindungi aset informasi dan belum memiliki standar dalam penggunaan enkripsi. Kondisi tersebut sesuai dengan kontrol A.10.1.1 tentang kebijakan dalam menggunakan kontrol kriptografi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan, standar, pedoman yang tepat terkait dengan kriptografi, algoritma dan kunci untuk enkripsi, dan otentikasi untuk melindungi kerahasiaan dan keaslian informasi. Misalnya dengan melakukan penerapan https untuk melindungi website instansi.

Desktop dan server pada instansi saat ini belum terlindungi dari penyerangan virus (*malware*). Kondisi tersebut sesuai dengan kontrol Annex A A.12.2.1 tentang kontrol terhadap *malware.* Rekomendasi yang diusulkan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menerapkan perlindungan terhadap *desktop* dan server yang dipakai dari serangan virus (*malware*) dengan menerapkan *software* antivirus termutakhir. Kemudian dilakukan pengecekan secara berkala terhadap *desktop* dan *server* tersebut untuk memastikan terhindar dari *malware*.

Berikutnya merupakan rekomendasi yang diusulkan untuk tahun ke 2 (dua) dalam penerapan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Kategori pengamanan 2 yakni terkait dengan efektivitas serta

konsistensi penerapan keamanan informasi atau penerapan operasional. Rekomendasi berikut diusulkan dilaksanakan sebagai lanjutan dari penerapan rekomendasi pada kategori pengamanan 1 sebelumnya. Berikut terdapat 7 (tujuh) rekomendasi perbaikan yang diusulkan pada kategori pengamanan 2.

Tabel 5. 32 Rekomendasi Perbaikan Area Teknologi dan Keamanan Informasi Kategori Pengamanan 2

No Pertanyaan	Area teknologi dan keamanan informasi (*as-is*)	Rekomendasi (to-be)	Kontrol ISO 27001
6.12	Instansi belum memiliki standar penggunaan enkripsi	Menetapkan kebijakan penggunaan kontrol kriptografi terkait standar penggunaan enkripsi	A.10.1.1
6.13	Belum diterapkannya bentuk pengamanan untuk pengelolaan kunci enkripsi	Menetapkan kebijakan dan pedoman terkait dengan pengggunaan, perlindungan serta masa pakai kunci kriptografi, sertifikat digital, tanda tangan digital dll	A.10.1.2
6.14	Aplikasi dan sistem belum didukung dan diterapkan perubahan *password* secara sistematis	Menetapkan kebijakan, prosedur, dan pedoman terkait manajemen kata sandi, penegakan dan pilihan kata sandi yang kuat dan kerahasiaan kata sandi yang interaktif	A.9.4.3
6.15	Belum terdapat pengamanan berlapis pada akses yang dipakai administrasi sistem dalam mengelola sistem	Menetapkan kebijakan, prosedur, pedoman terkait dengan kontrol akses ke kode sumber program	A.9.4.5
6.21	Belum memiliki dokumen perekaman serta hasil analisa jejak audit atau untuk memastikan antimalware atau antivirus yang digunakan telah	Dilakukan pembuktian bahwa instansi telah melakukan perancangan, pemeriksaan, pengelolaan, pemeliharaan dan menggunakan kontrol malware yang telah sesuai serta auditor memeriksa	A.12.2.1

	dimuktahirkan secara berkala	kebijakan, prosedur, pedoman, arsitektur/desain, kontrak dan catatan seperti detail insiden *malware*, program antivirus, catatan instalasi perangkat lunak, catatan kepatuhan organisasi	
6.22	Belum memiliki dokumen laporan terkait penyerangan *malware* atau virus yang gagal atau sukses ditindaklanjuti dan diselesaikan	Melakukan dokumentasi laporan penyerangan *malware* atau virus yang gagal atau sukses ditindaklanjuti untuk membuktikan bahwa instansi telah memelihara dan mengelola kontrol deteksi, pencegahan, dan pemulihan terhadap *malware*	A.12.2.1
6.24	Fungsi keamanan dan spesifikasi pada aplikasi belum dimiliki yang diverifikasi saat uji coba dan pengembangan sistem	Menetapkan prosedur, kebijakan, pedoman dan strategi terkait mengembankan perangkat lunak serta sistem dan mencakup verifikasi atau validasi terhadap fungsi serta dan spesifikasi keamanannya, misalnya pemilihan desain yang aman, metode pengembangan sistem terstruktur dengan analisa risiko terdokumentasi, pemilihan platform yang aman, pemilihan layanan/ fungsi/ proses yang aman, pengkodean yang aman, verifikasi pasca implementasi sistem, pemeliharaan sistem	A.14.2.1

Pengamanan untuk melakukan pengelolaan terhadap kunci enkripsi, termasuk sertifikat elektronik yang dipakai serta siklus pemakaiannya belum diterapkan. Kondisi tersebut sesuai dengan kontrol Annex A.10.1.2 tentang pengelolaan kunci. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan dan pedoman terkait dengan pengggunaan, perlindungan serta masa pakai kunci kriptografi yang harus diterapkan dan dikembangkan berdasarkan standar yang berlaku.

Aplikasi dan sistem belum didukung dan diterapkan perubahan *password* secara sistematis. Kondisi tersebut sesuai dengan kontrol Annex A A.9.4.3 tentang sistem manajemen kata sandi. Rekomendasi yang diajukan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan, prosedur, dan pedoman terkait pengelolaan kata sandi yang mencakup penegakan dan pilihan kata sandi yang kuat, kerahasiaan kata sandi yang interaktif dan harus dipastikan bahwa kata sandi yang diterapkan berkualitas.

Belum terdapat pengamanan berlapis pada akses yang dipakai administrasi sistem dalam mengelola sistem merupakan aspek Indeks KAMI yang belum diterapkan saat ini. Kondisi tersebut sesuai dengan kontrol Annex A A.9.4.5 tentang kontrol akses ke kode sumber program. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan, prosedur, pedoman kebijakan terkait kontrol akses ke sumber program yang perlu dibatasi hanya untuk orang yang berhak dan memiliki kewenangan.

Keadaan instansi saat ini yakni belum memiliki dokumen rekaman serta hasil analisa jejak audit atau untuk mengkonfirmasi antivirus/antimalware yang dimutakhirkan secara berkala dan sistematis. Kondisi tersebut sesuai dengan kontrol Annex A A.12.2.1 tentang kontrol terhadap *malware*. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu melakukan pembuktian bahwa instansi telah melakukan perancangan, pemeriksaan, pengelolaan, pemeliharaan dan menggunakan kontrol *malware* yang sesuai. Kemudian auditor memeriksa kebijakan, prosedur, pedoman, arsitektur/desain, kontrak dan catatan seperti detail insiden *malware*, program antivirus, catatan instalasi perangkat lunak, catatan kepatuhan organisasi. pemeriksaaan yang dilakukan harus dicatat, dikelola, dan dimutakhirkan secara rutin serta dilaporkan kepada pimpinan instansi.

Saat ini belum memiliki dokumen terkait laporan serangan *malware* atau virus yang gagal atau sukses ditindaklanjuti dan diselesaikan. Kondisi tersebut sesuai dengan kontrol Annex A A.12.2.1 tentang kontrol terhadap kontrol *malware*. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu melakukan dokumentasi atau mencatat dan membuat laporan terkait penyerangan virus atau *malware* yang suskes diselesaikan atau ditindaklanjuti atau yang gagal untuk membuktikan bahwa instansi telah memelihara dan mengelola pencegahan, kontrol deteksi, dan pemulihan terhadap *malware* yang kemudian harus dilaporkan ke pimpinan instansi.

Kondisi saat ini adalah fungsi keamanan dan spesifikasi pada aplikasi belum dimiliki yang diverifikasi saat uji coba dan pengembangan sistem. Kondisi tersebut sesuai dengan kontrol Annex A A.14.2.1 tentang kebijakan pembangunan yang aman. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan prosedur, strategi, pedoman dan kebijakan untuk mengembangkan sistem dan perangkat lunak mencakup verifikasi dan validasi terhadap fungsi dan spesifikasi keamananya. Misalnya pemilihan desain yang aman, metode pengembangan sistem terstruktur dengan analisa risiko terdokumentasi, pemilihan platform yang aman, pemilihan layanan/ fungsi/ proses yang aman, pengkodean yang aman, verifikasi pasca implementasi sistem, pemeliharaan sistem.

Berikutnya merupakan rekomendasi yang diusulkan untuk tahun ke 3 (tiga) dalam penerapan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Kategori pengamanan 3 yakni terkait dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi. Pada kategori pengamanan 3 memiliki persyaratan bahwa seluruh bentuk pengamanan pada kategori 1 dan 2 telah diterapkan. Sehingga rekomendasi berikut diusulkan dilaksanakan sebagai lanjutan dari penerapan rekomendasi pada kategori pengamanan 1 dan 2 sebelumnya. Berikut terdapat 2 (dua) rekomendasi perbaikan yang diusulkan pada kategori pengamanan 3.

Tabel 5. 33 Rekomendasi Perbaikan Area Teknologi dan Keamanan Informasi Kategori Pengamanan 3

No Pertanyaan	Area teknologi dan keamanan informasi (*as-is*)	Rekomendasi (to-be)	Kontrol ISO 27001
6.25	Belum diterapkannya menerapkan uji coba yang aman berdasarkan standar platform teknologi dan pengembangan sistem	Menetapkan kebijakan, prosedur dan pedoman terkait pengembangan dan uji coba sistem yang aman dan upaya pengitegrasian yang meliputi keseluruhan siklus hidup pengembangan sistem misalnya, pemilihan desain yang aman, metode pengembangan sistem terstruktur dengan analisa risiko terdokumentasi, pemilihan platform yang aman	A.14.2.6

Tabel 5. 34 Rekomendasi Perbaikan Area Teknologi dan Keamanan Informasi Kategori Pengamanan 3 (lanjutan)

6.26	Belum dilibatkannya pihak independen dalam melakukan kajian untuk mengukur kehandalan keamanan informasi secara berkala	Menetapkan mekanisme tertulis untuk mengelola keamanan informasi dan implementasinya dan dilakukan peninjauan oleh pihak independen secara berkala	A.18.2.1

Belum diterapkannya proses uji coba yang aman lingkungan pengembangan sistem yang aman berdasarkan standar platform teknologi. Kondisi tersebut sesuai dengan kontrol Annex A.14.2.6 tentang lingkungan pengembangan yang aman. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan, prosedur, dan pedoman terkait pelaksanaan pengembangan dan uji coba sistem yang aman bagi keseluruhan siklus hidup pengembangan sistemnya dan mencakup proses integrasinya. Misalnya pemilihan desain yang aman, teknik pengembangan sistem terstruktur berdasarkan hasil analisis risiko secara tertulis, penggunaan platform yang aman, pemilihan layanan/ fungsi/ proses yang aman, pengkodean yang aman.

Dinas Komunikasi dan Informatika Kabupaten Kediri saat ini dilibatkannya pihak independen dalam melakukan kajian untuk mengukur kehandalan keamanan informasi secara berkala. Kondisi tersebut sesuai dengan kontrol Annex A A.18.2.1 tentang tinjauan independen atas keamanan informasi. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan mekanisme untuk mengelola keamanan informasi dan implementasi. Kemudian harus dilakukan peninjauan secara independen terhadap tujuan pengendalian, kebijakan, proses, prosedur dan kontrol pada jangka waktu yang ditetapkan atau apabila terjadi perubahan yang signifikan.

Berdasarkan penjabaran diatas, secara garis besar perlu mendefinisikan dan menetapkan kebijakan kontrol jaringan. Menetapkan kebijakan dan prosedur untuk melakukan pemindaian secara rutin sistem, aplikasi dan jaringan. Melakukan pencatatan, peninjauan dan menganalisa log secara konsisten. Menetapkan kebijakan kriptografi. Menetapkan kebijakan dan pedoman manajemen kata sandi. Menetapkan kebijakan kontrol akses. Menerapkan *software* antivirus pada setiap *desktop* dan server. Melakukan pencatat hasil jejak audit. Mencatat dan membuat laporan penyerangan virus atau *malware*. Menetapkan kebijakan pengembangan perangkat lunak yang aman mencakup verifikasi dan validasi. Menetapkan kebijakan pengembangan dan uji coba sistem. Menetapkan kebijakan untuk pengelolaan keamanan informasi dan implementasi oleh pihak independen yang mencakup peninjauan secara

independen terhadap tujuan pengendalian, kebijakan, proses, prosedur dan kontrol.

5.6 Suplemen

Ketercapaian penerapan area suplemen pada Dinas Komunikasi dan Informatika Kabupaten Kediri pada pengamanan keterlibatan pihak ketiga adalah 0%, pengamanan layanan insfratruktur awan adalah 0% dan perlindungan data pribadi adalah 0% karena saat ini Dinas Komunikasi dan Informatika Kabupaten Kediri belum menerapan ketiga aspek tersebut. Sehingga, seluruh aspek pertanyaan indeks KAMI pada area suplemen tidak dilakukan dan diajukan sebagai rekomendasi perbaikan dengan dilakukan pemetaan pada kontrol Annex A dan *Information Security Management Documentation Checklist*. Berikut pada tabel 5.6 merupakan 9 rekomendasi perbaikan pada area suplemen dengan kategori pengamanan 1 terkait dengan penerapan kerangka kerja dasar.

Tabel 5. 35 Rekomendasi Perbaikan Area Suplemen Kategori Pengamanan 1

No Pertanyaan	Area suplemen (*as-is*)	Rekomendasi (to-be)	Kontrol ISO 27001
7.1.1	Instansi belum menerapkan kebijakan keamanan informasi, manajemen risiko, dan pengelolaan keamanan bagi pihak ketiga yang meliputi mengidentifikasi risiko keamanan informasi, mengkomunikasikan dan mengklarisikasi risiko, mengklarifikasi persyaratan mitigasi risiko dan menetapkan hak audit TI secara berkala yang dikomunikasikan dan disetujui dengan pihak ketiga pada dokumen kontrak	Menetapkan kebijakan, proses dan pedoman kebijakan keamanan informasi yang mencakup kebijakan manajemen risiko keamanan informasi terkait kerja sama bersama pihak ketiga. Dan didalamnya mencakup proses mengidentifikasi risiko kerja sama dengan pihak ketiga, proses mengkomunikasian dan mengklarifikasi risiko keamanan informasi pada pihak ketiga, proses mengklarifikasi persyaratan mitigasi risiko, menetapkan ekspektasi mitigasi risiko, persyaratan pengendalian akses layanan, proses penghancuran informasi dan data yang tidak digunakan, *Non Disclosure*	A.5.1.1 A.12.7.1 A.16.1.3 A.16.1.6 A.17.1.1 A.17.1.2 A.17.1.3 A.18.2.1

		Agreement (NDA) bagi karyawan pihak ketiga, melakukan audit TI sebagai bagian dari persyaratan kontrak yang harus disetujui oleh pihak ketiga dalam dokumen kontrak	
7.1.2	Belum teridentifikasi risiko berkaitan dengan pengalihan daya, subkontraktor atau penyedia teknologi atau infrastruktur yang dipakai, belum menerapkan pengendalian risiko dalam perjanjian dan belum melakukan pemantauan terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi atau infrastruktur oleh pihak ketiga	Menetapkan kebijakan, pedoman, proses dan strategi untuk mengelola sub-kontraktor/alih daya oleh pihak ketiga. Hal tersebut mencakup proses pengidentifikasian risiko alih daya, subkontraktor atau penyedia teknologi dan proses pengendalian risikonya, proses untuk memantau dan mengevaluasi kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur berdasarkan persyaratan keamanan yang ditentukan.	A.5.1.1 14.2.7
7.1.3	Instansi belum menetapkan kebijakan, proses, prosedur pengelolaan dan pemantauan layanan dan aspek keamanan informasi dengan pihak ketiga termasuk menetapkan tanggung jawab dan peran untuk memantau, mengevaluasi dan melakukan audit aspek kemanan informasi,	Menetapkan kebijakan, proses, pedoman, dan strategi terkait dengan pengelolaan layanan dalam hubungan dengan pihak ketiga mencakup pengamanan aset informasi dan infrastruktur milik instansi/perusahaaan, mendefinisikan tanggung jawab dan peran untuk memantau dan mengevalasi serta melakukan audit aspek keamanan informasi pihak ketiga, melakukan	A.5.1.1 A.6.1.1 A.12.7.1

	ketersediaan laporan secara berkala terkait pencapaian sasaran tingkat layanan (SLA), penjadwalan pertemuan secara bekala untuk dilakukan pemantauan dan evaluasi ketercapaian sasaran tingkat layanan untuk melakukan dokumentasi, mengkomunikasikan dan menindaklanjuti hasil pamentauan dan evaluasi, melakukan perencanaan audit pemenuhan persyaratan keamanan informasi dan menindaklanjuti hasil audit dengan melaporkan rencana perbaikan terukur dan menerapkan denda atau penalti terhadap ketidakpatuhan pihak ketiga pada persyaratan dan/tingkat layanan yang ditentukan	pencatatan dan mendokumentasikan laporan ketercapaian sasaran tingkat layanan dan aspek keamanan dan proses untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan, menetapkan jadwal audit, proses pelaporan rencana perbaikan dari hasil audit, menetapkan prosedur disipliner formal untuk mengambil tindakan berupa denda/penalti yang ditetapkan instansi kepada pihak ketiga apabila terjadi ketidakpatuhan terhadap persyaratan dan/atau tingkat layanan	

Tabel 5. 36 Rekomendasi Perbaikan Area Suplemen Kategori Pengamanan 1 (lanjutan)

7.1.4	Belum melakukan pengelolaan perubahan yang terjadi dalam hubungan pihak ketiga (perubahan layanan, perubahan kebijakan, kontrol risiko) dan belum mengkaji, dokumentasi dan menetapkan rencana mitigasi baru terhadap risiko	menetapkan proses mengelola perubahan hubungan dengan pihak ketiga yang mencakup untuk mengubah pihak ketiga, merevisi kebijakan, prosedur dan kontrol pihak ketiga. mengidentifikasi, mendokumentasi, mengkaji risiko yang mungkin dapat terjadi di masa depan dan mengidentifikasi rencana mitigasi yang akan diterapkan	A.15.2.2
7.1.5	Belum memiliki Mekanisme secara resmi untuk penanganan data selama siklus hidupanya yang mencakup membuat, mendaftar, mengubah, menghapus dan menghancurkan aset dan menerapkan mekanisme untuk menghancurkan data yang aman belum disepakati dengan pihak ketiga	Menetapkan kebijakan,pedoman dan prosedur terkait dengan pengelolaan dan penyimpanan data selama siklus hidup yaitu proses pembuatan, proses pendaftaran, proses perubahan dan dan proses penghapusan atau penghancuran aset yang aman	A.5.1.1 A.8.3.1 A.8.3.2

Tabel 5. 37 Rekomendasi Perbaikan Area Suplemen Kategori Pengamanan 1 (lanjutan)

7.1.6	Belum tersedianya mekanisme untuk melaporkan, memantau, menangani dan menganalisis insiden keamanan informasi serta dokumen bukti yang memadai dalam menangani insiden keamanan informasi	Menetapkan prosedur untuk mengelola insiden keamanan informasi yang meliputi pelaporan, pemantauan, penanganan insiden keamanan informasi secara tepat.	A.16.1.2 A.16.1.4 A.16.1.5 A.16.1.7
7.1.7	Belum memiliki perencanaan kelangsungan layanan pihak ketiga yang mencakup prosedur, kebijakan atau rencana yang tertulis untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat. Kemudian kebijakan, prosedur atau keberlangsungan layanan belum diuji coba, didokumentasi hasil dan dievaluasi keefektifannya serta pihak ketiga belum mempunyai tim yang dikhususkan dalam pengelolaan proses kelangsungan layanannya	Menetapkan kebijakan, prosedur atau rencana terdokumentasi yang telah di uji coba, dan diuji efektifitasnya untuk mengatasi keberlangsungan layanan pihak ketiga dalam keadaan darura dengan ditentukannya syarat-syarat untuk keamanan informasi dan kelangsungan manajemen keamanan informasi, mendefinisikan peran dan tanggung jawab untuk mengelola kelangsungan layanan	A.5.1.1 A.17.1.1 A.17.1.2 A.17.1.3

Tabel 5. 38 Rekomendasi Perbaikan Area Suplemen Kategori Pengamanan 1 (lanjutan)

7.2.	Instansi belum menetapkan kebijakan, pedoman dan prosedur terkait dengan pengamanan layanan infrastruktur awan. Hal ini meliputi pelaksanaan kajian risiko penggunaan layanan, penetapan data yang diolah pada layanan, pengamanan data pribadi pada layanan berbasis *cloud*, proses pengkajian penggunaan layanan, penjadwalan pelaksanaan evaluasi penyelenggara layanan, penetapan standar keamanan teknis dalam menggunakan layanan *cloud*, evaluasi kelayakan keamanan layanan *cloud*, proses pergantian layanan, proses pelaporan insiden layanan dan proses menghentikan layanan *cloud*	Menetapkan kebijakan, prosedur, proses dan pedoman terkait dengan pengamanan layanan infrastruktur awan. Yang mencakup proses kajian risiko penggunaan layanan infrastruktur awan, penetapan daftar data atau informasi yang dipertukarkan melalui layanan, proses pengamanan data pribadi yang dipertukarkan melalui layanan, proses pengkajian dan penetapan kriteria untuk memastikan aspek hukum penggunaan layanan, melaksanakan evaluasi terhadap penyelenggara layanan, menetapkan standar keamanan teknis penggunaan layanan yang disetujui, proses untuk mengevaluasi kelayakan keamanan layanan untuk pemenuhan sertifikasi, menetapkan proses untuk mengganti layanan *cloud* apabila terjadi gangguan, proses pelaporan insiden terkait layanan dan eskalasi pelaporannya serta menetepkan proses penghentian layanan	A.5.1.1 A.8.2.3 A.18.1.4 A.18.1.1 A.16.1.2

Tabel 5. 39 Rekomendasi Perbaikan Area Suplemen Kategori Pengamanan 1 (lanjutan)

7.3.1	Instansi belum menerapkan perlindungan data pribadi. Yang meliputi dokumentasi terhadap jenis dan bentuk data pribadi yang ditukar dengan pihak eksternal, melakukan pemetaan alur pemrosesan data internal dan pertukaran data, menetapkan proses penyimpanan dan mendokumentasikannya, menetapkan kebijakan perlindungan data pribadi, penetapan penanggung jawab penerapan kebijakan dan proses perlindungan data pribadi, menganalisa dampak terungkapnya data pribadi, melakukan kajian risiko keamanan perlindungan data pribadi, menetapkan program peningkatan pemahaman tentang perlindungan data pribadi, menetapkan proses pelaporan insiden terungkapnya data pribadi, proses menjamin hak pemilik data pribadi, proses validasi dan verifikasi	Menetapkan kebijakan, prosedur, pedoman dan proses terkait perlindungan data pribadi yang dalam penerapannya sesuai dengan keperluan mitigasi risiko. Yang mencakup proses mendokumentasikan jenis dan bentuk data pribadi, menetapkan proses penyimpanan, pengolahan, dan pertukaran data dengan pihak eksternal dan didokumentasikan, menetapkan penanggung jawab yang berwenang dalam penerapan perlindungan data pribadi, menetapkan program peningkatan kepedulian atau pemahaman terkait dengan perlindungan data pribadi, proses persetujuan pemilik data pribadi yang dapat dinyatakan dalam pernyataan tertulis secara elektronik/manual terkait pengamblan data, proses pelaporan insiden terungkapnya data pribadi, proses menjamin hak pemilik data, proses validasi dan verifikasi data pribadi, proses periode penyimpanan data pribadi, proses penghapusan/pemusnahan data yang tidak diperlukan atau atas permintaan pemilik data,	A.5.1.1 A.6.1.1 A.8.3.2 A.18.1.1 A.18.1.2 A.18.1.4

	data pribadi, proses periode penyimpanan data pribadi dan penghapusan/pemusnahannya, proses untuk mengungkapkan data pribadi atas permintaan aparat penegak hukum	dan proses pengungkapan data pribadi atas permintaan aparat penegak hukum.	

Saat ini belum menetapkan kebijakan keamanan informasi yang terkait dengan manajemen risiko dan pengelolaan keamanan bagi pihak ketiga. Kebijakan tersebut meliputi mengidentifikasi risiko keamanan informasi, mengkomunikasikan dan mengklarisikasi risiko, mengklarifikasi persyaratan mitigasi risiko dan menetapkan hak audit TI secara berkala yang dikomunikasikan dan disetujui dengan pihak ketiga pada dokumen kontrak. Kondisi tersebut diatas sesuai dengan kontrol Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi, A.12.7.1 tentang kontrol audit sistem informasi, A.16.1.3 tentang melaporkan kelemahan keamanan informasi, A.16.1.6 tentang belajar insiden keamanan informasi, A.7.1.1 tentang merencanakan keberlanjutan keamanan informasi, A.7.1.2 tentang menerapkan kontinuitas keamanan informasi, A.17.1.3 tentang verifikasi, tinjau dan evaluasi keberlanjutan keamanan informasi dan A.18.2.1 tentang tinjauan independen atas keamanan informasi.

Rekomendasi yang diberikan adalah perlu menetapkan kebijakan, proses dan pedoman kebijakan keamanan informasi yang mencakup kebijakan manajemen risiko keamanan informasi terkait kerja sama dengan pihak ketiga yang memuat proses mengidentifikasi risiko berkaitan dengan kerja sama bersama pihak ketiga, proses mengkomunikasian dan mengklarifikasi risiko keamanan informasi pada pihak ketiga, menetapkan proses klarifikasi syarat-syarat untuk mitigasi risiko yang ditetapkan oleh instansi dan menetapkan harapan mitigasi risiko yang diinginkan yang kemudian perlu dikomunikasikan, ditetapkan dan disetujui oleh manajemen pihak ketiga yang terlibat. Kemudian kebijakan keamanan informasi tersebut harus mancakup persyaratan pengendalian akses layanan, proses penghancuran informasi dan data yang tidak digunakan, serta mencakup *Non Disclosure Agreement* (NDA) bagi karyawan pihak ketiga yang mana kebijakan tersebut harus ditetapkan, diterbitkan, disetujui dan dikomunikasikan pada pihak ketiga dan pihak ketiga harus pertanyaan persetujuannya tercantum pada dokumen kontrak. Kemudian pada dokumen kontrak dengan pihak ketiga, harus melakukan audit TI sebagai bagian dari syarat kontrak yang dikomunikasikan serta disetujui oleh pihak ketiga untuk keamanan informasi dan keberlangsungan manajemen keamanan informasi

serta memastikan keberlanjutan keaamanan informasi untuk meminimalisir gangguan pada proses bisnis yang berlangsung.

Selanjutnya, pihak ketiga belum melakukan pengidentifikasian terhadap risiko terkait dengan subkontraktor, penyedia layanan atau infrastruktur yang dipakai dan pengalihan daya, belum menerapkan pengendalian risiko dalam perjanjian dan belum melakukan pemantauan terhadap kepatuhan subkontraktor, penyedia layanan atau infrastruktur yang dipakai dan alih daya daya. Kondisi tersebut diatas sesuai dengan kontrol Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi dan A.14.2.7 tentang pengembangan yang dialih dayakan. Rekomendasi yang diberikan adalah perlu ditetapkannya kebijakan, pedoman, proses dan strategi terkait dengan pengelolaan sub-kontraktor/alih daya pada pihak ketiga. Kebijakan tersebut mencakup proses pengidentifikasian terkait risiko alih daya, subkontraktor atau penyedia teknologi dan proses pengendalian risikonya. Kemudian menetapkan proses untuk memantau dan mengevaluasi kepatuhan alih subkontraktor, penyedia layanan atau infrastruktur dan alih daya berdasarkan syarat keamanan yang ditentukan. Kemudian dalam menjalankan kebijakan tersebut, instansi harus mengawasi kepatuhan pengelolaan subkontraktor/alih daya yang dilakukan oleh pihak ketiga. Kebijakan tersebut harus ditetapkan, disetujui, diterbitkan, serta dikomunikasikan pada pihak ketiga agar mudah dipahami.

Berkaitan dengan pengelolaan layanan dan keamanan pihak ketiga, saat ini ditetapkan kebijakan, proses, prosedur pengelolaan dan pemantauan layanan dan aspek keamanan informasi dengan pihak ketiga. Hal ini mencakup menetapkan peran dan tanggung jawab untuk memantau, mengevaluasi dan melakukan audit aspek keamanan informasi, ketersediaan laporan secara rutin terkait pencapaian sasaran tingkat layanan (SLA), penjadwalan rapat secara berkala untuk dilakukan pemantauan dan mengevaluasi ketercapaian sasaran tingkat layanan untuk melakukan dokumentasi, mengkomunikasikan dan menindaklanjuti hasil pamantauan dan evaluasi, melakukan perencanaan audit pemenuhan persyaratan keamanan informasi dan menindaklanjuti hasil audit dengan melaporkan rencana perbaikan terukur dan menerapkan denda atau penalti terhadap ketidakpatuhan pihak ketiga pada syrat dan/tingkat layanan yang telah ditetapkan. Kondisi tersebut diatas sesuai dengan kontrol Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi, 6.1.1 tentang peran dan tanggung jawab keamanan informasi dan A.12.7.1 tentang kontrol audit sistem informasi.

Rekomendasi yang diajukan adalah perlu ditetapkannya kebijakan, proses, pedoman, dan strategi terkait dengan pengelolaan layanan dalam hubungan dengan pihak ketiga termasuk untuk melakukan pengamanan aset informasi dan infrastruktur milik instansi/perusahaaan. Kemudian Dinas Komunikasi dan Informatika Kabupaten Kediri perlu mendefinisikan peran dan tanggung jawab untuk memantau, mengevaluasi dan melakukan audit aspek keamanan informasi pihak ketiga. Peran dan tanggung jawab tersebut harus tercantum dalam uraian

tugas, kebijakan keamanan informasi, buku pegangan karyawan, kontrak kerja, kontrak layanan dan lain-lain. Kemudian perlu mencatat, dan mendokumentasikan laporan ketercapaian sasaran tingkat layanan serta aspek keamanan tercantum dalam perjanjian kontrak. Laporan tersebut dipantau secara rutin dan dievaluasi pencapaiannya dan harus ditindaklanjuti oleh pihak ketiga dan harus melaporkan kemajuannya kepada instansi terkait. Kemudian Dinas Komunikasi dan Informatika Kabupaten Kediri harus menetapkan jadwal secara berkala untuk melakukan audit persyaratan keamanan informasi oleh pihak ketiga. Syarat-syarat dan audit ini harus melibatkan verifikasi sistem operasional harus yang direncanakan secara waspada untuk meminimalkan gangguan proses bisnis dan layanan. Hasil audit yang telah dilakukan harus didokumentasikan untuk ditindaklanjuti oleh pihak ketiga dengan menetapkan perbaikan-perbaikan serta untuk dilaporkan kepada pimpinan instansi. Pada pengelolaan layanan ini, instansi harus menetapkan prosedur disipliner formal untuk mengambil tindakan berupa denda atau penalti sesuai dengan yang ditetapkan instansi kepada pihak ketiga apabila terjadi ketidakpatuhan terhadap persyaratan dan/atau tingkat layanan. Prosedur ini harus didokumentasikan, dikomunikasikan agar mudah dimengerti oleh pihak terkait.

Terkait dengan pengelolaan perubahan layanan dan kebijakan pihak ketiga, saat ini belum dilakukan pengelolaan perubahan (perubahan layanan, perubahan kebijakan, kontrol risiko) dan belum mengkaji, dokumentasi dan menetapkan rencana mitigasi baru terhadap risiko. Kondisi tersebut diatas sesuai dengan kontrol Annex A A.5.1.2 tentang tinjau kebijakan untuk keamanan informasi dan 15.2.2 tentang mengelola perubahan pada layanan pemasok. Rekomendasi yang diberikan adalah perlu menetapkan proses untuk mengelola perubahan dalam hubungan dengan pihak ketiga yang mencakup proses untuk mengubah layanan pihak ketiga, perubahan terhadap prosedur, kontrol dan kebijakan pihak ketiga. Proses pengelolaan perubahan tersebut harus dilakukan pada jadwal yang ditentukan atau ketika apabila perubahan yang signifikan dengan melakukan peninjauan serta kekritisan informasi bisnis, proses dan sistem yang terlibat dan penilaian ulang terhadap risiko harus dipertimbangkan dengan baik. Proses perubahan dalam hubungan pihak ketiga tersebut harus mengidentifikasi, mendokumentasi, mengkaji kemungkinan risiko mungkinan dapat terjadi di masa depan serta harus mengidentifikasi rencana mitigasi yang akan diterapkan guna untuk mengurangi dampak yang terjadi sesuai yang ditetapkan.

Pada aspek penanganan aset, saat ini pihak ketiga belum memiliki mekanisme secara resmi untuk penanganan data selama siklus hidupanya yang mencakup membuat, mendaftar, mengubah, menghapus dan menghancurkan aset dan menerapkan mekanisme untuk menghancurkan data yang aman belum disepakati dengan pihak ketiga. Kondisi tersebut diatas sesuai dengan kontrol Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi, A.8.3.1 tentang pengelolaan media yang dapat dilepas, dan A.8.3.2 tentang pembuangan media. Rekomendasi yang diberikan adalah perlu menetapkan kebijakan,pedoman dan prosedur terkait dengan pengelolaan dan penyimpanan data selama dalam siklus

hidup yaitu proses penyusunan, proses pendaftaran, perubahan dan dan proses penghapusan atau penghancuran aset yang aman yang kemudian proses tersebut harus dikomunikasikan dan disepakati bersama dengan pihak ketiga terkait. Proses pengelolaan dan penghancuran aset tersebut harus dibuktikan pencatatan.

Terkait dengan pengelolaan insiden oleh pihak ketiga, saat ini belum memiliki prosedur untuk melakukan melaporkan, memantau, menangani dan menganalisis insiden keamanan informasi serta dokumen bukti yang sessuai dalam penanganan insiden keamanan informasi. Kondisi tersebut diatas sesuai dengan kontrol Annex A A.16.1.2 tentang pelaporan kejadian keamanan informasi, A.16.1.4 tentang penilaian dan keputusan tentang kejadian keamanan informasi, A.16.1.5 tentang tanggapan terhadap insiden keamanan informasi, A.16.1.6 tentang belajar dari insiden keamanan informasi dan A.16.1.7 tentang pengumpulan bukti. Rekomendasi yang diberikan adalah Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan prosedur terkait dengan mengelola insiden keamanan informasi yang meliputi pelaporan, pemantauan, menangani insiden keamanan informasi secara tepat. Insiden keamanan informasi harus didokumentasikan, kemudian harus melakukan pelaporan melalui saluran manajemen yang cepat, dicatat, dianalisis, diputuskan, dinilai, ditangani sebagai bukti kepatuhan dalam menyelesaikan insiden kegagalan keamanan informasi.

Rencana kelangsungan layanan pihak ketiga saat ini belum diterapkan. Hal ini mencakup prosedur, kebijakan atau rencana tertulis untuk mengatasi kelangsungan layanan pihak ketiga pada keadaan darurat. Kemudian kebijakan, prosedur atau keberlangsungan layanan belum diuji coba, didokumentasi hasil dan dievaluasi keefektifitasannya serta pihak ketiga belum mempuyi tim yang bertugas dalam proses pengelolaan kelangsungan layanan. Kondisi tersebut diatas sesuai dengan kontrol Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi, A.17.1.1 tentang merencanajan keberlanjutan keamanan informasi, A.17.1.2 tentang menerapkan kontinuitas keamanan informasi dan A.17.1.3 tentang verifikasi, tinjau, dan evaluasi keberlanjutan keamanan informasi. Rekomendasi yang diberikan adalah harus menetapkan kebijakan, prosedur atau rencana tertulis yang berguna mengatasi keberlangsungan layanan pihak ketiga pada kondisi darurat dengan ditentukannya persyaratan untuk keamanan informasi serta kelangsungan manajemen keamanan informasi. Kemudian kebijakan, prosedur atau rencana tersebut harus di verifikasi, ditinjau, ujioba, didokumentasikan hasilnya serta dievaluasi efektivitasnya untuk memastikan bahwa kebijakan tersebut valid dan efektif. Kemudian dalam pelaksanaan kelangsungan layanan, pihak ketiga harus mendefinisikan peran dan tanggung jawab serta menunjuk penanggung jawab atau membentuk tim yang bertugas untuk melakukan pengelolaan terhadap proses keberlangsungan layanan terkait dan mencakup pelaporan, pemantauan kelangsungan layanan.

Pada pengamanan layanan infrastruktur awan, saat ini belum menetapkan kebijakan, pedoman dan prosedur terkait dengan pengamanan layanan infrastruktur awan. Hal ini meliputi pelaksanaan kajian risiko penggunaan layanan, menetapan data yang diolah pada layanan, pengamanan data pribadi pada layanan berbasis *cloud*, proses pengkajian penggunaan layanan, penjadwalan mengevaluasi penyelenggara layanan, penetapan standar keamanan teknis penggunaan layanan *cloud*, evaluasi kelayakan keamanan layanan *cloud*, proses pergantian layanan, proses pelaporan insiden layanan dan proses menghentikan layanan *cloud*. Kondisi tersebut diatas sesuai dengan kontrol Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi, A.8.2.3 tentang penanganan aset, A.16.1.2 tentang pelaporan kejadian keamanan informasi, A.18.1.1 tentang identifikasi peraturan perundangan yang berlaku dan persyaratan kontrak, dan A.18.1.4 tentang privasi dan perlindungan informasi identitas pribadi.

Rekomendasi yang diberikan adalah perlu menetapkan kebijakan, prosedur, proses dan pedoman terkait dengan pengamanan layanan infrastruktur awan. Kebijakan, prosedur, proses dan pedoman tersebut mencakup proses kajian risiko terkasit penggunaan layanan infrastruktur awan, penetapan daftar data atau informasi yang dipertukarkan melalui layanan, proses pengamanan data pribadi yang dipertukarkan melalui layanan. Kemudian menetapkan proses pengkajian dan penetapan kriteria untuk memastikan aspek hukum penggunaan layanan, menetapkan dan melaksanakan evaluasi terhadap penyelenggara layanan, instansi perlu menetapkan standar keamanan teknis penggunaan layanan yang disetujui, menetapkan proses untuk mengevaluasi kelayakan keamanan layanan untuk pemenuhan sertifikasi. Kemudian instansi perlu menetapkan proses untuk mengganti layanan cloud apabila terjadi gangguan, menetapkan proses pelaporan insiden terkait layanan dan eskalasi pelaporannya serta menetepkan proses penghentian layanan. Kemudian pimpinan instansi perlu menetapkan, menyetujui, menerbitkan dan mengkomunikasian kebijakan, prosedur, proses dan pedoman pada pihak yang relevan agar mudah dipahami.

Pada aspek perlindungan data pribadi, saat ini belum menerapkan perlindungan data pribadi. Yang meliputi dokumentasi terhadap bentuk dan jenis data pribadi yang ditukar dengan pihak eksternal, melakukan pemetaan alur pemrosesan data internal dan pertukaran data, menetapkan proses penyimpanan dan mendokumentasikannya, menetapkan kebijakan perlindungan data pribadi, penetapan penanggung jawab penerapan kebijakan dan proses perlindungan data pribadi, menganalisa dampak terungkapnya data pribadi, melakukan kajian risiko keamanan perlindungan data pribadi, menetapkan program peningkatan pemahaman tentang perlindungan data pribadi, menetapkan proses pelaporan insiden terungkapnya data pribadi, proses menjamin hak pemilik data pribadi, proses validasi dan verifikasi data pribadi, proses periode penyimpanan data pribadi dan penghapusan/pemusnahannya, proses mengungkapkan data pribadi atas permintaan aparat penegak hukum.

Kondisi tersebut diatas sesuai dengan kontrol Annex A A.5.1.1 tentang kebijakan untuk keamanan informasi, A.6.1.1 tentang peran dan tanggung jawab keamanan informasi, A.8.3.2 tentang pembuangan media, A.18.1.1 tentang identifikasi peraturan perundangan yang berlaku dan persyaratan kontrak, A.18.1.2 tentang hak kekayaan intelektual dan A.18.1.4 tentang privasi dan perlindungan informasi identitas pribadi.

Rekomendasi yang diberikan adalah harus menetapkan kebijakan, prosedur, pedoman dan proses terkait dengan perlindungan data pribadi yang dalam penerapannya sesuai dengan keperluan mitigasi risiko. Kebijakan tersebut mencakup proses mendokumentasikan jenis dan bentuk data pribadi, menetapkan proses penyimpanan, pengolahan, dan pertukaran data dengan pihak eksternal dan didokumentasikan. Selanjutnya, perlu menetapkan penanggung jawab dan mendefinisikan peran dan tanggung jawab yang memiliki kewenangan dalam menerapkan kebijakan dan proses perlindungan data pribadi, menetapkan program khusus terkait peningkatan pemahaman/kepedulian terkait dengan perlindungan data pribadi, menetapkan proses persetujuan pemilik data pribadi untuk melakukan tindakan mendapatkan, pengumpulan data, pengolahan, menganalisis data, melakukan penyimpanan data, menampilkan data, mengumumkan, mengirim, dan menyebarluaskan serta kerasahasian atau ketidakrahasiaan data pribadi yang dapat dinyatakan dalam pernyataan tertulis secara elektronik/manual, proses pelaporan insiden terungkapnya data pribadi, proses menjamin hak pemilik data, menetapkan proses validasi dan verifikasi data pribadi, menetapkan proses periode penyimpanan data pribadi, menetapkan proses penghapusan/pemusnahan data yang tidak diperlukan atau atas permintaan pemilik data, menetapkan proses untuk mengungkapkan data pribadi atas permintaan aparat penegak hukum. Yang mana pimpinan harus menetapkan, menyetujui, menerbitkan dan mengkomunikasikannya kepada pihak eksternal dan karyawan.

Berdasarkan dari penjabaran diatas, dapat disimpulkan bahwa pada area suplemen, Dinas Komunikasi dan Informatika Kabupaten Kediri perlu menetapkan kebijakan keamanan informasi yang berkaitan dengan manajemen risiko dan untuk mengelola keamanan bagi pihak ketiga, kebijakan dan proses terkait dengan pengelolaan alih daya atau sub-kontraktor/alih daya pada pihak ketiga, kebijakan dan proses pengelolaan layanan dalam hubungan dengan pihak ketiga dan pengamanan aset informasi dan infrastruktur milik instansi, proses mengelola perubahan dalam hubungan pihak ketiga yang diterapkan pada interval yang ditentukan atau apabila terdapat perubahan yang signifikan, kebijakan dan prosedur pengelolaan dan penyimpanan data selama dalam siklus hidup dan penghapusan atau penghancuran aset yang aman, prosedur terkait dengan mengelola insiden keamanan informasi yang meliputi pelaporan, pemantauan, penanganan insiden keamanan informasi secara tepat, menetapkan kebijakan, prosedur atau rencana yang terdokumentasi yang berguna mengatasi keberlangsungan layanan pihak ketiga pada keadaan darurat/bencana dengan menentukan persyaratan untuk keamanan informasi

serta kelangsungan manajemen keamanan informasi. Kemudian perlu menetapkan kebijakan, prosedur, proses dan pedoman mencakup proses kajian risiko terkait penggunaan layanan infrastruktur awan, penetapan daftar data atau informasi yang dipertukarkan melalui layanan, proses pengamanan data pribadi yang dipertukarkan melalui layanan, dan menetapkan kebijakan, prosedur, pedoman dan proses terkait dengan perlindungan data pribadi yang dalam penerapannya berdasarkan keperluan mitigasi risiko dan peraturan perundangan yang berlaku .

BAB 6 PENUTUP

6.1 Simpulan

1. Hasil evaluasi terhadap tingkat kelengkapan penerapan standar ISO 27001 memperoleh skor "163" yang berada dalam area berwarna **"Merah"** dan dikategorikan sebagai **"Tidak Layak"** untuk menerapkan sertifikasi ISO/IEC 27001:2013**.** Pencapaian tingkat kematangan area tata kelola keamanan informasi adalah I+, tingkat kematangan area pengelolaan risiko adalah I, tingkat kematangan area kerangka kerja keamanan informasi adalah I, tingkat kematangan area pengelolaan aset informasi adalah I+, tingkat kematangan area teknologi dan keamanan informasi adalah I+.
2. Berdasarkan dari analisis yang dilakukan, diperoleh beberapa rekomendasi yang diajukan pada Dinas Komunikasi dan Informatika Kabupaten Kediri sebagai dasar untuk meningkatkan pengamanan informasi pada instansi. Pada Area tata kelola keamanan informasi terdapat 17 rekomendasi, pada area pengelolaan risiko keamanan informasi terdapat 16 rekomendasi, pada area kerangka kerja keamanan informasi terdapat 28 rekomendasi, pada area pengelolaan aset informasi terdapat 32 rekomendasi, pada area teknologi dan keamanan informasi terdapat 15 rekomendasi dan pada area suplemen terdapat 9 rekomendasi.

6.2 Saran

1. Melakukan peninjauan ulang menggunakan Indeks KAMI setidaknya 2 kali dalam setahun terhadap kesiapan pengamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Kediri untuk mengukur keberhasilan inisiatif perbaikan yang diterapkan pada penelitian ini.
2. Pada penelitian selanjutnya dilakukan menggunakan responden yang lebih kompeten, sesuai dengan tugas dan tanggung jawab agar lebih memahami terkait dengan kondisi keamanan informasi.

DAFTAR REFERENSI

Badan Siber dan Sandi Negara, 2019. Indeks Keamanan Informasi (Indeks KAMI).

Bupati Kediri Provinsi Jawa Timur. 2016. Peraturan Bupati Kabupaten Kediri Nomor 51 Tahun 2016. Tentang Kedudukan, Susunan Organisasi, Uraian Tugas dan Fungsi serta Tata Kerja Dinas Komunikasi dan Informatika Kabupaten Kediri.

Alter, S., 2008. Defining Information Systems as Work Systems : Implications for the IS Field. *Europan Journal of Information Systems*, pp.448-69.

Bachri, B.S., 2010. *Meyakinkan Validitas Data Melalui Triangulasi Pada Penelitian Kualitatif*. [Online] Available at: http://yusuf.staff.ub.ac.id/files/2012/11/meyakinkan-validitas-data-melalui-triangulasi-pada-penelitian-kualitatif.pdf [Accessed 16 Oktober 2020].

Cronholm, S. & Göbel, H., 2016. Evaluation of the Information Systems Research Framework: Empirical Evidence form a Design Science Research Project. *The Electronic Journal Information Systems Evaluation*, 19(3), pp.158-68.

Chronholm, S. & Goldkuhl, G., 2003. Strategies for Information Systems Evaluation- Six Generic Types. *Electronic Journal of Information Systems Evaluation*, 6(2), pp.1-13.

Ferdiansyah, P., Subektiningsih & Indrayani, R., 2019. Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI 4.0 Pada Lembaga UPTD XYZ. *Jurnal Mobile and Forensics*, 1(2), pp.1-10.

Hambali & Musa, P., 2020. Analysis Of Governance Security Management Information System Using Index KAMI in Central Government Institution. *Angkasa: Jurnal Ilmiah Bidang Teknologi*, pp.89-98.

Hasan, F.F., 2019. A review Study of Information Systems. *International Journal of Computer Applications*, 179(18), pp.15-19.

Helaluddin & Wijaya, H., 2019. *Analisis Data Kualitatif: Sebuah Tinjauan Teori & Praktik*. [Online] Sekolah Tinggi Theologia Jaffray Available at: https://books.google.co.id [Accessed 16 Oktober 2020].

IBISA, 2011. *Keamanan Sistem Informasi*. Yogyakarta: Andi.

Juliharta, I.G., Werthi, K.T. & Astawa, N.L., 2020. Penilaian Keamanan Informasi E-Government Menggunakan Index Keamanan Informasi (KAMI) 4.0. *Jurnal Teknologi Informasi dan Kompute*, pp.238-44.

O'brien, J.A., 2005. *Pengantar Sistem Informasi: Perspektif Bisnis dan Manajerial*. 12th ed. Jakarta: Salemba Empat.

Pamungkas, W.C. & Saputra, F.T., 2020. Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001:2013. *Jurnal Sistem Komputer dan Informatika (JSON)*, pp.101-06.

Pimenov, D.Y., Syreyshchikova, N.V., Mikolajczyk, t. & Moldovan, L., 2019. Information Safety Process Development According to ISO 27001 for an Industrial Enterprise. In *The 12th International Conference Interdisciplinarity in Engineering*. Romania, 2019. Procedia Manufacturing 32.

Pritchard, C.L., 2015. *Risk Management: Concepts and Guidance Fiftt Edition*. Boca Raton: CRC Press.

Rahardjo, B., 1998. *Keamanan Sistem Informasi Berbasis Internet*. Bandung: PT Insan Komunikasi.

Riswaya, A.R., Sasongko, A. & Maulana, A., 2020. Evaluasi Tata Kelola Keamanan Teknologi Informasi Menggunakan Indeks KAMI Untuk Persiapan SNI ISO/IEC 27001 (Studi Kasus: STMIK Mardadira Indonesia). *Jurnal Computech & Bisnis*, pp.10-18.

Siregar, A.Z. & Harahap, N., 2019. *Strategi dan Teknik Penulisan Karya Tulis Ilmiah Publikasi*. Sleman: Deepublish.

Sutabri, T., 2012. *Konsep Sistem Informasi*. Yogyakarta: Penerbit Andi.

Syreyshchikova, N.V., Yu., D.P., Mikolajczyk, T. & Moldovan, L., 2019. Information Safety Process Development According to ISO 27001 for an Industrial Enterprise. In *The 12th International Conference Interdisciplinarity in Engineering*. Romania, 2019. Procedia Manufacturing 32.

Thompson, N., Mullins, A. & Chongsutakawewong, T., 2019. Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand. *Government Information Quartely*, pp.1-9.

Tim Direktorat Keamanan Informasi kementerian Komunikasi dan Informatika RI, 2017. *Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi* (Indeks KAMI). KOMINFO.

Tim Direktorat Keamanan Informasi kementrian Komunikasi dan Informatika RI. 2011. *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik*. KOMINFO.

LAMPIRAN A TRANSKRIP WAWANCARA

Nama Instansi	Dinas Komunikasi dan Informatika Kabupaten Kediri
Hari/Tanggal	16 Oktober 2020
Jam wawancara	09.00-10.00
Nama Responden	Arik Fefriyono, A.Md
jabatan	Pengelola Keamanan Sistem Informasi / Seksi Sandi dan Keamanan Teknologi Informasi

Pertanyaan
1. Apakah Diskominfo Kab Kediri telah memiliki Dokumen SMKI? Apabila memiliki, bagaimana penerapannya? Apakah penerapan berjalan dengan baik?
Jawaban: Belum memiliki dokumen terkait dengan Sistem Manajemen Keamanan Informasi (SMKI).
2. Apakah Diskominfo Kab Kediri telah melakukan sertifikasi ISO/IEC 27001:2013 atau melakukan pernah melakukan penilaian Sistem Manajemen Keamanan Informasi yang dilakukan oleh BSSN menggunakan Indeks KAMI?
Jawaban: Belum melakukan sertifikasi ISO/IEC 27001:2013, saat ini sedang merencakan untuk melakukan sertifikasi tersebut. untuk penilaian Sistem Manajemen Keamanan Informasi belum pernah dilakukan.
3. Apakah ada permasalahan pada bagian keamanan informasi yang dapat menimbulkan ancaman risiko keamanan informasi? Contohnya permasalahan seperti apa? Cara mengatasinya bagaimana? Dan dampak dari permasalahannya seperti apa?
Jawaban : iya ada, sering terjadi malware, serangan/hack pada aplikasi dan website yang dikelola diskominfo.
4. Apakah Diskominfo Kabupaten Kediri sudah memiliki kebijakan secara khusus yang mengatur tentang keamanan informasi?
Jawaban: untuk kebijakan secara khusus mengatur keamanan informasi belum memiliki, saat ini hanya mengacu pada Peraturan bupati tentang SPBE kabupaten Kediri
5. Apakah saat ini Diskominfo Kab kediri mengelola data center? Apabila iya, Data center apa saja yang dikelola? Apabila tidak, apakah kedepannya telah direnakan Diskominfo akan mengelola suatu Data Center?
Jawab : Iya, Data Center Website dari SKPD, Kecamatan dan Desa.

Mengetahui,
Responden

Arik Fefriyono, A.Md
NIP 19870215 201903 1005

LAMPIRAN B VALIDASI CHECKLIST

Indeks Keamanan Informasi (Indeks KAMI)

Identitas Instansi atau Perusahaan Dinas Komunikasi dan Informatika Kapupaten Kediri

Alamat Jl. Sekartaji No 2, Doko, Kec. Ngasem, Kab. Kediri

Nomor Telepon

Email

Pengisi Lembar Evaluasi Arik Fefriyono

Jabatan Pengelola Keamanan Sistem Informasi

Tanggal Pengisian 2 November 2020

Deskripsi Ruang Lingkup

Isi dengan deskripsi ruang lingkup struktur organisasi (Departemen, Bagian atau Satuan Kerja) dan infrastruktur TIK

- Pengelolaan infrastruktur TIK (termasuk IS server) yang ada dilakukan oleh Diskominfo Kab. Kediri
- Tanggung Jawab Diskominfo dalam mengelola infrastruktur hanya sebatas Pada SKPD Induk Kantor & Kecamatan

Mengetahui,
Responden

Arik Fefriyono A.Md
NIP 19870215 201903 1005

Bagian II: Tata Kelola Keamanan Informasi

Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				Status	NOMOR DOKUMEN	NAMA DOKUMEN
#	Fungsi/Organisasi Keamanan Informasi					
2.1	II	1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	D	Nomor 51 tahun 2016	Peraturan Bupati Kabupaten Kediri
2.2	II	1	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	D	Nomor 51 tahun 2016	Peraturan Bupati Kabupaten Kediri
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	D	Nomor 51 tahun 2016	Perbup Kab. Kediri tentang Kedudukan, Susunan
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	D		Rencana Strategis (Renstra) 2016 - 2021
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	A		
2.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	B		
2.7	II	1	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	C		Tidak ada
2.8	II	1	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	D		Foto Kegiatan Sosialisasi
2.9	II	2	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	B		
2.10	II	2	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	B		
2.11	II	2	Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	B		
2.12	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	B		
2.13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	B		

2.14	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	B		
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?	B		
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?	B		
2.17	IV	3	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	B		
2.18	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	A		
2.19	IV	3	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	A		
2.20	IV	3	Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?	B		
2.21	IV	3	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	B		
2.22	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	A		

Mengetahui,

Responden

Arik Fefriyono A.Md

NIP 19870215 201903 1005

Bagian III: Pengelolaan Risiko Keamanan Informasi

Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan i

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	**NOMOR DOKUMEN**	**NAMA DOKUMEN**
#			**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?	A		
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?	C		
3.3	II	1	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	A		
3.4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?	A		
3.5	II	1	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	A		
3.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola *(custodian)* aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	A		
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	A		
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	A		
3.9	II	1	Apakah instansi/perusahaan anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	B		
3.10	II	1	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	B		

3.11	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?	B		
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	B		
3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	B		
3.14	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	A		
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	A		
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	A		

Mengetahui,
Responden

Arik Fefriyono A.Md
NIP 19870215 201903 1005

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi							
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.							
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh					**Status**	**NOMOR DOKUMEN**	**NAMA DOKUMEN**
#			**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**				
4.1	II	1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya?		B		
4.2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?		B		
4.3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?		A		
4.4	II	1	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?		A		
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?		B		
4.6	II	1	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?		B		
4.7	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?		A		
4.8	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?		A		
4.9	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini?		B		

4.10	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	A		
4.11	III	2	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	A		
4.12	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	C		
4.13	III	2	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?	C		
4.14	III	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?	A		
4.15	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	~~B~~ A		
4.16	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	B		
4.17	III	3	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	~~A~~ B		
4.18	IV	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan)* dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan - misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	A		
4.19	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	A		
#			**Pengelolaan Strategi dan Program Keamanan Informasi**			
4.20	II	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	C		
4.21	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	D		
4.22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	D		

4.23	III	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada	B		
4.24	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	B		
4.25	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	B		
4.26	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	B		
4.27	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?	C		analisa dilakukan secara lisan
4.28	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?	A		
4.29	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	C		- Renja 2020 - Renstra 2016 - 2021

Mengetahui,
Responden

Arik Fefriyono A.Md
NIP 19870215 201903 1005

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**	NOMOR DOKUMEN	NAMA DOKUMEN
#			**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)	C		Tidak terdapat kepemilikan aset
5.2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	A		
5.3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	B		
5.4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut	B		
5.5	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	B		
5.6	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	B		
5.7	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	A		
			Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?			
5.8	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda	B		
5.9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	C		diterapkan secara lisan
5.10	II	1	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	B		
5.11	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	C		Tidak ada bukti
5.12	II	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	A		
5.13	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	C		Tidak ada bukti

5.14	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	C		Tidak ada bukti
5.15	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	A		
5.16	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	A		
5.17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	B		
5.18	II	1	Prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala	B		
5.19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	C		Tidak ada bukti
5.20	III	2	Proses pengecekan latar belakang SDM	C		Tidak ada bukti
5.21	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	B		
5.22	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	B		
5.23	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	C		Tidak ada bukti
5.24	III	2	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	B		
5.25	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	B		
5.26	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	B		
5.27	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?	A		
#			**Pengamanan Fisik**			
5.28	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?	D		- Foto mesin finger lock - laporan pengelolaan
5.29	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	D		- Foto - laporan pengelolaan
5.30	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	D		- Foto (Genset, UPS) - laporan pengelolaan

5.31	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	D		
5.32	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	A		
5.33	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)?	A		
5.34	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?	D		- laporan pengelolaan infrastruktur TIK - Foto
5.35	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	C		- SOP Pemeliharaan Ab sensi, CCTV, perbaikan aplikasi, maintance server
5.36	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	A		
5.37	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? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	C		Tidak valid
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?	D		Tidak valid.

Mengetahui,
Responden

Arik Fefriyono A.Md
NIP 19870215 201903 1005

Bagian VI: Teknologi dan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**	**NOMOR DOKUMEN**	**NAMA DOKUMEN**
#			**Pengamanan Teknologi**			
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	D		Firewall
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	D		Screenshot Virtual LAN
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?	D		Tidak valid
6.4	II	1	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	C		Tidak Valid
6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	D		Tidak valid
6.6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	C		- laporan pengelolaan infrastruktur TIK
6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	D		Monitoring Zabbix & Plesk
6.8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	C		SS rekaman perubahan
6.9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	C		SS log aktivitas
6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	C		Tidak terdokumentasi
6.11	II	1	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	A		
6.12	III	2	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	B		
6.13	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	A		
6.14	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?	C		Tidak ada bukti

6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	A		
6.16	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*, dan penarikan akses?	C		SS gagal untuk login
6.17	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	D		Penggunaan Firewall
6.18	II	1	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	C		screenshoot VPN
6.19	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	C		update OS Desktop
6.20	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	B		
6.21	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?	C		Tidak ada
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	D		Tidak ada
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	D		screenshoot NTP
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	B		
6.25	III	3	Apakah instansi/perusahaan ada 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?	B		
6.26	IV	3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	B		

Mengetahui,
Responden

Arik Fefriyono A.Md

Bagian VII: Suplemen

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	NOMOR DOKUMEN	NAMA DOKUMEN
7.1			**Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**			
7.1.1			**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**			
7.1.1.1		1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	A		
7.1.1.2		1	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	A		
7.1.1.3		1	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	A		
7.1.1.4		1	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	A		
7.1.1.5		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?	A		
7.1.1.6		1	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?	A		
7.1.1.7		1	Apakah hak audit TI secara berkala ke pihak ketiga/pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga? Termasuk di dalamnya akses terhadap laporan audit internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?	A		
7.1.2			**Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga**			
7.1.2.1		1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?	A		
7.1.2.2		1	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	A		
7.1.2.3		1	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?	A		
7.1.3			**Pengelolaan Layanan dan Keamanan Pihak Ketiga**			

7.1.3.1		1	Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instansi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?	A		
7.1.3.2		1	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?	A		
7.1.3.3		1	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?	A		
7.1.3.4		1	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?	A		
7.1.3.5		1	Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuannya kepada instansi/perusahaan?	A		
7.1.3.6		1	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?	A		
7.1.3.7		1	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?	A		
7.1.3.8		1	Apakah kondisi terkait denda / penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	A		
7.1.4			**Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga**			
7.1.4.1		1	Apakah instansi/perusahaan mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain? - Perubahan layanan pihak ketiga; - Perubahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?	A		
7.1.4.2		1	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	A		
7.1.5			**Penanganan Aset**			
7.1.5.1		1	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan / penghancuran aset?	A		
7.1.5.2		1	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	A		
7.1.6			**Pengelolaan Insiden oleh Pihak Ketiga**			
7.1.6.1		1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?	A		

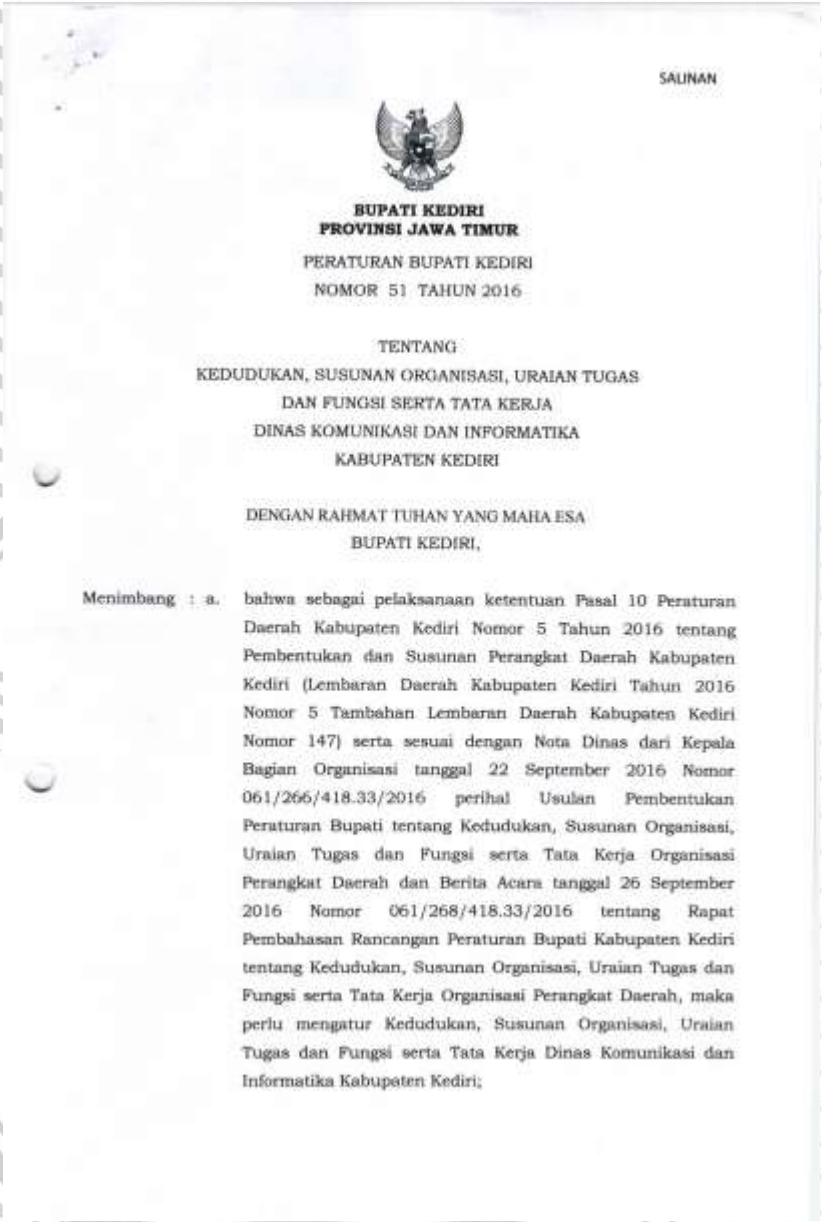
7.1.6.2		1	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	A		
7.1.7			**Rencana Kelangsungan Layanan Pihak Ketiga**			
7.1.7.1		1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?	A		
7.1.7.2		1	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	A		
7.1.7.3		1	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	A		
7.2			**Pengamanan Layanan Infrastruktur Awan (*Cloud Service*)**			
7.2.1		1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis *cloud* dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?	A		
7.2.2		1	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*?	A		
7.2.3		1	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan *cloud*?	A		
7.2.4		1	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*?	A		
7.2.5		1	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan *cloud* terkait reputasi penyelenggaranya?	A		
7.2.6		1	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan *cloud*, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	A		
7.2.7		1	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?	A		
7.2.8		1	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan *cloud* atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?	A		
7.2.9		1	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan *cloud*?	A		
7.2.10		1	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan *cloud*, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?	A		
7.3			**Perlindungan Data Pribadi**			
7.3.1		1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?	A		
7.3.2		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?	A		

7.3.3		1	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	A		
7.3.4		1	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	A		
7.3.5		1	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (*Data Protection Officer, Data Controller, Data Processor*) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?	A		
7.3.6		1	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?	A		
7.3.7		1	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	A		
7.3.8		1	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?	A		
7.3.9		1	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?	A		
7.3.10		1	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 ?	A		
7.3.11		1	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?	A		
7.3.12		1	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?	A		
7.3.13		1	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?	A		
7.3.14		1	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?	A		
7.3.15		1	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?	A		
7.3.16		1	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	A		

Mengetahui,
Responden

Arik Fefriyono A.Md
NIP 19870215 201903 1005

LAMPIRAN C DOKUMEN PENDUKUNG



SALINAN

BUPATI KEDIRI
PROVINSI JAWA TIMUR

PERATURAN BUPATI KEDIRI
NOMOR 51 TAHUN 2016

TENTANG
KEDUDUKAN, SUSUNAN ORGANISASI, URAIAN TUGAS
DAN FUNGSI SERTA TATA KERJA
DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN KEDIRI

DENGAN RAHMAT TUHAN YANG MAHA ESA
BUPATI KEDIRI,

Menimbang : a. bahwa sebagai pelaksanaan ketentuan Pasal 10 Peraturan Daerah Kabupaten Kediri Nomor 5 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Kediri (Lembaran Daerah Kabupaten Kediri Tahun 2016 Nomor 5 Tambahan Lembaran Daerah Kabupaten Kediri Nomor 147) serta sesuai dengan Nota Dinas dari Kepala Bagian Organisasi tanggal 22 September 2016 Nomor 061/266/418.33/2016 perihal Usulan Pembentukan Peraturan Bupati tentang Kedudukan, Susunan Organisasi, Uraian Tugas dan Fungsi serta Tata Kerja Organisasi Perangkat Daerah dan Berita Acara tanggal 26 September 2016 Nomor 061/268/418.33/2016 tentang Rapat Pembahasan Rancangan Peraturan Bupati Kabupaten Kediri tentang Kedudukan, Susunan Organisasi, Uraian Tugas dan Fungsi serta Tata Kerja Organisasi Perangkat Daerah, maka perlu mengatur Kedudukan, Susunan Organisasi, Uraian Tugas dan Fungsi serta Tata Kerja Dinas Komunikasi dan Informatika Kabupaten Kediri;

Gambar 1

Pada gambar 1 menunjukkan Peraturan Bupati Kediri Nomor 51 tentang Kedudukan, Susunan Organisasi, Uraian Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi dan Informatika Kabupaten Kediri. Pada peraturan ini tugas dan fungsi setiap bidang dan seksi pada Dinas Komunikasi dan Informatika Kabupaten Kediri khususnya pada seksi sandi dan keamanan teknologi informasi.

Gambar 2

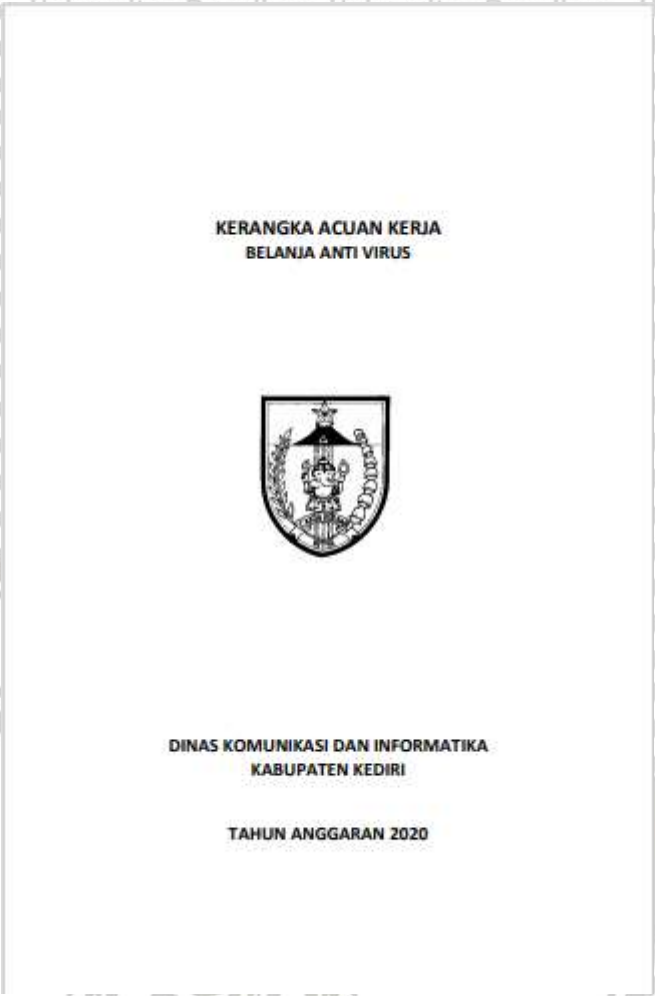
Gambar 3

Pada gambar 2 dan gambar 3 menunjukkan program sosilasi atau pelatihan sebagai ajang untuk peningkatan pemahaman keamanan informasi dengan melakukan pelatihan VPN (*Virtual Private Network*) Bendahara Gaji dan

Operator SIM Gaji SD dan SMP untuk wilayah Dinas pendidikan yang diikuti oleh 100 (seratus) peserta.

Gambar 4

Pada gambar 4 menunjukkan dokumen Rencana Strategis (RENSTRA) Dinas Komunikasi dan Informatika Kabupaten Kediri Tahun 2016-2021 yang berisikan perencanaan strategis Dinas Komunikasi dan Informatika Kabupaten Kediri serta program kegiatan yang akan dilaksanakan dalam kurun waktu 5 (lima) tahun kedepan.



KERANGKA ACUAN KERJA
BELANJA ANTI VIRUS

DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN KEDIRI

TAHUN ANGGARAN 2020

Gambar 5

Pada gambar 5 menujukkan dokumen pendukung yait Kerangka Acuan Kerja Belanja Anti Virus yang mana dokumen ini menggambarkan strategi penerapan keamanan informasi yang dilakukan dengan di terapkannya antivirus pada Komputer Server, Personal Computer dan Laptop yang ada di Dinas Komunikasi dan Informatika, SKPD dan Kecamatan yang ada di Pemerintahan Kabupaten Kediri yang terdiri dari Central Intercept X Advanced – 1000 – 1999 USERS – 12 MOS – GOV dan Central Intercept X Advanced For Server (Previously Central Server Protection Advanced) – 10-24 SERVER – 12 MOS – GOV.

Gambar 6

Pada gambar 6 laporan pengelolaan infrastruktur TIK tahun 2019 pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Laporan ini mencakup rekapitulasi terkait laporan pengelolaan jaringan internet, intranet, jaringan wireless radio, data center, laporan terkait pengelolaan fasilitas pendukung pada ruang data center seperti AC, sistem keamanan, sistem pemadam kebakaran, listrik. Selain itu terdapat laporan mengenai dokumentasi perbaikan jaringan,

pemasangan rack server, perbaikan atau pemasangan CCTV, perawatan tower, pemeliharaan atau perbaikan finger print serta pemeliharaan ruang server.


1 2 3
4 5 6
7 8 9
* 0 #
DORONG
PUSH
KARYA MANDIRI
DORONG
PUSH
KARYA MANDIRI

Gambar 7

Gambar 8

Pada gambar 7 dan gambar 8 menunjukkan pengamanan fisik pada ruang server yaitu menggunakan kunci pintu digital menggunakan *password* dan kartu serta menggunakan *finger lock*.

PEMERINTAH KABUPATEN KEDIRI
DINAS KOMUNIKASI DAN INFORMATIKA
Jl. Sekartaji No 2 Doko Kab. Kediri Telepon (0354) 682152 Fax. (0354) 692279
Website : www.kedirikab.go.id – subdomain www.diskominfo.kedirikab.go.id
K E D I R I

Nomor SOP	
Tanggal Pembuatan	18 Oktober 2019
Tanggal Revisi	
Tanggal Efektif	
Disahkan Oleh	KEPALA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN KEDIRI **KRISNA SETIAWAN, S.AP, M.SI** Pembina IV/a NIP. 19840127 200604 1 005
Nama SOP	CARA MEMASUKI SERVER DI KOMINFO PEMKAB KEDIRI

Gambar 9

Pada gambar 9 merupakan dokumen Standar Operasional Prosedur (SOP) cara memasuki ruang server. SOP cara memasuki ruang server ini berguna untuk memberikan panduan mengenai cara memasuki ruang server secara terkoordinasi.

Gambar 10

Gambar 10 menunjukkan AC pada ruang server di Dinas Komunikasi dan Informatika Kabupaten Kediri. AC yang digunakan memiliki sistem kerja setiap 4 jam sekali akan bergantian menyala untuk menjaga kestabilan suhu ruang yaitu pada 16 derajat celcius.

Gambar 11

Gambar 12

Gambar 11 dan gambar 12 merupakan alat untuk membantu *supply* listrik pada Dinas Komunikasi dan Informatika Kabupaten Kediri. Pada gambar 13 merupakan Genset (Generator Set) yang berfungsi untuk menghasilkan daya listrik. Pada gmabr 14 merupakan UPS (*Uninteruptible Power Supply*) untuk memberikan *supply* listrik ketika listrik utama tidak berfungsi (pemadaman listrik).

Gambar 13

Pada gambar 13 merupakan tabung pemadam kebakaran pada ruang center di Dinas Komunikasi dan Informatika Kabupaten Kediri. Tabung pemadam kebakaran yang digunakan adalah tipe C yang merupakan pemadam untuk jenis api dari sumber yang menghantarkan listrik.

PEMERINTAH KABUPATEN KEDIRI
DINAS KOMUNIKASI DAN INFORMATIKA
Jl. Sekartaji No 2 Doko Kab. Kediri Telepon (0354) 682152 Fax. (0354) 692279
Website : www.kedirikab.go.id – subdomain :www.diskominfo.kedirikab.go.id
K E D I R I

Nomor SOP	
Tanggal Pembuatan	27 Mei 2019
Tanggal Revisi	
Tanggal Efektif	
Disahkan Oleh	KEPALA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN KEDIRI KRISNA SETIAWAN, S.AP, M.Si Pembina IVa NIP. 19840127 200604 1 005
Nama SOP	PEMELIHARAAN MESIN ABSENSI DI KOMINFO PEMKAB KEDIRI

Gambar 14

Gambar 14 menunjukkan standar operasional prosedur (SOP) pemeliharaan mesin absensi yang dengan tujuan melakukan pemeliharaan mesin absensi agar berjalan dengan optimal sesuai dengan prosedur yang telah ditetapkan.

PEMERINTAH KABUPATEN KEDIRI
DINAS KOMUNIKASI DAN INFORMATIKA
Jl. Sekartaji No 2 Doko Kab. Kediri Telepon (0354) 682152 Fax. (0354) 692279
Website : www.kedirikab.go.id – subdomain :www.diskominfo.kedirikab.go.id
K E D I R I

Nomor SOP	
Tanggal Pembuatan	20 Mei 2019
Tanggal Revisi	
Tanggal Efektif	
Disahkan Oleh	KEPALA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN KEDIRI KRISNA SETIAWAN, S.AP, M.Si Pembina IVa NIP. 19840127 200604 1 005
Nama SOP	PEMELIHARAAN CCTV DI KOMINFO PEMKAB KEDIRI

Gambar 15

Gambar 15 menunjukkan standar operasional prosedur (SOP) pemeliharaan CCTV yang dengan tujuan melakukan pemeliharaan CCTV agar berjalan dengan optimal sesuai dengan prosedur yang telah ditetapkan.

PEMERINTAH KABUPATEN KEDIRI
DINAS KOMUNIKASI DAN INFORMATIKA
Jl. Sekartaji No 2 Doko Kab. Kediri Telepon (0354) 682152 Fax. (0354) 692279
Website : www.kedirikab.go.id – subdomain :www.diskominfo.kedirikab.go.id
K E D I R I

Nomor SOP	
Tanggal Pembuatan	20 Mei 2019
Tanggal Revisi	
Tanggal Efektif	
Disahkan Oleh	KEPALA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN KEDIRI KRISNA SETIAWAN, S.AP, M.Si Pembina IVa NIP. 19840127 200604 1 005
Nama SOP	PERBAIKAN CCTV DI KOMINFO PEMKAB KEDIRI

Gambar 16

Gambar 16 menunjukkan standar operasional prosedur (SOP) perbaikan CCTV dengan tujuan melakukan perbaikan CCTV agar memberikan prosedur yang jelas terkait perbaikan CCTV supaya proses perbaikan berjalan dengan cepat.

PEMERINTAH KABUPATEN KEDIRI
DINAS KOMUNIKASI DAN INFORMATIKA
Jl. Sekartaji No 2 Doko Kab. Kediri Telepon (0354) 682152 Fax. (0354) 692279
Website : www.kedirikab.go.id – subdomain :www.diskominfo.kedirikab.go.id
K E D I R I

Nomor SOP	
Tanggal Pembuatan	27 Mei 2019
Tanggal Revisi	
Tanggal Efektif	
Disahkan Oleh	KEPALA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN KEDIRI KRISNA SETIAWAN, S.AP, M.Si Pembina IV/a NIP. 19840127 200604 1 005
Nama SOP	PERBAIKAN MESIN ABSENSI DI KOMINFO PEMKAB KEDIRI

Gambar 17

Gambar 17 menunjukkan standar operasional prosedur (SOP) perbaikan mesin absensi dengan tujuan melakukan perbaikan mesin absensi agar memberikan prosedur yang jelas terkait perbaikan mesin absensi supaya proses perbaikan berjalan dengan cepat.

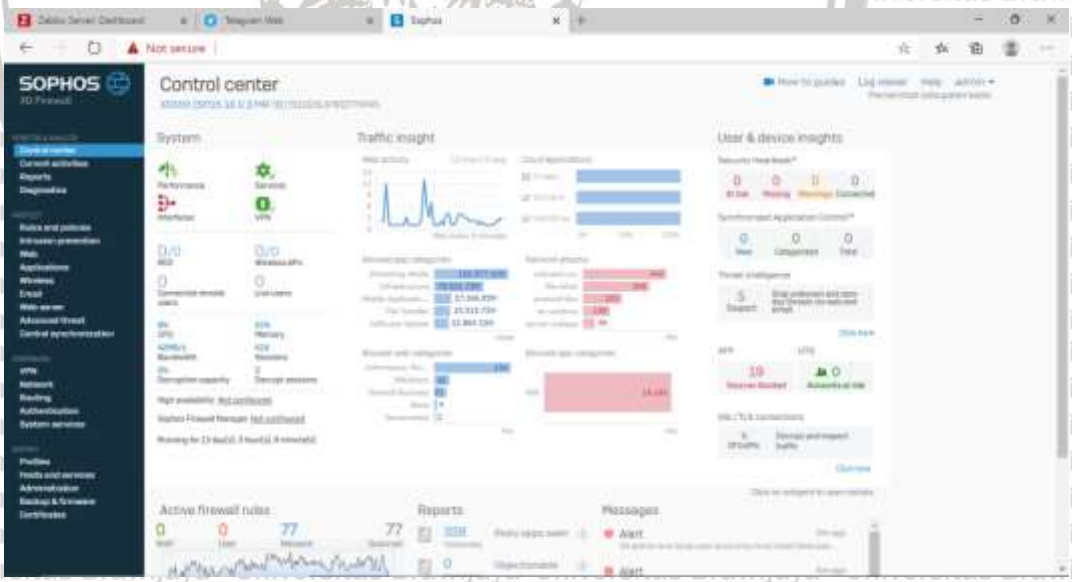
PEMERINTAH KABUPATEN KEDIRI
DINAS KOMUNIKASI DAN INFORMATIKA
Jl. Sekartaji No 2 Doko Kab. Kediri Telepon (0354) 682152 Fax. (0354) 692279
Website : www.kedirikab.go.id – subdomain :www.diskominfo.kedirikab.go.id
K E D I R I

Nomor SOP	
Tanggal Pembuatan	18 Oktober 2019
Tanggal Revisi	
Tanggal Efektif	
Disahkan Oleh	KEPALA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN KEDIRI KRISNA SETIAWAN, S.AP, M.Si Pembina IV/a NIP. 19840127 200604 1 005
Nama SOP	MAINTENANCE SERVER DI KOMINFO PEMKAB KEDIRI

Gambar 18

Gambar 18 menunjukkan standar operasional prosedur (SOP) maintenance server bertujuan untuk meremajakan serta merawat hardware dan software perangkat server beserta perangkat penunjang ruang server.

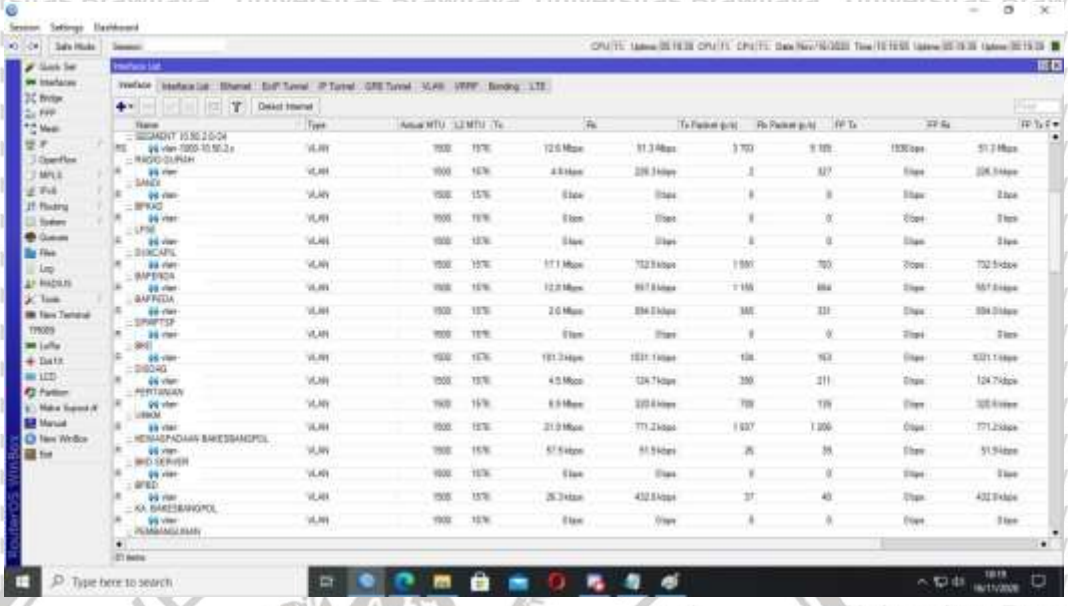
Gambar 19



Gambar 20

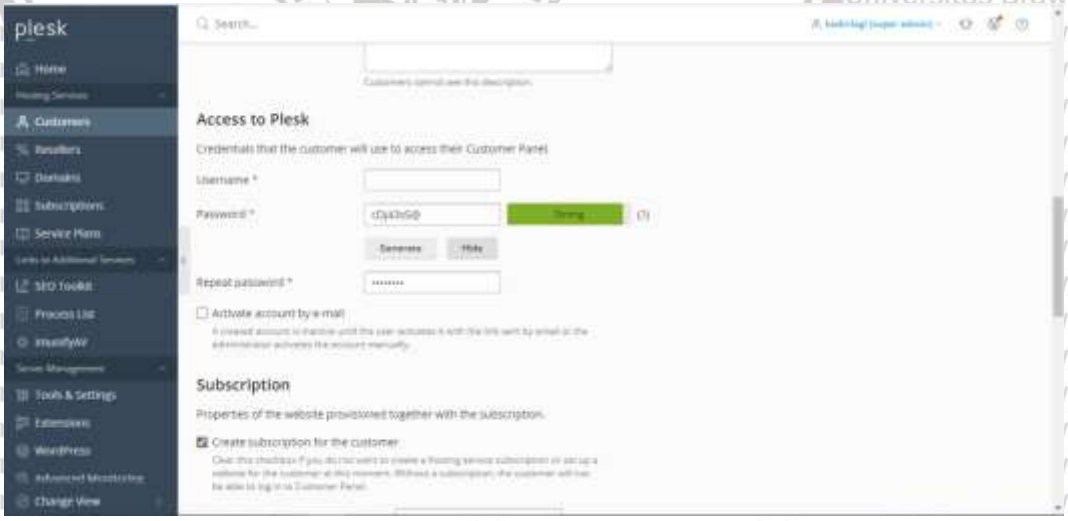
Pada gambar 19 dan gambar 20 merupakan hardware firewall serta *software* firewall yang digunakan pada Dinas Komunikasi dan Informatika Kabupaten Kediri untuk melindungi sistem komputer dari ancaman luar, firewall yang digunakan juga dapat mendektsi akses jaringan yang tidak berhak yang dilakukan

pihak luar. *Software* firewall yang digunakan pada Dinas Komunikasi dan Informatika Kabupaten Kediri adalah Shopos.

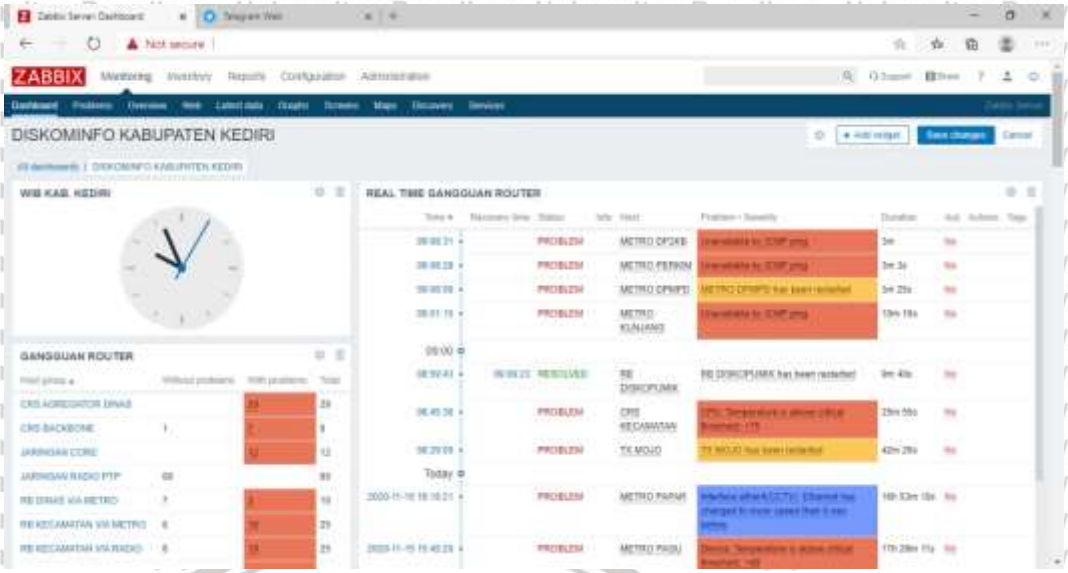


Gambar 21

Gambar 21 menunjukkan dokumen pendukung tangkapan layar Virtual LAN yang digunakan pada Dinas Komunikasi dan Informatika Kabupaten Kediri untuk membagi jaringan sesuai kebutuhan instansi, dimana pada gambar 21 sebagai contohnya pembagiannya pada Dukcapil, Radio Gurah, Bappeda, dan lain sebagainya.

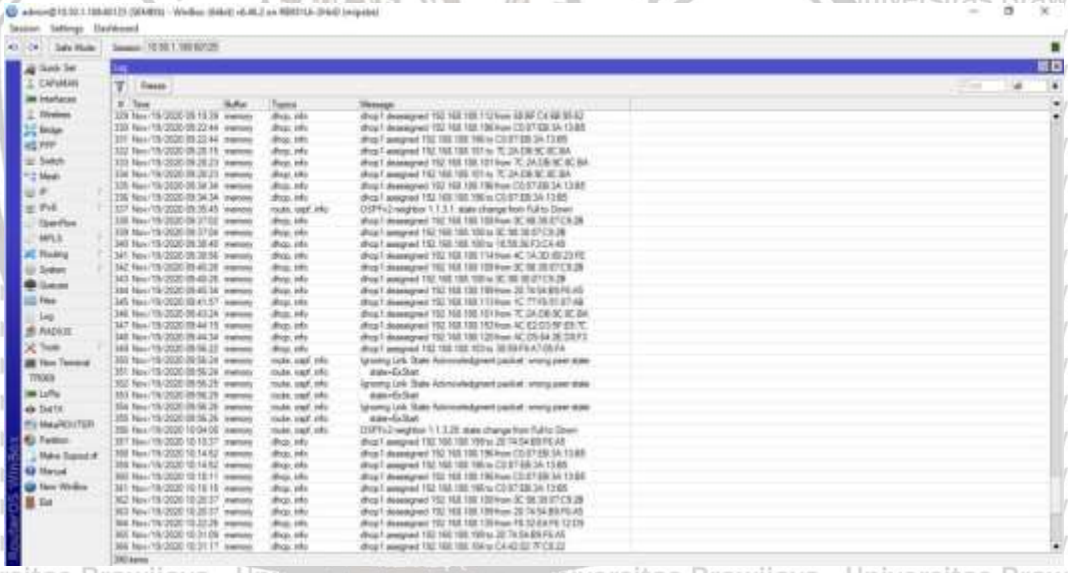


Gambar 22



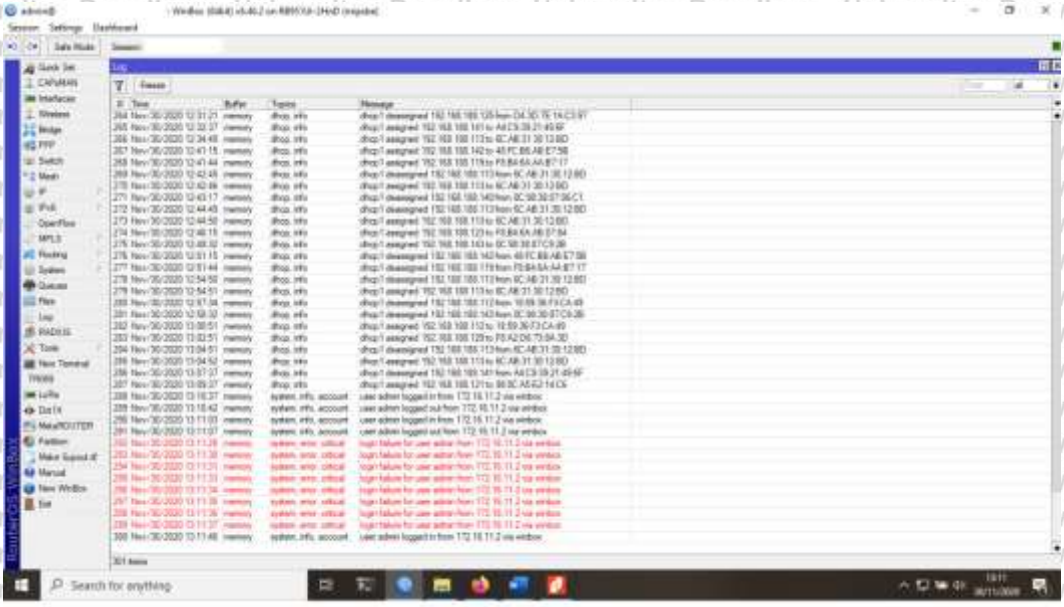
Gambar 23

Pada gambar 22 dan 23 merupakan *software* yang digunakan pada Dinas Komunikasi dan Informatika Kabupaten Kediri untuk melakukan monitoring terhadap jaringan, sistem, aplikasi serta website menggunakan Zabbix dan Plesk.



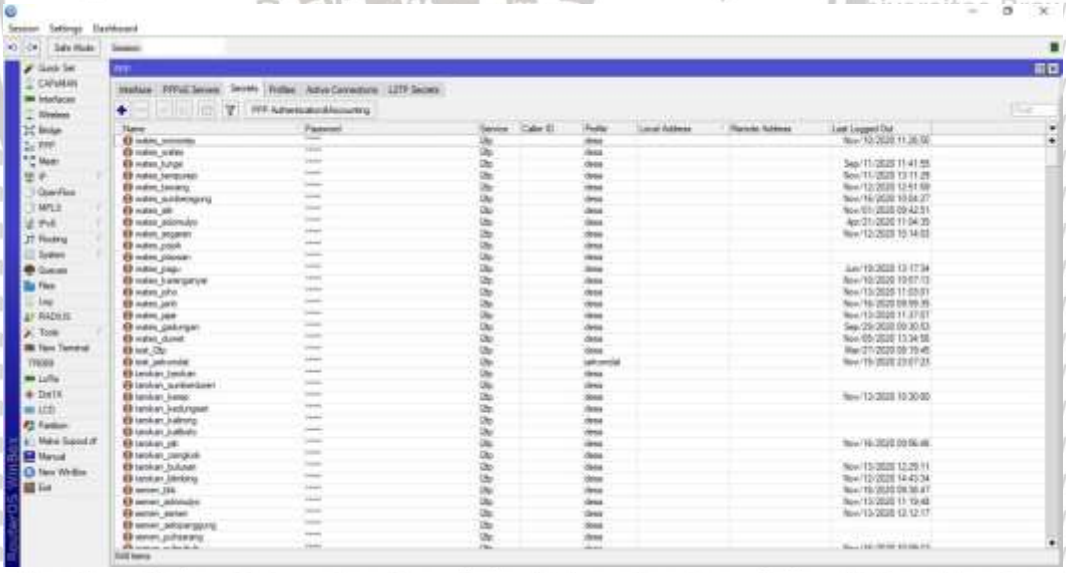
Gambar 24

Gambar 24 menunjukkan contoh salah satu log pada salah satu Kecamatan di Kabupaten Kediri yang merekam setiap aktivitas yang terjadi.



Gambar 25

Pada gambar 25 menunjukkan log perekaman aktivitas upaya akses yang tidak berwenang pada Dinas Komunikasi dan Informatika Kabupaten Kediri. pada gambar 24 menunjukkan log aktivitas gagal login yang dilakukan oleh pihak yang tidak berkepentingan.

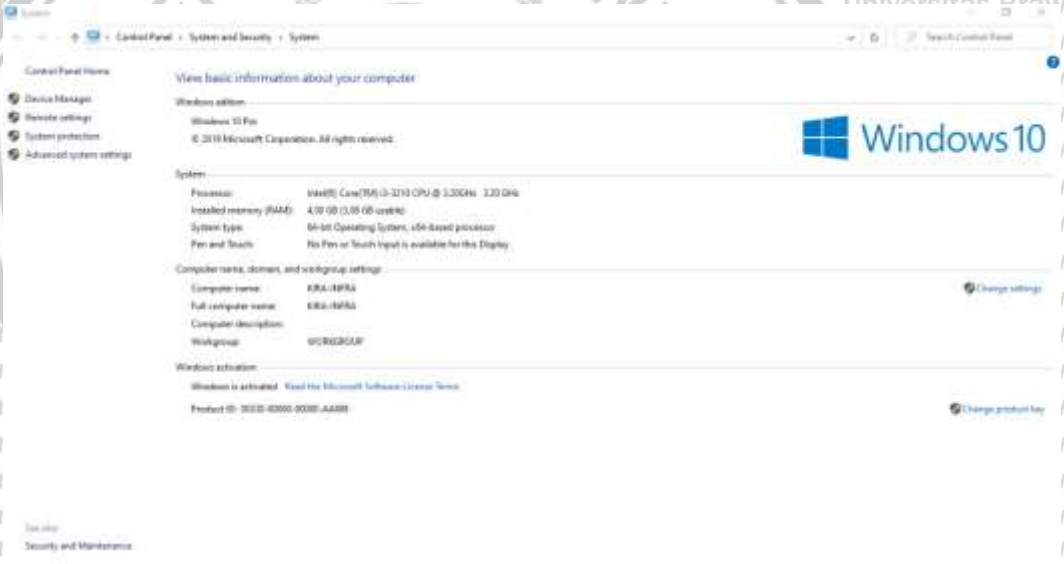


Gambar 26

Pada gambar 26 menunjukkan VPN (*Virtual Private Network*) pada Dinas Komunikasi dan Informatika Kabupaten Kediri untuk memungkinkan mengakses situs pada Dinas Komunikasi dan Informatika Kabupaten Kediri secara aman.

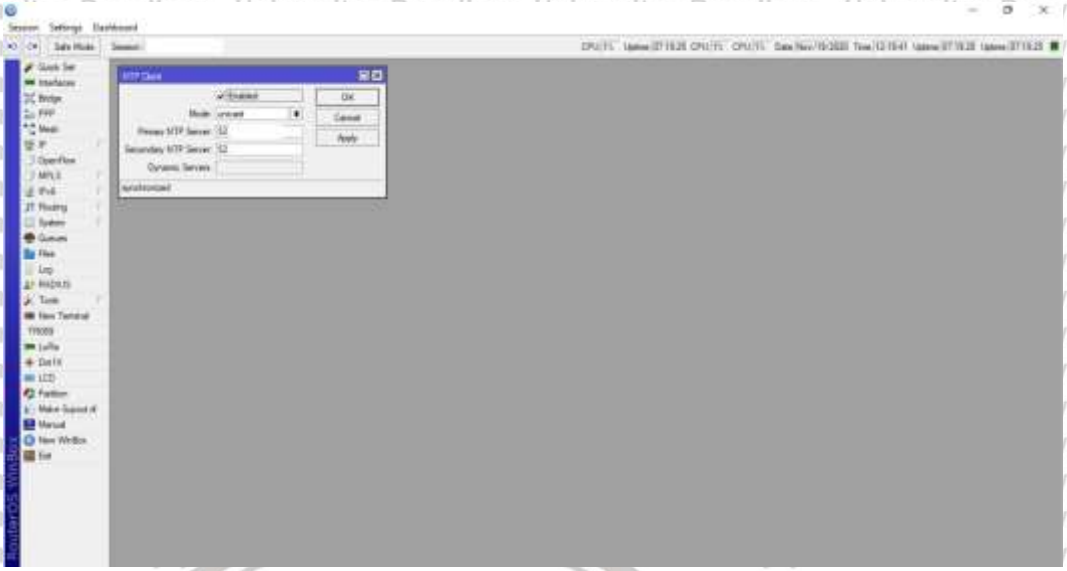
Gambar 27

Pada gambar 27 menunjukkan salah satu contoh aplikasi yang menerapkan pembatasan waktu akses dan lockout setelah kegagalan login yang mana diberikan kesempatan 4 kali untuk melakukan login, apabila gagal maka akan terkunci selama 5 menit.



Gambar 28

Pada gambar 28 merupakan tangkapan layar perangkat *desktop* yang digunakan di Dinas Komunikasi dan Informatika Kabupaten Kediri yang dimutakhirkan dengan versi terkini yaitu Windows 10.



Gambar 29

Gambar 29 menunjukkan NTP (*Network Time Protocol*) yang digunakan pada Dinas Komunikasi dan Informatika Kabupaten Kediri untuk melakukan sinkronisasi waktu pada jaringan dan sistem komputer.

LAMPIRAN D ISO ANNEX A

A.5 Kebijakan keamanan informasi		
A.5.1 Arahan manajemen untuk keamanan informasi (Kontrol Objektif)		
Tujuan: Untuk memberikan arahan manajemen dan dukungan untuk keamanan informasi sesuai dengan persyaratan bisnis dan undang-undang dan peraturan yang relevan.		
A.5.1.1	Kebijakan untuk keamanan informasi	Kontrol : Seperangkat kebijakan untuk keamanan informasi harus ditetapkan, disetujui oleh manajemen, diterbitkan dan dikomunikasikan kepada karyawan dan pihak eksternal yang relevan.
A.5.1.2	Tinjau kebijakan untuk keamanan informasi	Kontrol : Kebijakan untuk keamanan informasi harus ditinjau pada interval yang direncanakan atau jika terjadi perubahan yang signifikan untuk memastikan kesesuaian, kecukupan dan efektivitas berkelanjutan mereka.
A.6 Organisasi keamanan informasi		
A.6.1 Organisasi internal		
Tujuan: Untuk menetapkan kerangka manajemen untuk memulai dan mengendalikan implementasi dan operasi keamanan informasi dalam organisasi. Seperangkat kebijakan untuk keamanan informasi harus ditetapkan, disetujui oleh manajemen, diterbitkan dan dikomunikasikan kepada karyawan dan pihak eksternal yang relevan.		
A.6.1.1	Peran dan tanggung jawab keamanan Informasi	Kontrol : Semua tanggung jawab keamanan informasi harus ditentukan dan dialokasikan.
A.6.1.2	Pemisahan tugas	Kontrol: Kontak yang sesuai dengan otoritas yang relevan harus dijaga
A.6.1.3	Kontak dengan pihak berwenang	Kontrol: Kontak yang sesuai dengan otoritas yang relevan harus dijaga.
A.6.1.4	Kontak dengan kelompok minat khusus	Kontrol Kontak yang sesuai dengan kelompok minat khusus atau forum keamanan spesialis dan asosiasi profesional lainnya harus dipelihara
A.6.1.5	Keamanan informasi dalam manajemen proyek	Kontrol : Keamanan informasi harus ditangani dalam manajemen proyek, terlepas dari jenis proyeknya

A.6.2 Perangkat seluler dan teleworking		
Tujuan: Untuk memastikan keamanan teleworking dan penggunaan perangkat seluler.		
A.6.2.1	Kontrol kebijakan perangkat seluler	Kebijakan dan langkah-langkah keamanan pendukung harus diadopsi untuk mengelola risiko yang diperkenalkan dengan menggunakan perangkat seluler
A.6.2.2	Teleworking	Kontrol Kebijakan dan langkah-langkah keamanan pendukung harus dilaksanakan untuk melindungi informasi yang diakses, diproses atau disimpan di situs-situs teleworking.
A.7 Keamanan sumber daya manusia		
A.7.1 Sebelum bekerja		
Tujuan: Untuk memastikan bahwa karyawan dan kontraktor memahami tanggung jawab mereka dan cocok untuk peran yang mereka pertimbangkan.		
A.7.1.1	Penyaringan	Kontrol Pemeriksaan verifikasi latar belakang pada semua kandidat untuk pekerjaan harus dilakukan sesuai dengan hukum, peraturan dan etika yang relevan dan harus proporsional dengan persyaratan bisnis, klasifikasi informasi yang akan diakses dan risiko yang dirasakan
A.7.1.2	Syarat dan ketentuan pekerjaan	Perjanjian kontrak dengan karyawan dan kontraktor harus menyatakan tanggung jawab mereka dan organisasi untuk keamanan informasi
A.7.2 Selama bekerja		
Tujuan: Untuk memastikan bahwa karyawan dan kontraktor sadar dan memenuhi tanggung jawab keamanan informasi mereka.		
A.7.2.1	Tanggung jawab manajemen	Kontrol Manajemen mengharuskan semua karyawan dan kontraktor untuk menerapkan keamanan informasi sesuai dengan kebijakan dan prosedur organisasi yang ditetapkan
A.7.2.2	Kesadaran keamanan informasi, pendidikan dan pelatihan	Kontrol Semua karyawan organisasi dan, di mana ketinggian, kontraktor harus menerima pendidikan dan pelatihan kesadaran yang sesuai dan pembaruan rutin dalam kebijakan dan prosedur organisasi, yang relevan untuk fungsi pekerjaan mereka
A.7.2.3	Proses pendisiplinan	Kontrol

		Akan ada proses disipliner formal dan dikomunikasikan untuk mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran keamanan informasi.
A.7.3 Pengakhiran dan perubahan pekerjaan		
Tujuan: Untuk melindungi kepentingan organisasi sebagai bagian dari proses mengubah atau mengakhiri pekerjaan		
A.7.3.1	Penghentian atau perubahan tanggung jawab pekerjaan	Kontrol Tanggung jawab keamanan informasi dan tugas yang tetap berlaku setelah pengakhiran atau perubahan pekerjaan harus ditetapkan, dikomunikasikan kepada karyawan atau kontraktor dan diberlakukan.
A.8 Manajemen aset		
A.8.1 Tanggung jawab untuk aset		
Tujuan: Untuk mengidentifikasi aset organisasi dan menentukan tanggung jawab perlindungan yang sesuai.		
A.8.1.1	Inventarisasi aset	Aset yang terkait dengan informasi dan fasilitas pemrosesan informasi harus diidentifikasi dan inventarisasi aset-aset ini harus dibuat dan dipelihara
A.8.1.2	Kepemilikan aset	Kontrol Aset yang dipelihara dalam inventaris harus dimiliki.
A.8.1.3	Penggunaan aset yang dapat diterima Kontrol	Kontrol : Aturan untuk penggunaan informasi yang dapat diterima dan aset yang terkait dengan informasi dan fasilitas pemrosesan informasi harus diidentifikasi, didokumentasikan dan diimplementasikan.
A.8.1.4	Pengembalian aset	Kontrol Semua karyawan dan pengguna pihak eksternal harus mengembalikan semua aset organisasi yang mereka miliki saat pengakhiran kontrak kerja, kontrak, atau perjanjian mereka.
A.8.2 Klasifikasi informasi		
Tujuan: Untuk memastikan bahwa informasi menerima tingkat perlindungan yang tepat sesuai dengan kepentingannya bagi organisasi		
A.8.2.1	Klasifikasi informasi	Kontrol Informasi harus diklasifikasikan dalam persyaratan hukum, nilai, kekritisan dan

		kepekaan terhadap pengungkapan atau modifikasi yang tidak sah
A.8.2.2	Pemberian label informasi	Kontrol Prosedur untuk menangani aset harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.
A.8.2.3	Penanganan aset	Kontrol Prosedur untuk menangani aset harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi
A.8.3 Penanganan media		
Tujuan: Untuk mencegah pengungkapan yang tidak sah, modifikasi, penghapusan atau penghancuran informasi yang tersimpan di media		
A.8.3.1	Pengelolaan media yang dapat dilepas	Kontrol : Prosedur harus diterapkan untuk manajemen media yang dapat dipindahkan sesuai dengan skema klasifikasi yang diadopsi oleh organisasi
A.8.3.2	Pembuangan media	Kontrol Media harus dibuang dengan aman ketika tidak lagi diperlukan, menggunakan prosedur formal
A.8.3.3	Transfer media fisik	Kontrol Informasi yang mengandung media harus dilindungi terhadap akses tidak sah, penyalahgunaan atau korupsi selama transportasi
A.9 Kontrol akses		
A.9.1 Persyaratan bisnis untuk kontrol akses		
Tujuan: Untuk membatasi akses ke fasilitas informasi dan pengolahan informasi.		
A.9.1.1	Kebijakan kontrol akses	Kontrol Kebijakan kontrol akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan bisnis dan informasi
A.9.1.2	Akses ke jaringan dan layanan jaringan	Kontrol Pengguna hanya akan diberikan akses ke jaringan dan layanan jaringan yang telah secara khusus diizinkan untuk digunakan
A.9.2 Manajemen akses pengguna		

Tujuan: Untuk memastikan akses pengguna yang sah dan untuk mencegah akses tidak sah ke sistem dan layanan		
A.9.2.1	Registrasi dan registrasi pengguna	Kontrol Proses pendaftaran dan de-registrasi pengguna formal harus dilaksanakan untuk memungkinkan penugasan hak akses.
A.9.2.2	Provisioning akses pengguna	Kontrol Proses penyediaan akses pengguna formal harus diterapkan untuk menetapkan atau mencabut hak akses untuk semua jenis pengguna ke semua sistem dan layanan
A.9.2.3	Manajemen hak akses istimewa	Kontrol Alokasi dan penggunaan hak akses istimewa harus dibatasi dan dikendalikan.
A.9.2.4	Pengelolaan informasi otentikasi rahasia pengguna	Kontrol Alokasi informasi otentikasi rahasia harus dikontrol melalui proses manajemen formal
A.9.2.5	Tinjauan hak akses pengguna	Kontrol Pemilik aset harus meninjau hak akses pengguna secara berkala.
A.9.2.6	Penghapusan atau penyesuaian hak akses	Kontrol Hak akses semua karyawan dan pengguna pihak eksternal ke fasilitas pemrosesan informasi dan informasi harus dihapus pada saat pemutusan hubungan kerja, kontrak atau perjanjian, atau disesuaikan dengan perubahan.
A.9.3 Tanggung jawab pengguna		
Tujuan: Untuk membuat pengguna bertanggung jawab untuk menjaga informasi otentikasi mereka		
A.9.3.1	Penggunaan informasi otentikasi rahasia	Kontrol Pengguna harus mengikuti praktik organisasi dalam penggunaan informasi otentikasi rahasia.
A.9.4 Sistem dan kontrol akses aplikasi		
Tujuan: Untuk mencegah akses tidak sah ke sistem dan aplikasi		
A.9.4.1	Pembatasan akses informasi	Kontrol Akses ke informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan kontrol akses
A.9.4.2	Prosedur log-on yang aman	Kontrol

		Jika diperlukan oleh kebijakan kontrol akses, akses ke sistem dan aplikasi harus dikontrol oleh prosedur log-on yang aman
A.9.4.3	Sistem manajemen kata sandi	Kontrol Sistem manajemen kata sandi harus interaktif dan harus memastikan kata sandi berkualitas.
A.9.4.4	Penggunaan program utilitas istimewa	Kontrol Penggunaan program utilitas yang mungkin mampu mengesampingkan sistem dan kontrol aplikasi harus dibatasi dan dikontrol ketat
A.9.4.5	Kontrol akses ke kode sumber program	Kontrol Akses ke kode sumber program harus dibatasi
A.10 Kriptografi		
A.10.1 Kontrol kriptografi		
Tujuan: Untuk memastikan penggunaan kriptografi yang tepat dan efektif untuk melindungi kerahasiaan, keaslian dan / atau integritas informasi		
A.10.1.1	Kebijakan tentang penggunaan kontrol kriptografi	Kontrol Kebijakan tentang penggunaan kontrol kriptografi untuk perlindungan informasi harus dikembangkan dan diimplementasikan
A.10.1.2	Pengelolaan kunci	Kontrol Kebijakan tentang penggunaan, perlindungan, dan masa pakai kunci kriptografi harus dikembangkan dan diterapkan melalui seluruh siklus hidupnya
A.11 Keamanan fisik dan lingkungan		
A.11.1 Area aman		
Tujuan: Untuk mencegah akses fisik yang tidak sah, kerusakan, dan gangguan pada fasilitas informasi dan pemrosesan informasi organisasi		
A.11.1.1	Perimeter keamanan fisik	Kontrol Batas keamanan harus ditentukan dan digunakan untuk melindungi area yang mengandung informasi sensitif atau penting dan fasilitas pemrosesan informasi.
A.11.1.2	Kontrol entri fisik	Kontrol Area aman harus dilindungi oleh kontrol entri yang tepat untuk memastikan bahwa hanya personel yang berwenang yang diperbolehkan mengakses

A.11.1.3	Mengamankan kantor, ruangan dan fasilitas	Kontrol Keamanan fisik untuk kantor, kamar dan fasilitas harus dirancang dan diterapkan
A.11.1.4	Melindungi terhadap ancaman eksternal dan lingkungan	Kontrol Perlindungan fisik terhadap bencana alam, serangan atau kecelakaan jahat harus dirancang dan diterapkan
A.11.1.5	Bekerja di area yang aman	Kontrol Prosedur untuk bekerja di area aman harus dirancang dan diterapkan
A.11.1.6	Area pengiriman dan pemuatan	Kontrol Jalur akses seperti area pengiriman dan pemuatan dan tempat lain di mana orang yang tidak berwenang dapat memasuki tempat akan dikendalikan dan, jika mungkin, diisolasi dari fasilitas pemrosesan informasi untuk menghindari akses yang tidak sah
A.11.2 Peralatan		
Tujuan: Untuk mencegah kehilangan, kerusakan, pencurian atau kompromi aset dan gangguan terhadap operasi organisasi.		
A.11.2.1	Penempatan dan perlindungan peralatan	Kontrol Peralatan harus diletakkan dan dilindungi untuk mengurangi risiko dari ancaman dan bahaya lingkungan, dan peluang untuk akses yang tidak sah.
A.11.2.2	Utilitas pendukung	Kontrol Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam mendukung utilitas
A.11.2.3	Keamanan kabel	Kontrol Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari gangguan, gangguan atau kerusakan
A.11.2.4	Pemeliharaan peralatan	Kontrol Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan
A.11.2.5	Penghapusan aset	Kontrol Peralatan, informasi atau perangkat lunak tidak boleh diambil di luar lokasi tanpa izin sebelumnya

A.11.2.6	Keamanan peralatan dan aset di luar lokasi	Kontrol Keamanan harus diterapkan pada aset di luar lokasi dengan mempertimbangkan risiko berbeda bekerja di luar tempat organisasi
A.11.2.7	Pembuangan atau penggunaan kembali peralatan secara aman	Kontrol Semua peralatan yang mengandung media penyimpanan harus diverifikasi untuk memastikan bahwa data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa secara aman sebelum dibuang atau digunakan kembali
A.11.2.8	Peralatan pengguna yang tidak diawasi	Kontrol Pengguna harus memastikan bahwa peralatan yang tidak dijaga memiliki perlindungan yang tepat
A.11.2.9	Meja yang jelas dan kebijakan layar yang jelas	Kontrol Kebijakan meja yang jelas untuk kertas dan media penyimpanan yang dapat dilepas dan kebijakan layar yang jelas untuk fasilitas pemrosesan informasi harus diadopsi.
A.12 Keamanan operasi		
A.12.1 Prosedur dan tanggung jawab operasional		
Tujuan: Untuk memastikan operasi yang benar dan aman dari fasilitas pemrosesan informasi		
A.12.1.1	Prosedur operasi terdokumentasi	Kontrol Prosedur operasi harus didokumentasikan dan tersedia bagi semua pengguna yang membutuhkannya.
A.12.1.2	Manajemen perubahan	Kontrol Perubahan pada organisasi, proses bisnis, fasilitas pemrosesan informasi dan sistem yang mempengaruhi keamanan informasi harus dikontrol
A.12.1.3	Manajemen kapasitas	Kontrol Penggunaan sumber daya harus dipantau, disesuaikan, dan proyeksi yang dibuat dari kebutuhan kapasitas masa depan untuk memastikan kinerja sistem yang diperlukan
A.12.1.4	Pemisahan pengembangan, pengujian dan lingkungan operasional	Kontrol : Pemisahan lingkungan pengembangan, pengujian dan operasional Pengendalian Pengembangan, pengujian, dan lingkungan operasional harus dipisahkan untuk

		mengurangi risiko akses tidak sah atau perubahan pada lingkungan operasional
A.12.2 Perlindungan dari malware		
Tujuan: Untuk memastikan bahwa fasilitas pemrosesan informasi dan informasi dilindungiterhadap malware.		
A.12.2.1	Kontrol terhadap malware	Kontrol Kontrol deteksi, pencegahan, dan pemulihan untuk melindungi terhadap malware harus diterapkan, dikombinasikan dengan kesadaran pengguna yang sesuai
A.12.3 Cadangkan		
Tujuan: Untuk melindungi terhadap hilangnya data.		
A.12.3.1	Pencadangan informasi	Kontrol Salinan cadangan informasi, perangkat lunak dan gambar sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati
A.12.4 Penebangan dan pemantauan		
Tujuan: Untuk merekam peristiwa dan menghasilkan bukti		
A.12.4.1	Pencatatan kejadian	Kontrol Log peristiwa yang merekam aktivitas pengguna, pengecualian, kesalahan dan kejadian keamanan informasi harus dibuat, dijaga dan ditinjau secara berkala
A.12.4.2	Perlindungan informasi log	Kontrol Fasilitas logging dan informasi log harus dilindungi terhadap gangguan dan akses yang tidak sah.
A.12.4.3	Log administrator dan operator	Kontrol Administrator sistem dan kegiatan operator sistem harus dicatat dan log dilindungi dan ditinjau secara berkala
A.12.4.4	Sinkronisasi jam	Kontrol Administrator sistem dan kegiatan operator sistem harus dicatat dan log dilindungi dan ditinjau secara berkala.
A.12.5 Kontrol perangkat lunak operasional		
Tujuan: Untuk memastikan integritas sistem operasional		
A.12.5.1	Pemasangan perangkat lunak pada sistem operasional	Kontrol Prosedur harus dilaksanakan untuk mengontrol pemasangan perangkat lunak pada sistem operasional
A.12.6 Pengelolaan kerentanan teknis		

Tujuan: Untuk mencegah eksploitasi kerentanan teknis		
A.12.6.1	Pengelolaan kerentanan teknis	Kontrol Informasi tentang kerentanan teknis dari sistem informasi yang digunakan harus diperoleh secara tepat waktu, paparan organisasi terhadap kerentanan tersebut dievaluasi dan tindakan yang tepat diambil untuk mengatasi risiko terkait.
A.12.6.2	Pembatasan pada instalasi perangkat lunak	Kontrol Aturan yang mengatur pemasangan perangkat lunak oleh pengguna harus ditetapkan dan diimplementasikan
A.12.7 Pertimbangan audit sistem informasi		
Tujuan: Untuk meminimalkan dampak kegiatan audit pada sistem operasional		
A.12.7.1	Kontrol audit sistem informasi	Kontrol Persyaratan dan kegiatan audit yang melibatkan verifikasi sistem operasional harus direncanakan secara hati-hati dan disetujui untuk meminimalkan gangguan terhadap proses bisnis
A.13 Keamanan komunikasi		
A.13.1 Manajemen keamanan jaringan		
Tujuan: Untuk memastikan perlindungan informasi dalam jaringan dan fasilitas pemrosesaninformasi pendukungnya		
A.13.1.1	Kontrol jaringan	Kontrol Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi
A.13.1.2	Keamanan layanan jaringan	Kontrol Mekanisme keamanan, tingkat layanan, dan persyaratan manajemen semua layanan jaringan harus diidentifikasi dan dimasukkan dalam perjanjian layanan jaringan, apakah layanan ini disediakan di rumah atau dialihdayakan
A.13.1.3	Segregasi dalam jaringan	Kontrol Kelompok layanan informasi, pengguna, dan sistem informasi harus dipisahkan pada jaringan.
A.13.2 Transfer informasi		
Tujuan: Untuk menjaga keamanan informasi yang ditransfer dalam suatu organisasi dan denganentitas eksternal apa pun		
A.13.2.1	Kebijakan dan prosedur pengalihan informasi	Kontrol

		Kebijakan, prosedur, dan kendali transfer formal harus diberlakukan untuk melindungi transfer informasi melalui penggunaan semua jenis fasilitas komunikasi
A.13.2.2	Kesepakatan tentang transfer informasi	Kontrol Perjanjian harus menangani transfer aman informasi bisnis antara organisasi dan pihak eksternal.
A.13.2.3	Pesan elektronik	Kontrol Informasi yang terlibat dalam pesan elektronik harus dilindungi dengan tepat
A.13.2.4	Perjanjian kerahasiaan atau nondisclosure	Kontrol Persyaratan untuk kerahasiaan atau perjanjian kerahasiaan non-mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, secara teratur ditinjau dan didokumentasikan
A.14 Akuisisi, pengembangan, dan pemeliharaan sistem		
A.14.1 Persyaratan keamanan sistem informasi		
Tujuan: Untuk memastikan bahwa keamanan informasi merupakan bagian integral dari sistem informasi di seluruh siklus hidup. Ini juga termasuk persyaratan untuk sistem informasi yang menyediakan layanan melalui jaringan publik.		
A.14.1.1	Analisis dan spesifikasi kebutuhan keamanan informasi	Kontrol Persyaratan terkait keamanan informasi harus dimasukkan dalam persyaratan untuk sistem informasi baru atau penyempurnaan sistem informasi yang ada
A.14.1.2	Mengamankan layanan aplikasi di jaringan publik	Kontrol Informasi yang terlibat dalam layanan aplikasi yang melewati jaringan publik harus dilindungi dari kegiatan penipuan, perselisihan kontrak dan pengungkapan tidak sah dan modifikasi
A.14.1.3	Melindungi transaksi layanan aplikasi	Kontrol Informasi yang terlibat dalam transaksi layanan aplikasi harus dilindungi untuk mencegah transmisi yang tidak lengkap, mis-routing, perubahan pesan yang tidak sah, pengungkapan yang tidak sah, duplikasi pesan tidak sah atau replay.
A.14.2 Keamanan dalam proses pengembangan dan dukungan		
Tujuan: Untuk memastikan keamanan informasi dirancang dan diimplementasikan dalam sikluspengembangan sistem informasi		

A.14.2.1	Kebijakan pembangunan yang aman	Kontrol Aturan untuk pengembangan perangkat lunak dan sistem harus ditetapkan dan diterapkan untuk perkembangan dalam organisasi.
A.14.2.2	Prosedur kontrol perubahan sistem	Kontrol Perubahan sistem dalam siklus hidup pengembangan harus dikendalikan oleh penggunaan prosedur kontrol perubahan formal
A.14.2.3	Tinjauan teknis aplikasi setelah perubahan platform operasi	Kontrol Ketika platform operasi berubah, aplikasi bisnis penting harus ditinjau dan diuji untuk memastikan tidak ada dampak negatif pada operasi atau keamanan organisasi
A.14.2.4	Batasan pada perubahan paket perangkat lunak	Kontrol Modifikasi paket perangkat lunak harus dihalangi, terbatas pada perubahan yang diperlukan dan semua perubahan harus dikontrol secara ketat
A.14.2.5	Prinsip rekayasa sistem yang aman	Kontrol Prinsip-prinsip untuk rekayasa sistem keamanan harus ditetapkan, didokumentasikan, dipelihara dan diterapkan pada setiap upaya implementasi sistem informasi.
A.14.2.6	Lingkungan pengembangan yang aman	Kontrol Organisasi harus menetapkan dan secara tepat melindungi lingkungan pengembangan yang aman untuk pengembangan sistem dan upaya integrasi yang mencakup seluruh siklus hidup pengembangan sistem.
A.14.2.7	Pengembangan yang dialih dayakan	Kontrol Organisasi harus mengawasi dan memantau aktivitas pengembangan sistem yang dialihdayakan
A.14.2.8	Pengujian keamanan sistem	Kontrol Pengujian fungsi keamanan harus dilakukan selama pengembangan.
A.14.2.9	Pengujian penerimaan sistem	Kontrol Program pengujian penerimaan dan kriteria terkait harus ditetapkan untuk

		sistem informasi baru, peningkatan versi dan versi baru
A.14.3 Data uji		
Tujuan: Untuk memastikan perlindungan data yang digunakan untuk pengujian		
A.14.3.1	Perlindungan data uji	Kontrol Data uji harus dipilih dengan hati-hati, terlindungi dan terkontrol
A.15 Hubungan pemasok		
A.15.1 Keamanan informasi dalam hubungan pemasok		
Tujuan: Untuk memastikan perlindungan aset organisasi yang dapat diakses oleh pemasok		
A.15.1.1	Kebijakan keamanan informasi untuk hubungan pemasok	Kontrol Persyaratan keamanan informasi untuk memitigasi risiko yang terkait dengan akses pemasok ke aset organisasi harus disetujui oleh pemasok dan didokumentasikan
A.15.1.2	Mengatasi keamanan dalam perjanjian pemasok	Kontrol Semua persyaratan keamanan informasi yang relevan harus ditetapkan dan disepakati dengan masing-masing pemasok yang dapat mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur TI untuk, informasi organisasi
A.15.1.3	Rantai pasokan teknologi informasi dan komunikasi	Kontrol Perjanjian dengan pemasok harus mencakup persyaratan untuk mengatasi risiko keamanan informasi yang terkait dengan layanan teknologi informasi dan komunikasi dan rantai pasokan produk.
A.15.2 Manajemen pengiriman layanan pemasok		
Tujuan: Untuk menjaga tingkat keamanan informasi dan penyediaan layanan yang disepakatisesuai dengan perjanjian pemasok.		
A.15.2.1	Pemantauan dan peninjauan layanan pemasok	Kontrol Organisasi harus secara teratur memantau, meninjau, dan mengaudit layanan pemasok
A.15.2.2	Mengelola perubahan pada layanan pemasok	Kontrol Perubahan pada penyediaan layanan oleh pemasok, termasuk mempertahankan dan meningkatkan kebijakan keamanan informasi yang ada, prosedur dan kontrol, harus dikelola, dengan mempertimbangkan kekritisan informasi

		bisnis, sistem dan proses yang terlibat dan penilaian ulang risiko.
A.16 Manajemen insiden keamanan informasi		
A.16.1 Manajemen insiden keamanan informasi dan perbaikan		
Tujuan: Untuk memastikan pendekatan yang konsisten dan efektif terhadap manajemen insiden keamanan informasi, termasuk komunikasi tentang peristiwa keamanan dan kelemahan		
A.16.1.1	Tanggung jawab dan prosedur	Kontrol Tanggung jawab manajemen dan prosedur harus ditetapkan untuk memastikan tanggapan yang cepat, efektif dan teratur terhadap insiden keamanan informasi
A.16.1.2	Pelaporan kejadian keamanan informasi	Kontrol Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang tepat secepat mungkin
A.16.1.3	Melaporkan kelemahan keamanan informasi	Kontrol Karyawan dan kontraktor menggunakan informasi organisasi sistem dan layanan harus diminta untuk mencatat dan melaporkan setiap kelemahan keamanan informasi yang diamati atau dicurigai dalam sistem atau layanan
A.16.1.4	Penilaian dan keputusan tentang kejadian keamanan informasi	Kontrol Kejadian keamanan informasi harus dinilai dan diputuskan apakah akan diklasifikasikan sebagai insiden keamanan informasi
A.16.1.5	Tanggapan terhadap insiden keamanan informasi	Kontrol Insiden keamanan informasi harus direspons sesuai dengan prosedur terdokumentasi
A.16.1.6	Belajar dari insiden keamanan informasi	Kontrol Pengetahuan yang diperoleh dari menganalisa dan menyelesaikan insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan atau dampak dari insiden masa depan
A.16.1.7	Pengumpulan bukti	Kontrol Organisasi harus menetapkan dan menerapkan prosedur untuk identifikasi, pengumpulan, perolehan, dan pelestarian informasi, yang dapat berfungsi sebagai bukti

A.17 Aspek keamanan informasi manajemen kesinambungan bisnis		
A.17.1 Ketahanan keamanan informasi		
Sasaran: Keberlanjutan keamanan informasi harus disematkan dalam sistem manajemen kesinambungan bisnis organisasi.		
A.17.1.1	Merencanakan keberlanjutan keamanan informasi	Kontrol Organisasi harus menentukan persyaratannya untuk keamanan informasi dan kelangsungan manajemen keamanan informasi dalam situasi yang merugikan, misalnya selama krisis atau bencana
A.17.1.2	Menerapkan kontinuitas keamanan informasi	Kontrol Organisasi harus menetapkan, mendokumentasikan, menerapkan dan memelihara proses, prosedur dan kontrol untuk memastikan tingkat keberlanjutan yang diperlukan untuk keamanan informasi selama situasi yang merugikan.
A.17.1.3	Verifikasi, tinjau, dan evaluasi keberlanjutan keamanan informasi	Kontrol Organisasi harus memverifikasi kontrol kontinuitas keamanan informasi yang ditetapkan dan diimplementasikan secara berkala untuk memastikan bahwa mereka valid dan efektif selama situasi yang merugikan
A.17.2 Redudansi		
Tujuan: Untuk memastikan ketersediaan fasilitas pemrosesan informasi.		
A.17.2.1	Ketersediaan fasilitas pengolahan informasi	Kontrol Fasilitas pemrosesan informasi harus dilaksanakan dengan redundansi yang cukup untuk memenuhi persyaratan ketersediaan
A.18 Kepatuhan		
A.18.1 Kepatuhan dengan persyaratan hukum dan kontrak		
Tujuan: Untuk menghindari pelanggaran kewajiban hukum, undang-undang, peraturan atau kontrak yang terkait dengan keamanan informasi dan persyaratan keamanan apa pun		
A.18.1.1	Identifikasi peraturan perundangan yang berlaku dan persyaratan kontrak	Kontrol Semua peraturan perundang-undangan yang relevan, peraturan, persyaratan kontrak dan pendekatan organisasi untuk memenuhi persyaratan ini harus secara eksplisit diidentifikasi, didokumentasikan dan diperbarui untuk setiap sistem informasi dan organisasi
A.18.1.2	Hak kekayaan intelektual	Kontrol

		Prosedur yang sesuai harus dilaksanakan untuk memastikan kepatuhan dengan persyaratan legislatif, peraturan dan kontrak yang terkait dengan hak kekayaan intelektual dan penggunaan produk perangkat lunak berpemilik
A.18.1.3	Perlindungan rekaman	Kontrol Rekaman harus dilindungi dari kehilangan, perusakan, pemalsuan, akses yang tidak sah dan pelepasan yang tidak sah, sesuai dengan persyaratan legislatif, peraturan, kontrak dan bisnis
A.18.1.4	Privasi dan perlindungan informasi identitas pribadi	Kontrol Privasi dan perlindungan informasi identitas pribadi harus dipastikan sebagaimana disyaratkan dalam undang-undang dan peraturan yang relevan jika berlaku
A.18.1.5	Pengaturan kontrol kriptografi	Kontrol Kontrol kriptografi harus digunakan sesuai dengan semua perjanjian, undang-undang dan peraturan yang relevan
A.18.2 Tinjauan keamanan informasi		
Tujuan: Untuk memastikan keamanan informasi diimplementasikan dan dioperasikan sesuai dengan kebijakan dan prosedur organisasi		
A.18.2.1	Tinjauan independen atas keamanan informasi	Kontrol Pendekatan organisasi untuk mengelola keamanan informasi dan implementasinya (yaitu tujuan pengendalian, kontrol, kebijakan, proses dan prosedur untuk keamanan informasi) harus ditinjau secara independen pada interval yang direncanakan atau ketika terjadi perubahan yang signifikan
A.18.2.2	Kepatuhan dengan kebijakan dan standar keamanan	Kontrol Manajer harus secara teratur meninjau kepatuhan pemrosesan informasi dan prosedur di dalam wilayah tanggung jawab mereka dengan kebijakan keamanan yang sesuai, standar dan persyaratan keamanan lainnya.
A.18.2.3	Tinjauan kepatuhan teknis	Kontrol Sistem informasi harus ditinjau secara berkala untuk kepatuhan terhadap kebijakan dan standar keamanan informasi organisasi.