ANALISIS TINGKAT KESIAPAN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KAMI (KEAMANAN INFORMASI) 4.0 (STUDI KASUS : DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR)

SKRIPSI

Untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun oleh:
Gede Dandy Salodivansa Barani
NIM: 165150400111033

PROGRAM STUDI SISTEM INFORMASI
JURUSAN SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER
UNIVERSITAS BRAWIJAYA
MALANG
TAHUN 2020

PENGESAHAN

ANALISIS TINGKAT KESIAPAN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KAMI (KEAMANAN INFORMASI) 4.0 (STUDI KASUS : DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR)

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun Oleh :
Gede Dandy Salodivansa Barani
NIM: 165150400111033

Skripsi ini telah diuji dan dinyatakan lulus pada
6 Agustus 2020
Telah diperiksa dan disetujui oleh:

Dosen Pembimbing I	Dosen Pembimbing II
Widhy Hayuhardhika Nugraha Putra, S.Kom., M.Kom.	Bondan Sapta Prakoso, S.T., M.Kom
NIK: 2017128704092001	NIP: 197408072003121002

Mengetahui
Ketua Jurusan NamaJurusan

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 pustaka.

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, 6 Agustus 2020

Gede Dandy Salodivansa B.

NIM: 165150400111033

KATA PENGANTAR

Puji Syukur ke hadirat Tuhan Yang Maha Esa atas segala rahmat dan karunianya yang telah di berikan sehingga memberikan kemudahan dan kelancaran dalam menyelesaikan skripsi yang berjudul " ANALISIS TINGKAT KESIAPAN KEAMANAN INFORMASI MENGGUNAKAN INDEKS KAMI (KEAMANAN INFORMASI) 4.0 (STUDI KASUS : DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR) " dapat diselesaikan. Penulis ingin megucapkan terimakasih kasih kepada pihak – pihak yang telah membantu proses pengerjaan skripsi, baik secara moril maupun materil dan secara langsung maupun tidak langsung. Penulis ingin mengucapkan terima kasih kepada:

1. Widhy Hayuhardhika Nugraha Putra, S.Kom., M.Kom. selaku Dosen Pembimbing I atas petunjuk, arahan, serta masukan yang telah diberikan kepada penulis
2. Bondan Sapta Prakoso, S.T., M.Kom. selaku Dosen Pembimbing II atas bimbingan, saran, arahan, serta masukan kepada penulis.
3. Bapak Wayan Firdaus Mahmudy, S.Si., M.TI., Ph.D. selaku Dekan Fakultas Ilmu Komputer Universitas Brawijaya
4. Bapak Issa Arwani, S.Kom, M.Sc. selaku Ketua Jurusan Sistem Informasi Fakultas Ilmu Komputer Universitas Brawijaya.
5. Bapak Yusi Tyroni Mursityo, S.Kom., M.AB. selaku Ketua Program Studi Sistem Informasi Jurusan Sistem Informasi Fakultas Ilmu Komputer Universitas Brawijaya.
6. Kepada Papa, Mama, Adik, Kakak, dan semua Keluarga yang telah memberikan motivasi, kepercayaan, dukungan, semangat serta cinta kepada penulis.
7. Lembaga KBMSI Periode 2017/2018, 2018/2019, 2019/2020, khususnya BPH EMSI Periode 2019/2020 dan Departemen MEDKOMINFO EMSI yang selalu membantu dan menghibur penulis dalam menyelesaikan penelitian ini.
8. Teman teman AWWC, Bunga Asmara, Nadia Humairo, Ata Salsabila, Chika Apsari, Restian Parengga, Sarah Tsamara, Nabilla Diva, Wirdhayanti Paulina selaku sahabat penulis yang selalu percaya, menyemangati, dan memberi dukungan selama penulis menempuh perkuliahan dan menyelesaikan penelitian ini.
9. Seluruh Civitas Akademika Fakultasi Ilmu Komputer Universitas Brawijaya yang telah memberikan bantuan dan arahan.

10. Seluruh pihak yang tidak dapat disebutkan satu persatu yang menjadi penyemangat dan memberi banyak pengetahuan dan pembelajaran kepada penulis.

Malang, 6 Agustus 2020

Gede Dandy Salodivansa Barani

dandysdb@student.ub.ac.id

ABSTRAK

Dinas Komunikasi dan Informatika Provinsi Jawa Timur merupakan badan Pemerintahan yang melaksanakan urusan pemerintahan pada bidang komunikasi dan informatika, bidang statistik dan bidang persandian atau keamanan. Keamanan informasi merupakan kunci penting dalam pengamanan informasi, sehingga Kementrian Komunikasi dan Informatika mengeluarkan regulasi terkait Sistem Manajemen Pengamanan Informasi pada instansi pemerintahan dalam Peraturan Menteri Komunikasi dan Informatika No 4 tahun 2016, oleh karena itu Dinas Komunikasi dan Informatika Provinsi Jawa Timur sebagai pelaksana kebijakan pada bidang komunikasi dan informasi perlu mengevaluasi dan analisis terkait keamanan informasi. Pada penelitian ini, evaluasi dan analisis dilakukan menggunakan Indeks Keamanan Informasi (KAMI) 4.0 dengan menggunakan instrument kuisioner untuk mengetahui tingkat kematangan serta tingkat kelengkapan keamanan informasi pada enam area yaitu tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan aset, teknologi dan keamanan informasi, serta suplemen. Dari evaluasi yang dilakukan, diketahui bahwa tingkat kematangan pada lima area berada pada level I sampai dengan II dan tingkat kelengkapan mendapatkan skor 258. Dengan skor dan level tersebut, dapat dinyatakan Dinas Komunikasi dan Informatika Provinsi Jawa Timur perlu perbaikan untuk melakukan sertifikasi ISO27001. Hasil analisis tersebut menjadi dasar rekomendasi-rekomendasi yang diperoleh dari kontrol ISO27001, salah satu rekomendasi yang diberikan adalah terkait kebijakan keamanan informasi berdasarkan kontrol A.5.1.1.

Kata kunci: Analisis, Keamanan Informasi, Indeks KAMI 4.0, ISO/IEC 27001:2013

ABSTRACT

The Communication and informatics Agency of East Java is a government agency that organize communication dan informatics, statistics and encryption or security fields. Information security is a key in securing informations, hence The Ministry of Communication dan Informatics issued Information Security Management System related regulation on government agencies in Indonesia Minister of Communication and Informatic regulation number 4 of 2016, hence the Communication and Informatics Agency of East Java Province as the communication and informatics executor need to evaluate and analyze their information security. In this study, evaluation and analysis conducted using KAMI (Keamanan Informasi) Index questionnaires to determine the maturity and completeness level of information secutiry on six areas such as governance, risk management, frameworks, assets management, technology and information security, and supplement. From the evaluation, the maturity level on five areas are between level I to II and the completeness level gets a score of 258. With these score and levels, The Communication and Informatics Agency of East Java determined needs improvements to conduct with ISO27001 sertification. The result of the analysis form basis of recommendations obtained from ISO2700 control, one of the recommendations is information security regulations related to A.5.1.1 control of ISO27001.

Keywords: Analysis, Information Security, KAMI Index 4.0, ISO/IEC 27001:2013

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Di era globalisasi saat ini, hampir seluruh informasi kini sangat mudah untuk diakses dan ditemukan. Menurut Tata Sutabri (2012), informasi adalah sekumpulan data-data yang telah diklasifikasikan dan diinterpretasi yang akan digunakan dalam mengambil sebuah keputusan. Perkembangan Teknologi Informasi dan Komunikasi yang sangat pesat juga mendorong berbagai bidang kehidupan mulai dari Pendidikan hingga instansi Pemerintahan untuk berkembang seperti pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur (DISKOMINFO PROV. JATIM) yang memanfaatkan perkembangan Teknologi Informasi dan Komunikasi untuk melaksanakan berbagai macam fungsi dan tugas untuk membantu Gubernur dalam menjalankan kewenangan Pemerintah Provinsi Jawa Timur. Sehingga, Informasi dapat dikatakan sebagai aset yang sangat berharga bagi individu, kelompok, swasta hingga instansi pemerintahan.

Tata Kelola Teknologi Informasi dan Komunikasi yang baik dapat memberikan banyak manfaat bagi organisasi pada level eksekutif untuk mencapai tujuan strategis organisasi tersebut. Terkait Tata Kelola Teknologi Informasi dan Komunikasi, khususnya pada bidang keamanan informasi sesuai dengan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 yang dikeluarkan pada tanggal 11 April 2016 tentang Sistem Manajemen Pengamanan Informasi (SMPI) maka Dinas Komunikasi dan Informatika Provinsi Jawa Timur (DISKOMINFO PROV. JATIM) diharuskan melaksanakan pengamanan terhadap informasi-informasi yang dikelola.

Salah satu cara yang dapat dilakukan oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur (DISKOMINFO PROV. JATIM) dalam meningkatkan kualitas keamanan informasi khususnya pada Tata Kelola aspek Kemanan Informasi, yaitu dengan melakukan analisis terhadap Keamanan Informasi mengingat keamanan informasi yang buruk dapat mengganggu kinerja dari Tata Kelola Teknologi Informasi dan Komunikasi apabila informasi yang dimiliki mengalami masalah yang berhubungan dengan kerahasiaan, integritas, dan ketersediaan. Keamanan Informasi akan dievaluasi menggunakan kerangka kerja atau alat bantu yang telah memiliki standar yang didasari oleh peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016. Alat bantu Indeks KAMI (Keamanan Informasi) berfungsi sebagai perangkat untuk memberikan gambaran kondisi kesiapan keamanan informasi kepada pimpinan Instansi.

Indeks KAMI menganalisis keamanan informasi yang mencakup aspek pembenahan, pembangunan dan penerapan. Evaluasi menggunakan Indeks KAMI 4.0 mencakup 7 target area. Data atau informasi yang dihasilkan pada evaluasi ini lalu dianalisis dan akan memberikan gambaran kesiapan dari aspek kelengkapan hingga kematangan kerangka kerja keamanan informasi yang diterapkan sehingga indeks KAMI juga dapat digunakan sebagai pembanding untuk melakukan

perbaikan. Terdapat satu area baru pada indeks KAMI 4.0 dibandingkan dengan versi indeks KAMI sebelumnya versi 3.1 yaitu area Suplemen yang akan mengevaluasi aspek pengamanan keterlibatan pihak ketiga sebagai penyedia layanan, Pengamanan Layanan berbasis *cloud,* dan perlindungan data pribadi. Pada area atau bagian ini akan melakukan evaluasi terhadap kelengkapan, konsistensi dan efektivitas penggunaan teknologi didalam pengamanan aset informasi dari objek yang akan dianalisis.

Pada penelitian sebelumnya yang dilakukan oleh Shella Indah Dwi Octaviani di Dinas Komunikasi dan Informatika Kota Batu, menerangkan bahwa sarana dalam mengelola informasi dari sistem yang diimplementasikan, Dinas Komunikasi dan Informatika Kota Batu memilki *service center* yang berisi informasi-informasi penting yang dilindungi, sehingga diperlukan pengamanan informasi dengan prosedur dan standar yang jelas. Berdasarkan hasil evaluasi menggunakan indeks Keamanan Informasi (KAMI) 3.1, kategori sistem elektronik yang digunakan oleh Dinas Komunikasi dan Informatika Kota Batu mendapatkan skor 24 dimana skor ini termasuk dalam kategori "tinggi" dan pada tingkat kelengkapan penerapan standar ISO/IEC 27001:2013 mendapatkan skor sebesar 203 dimana skor ini termasuk dalam kategori "tidak layak". Dari evaluasi 5 area yang ada pada indeks KAMI, 2 area pada indeks ini belum memenuhi kerangka kerja dasar pengelolaan keamanan informasi yaitu pada area pengelolaan risiko dan pengelolaan aset.

Berdasarkan latar belakang yang telah dijabarkan pada paragraf-paragraf sebelumnya, penulis tertarik untuk melakukan penelitian yang berjudul "**Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks KAMI (Keamanan Informasi) 4.0 (Studi Kasus : Dinas Komunikasi dan Informatika Provinsi Jawa Timur)**"

1.2 Rumusan Masalah

Dari latar belakang yang telah di jabarkan, adapun rumusan masalah yang di dapat sebagai berikut:

1. Bagaimana analisis kesiapan keamanan informasi dari Dinas Komunikasi dan Informatika Provinsi Jawa Timur (DISKOMINFO PROV. JATIM) berdasarkan Indeks KAMI (Keamanan Informasi) 4.0 ?
2. Bagaimana rekomendasi perbaikan guna meningkatkan keamanan informasi dengan berdasarkan analisis kesiapan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur (DISKOMINFO PROV. JATIM)?

1.3 Tujuan

Dari permasalahan yang telah dipaparkan pada latar belakang maka didapatkan tujuan dari penelitian ini, yaitu diantaranya:

1. Penelitian ini diharapkan dapat membantu penilaian tingkat kesiapan keamanan informasi dari Dinas Komunikasi dan Informatika Provinsi Jawa Timur (DISKOMINFO PROV. JATIM).
2. Penelitian ini diharapkan dapat memberikan rekomendasi perbaikan untuk peningkatan tingkat kesiapan keamanan dan kelengkapan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur (DISKOMINFO PROV. JATIM).

1.4 Manfaat

Dengan adanya penelitian ini, ada beberapa manfaat yang didapatkan antara lain:

1. Dapat mengetahui tingkat kesiapan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.
2. Dapat memberikan hasil rekomendasi perbaikan terhadap area-area yang akan dinilai untuk meningkatkan tingkat kesiapan keamanan dan kelengkapan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur (DISKOMINFO PROV. JATIM).

1.5 Batasan Masalah

Agar permasalahan yang dirumuskan dapat terfokus sesuai dengan kebutuhan yang di harapkan, maka penelitian ini di batasi dalam hal:

1. Penelitian ini menilai tingkat kesiapan keamanan informasi menggunakan alat bantu Indeks Keamanan Informasi (KAMI) versi 4.0 pada 2 area besar yaitu area kategori sistem elektronik dan area keamanan informasi, yang berisi pertanyaan-pertanyaan seputar penggunaan sistem elektronik dan keamanan informasi.
2. Rekomendasi perbaikan yang akan diberikan mengacu kepada standar yang telah ada pada ISO/IEC 27001:2013.
3. Bagian atau Divisi yang akan menjadi responden pada skripsi ini adalah seksi Persandian dan Keamanan Informasi serta bidang Aplikasi Informatika Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

1.6 Sistematika Pembahasan

Susunan dari pembahasan bertujuan untuk memberikan uraian dari penulisan skripsi secara garis besar mulai dari pendahuluan sampai dengan susunan sebagai berikut:

BAB 1 PENDAHULUAN

Bab ini akan menjelaskan mengenai latar belakang mengapa penelitian ini dilakukan, rumusan masalah, tujuan penelitian, manfaat penelitian, Batasan masalah dalam melakukan penelitian, dan sistematika penulisan penelitian ini.

BAB 2 LANDASAN KEPUSTAKAAN

Bab ini akan menjelaskan mengenai teori-teori yang digunakan sebagai acuan dalam melakukan penelitian yang disitasi dari berbagai sumber atau referensi.

BAB 3 METODOLOGI

Bab ini akan menjelaskan mengenai tahapan proses dalam melakukan penilitian dalam menganalisis tingkat kesiapan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur (DISKOMINFO PROV. JATIM).

BAB 4 PENGUMPULAN DATA

Bab ini akan menjelaskan mengenai pengumpulan data penelitian yang akan dilakukan oleh peneliti sesuai dengan metodologi penelitian.

BAB 5 HASIL DAN PEMBAHASAN

Bab ini akan menjelaskan mengenai pengolahan data yang didapatkan, lalu pada bab ini juga akan membahas bagaimana analisis tingkat kesiapan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur (DISKOMINFO PROV. JATIM) berdasarkan data yang dikumpulkan pada bab sebelumnya.

BAB 6 KESIMPULAN DAN SARAN

Bab ini akan menjelaskan mengenai kesimpulan dari keseluruhan penelitian yang dilakukan dan saran atau rekomendasi yang akan diberikan berdasarkan penelitian yang telah dilakukan.

BAB 2 LANDASAN KEPUSTAKAAN

2.1 Tinjauan Pustaka

Penelitian pertama dilakukan oleh Roodhim Firmana pada tahun 2013. Penelitian tersebut menjelaskan mengenai evaluasi keamanan informasi menggunakan alat bantu Indeks KAMI (Keamanan Informasi) pada PT. PLN (Perusahaan Listrik Negara) Distribusi Jawa Timur. Penelitian tersebut mengevaluasi PT. PLN Distribusi Jawa Timur dengan menggunakan indeks KAMI dan menghasilkan skor sebesar 190 dengan tingkat kematangan I+ dan dimana ketergantungan TIK (Teknologi Informasi dan Komunikasi) termasuk dalam golongan kritis, sehingga peran TIK dianggap penting untuk mendukung proses bisnis yang masih kurang layak, dan penelitian ini memberikan saran perbaikan dan implementasi yang tepat untuk meningkatkan keamanan informasi pada PT. PLN Distribusi Jawa Timur.

Penelitian kedua dilakukan oleh Ferdian Satria Sujalma, Awalludiyah Ambarwati, dan Natalia Damastuti pada tahun 2017. Penelitian tersebut menjelaskan tentang evaluasi keamana informasi menggunakan Indeks KAMI pada PT. Ma-Ri. PT. Ma-Ri merupakan sebuah perusahaan yang bergerak di industri pengolahan makanan ringan yang berada di Kabupaten Sidoarjo, Provinsi Jawa Timur. Penelitian ini dilakukan untuk mengetahui kondisi keamanan informasi terkini yang kemudian akan memberikan rekomendasi perbaikan. Hasil penilaian lima area dengan menggunakan Indeks KAMI di PT.Ma-Ri menghasilkan skor sebesar 249 dari total skor yang sebesar 588 dan PT.Ma-Ri berada pada level I sampai dengan I+ dimana level ini masih berada pada kondisi awal penerapan keamanan informasi.

Penelitian ketiga dilakukan oleh Edo Rizky Pratama yang dilakukan pada tahun 2017. Penelitian tersebut menjelaskan tentang evaluasi tata kelola sistem keamanan informasi menggunakan Indeks KAMI di Dinas KOMINFO (Komunikasi dan Informatika) Provinsi Jawa Timur yang harus melakukan pengamanan informasi sesuai dengan peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 tahun 2016. Penelitian ini menghasilkan evaluasi Indeks KAMI Dinas KOMINFO Provinsi Jawa Timur berada pada tingkat I+, sehingga perlu dibuatkan rekomendasi dengan membandingkan kekurangan dari area pada Indeks KAMI.

2.2 Profil Dinas Komunikasi dan Informatika Provinsi Jawa Timur

Dinas Komunikasi dan Informatika Provinsi Jawa Timur merupakan badan instansi atau unsur pelaksana otonomi daerah yang dipimpin oleh seorang kepala dinas yang kedudukannya berada dibawah Gubernur dan juga bertanggung jawab kepada Gubernur melalui Sekretaris Daerah. Dinas Komunikasi dan Informatika Provinsi Jawa Timur memiliki kewenangan daerah dibidang pengelolaan Teknologi Informasi dan Komunikasi, dan membantu melaksanakan tugas yang diberikan oleh Pemerintah Pusat maupun Provinsi yang setiap kegiatan yang dilakukan akan

berhubungan dengan Pengembangan Sistem Informasi, Pembangunan dan Pemeliharaan Jaringan Komputer, dan Pengelolaan informasi dan publikasi.

Berikut merupakan tugas dan fungsi dari Dinas Komunikasi dan Informatika Provinsi Jawa Timur :

Tugas : Membantu Gubernur menyiapkan bahan pelaksanaan urusan pemerintahan yang menjadi kewenangan Pemerintah Provinsi di Bidang Komunikasi dan Informasi serta tugas pembantuan.

Fungsi :

1. Perumusan kebijakan di bidang komunikasi dan informasi.
2. Pelaksanaan kebijakan di bidang komunikasi dan informasi.
3. Pelaksanaan evaluasi dan pelaporan di bidang komunikasi dan informasi.
4. Pelaksanaan administrasi dinas di bidang komunikasi dan informasi.
5. Pelaksanaan fungsi lain yang diberikan oleh Gubernur terkait dengan tugas dan fungsinya.

Selain itu, Dinas Komunikasi dan Informatika Provinsi Jawa Timur juga memiliki visi dan misi sebagai acuan dari tugas dan fungsi organisasi ini dan juga sebagai kontrol dalam mencapai objektif yang ingin dicapai. Visi dan misi dari Dinas Komunikasi dan Informatika Provinsi Jawa Timur adalah sebagai berikut:

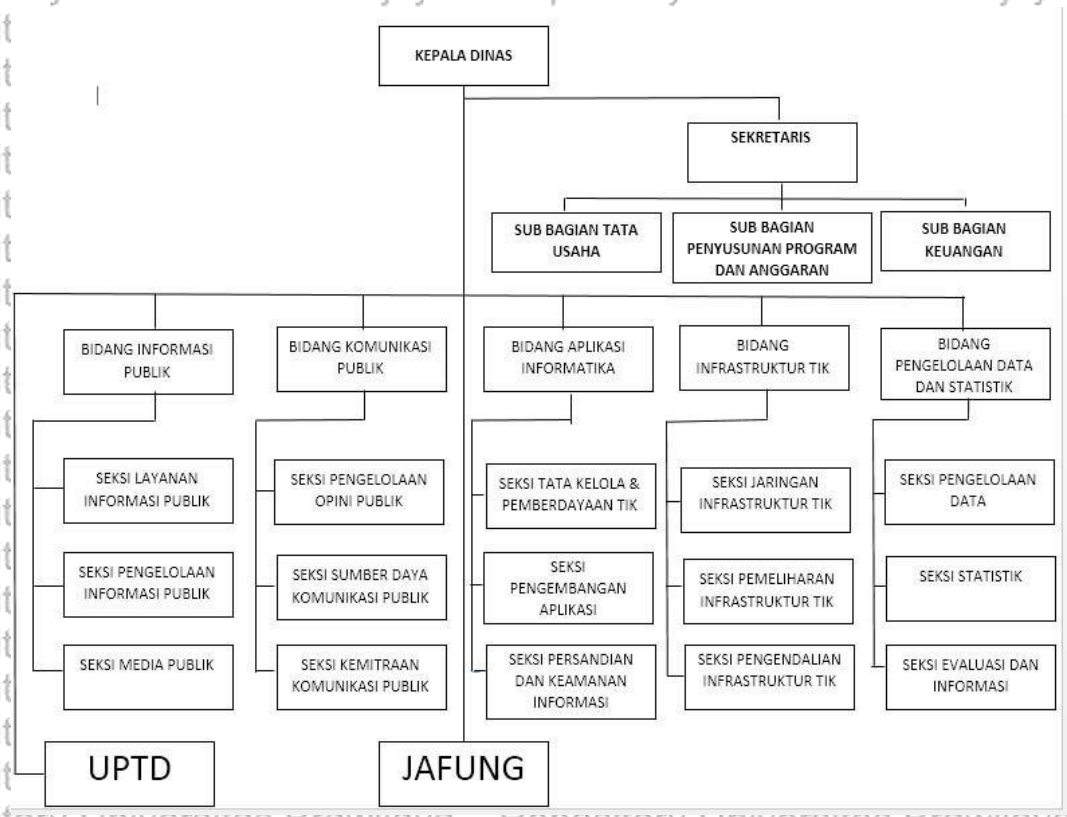
Visi : "Terwujudnya Penyebarluasan Informasi dan Pelayanan Publik melalui TIK di Jawa Timur"

Misi :

1. Meningkatkan kapasitas layanan penyebaran informasi, memberdayakan potensi masyarakat serta kerjasama lembaga komunikasi dan informatika.
2. Mengembangkan aplikasi, muatan layanan publik, standarisasi penyelenggaraan pos dan telekomunikasi serta pemanfaatan jaringan TIK dalam rangka peningkatan pelayanan publik.

2.2.1 Struktur Organisasi Dinas Komunikasi dan Informatika Provinsi Jawa Timur

Struktut Organisasi Dinas Komunikasi dan Informatika Provinsi Jawa Timur adalah sebagai berikut :



Gambar 2.1 Struktur Organisasi Dinas Komunikasi dan Informatika Provinsi Jawa Timur

Sumber :
http://kominfo.jatimprov.go.id/ppid/uploads/berkasppid/SO%20KOMINFO.jpg

2.3 Analisis

Secara umum, arti analisis adalah aktivitas yang memuat sejumlah kegiatan seperti mengurai, membedakan, memilah sesuatu untuk digolongkan dan dikelompokkan kembali menurut kriteria tertentu kemudian dicari kaitannya dan ditafsirkan maknanya. Menurut Spradley (Sugiyono, 2015) mengatakan bahwa analisis adalah sebuah kegiatan untuk mencari suatu pola selain itu analisis merupakan cara berpikir yang berkaitan dengan pengujian secara sistematis terhadap sesuatu untuk menentukan bagian, hubungan antar bagian dan hubungannya dengan keseluruhan. Analisis adalah suatu usaha untuk mengurai suatu masalah atau fokus kajian menjadi bagian-bagian (*decomposition*) sehingga susunan/tatanan bentuk sesuatu yang diurai itu tampak dengan jelas dan

karenanya bisa secara lebih terang ditangkap maknanya atau lebih jernih dimengerti duduk perkaranya.

Nasution dalam Sugiyono (2015) melakukan analisis adalah pekerjaan sulit, memerlukan kerja keras. Tidak ada cara tertentu yang dapat diikuti untuk mengadakan analisis, sehingga setiap peneliti harus mencari sendiri metode yang dirasakan cocok dengan sifat penelitiannya. Bahan yang sama bisa diklasifikasikan berbeda.

2.4 Evaluasi

Evaluasi disadur dari Bahasa Inggris "*evaluation*" yang dapat diartikan sebagai penilaian. Evaluasi merupakan proses dalam menentukan suatu nilai pada suatu hal atau objek yang didasarkan kepada acuan tertentu sehingga mendapatkan hasil atau tujuan dimana penilaian ini bisa bersifat netral, positif atau negatif. Saat melakukan evaluasi, biasanya akan diikuti dengan pengambilan keputusan terhadap objek evaluasi. Menurut Kamus Besar Bahasa Indonesia (KBBI), evaluasi merupakan suatu penilaian secara teknis dan ekonomis terhadap suatu permasalahan untuk perkembangan objek yang akan dievaluasi. Lalu menurut Suharsimi Arikunto (2003), evaluasi merupakan serangkaian aktivitas yang memiliki tujuan dalam mengukur tingkat keberhasilan pada suatu program. Sehingga dapat disimpulkan evaluasi merupakan serangkaian aktivitas secara teknis terhadap suatu objek permasalahan untuk mengukur tingkat keberhasilan agar dapat digunakan sebagai perkembangan objek yang akan dievaluasi.

2.5 Sistem Informasi

Sistem Informasi merupakan sebuah sistem yang dibuat dan digunakan oleh sebuah organisasi yang didalamnya terdapat kombinasi antara teknologi, fasilitas dan *user* atau pengguna yang saling berhubungan sehingga menciptakan alur komunikasi yang beragam sehingga dapat dijadikan sebagai dasar dalam pembuatan keputusan. Menurut Gordon B. Davis (1991) Sistem informasi adalah sebuah sistem yang menerima masukan atau *input* yang berupa data maupun instruksi-instruksi lalu sistem tersebut akan mengola data tersebut sesuai dengan instruksi yang tepat sehinggal menghasilkan suatu keputusan. Lalu menurut Hanif Al Fatta (2009) Sistem Informasi merupakan sekumpulan data yang telah terorganisir dan tata cara penggunaannya yang mencakup lebih jauh dari sekedar penyajian data. Keberhasilan sebuah sistem informasi diukur berdasarkan tujuan pembuatannya berdasarkan tiga faktor yaitu keserasian dan mutu data, pengorganisasian data, dan tata cara penggunaannya. untuk memenuhi permintaan penggunaan tertentu, maka struktur dan cara kerja sistem informasi berbeda-beda ber gantung pada macam keperluan atau macam permintaan yang harus dipenuhi. Suatu persamaan yang menonjol ialah suatu sistem informasi menggabungkan berbagai ragam data yang dikumpulkan dari berbagai sumber untuk dapat menggabungkan data yang berasal dari berbagai sumber suatu sistem alih rupa (*transformation*) data sehingga jadi tergabungkan (*compatible*). Berapa pun ukurannya dan apapun ruang lingkupnya suatu sistem informasi perlu memiliki ketergabungan (*compatibility*) data yang disimpannya.

2.6 Keamanan Informasi

Menurut O'brien dan Marakas (2010), informasi didefinisikan sebagai data yang telah diubah sedimikian rupa sehingga mempunyai arti tertentu dan memiliki guna bagi pengguna atau *user.* Data adalah fakta atau observasi mengenai transaksi-transaksi bisnis. Dengan demikian, didapatkan sebuah kesimpulan yaitu informasi merupakan data yang telah diatur sedimikian rupa lalu diproses sehingga memiliki nilai dan arti sehingga bisa digunakan untuk memenuhi kebutuhan pengguna atau *user.*

Keamanan informasi mendukung pengamanan informasi yang terjamin kerahasiannya (*confidentiality)*, ketersediaannya (*availability)*, dan keutuhannya (*integrity*). Dengan adanya tata kelola keamanan informasi sebagai bentuk dukungan keamanan informasi agar risiko-risiko yang dapat disebabkan oleh kurangnya pengelolaan keamanan informasi dapat diminimalisir, dikurangi maupun dihindari. Keamanan informasi adalah salah satu aspek yang penting dari beberapa aspek lainnya pada tata kelola teknologi informasi dimana kinerja teknologi informasi dapat terganggu jika data yang dimiliki oleh suatu organsisasi tidak dikelola sesuai dengan tata kelola kemanan informasi yang baik terkait kerahasiannya (*confidentiality)*, ketersediaannya (*availability)*, dan keutuhannya (*integrity*).

2.7 ISO/IEC 27001:2013

International Organization for Standarization (ISO) dan *International Electrotecnical Comission* (IEC) membentuk sistem khusus untuk standarisasi diseluruh dunia. Untuk memberi gambaran awal kepada organisasi terkait sistem manajemen keamanan mereka, ISO dan IEC sudah mengembangkan beberapa standar yang disebut sebagai standar keluarga sistem manajemen keamanan informasi 27000:2013. Standar ini dimulai dari ISO/IEC 27001, standar ini disiapkan untuk memberikan persyaratan untuk menetapkan, menerapkan, memelihara dan terus meningkatkan Sistem Manajemen Keamanan Informasi (SMKI) bagi organisasi. Penting untuk diketahui bahwa standar ini bersifat independen terhadap produk teknologi informasi, penggunaan pendekatan manajemen berbasis resiko untuk menjamin supaya kontrol-kontrol keamanan yang dipilih mampu melindungi dan menjaga informasi dari berbagai macam ancaman, dan memberikan keyakinan keamanan bagi pihak yang berkepentingan. Standar ini dapat digunakan oleh pihak internal dan eksternal untuk menilai kemampuan organisasi untuk memenuhi persyaratan keamanan informasi organisasi mereka.

ISO 27001:2013 adalah sebuah standar Internasional yang berguna dalam penerapan sistem manajemen keamanan informasi (SMKI) atau *Information Security Management System* (ISMS). Sistem manajemen keamanan informasi merupakan seperangkat unsur yang saling berkaitan antara organisasi, instansi maupun perusahaan yang dapat digunakan untuk mengelola dan mengendalikan risiko-risiko keamanan informasi. Selain itu, Sistem manajemen keamanan informasi juga berfungsi untuk melindungi dan menjaga kerahasiaan,

ketersediaan, dan integritas informasi. ISO 27001:2013 memiliki beberapa manfaat yaitu untuk melindungi informasi tentang klien dan informasi tentang karyawan, lalu untuk mengelola risiko keamanan informasi secara efektif, mencapai kepatuhan terhadap kontrol-kontrol objektif yang ada pada ISO 27001:2013, dan manfaat terakhir adalah untuk melindungi citra perusahaan dalam perlindungan data dan informasi.

ISO 27001:2013 terdiri dari 10 klausa sebagai *mandatory process* yang merupakan persyaratan yang harus diterapkan dan dipenuhi dalam penerapan sistem manajemen keamanan informasi meliputi :

1. Lingkup standar.
2. Diferensiasi dokumen.
3. Istilah maupun definisi pada ISO/IEC 27000.
4. Hubungan antara organisasi atau instansi dengan *stakeholder.*
5. Dukungan terhadap kebijakan keamanan informasi.
6. Perencanaan sistem manajemen keamanan informasi, perkiraan terhadap risiko dan kontrol terhadap risiko.
7. Dukungan terhadap sistem manajemen keamanan informasi.
8. Pembuatan operasional sistem manajemen keamanan informasi.
9. Peninjauan kinerja sistem.
10. Tindakan korektif terhadap risiko kemanan informasi.

Standar internasional ini menerapkan struktur tingkat tinggi, dimana struktur ISO/IEC 27001:2013 dibagi 2 bagian didalam strukturnya, yang pertama adalah *mandatory process,* lalu terdapat *Annex A: Security Control* yang merupakan bagian penting yang menjadi persyaratan sertifikasi bagi organisasi berupa lampiran yang disediakan untuk menentukan kontrol keamanan yang perlu diterapkan dalam sistem manajemen keamanan informasi. *Annex A: Security Control* terdiri dari 114 kontrol dalam 14 area kontrol yaitu :

1. A.5: Kebijakan keamanan (*Security policy)*
2. A.6: Organisasi keamanan informasi (*Organization of information security)*
3. A.7: Keamanan sumber daya manusia (*Human resource security)*
4. A.8: Manajemen aset (*Asset management)*
5. A.9: Kontrol akses (*Access control*)
6. A.10: Kriptografi (*Cryptography*)
7. A.11: Keamanan fisik dan lingkungan (*Physical and environmental security*)
8. A.12: Keamanan operasi (*Operation security*)
9. A.13: Keamanan komunikasi (*Communication security*)

10. A.14: Akuisisi, pengembangan, dan pemeliharaan sistem (*System acquisition, development, and maintenance*)
11. A.15: Hubungan dengan pemasok (*Supplier relationship*)
12. A.16: Manajemen insiden keamanan informasi (*Information security incident management*)
13. A.17: Aspek keamanan informasi dari manajemen kelangsungan bisnis (*Information security aspect of business continuity management*)
14. A.18: Kepatuhan (*Compliance*)

2.8 Peraturan Menteri Komunikasi dan Informatika No 4 Tahun 2016

Berdasarkan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi, Dinas Komunikasi dan Informatika Provinsi Jawa Timur selaku penyelenggara sistem elektronik perlu melakukan evaluasi pada sistem elektronik yang dimiliki seperti berbagai perangkat dan prosedur elektronik yang memiliki fungsi untuk mengumpulkan, mengolah, menganalisis, hingga menampilkan informasi yang bersifat elektronik. Pada peraturan ini membahas 12 bab terkait ketentuan umum, kategorisasi sistem elektronik, standar sistem manajemen pengamanan informasi, penyelenggaraan, Lembaga sertifikasi, penerbitan sertifikat, pelaporan hasil sertifikasi, dan pencabutan sertifikat, penilaian mandiri, pembinaan, pengawasan, sanksi, ketentuan peralihan, dan yang terakhir yaitu ketentuan penutup.

Lalu pada peraturan ini juga terdapat beberapa lampiran seperti format lampiran pernyataan kategori sistem elektronik yang berisi kuisioner untuk menentukan kategori sistem elektronik yang dimiliki oleh penyelenggara sistem elektronik apakah termasuk pada kategori rendah, tinggi, atau strategis, dimana setiap kategori memiliki ambang batas nilai untuk mencapai kategori tersebut. Jika penyelenggara sistem elektronik mendapatkan kategori "rendah", maka harus menerapkan pedoman Indeks Keamanan Informasi atau Indeks KAMI, lalu jika mendapat kategori "Tinggi" maka penyelenggara sisten elektronik harus menerapkan standar SNI ISO/IEC 27001, dan jika mendapatkan kategori "Strategis", penyelenggara sistem elektronik harus menerapkan standar SNI ISO/IEC 27001 dan ketentuan pengamanan yang ditetapkan oleh Instansi Pengawas dan Pengatur Sektornya. Kuisioner ini juga telah dilampirkan pada kuisioner Indeks KAMI sehingga Indeks KAMI mampu mengukur kategori sistem elektronik yang dimiliki oleh penyelenggara sistem elektronik selain menilai aspek pengamanan informasi.

Lalu terdapat lampiran permohonan pengakuan sebagai Lembaga sertifikasi sistem manajemen pengamanan informasi, lampiran surat pernyataan lembaga sertifikasi yang beris. Selanjutnya terdapat lampiran sertifikat penetapan pengakuan Lembaga sertifikasi sistem manajemen pengamanan informasi dan lampiran laporan Lembaga sertifikasi sistem manajemen pengamanan informasi.

2.9 Korelasi Indeks KAMI dengan ISO 27001

Setiap area yang berada pada indeks KAMI didasari oleh aspek keamanan yang ditetapkan dalam standar ISO/IEC 27001:2013. Indeks KAMI meenggunakan 14 kontrol keamanan pada Annex A ISO/IEC 27001:2013 yang digambarkan pada gambar 2.2

	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 Environtmental Security				✓		
Operation Security			✓	✓	✓	✓
Communication Security	✓		✓	✓	✓	✓
System Acquisition, Development and Maintenance			✓	✓	✓	
Supplier Relationship				✓		
Information Security Incident Management	✓	✓	✓	✓	✓	✓
Information Security Aspects of BCM	✓	✓	✓		✓	✓
Compliance	✓	✓	✓	✓	✓	✓

Gambar 2.2 Hubungan Indeks KAMI versi 4.0 dengan ISO/IEC 27001:2013

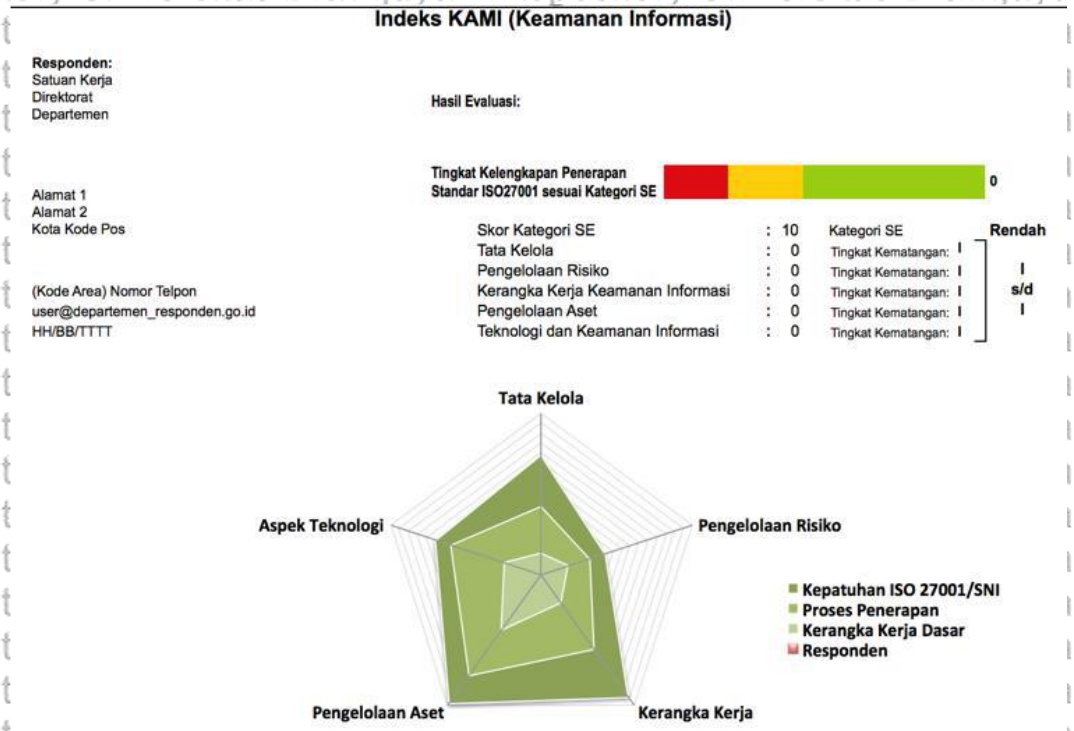
Pada gambar 2.2 digambarkan bahwa hubungan setiap area pada Indeks KAMI versi 4.0 berada pada beberapa area kontrol ISO/IEC 27001:2013.

2.10 Indeks Keamanan Informasi 3.1 (KAMI 3.1)

Menurut Direktorat Keamanan Informasi dan Kementrian Komunikasi dan Informatika, Indeks Keamanan Informasi (KAMI) adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan instansi. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenhi semua aspek keamanan yang didefiniskan oleh standar SNI ISO/IEC 27001:2013. Bentuk evaluasi yang diterapkan dalam indeks Keamanan Informasi (KAMI) dirancang untuk dapat digunakan oleh suatu organisasi dari berbagai tingkatan, ukuran, maupun tingkat kepentingan TIK dalam mendukung terlaksananya proses yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan *snapshot* indeks kesiapan dari aspek kelengkapan maupun kematangan kerangka kerja keamanan informasi yang diterapkan dan dapat digunakansebagai pembanding dalam rangka menyusun langkah perbaikan dalam penetapan prioritasnya.

Organisasi dapat menggunakan indeks Keamanan Informasi (KAMI) untuk

mendapatkan gambaran mengenai kematangan program kerja keamanan informasi yang dijalankannya seperti pada Gambar 2.2.



Gambar 2.2 Tampilan *Dashboard* Indeks KAMI Versi 3.1

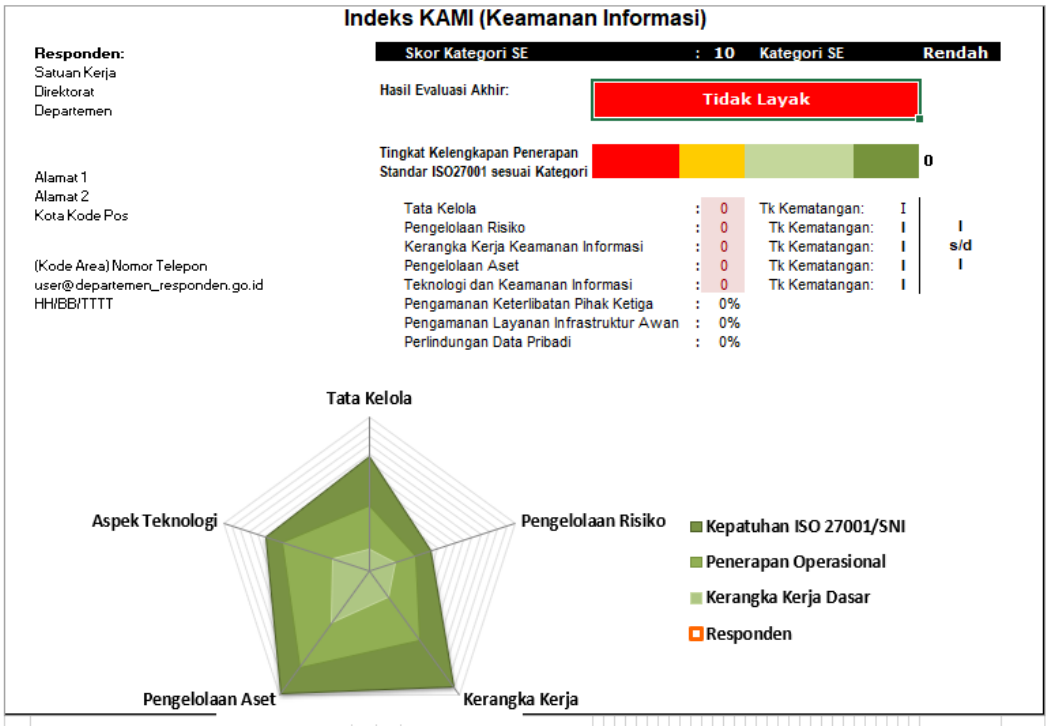
Sumber: Indeks Keamanan Informasi (KAMI) Versi 3.1 (2015)

Pada proses evaluasi indeks Keamanan Informasi (KAMI) terdapat 2 kategori yaitu kategori sistem elektronik dimana pada kategori ini bertujuan untuk mengetahui kondisi, karakteristik maupun tingkatan sistem elektronik yang digunakan suatu instansi untuk mendukung proses bisnisnya dan bagian ini bertujuan untuk mengevaluasi tingkat atau kategori sistem elektronik yang digunakan pada instansi. Kemudian, kategori terkait dengan keamanan informasi yang dilakukan di lima area yang menjadi target dari indeks Keamanan informasi, yaitu tata kelola keamanan informasi, bagian ini bertujuan untuk mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi, pengelolaan risiko keamanan informasi, bagian ini bertujuan untuk mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagi dasar penerapan strategi keamanan informasi, Kerangka kerja keamanan informasi, bagian ini bertujuan untuk mengevaluasi kelengkapan dan kesiapan kerangka kerja pengeloaan keamanan informasi dan strategi penerapannya, pengelolaan aset informasi, bagian ini bertujuan untuk mengevaluasi kelengkapan aset informasi, dan teknologi keamanan informasi, bagian ini bertujuan untuk mengevaluasi kelengkapan, konsistensi, dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.

2.11 Indeks Keamanan Informasi 4.0 (KAMI 4.0)

Indeks KAMI merupakan sebuah alat evaluasi yang digunakan untuk menganalisis tingkat kesiapan (kelengkapan dan kematangan) keamanan informasi di intansi pemerintahan. Indeks KAMI tidak ditujukan untuk menganalisis kelayakan atau efektifitas bentuk pengaman yang ada melainkan digunakan sebagai alat bantu yang menggambarkan kesiapan kerangka kerja keamanan informasi kepada pimpinan eksekutif instansi pemerintahan tersebut. Penilaian ini dilakukan terhadap dua area besar target penerapan keamanan informasi yaitu area Sistem Elektronik dan area Kemanan Informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2013, yaitu kategori sistem elektronik, tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, teknologi keamanan informasi dan area terbaru yaitu suplemen.

Hasil evaluasi dari indeks KAMI akan menggambarkan tingkat kelengkapan penerapan ISO/IEC 27001:2013 dan peta area tata kelola keamanan sistem informasi di instansi pemerintahan seperti pada gambar 2.3 dibawah ini.



Gambar 2.3 Tampilan *dashboard* Indeks KAMI Versi 4.0

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Pada kategori Sistem Elektronik, menggambarkan tentang bagaimana keadaan Sistem Elektronik yang diimplementasikan pada instansi terkait untuk mendukung proses kerja dari instansi terkait dimana hasil penggambarannya berupa tingkatan atau kategori. Area I yaitu kategori sistem elektronik, pada bagian ini responden atau narasumber diminta untuk mendefinisikan tingkat atau kategori sistem elektronik yang terdapat di organisasi.

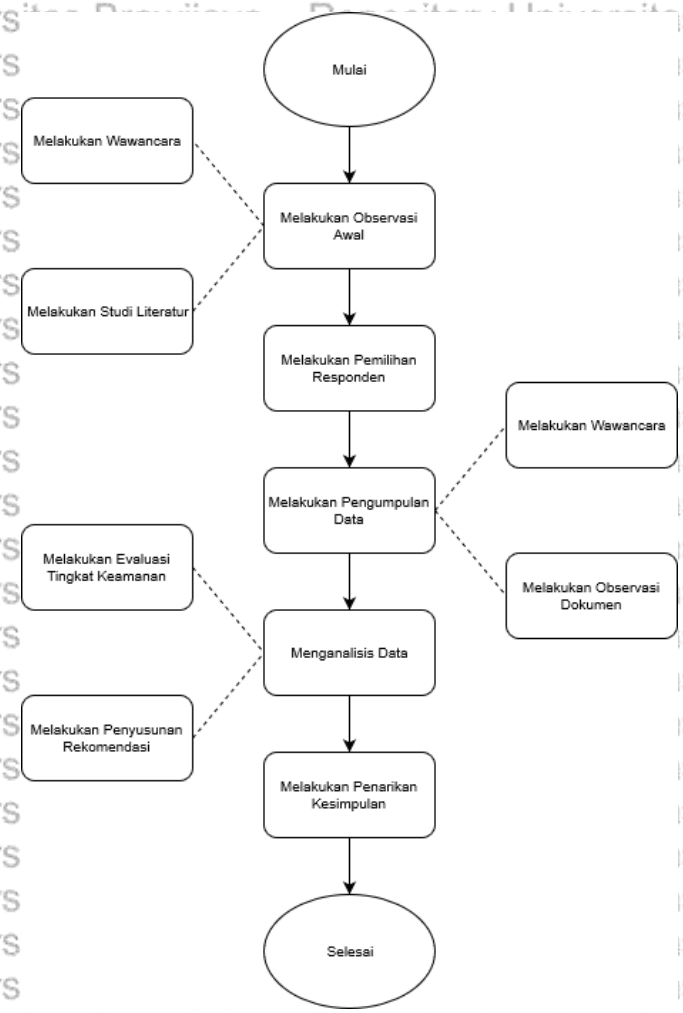
Area Keamanan Informasi terdiri dari 6 area, yaitu dimulai dari area II sampai area VII, area II terkait tata kelola keamanan informasi; area III pengelolaan risiko kemanan informasi, area IV kerangka kerja pengelolaan keamanan informasi, area V pengelolaan aset informasi, dan area VI teknologi dan keamanan informasi dan area VII suplemen.

BAB 3 METODOLOGI

Penelitian ini menggunakan alat bantu Indeks Keamanan Informasi (KAMI) dengan objek penelitian yaitu Dinas Komunikasi dan Informatika Provinsi Jawa Timur (DISKOMINFO PROV. JATIM) untuk menganalisis tingkat kesiapan keamanan informasi organisasi saat ini.

3.1 Metodologi Penelitian

Metodologi penelitian merupakan langkah-langkah yang dilakukan oleh peneliti dalam mengumpulkan informasi atau data untuk melakukan investigasi pada informasi atau data yang telah didapatkan tersebut. Metodologi berisi alur atau tahapan dalam melakukan analisis tingkat kesiapan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur (DISKOMINFO PROV. JATIM). Penelitian ini merupakan penelitian non-implementatif deskriptif.



Gambar 3.1 Alur Metodologi Penelitian

Gambar 3.1 menjelaskan alur bagaimana penelitian ini akan dilakukan dengan rincian sebagai berikut:

1. Observasi awal dilakukan melalui dua cara yaitu melalui wawancara dan studi literatur. Wawancara dilakukan berdasarkan panduan penerapan Indeks Keamanan Informasi (KAMI) kepada *stakeholder* yang berwenang di Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Lalu studi literatur dilakukan dengan membaca buku, penelitian-penelitian yang menggunakan Indeks KAMI, *paper,* maupun jurnal sehingga penelitian ini semakin kaya akan referensi dan mendapatkan metode yang sesuai untuk melakukan analisis.
2. Pemilihan responden dilakukan dengan melihat struktur organisasi yang ada pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur dan melihat jabatan yang berhubungan dengan keamanan informasi dan berwenang dengan bidang teknologi informasi.
3. Pengumpulan data dilakukan dengan memetakan dengan wawancara dan mengisi instrument berupa kuisioner yang akan diisi oleh *stakeholder* yang berwenang di Bidang Teknologi Informasi dan Komunikasi Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Kemudian akan dilanjutkan dengan observasi dokumen yang selanjutnya akan dikonfirmasi dan validasi dengan metode *checklist* untuk memverifikasi data dan dokumen yang dibutuhkan dengan keadaan sebenarnya.
4. Analisis data dilakukan dengan melakukan perhitungan hasil kuisioner dengan menggunakan standar yang telah disediakan oleh Indeks Keamanan Informasi (KAMI) sehingga akan menghasilkan tingkat kelengkapan dan keamanan informasi. Lalu akan dibandingkan dengan ISO/IEC 27001:2013 yang kemudian akan dilanjutkan dengan penyusunan rekomendasi perbaikan.
5. Penarikan kesimpulan atas analisis yang dilakukan yang kemudian pemberian saran-saran untuk penelitian selanjutnya pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

3.2 Observasi Awal

Penelitian ini dimulai dengan melakukan observasi awal. Terdapat dua pendekatan, pendekatan pertama adalah dengan cara wawancara penggalian informasi dari narasumber agar mendapat informasi yang akurat dan aktual. Berdasarkan panduan Indeks Keamanan Informasi, wawancara dilakukan kepada *stakeholder* yang bertanggung jawab pada bidang keamanan informasi yang terdapat pada Dinas Komunikasi dan Informasi Provinsi Jawa Timur yaitu pada seksi persandian dan keamanan informasi. Pendekatan berikutnya dilakukan dengan studi literatur referensi-referensi teori yang memiliki relevansi dengan kasus maupun masalah yang ditemukan melalui referensi seperti jurnal, buku, maupun *paper* sehingga dengan studi literatur dapat memberikan metode yang sesuai yaitu dengan Indeks Keamanan Informasi (KAMI) dan ISO 27001:2013.

3.3 Pemilihan Responden

Setelah melakukan observasi awal, lalu penelitian akan dilanjutkan dengan pemilihan responden. Pemilihan responden didasarkan kepada Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (KAMI) yaitu pejabat yang bertanggung jawab dan mempunyai wewenang dalam bidang keamanan informasi. Pada penelitian ini memilih responden khususnya pejabat yang berwenang di Bidang Teknologi Informasi dan Komunikasi terutama di Seksi Persandian dan Keamanan Informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

3.4 Pengumpulan Data

Tahap berikutnya dalam penelitian ini adalah melakukan pengumpulan data. Langkah pertama yang dilakukan dalam pengumpulan data dilakukan setelah memilih responden adalah dengan cara pengisian kuisioner dan tanya jawab pada saat proses penggalian dan pengumpulan data. Teknik atau metode yang digunakan peneliti pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur adalah melalui observasi yang selanjutnya dengan memberikan kuisioner kepada responden. Kuisioner yang akan diberikan kepada responden beracuan kepada Indeks Keamanan Informasi (KAMI) versi 4.0. Setelah responden mengisi kuisioner, dilanjutkan dengan melakukan ulasan terhadap kuisioner yang telah diisi, namun sebelum responden menjawab pertanyaan terkait pengamanan informasi, responden akan diminta untuk mendefinisikan kategori sistem elektronik dan mendeskripsikan infrastruktur Teknologi Informasi dan Komunikasi (TIK) yang ada dalam unit kerjanya secara singkat pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Tabel 3.1 Tingkat Kategori Sistem Elektronik

Total Skor Bagian I (Kategori Sistem Elektronik)	**10-15**	**16-34**	**35-50**
Tingkat Kategori Sistem Elektronik	Rendah	Tinggi	Strategis

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Adapun tujuan proses ini adalah untuk mengkategorikan sistem elektronik yang dimiliki dan digunakan ke dalam tingkat tertentu yaitu rendah, tinggi, atau strategis seperti pada tabel 3.1 diatas. Pada kategori Sistem Elektronik berisi sepuluh pertanyaan untuk mengevaluasi kategori sistem elektronik yang dimiliki dan digunakan oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

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**		
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	A	5
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	A	5
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	A	5
1.4	Menggunakan algoritma khusus untuk keamanan informasi dalam Sistem Elektronik [A] Algoritma khusus yang digunakan Negara [B] Algoritma standar publik [C] Tidak ada algoritma khusus	A	5

Gambar 3.2 Kuisioner I Kategori Sistem Elektronik

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Lalu pada gambar 3.2 menggambarkan tentang kuisioner pada area pertama pada Indeks Keamanan Informasi yaitu kategori Sistem Elektronik. Dalam kuisioner kategori Sistem Elektronik berisi beberapa pertanyaan yang berkaitan dengan karakteristik Sistem Elektronik yang dimiliki dan digunakan pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur, dimana terdapat kolom status untuk yang didalamnya berisi opsi-opsi yang dapat dipilih yang berbeda disetiap nomornya. Setelah memilih opsi yang tersedia, setiap pertanyaan akan memberikan nilai pada kolom skor dimana skor ini berubah sesuai dengan opsi yang dipilih dari seluruh pertanyaan akan diakumulasi dan nantinya akan menggambarkan tingkat kategori Sistem Elektronik pada tabel 3.1.

Area Pengamanan Informasi memiliki tujuan untuk menggambarkan kondisi keamanan informasi sebagai hasil dari pogram kerja yang dijalankan. Pada area pengamanan informasi terdapat 6 bagian yaitu pada area II sampai dengan area VII, yaitu area II: Tata Kelola Keamanan Informasi, area III: Pengelolaan Risiko Keamanan Informasi, area IV: Kerangka Kerja Pengelolaan Informasi, area V: Pengelolaan Aset Informasi, area VI: Teknologi dan Keamanan Informasi, dan area VII: Suplemen. Pada setiap pertanyaan area pengamanan informasi ini terdapat tingkatan kategori, diantaranya:

1. Kategori 1 (Label 1) adalah pertanyaan area yang terkait dengan bentuk kerangka kerja dasar keamanan informasi.
2. Kategori 2 (Label 2) adalah pertanyaan area yang terkait dengan efektifitas dan efisiensi penerapan keamanan informasi.
3. Kategori 3 (Label 3) adalah pertanyaan area yang terakit dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi. Dimana pada tingkat ini merupakan tingkat kesiapan

minimum yang di prasyaratkan oleh proses sertifikasi standar ISO/IEC:27001:2013.

Dimana pada kuisioner pada area pengamanan informasi menetapkan pilihan jawaban pada setiap pertanyaannya yang terkait dengan kondisi atau status penerapan keamanan informasi pada instansi. Status atau kondisi yang menjadi pilihan jawaban yaitu, "Tidak Dilakukan"; "Dalam Perencanaan", "Dalan Penerapan atau Diterapkan Sebagian"; dan "Diterapkan Secara Menyeluruh". Setiap opsi jawaban diatas memiliki skor yang berbeda berdasarkan tahapan atau status penerapan dan kategori dari setiap area pengamanan informasi. Pada status penerapan, status penerapan tingkat awal nilainya akan lebih rendah dibandingkan status penerapan tingkat selanjutnya. Seperti pada Tabel 3.2 yang membentuk sebuah matriks antara status penerapan dan kategori pengamanan.

Tabel 3.2 Matriks Kategori Pengamanan Informasi

Status Penerapan	Kategori Pengamanan Informasi		
	Kategori 1	**Kategori 2**	**Kategori 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 (KAMI) Versi 4.0 (2019)

Pada Gambar 3.3 menjelaskan gambaran kuesioner pada area pengamanan informasi dan penjelasan setiap kolom yang terdapat pada kuisioner area pengamanan informasi pada area II sampai dengan area VII yang mempunyai atribut dan kolom yang sama, berikut adalah penjelasannya:

1. Tingkat Kematangan merupakan tingkatan kematangan keamanan informasi yang terdiri dari 5 tingkatan yaitu, Kondisi Awal; Penerapan Kerangka Kerja; Terdefinisi dan Konsisten; Terkelola dan Terstruktur; dan Optimal.
2. Kategori Pengamanan Informasi merupakan kategori pertanyaan yang terdiri dari 3 kategori.
3. Daftar Pertanyaan merupakan pertanyaan yang akan dijawab oleh responden.
4. Status Penerapan merupakan opsi jawaban yang menggambarkan kondisi atau status dari setiap pertanyaan.
5. Skor merupakan nilai berdasarkan status penerapan dan kategori pengamanan informasi.

Konfirmasi data dilakukan untuk pengecekan kesahan dan validasi suatu data. Konfirmasi data dilakukan dengan metode triangulasi data, yaitu menggali kebeneran informasi atau data tertentu melalui berbagai metode dan sumber perolehan data. Dalam penelitian ini dilakukan metode *checklist* untuk konfirmasi data dengan membandingkan antara hasil kuisioner dari responden dan kondisi atau keadaan yang sebenarnya. *Checklist* dilakukan langsung terhadap responden atau secara tatap muka, pada penelitian ini juga membutuhkan dokumen bukti dari hasil kuisioner untuk mendukung kuisioner dengan status penerapan "Dalam Penerapan atau Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh.

3.5 Analisis Data

Analisis data dilakukan apabila semua data yang dibutuhkan telah didapatkan melalui kuisioner dan *checklist,* maka selanjutnya data tersebut akan dijumlahkan dan dianalisis untuk menghasilkan rekomendasi. Perhitungan skor didapatkan dari penjumlahan masing-masing area yang disajikan dalam dua instrument yaitu tabel penilaian tiap area dan diagram radar dengan lima sumbu. Lalu dilakukan penghitungan untuk menentukan ambang batas pencapaian tingkat kematangan dan kesiapan mulai dari tingkat I hingga V dan setiap ambang batas diberikan nilai + guna memberikan penialain yang rinci pada setiap area. Hasil setiap penjumlahan skor pada tiap area keamanan informasi akan ditampilkan kedalam dua instrument seperti dibawah ini:

3.5.1 Tabel nilai tiap area kemanan informasi

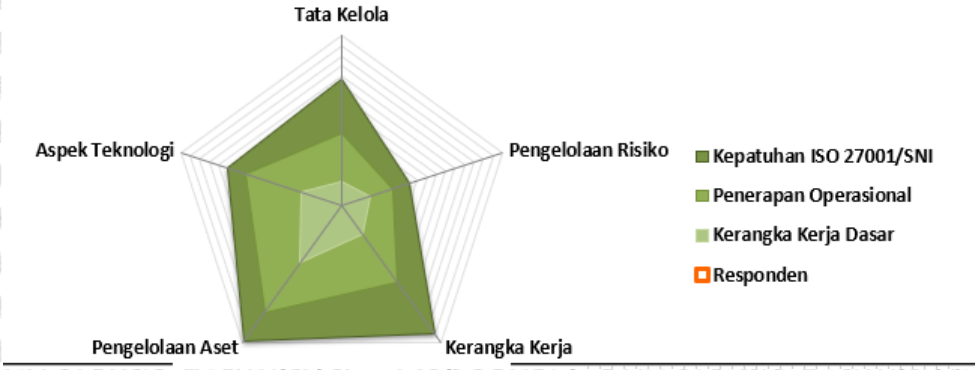
Tata Kelola	:	0
Pengelolaan Risiko	:	0
Kerangka Kerja Keamanan Informasi	:	0
Pengelolaan Aset	:	0
Teknologi dan Keamanan Informasi	:	0
Pengamanan Keterlibatan Pihak Ketiga	:	0%
Pengamanan Layanan Infrastruktur Awan	:	0%
Perlindungan Data Pribadi	:	0%

Gambar 3.3 Skor tiap area

Sumber: Indeks KAMI versi 4.0 (2019)

Gambar 3.3 merupakan tabel yang berisikan total skor pada tiap area yang dievaluasi yang berguna untuk menghitung nilai akhir keamanan informasi.

3.5.2 Radar chart



Gambar 3.4 *Radar Chart*

Sumber: Indeks KAMI versi 4.0 (2019)

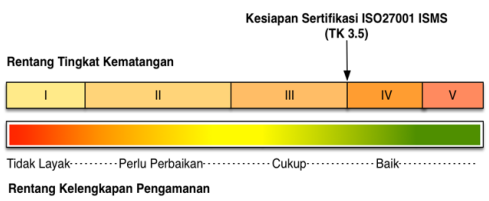
Pada gambar 3.4 merupakan *Radar Chart* yang berisi ambang batas tingkat kelengkapan kategori 1 hingga 3 yang ditunjukkan dengan latar belakang area dengan warna hijau muda hingga hijau tua. Setiap nilai are keamanan infromasi ditunjukkan oleh area yang berwarna merah. *Radar Chart* ini akan menampilkan perbandingan kondisi kesiapan sebagai hasil dari proses evaluasi.

Tingkat keamanan pada Indeks KAMI versi 4.0 terdiri dari 5 tingkatan yaitu:

1. Tingkat I : Kondisi Awal
2. Tingkat II : Penerapan Kerangka Kerja Dasar
3. Tingkat III : Terdefinisi dan Konsisten
4. Tingkat IV : Terkelola dan Terukur
5. Tingkat V : Optimal

Untuk membantu memberikan penialian yang lebih rinci terhadap tingkat kematang, maka tingkat ini dikembangkan menjadi 9 tingkatan dengan tambahan atribut + pada setiap tingkatnya mulai dari tingkat I+ hingga IV+.

Padanan terhadap standar ISO/IEC 2700:2005, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah Tingkat III+ (3,5) atau garis ukur berada pada warna hijau dan dapat dikatan baik seperti pada Gambar 3.5



Gambar 3.5 Tingkat Kesiapan sertifikasi ISO 27001

Sumber: Indeks KAMI versi 4.0 (2019)

3.5.3 Membuat Rekomendasi

Setelah melakukan analisis data dari perhitungan Indeks KAMI, kemudian dilakukan penilai terhadap syarat-syarat yang ada pada ISO 27001, dengan cara melakukan perbandingan terhadap syarat-syarat yang terpenuhi dan syarat-syarat yang belum terpenuhi. Syarat-syarat yang belum memenuhi persyaratan ISO 27001 akan diberikan rekomendasi. Rekomendasi dibuat untuk digunakan sebagai acuan bagi organisasi untuk melakukan perbaikan agar keadaan tata kelola keamanan informasi saat ini dapat sesuai dengan standar ISO 27001.

3.6 Penarikan Kesimpulan

Pembuatan kesimpulan dilakukan dengan mengulas dan membahas terkait keamanan informasi, evaluasi keamanan informasi pada penelitian ini, yang akan digunakan untuk dasar atau acuan perbaikan berbentuk rekomendasi untuk mencapai tujuan instansi atau organisasi di masa yang akan datang.

BAB 4 PENGUMPULAN DATA

4.1 Pemilihan Responden

Pada tahap pengumpulan data, sebelumnya dilakukan dengan memilih responden yang memiliki tugas pokok kerja yang berkorelasi dengan keamanan informasi dan berwenang pada bidang teknologi informasi. Lalu, pengumpulan data dilakukan dengan menggunakan wawancara dan instrumen kuisioner sehingga kuisioner ini akan menghasilkan tingkat kematangan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Pemilihan responden didasarkan pada Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (KAMI) yaitu petugas atau pejabat yang bertanggung jawab dan berwenang dalam bidang keamanan informasi, dalam organisasi Dinas Komunikasi dan Informatika Provinsi Jawa Timur, responden diambil dari Seksi Persandian dan Keamanan Informasi dan Bidang Aplikasi Informatika.

Tabel 4.1 Data Responden

No	Nama	Divisi	Tugas
1	Aulia Bahar Pernama, S.Kom, M.ISM	Seksi Persandian dan Keamanan Informasi	1. menyiapkan bahan perumusan kebijakan teknis persandian dan keamanan informasi. 2. menyiapkan bahan perencanaan dan pelaksanaan pengelolaan persandian dan keamanan informasi. 3. menyiapkan bahan koordinasi, sinkronisasi dan fasilitasi peningkatan persandian dan keamanan informasi. 4. menyiapkan bahan pelaksanaan kegiatan peningkatan kapasitas sumber daya aparatur di bidang persandian dan keamanan informasi. 5. menyiapkan bahan pengelolaan Security Operation Center (SOC). 6. menyiapkan bahan analisis sistem keamanan dalam upaya penguatan persandian dan keamanan informasi.

			7. menyiapkan bahan pelaksanaan penanganan dan pemulihan data insiden keamanan informasi. 8. menyiapkan bahan pelaksanaan monitoring, evaluasi, dan pelaporan persandian dan keamanan informasi. 9. melaksanakan tugas-tugas lain yang diberikan oleh Kepala Bidang.
2	Ali Firman Herlambang, S.T	Bidang Aplikasi Informatika	1. Menyiapkan bahan perumusan kebijakan teknis aplikasi informatika. 2. Menyiapkan bahan pelaksanaan teknis aplikasi informatika. 3. Melakasanakan tugas bidang ketata usahaan. 4. Menyiapkan bahan laporan pelaksanaan teknis aplikasi informatika. 5. Melaksanakan tugas lain yang diberikan oleh kepala Sub Bagian Tata Usaha.

4.2 Kategori Sistem Elektronik

Kategori Sistem Elektronik bertujuan untuk mengatahui situasi dan kondisi, karakteristik, alokasi dana, hingga jumlah pengguna sistem elektronik yang digunakan oleh suatu organisasi atau instansi khususnya pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur dalam mendukung proses bisnisnya. Skor yang diperoleh dari kategori sistem elektronik pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur adalah sebesar 25, dimana skor ini menunjukkan bahwa peranan sistem elektronik yang dimiliki oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur termasuk pada kategori "Tinggi" dengan hasil yang diperoleh seperti pada tabel 4.2

Tabel 4.2 Hasil data penilaian pada kategori Sistem Elektronik

Bagian I: Kategori Sistem Elektronik		
Total pertanyaan		10
Pilihan Jawaban	Hasil	Skor
[A]	2	5
[B]	7	2
[C]	1	1
	Total Skor	25

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Tabel 4.2 merupakan hasil dari data kuisioner yang diberikan kepada responden terkait penilaian penetapan kategori Sistem Elektronik yang digunakan oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Setiap butir pertanyaan berisikan 3 pilihan jawaban berupa huruf "A", "B", "C" yang berisi kriteria masing-masing. Kuisioner bagian kategori Sistem Elektronik berisikan 10 pertanyaan dan diperoleh 2 jawaban "A" dengan skor 10, 7 jawaban "B" dengan skor 14, dan 1 jawaban "C" dengan skor 1 sehingga total skor yang diperoleh oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada kategori Sistem Elektronik yaitu 25. Dengan total skor yang diraih ini dapat diartikan bahwa sistem elektronik yang dimiliki oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur berada pada tingkat ketergantungan "Tinggi" dan tidak dapat dipisah dengan proses kerja dan aktivitas-aktivitas instansi.

4.3 Tata Kelola Keamanan Informasi

Pada bagian ini, area tata kelola keamanan informasi akan mengevaluasi bentuk tata kelola keamanan informasi pada Instansi maupun fungsi, tugas dan tanggung jawab pengelolaan keamanan informasi. Pada dalam evaluasi area ini adalah responden akan diberikan kuisioner yang berisi serangkaian pertanyaan berhubungan dengan tata kelola keamanan informasi dengan metode *checklist* untuk mendukung kondisi kondisi yang terjadi sebenarnya pada instansi dengan hasil kuisioner yang diberikan. Pemberian *checklist* hanya pada pilihan kolom status "Dalam penerapan atau Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh". Lalu berikutnya setelah melakukan pemberian *checklist* adalah pemberian tingkat kematangan area tata kelola keamanan informasi berdasarkan hasil kuisioner.

Tabel 4.3 Hasil data penilaian pada Tata Kelola Keamanan Informasi

Bagian II: Tata Kelola Keamanan Informasi							
Jumlah Pertanyaan	KP 1		KP 2		KP 3		Total
	8		8		6		22
Status Pengamanan	Kategori Pengamanan						
	KP 1	Skor KP 1	KP 2	Skor KP 2	KP 3	Skor KP 3	Total
Tidak dilakukan	0	0	0	0	0	0	0
Dalam perencanaan	1	1	1	2	2	3	9
Dalam penerapan atau diterapkan sebagian	3	2	4	4	3	6	40
Diterapkan secara menyeluruh	4	3	3	6	1	9	39
						Total Skor	88

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Tabel 4.3 diatas merupakan hasil penilaian data pada Tata Kelola Keamanan Informasi berupa instrument penelitian kuisioner terkait kesiapan bentuk tata kelola keamanan informasi, tugas dan tanggung jawab tata kelola keamanan informasi. Area Tata Kelola Keamanan Informasi ini terdapat 8 pertanyaan yang berkaitan dengan kategori pengamanan 1 atau yang disingkat dengan KP 1, lalu 8 pertanyaan yang berkaitan dengan kategori pengamanan 2 yang disingkat menjadi KP 2, dan 6 pertanyaan yang berkaitan dengan kategori pengamanan 3 yang lalu disingkat menjadi KP 3 sehingga jika seluruh kategori pengamanan ini dijumlah akan menghasilkan 22 pertanyaan.

Dalam melakukan pengambilan data, responden menjawab pertanyaan berdasarkan opsi pilihan yang telah tersedia yaitu "Tidak dilakukan","Dalam perencanaan","Dalam penerapan / diterapkan sebagian", dan "Diterapkan secara menyeluruh" yang masing-masing opsi pilihan tersebut telah memliki nilainya masing-masing berdasarkan kategori pengamanan. Pada kuisioner bagian Tata Kelola Keamanan informasi yang diberikan didapatkan hasil opsi "Tidak dilakukan" sebanyak 0. Lalu didapatkan hasil opsi "Dalam perencanaan" pada kategori pengamanan 1 sebanyak 1, pada kategori pengamanan 2 sebanyak 1, dan pada kategori pengamanan 3 sebanyak 2 sehingga jika dijumlah akan menghasilkan 4 jawaban opsi "Dalam perencanaan" dengan total skor yang diperoleh yaitu 9. Pada opsi "Dalam penerapan atau diterapkan sebagian" didapakan hasil jawaban

pada kategori pengamanan 1 sebanyak 3, lalu pada kategori pengamanan 2 sebanyak 4 dan pada kategori pengamanan 3 sebanyak 3 sehingga jika dijumlah akan menghasilkan 10 jawaban opsi "Dalam penerapan atau diterapkan sebagian" dengan total skor 40. Dan pada opsi "Diterapkan secara menyeluruh" didapatkan hasil jawaban pada kategori pengamanan 1 sebanyak 4, kategori pengamanan 2 sebanyak 3, dan pada kategori pengamanan 3 sebanyak 1 sehingga jika dijumlah akan menghasilkan 8 jawaban opsi "Diterapkan secara menyeluruh" dengan total skor 39. Jika seluruh skor digabung akan menghasilkan total skor 88 pada bagian Tata Kelola Keamanan Informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Tabel 4.4 Data Penilaian Kematangan Tata Kelola Keamanan Informasi

Jumlah Pertanyaan Tingkat Pertanyaan	II	III	IV	V	Total
	13	3	6	0	22
Status Pengamanan	Tingkat Kematangan				
	II	III	IV	V	Total
Tidak dilakukan	0	0	0	0	0
Dalam perencanaan	2	0	2	0	4
Dalam penerapan / diterapkan sebagian	5	2	3	0	10
Diterapkan secara menyeluruh	6	1	1	0	8
Total	13	3	6	0	22

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Tabel 4.4 menunjukkan data hasil penilaian pada aspek kematangan pada area tata kelola keamanan informasi yang sudah dilakukan pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Pada tingkat kematangan II terdiri dari 13 pertanyaan pada area tata kelola keamanan informasi dimana sebanyak 0 pertanyaan dengan opsi pilihan "Tidak dilakukan", 2 pertanyaan dengan opsi pilihan "Dalam perencanaan", 5 pertanyaan dengan opsi pilihan "Dalam penerapan / diterapkan sebagian", dan 6 jawaban dengan opsi pilihan "Diterapkan secara menyeluruh". Lalu pada tingkat selanjutnya yaitu tingkat kematangan III terdiri dari 3 pertanyaan dimana sebanyak 0 pertanyaan dengan opsi pilihan "Tidak dilakukan", 0 pertanyaan dengan opsi pilihan "Dalam perencanaan", 2 pertanyaan dengan opsi pilihan "Dalam penerapan / diterapkan sebagian", dan 1 jawaban dengan opsi pilihan "Diterapkan secara menyeluruh". Lalu pada tingkat selanjutnya yaitu tingkat kematangan IV terdiri dari 6 pertanyaan dimana sebanyak 0 pertanyaan dengan opsi pilihan "Tidak dilakukan", 2 pertanyaan dengan opsi pilihan "Dalam perencanaan", 3 pertanyaan dengan opsi pilihan "Dalam penerapan / diterapkan sebagian", dan 1 jawaban dengan opsi pilihan "Diterapkan secara menyeluruh". Sedangkan pada area Tata Kelola Keamanan Informasi ini tidak terdapat tingkat kematangan V. Sehingga didasarkan pada data tabel diatas, didapatkan hasil penilaian tingkat kematangan yang berhasil dicapai oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur yaitu pada tingkat II. Tingkat II menandakan bahwa Dinas Komunikasi dan Informatika Provinsi Jawa Timur berada pada tahap

kondisi awal dimana hal ini berarti instansi ini bersifat aktif terhadap risiko keamanan informasi.

4.4 Pengelolaan Risiko Keamanan Informasi

Pada bagian ini, area pengelolaan risiko keamanan informasi akan mengevaluasi kesiapan implementasi terhadap pengelolaan risiko keamanan informasi sebagai dasar dalam implementasi strategi keamanan informasi. Pada evaluasi area ini, responden akan diberikan kuisioner yang berisi serangkaian pertanyaan berhubungan dengan pengelolaan risiko keamanan informasi dengan metode *checklist* untuk mendukung kondisi yang terjadi sebenarnya pada instansi dengan hasil kuisioner yang diberikan. Pemberian *checklist* hanya pada pilihan kolom status "Dalam penerapan atau Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh". Lalu berikutnya setelah melakukan pemberian *checklist* adalah pemberian tingkat kematangan area pengelolaan risiko keamanan informasi berdasarkan hasil kuisioner.

Tabel 4.5 Hasil data penilaian pada Pengelolaan Risiko Keamanan Informasi

Bagian III: Pengelolaan Risiko Keamanan Informasi							
Jumlah Pertanyaan	KP 1		KP 2		KP 3		Total
	10		4		2		16
Status Pengamanan	Kategori Pengamanan						
	KP 1	Skor KP 1	KP 2	Skor KP 2	KP 3	Skor KP 3	Total
Tidak dilakukan	0	0	0	0	0	0	0
Dalam perencanaan	5	1	4	2	2	3	13
Dalam penerapan atau diterapkan sebagian	4	2	0	4	0	6	8
Diterapkan secara menyeluruh	1	3	0	6	0	9	3
						Total Skor	24

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Tabel 4.5 diatas merupakan hasil penilaian data pada Pengelolaan Risiko Keamanan Informasi berupa instrument penelitian kuisioner terkait kesiapan penerapan pengelolaan risiko keamanan informasi dalam penerapan strategi keamanan informasi. Area Pengelolaan Risiko Keamanan Informasi ini terdapat 10

pertanyaan yang berkaitan dengan kategori pengamanan 1 atau yang disingkat dengan KP 1, lalu 4 pertanyaan yang berkaitan dengan kategori pengamanan 2 yang disingkat menjadi KP 2, dan 2 pertanyaan yang berkaitan dengan kategori pengamanan 3 yang lalu disingkat menjadi KP 3 sehingga jika seluruh kategori pengamanan ini dijumlah akan menghasilkan 16 pertanyaan.

Dalam melakukan pengambilan data, responden menjawab pertanyaan berdasarkan opsi pilihan yang telah tersedia yaitu "Tidak dilakukan","Dalam perencanaan","Dalam penerapan / diterapkan sebagian", dan "Diterapkan secara menyeluruh" yang masing-masing opsi pilihan tersebut telah memliki nilainya masing-masing berdasarkan kategori pengamanan. Pada kuisioner bagian Pengelolaan Risiko Keamanan informasi yang diberikan didapatkan hasil opsi "Tidak dilakukan" sebanyak 0. Lalu didapatkan hasil opsi "Dalam perencanaan" pada kategori pengamanan 1 sebanyak 5, pada kategori pengamanan 2 sebanyak 4, dan pada kategori pengamanan 3 sebanyak 2 sehingga jika dijumlah akan menghasilkan 11 jawaban opsi "Dalam perencanaan" dengan total skor yang diperoleh yaitu 13. Pada opsi "Dalam penerapan atau diterapkan sebagian" didapakan hasil jawaban pada kategori pengamanan 1 sebanyak 4, lalu pada kategori pengamanan 2 sebanyak 0 dan pada kategori pengamanan 3 sebanyak 0 sehingga jika dijumlah akan menghasilkan 4 jawaban opsi "Dalam penerapan atau diterapkan sebagian" dengan total skor 8. Dan pada opsi "Diterapkan secara menyeluruh" didapatkan hasil jawaban pada kategori pengamanan 1 sebanyak 1, kategori pengamanan 2 sebanyak 0, dan pada kategori pengamanan 3 sebanyak 0 sehingga jika dijumlah akan menghasilkan 1 jawaban opsi "Diterapkan secara menyeluruh" dengan total skor 3. Jika seluruh skor digabung akan menghasilkan total skor 24 pada bagian Pengelolaan Risiko Keamanan Informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Tabel 4.6 Data Penilaian Kematangan Pengelolaan Risiko Keamanan Informasi

Jumlah Pertanyaan Tingkat Pertanyaan	II	III	IV	V	Total
	10	2	2	2	16
Status Pengamanan	Tingkat Kematangan				
	II	III	IV	V	Total
Tidak dilakukan	0	0	0	0	0
Dalam perencanaan	5	2	2	2	11
Dalam penerapan / diterapkan sebagian	4	0	0	0	4
Diterapkan secara menyeluruh	1	0	0	0	1
Total	10	2	2	2	16

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Tabel 4.6 menunjukkan data hasil penilaian pada aspek kematangan pada area pengelolaan risiko keamanan informasi yang sudah dilakukan pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Pada tingkat kematangan II terdiri dari 10 pertanyaan pada area tata kelola keamanan informasi dimana sebanyak 0 pertanyaan dengan opsi pilihan "Tidak dilakukan", 5 pertanyaan dengan opsi pilihan "Dalam perencanaan", 4 pertanyaan

dengan opsi pilihan "Dalam penerapan / diterapkan sebagian", dan 1 jawaban dengan opsi pilihan "Diterapkan secara menyeluruh". Lalu pada tingkat selanjutnya yaitu tingkat kematangan III terdiri dari 2 pertanyaan dimana sebanyak 0 pertanyaan dengan opsi pilihan "Tidak dilakukan", 2 pertanyaan dengan opsi pilihan "Dalam perencanaan". Lalu pada tingkat selanjutnya yaitu tingkat kematangan IV terdiri dari 2 pertanyaan dimana sebanyak 0 pertanyaan dengan opsi pilihan "Tidak dilakukan", 2 pertanyaan dengan opsi pilihan "Dalam perencanaan". Dan pada tingkat kematangan V terdapat terdiri dari 2 pertanyaan dimana sebanyak 0 pertanyaan dengan opsi pilihan "Tidak dilakukan", 2 pertanyaan dengan opsi pilihan "Dalam perencanaan" sehingga didasarkan pada data tabel diatas, didapatkan hasil penilaian tingkat kematangan yang berhasil dicapai oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur yaitu pada tingkat I+. Tingkat I+ menandakan bahwa Dinas Komunikasi dan Informatika Provinsi Jawa Timur berada pada tahap kondisi awal dimana hal ini berarti instansi ini bersifat reaktif terhadap risiko keamanan informasi.

4.5 Kerangka Kerja Keamanan Informasi

Pada bagian ini, area kerangka kerja keamanan informasi akan mengevaluasi kelengkapan dan kesiapan kerangka kerja yaitu berupa kebijakan maupun prosedur dalam pengelolaan keamanan informasi dan strategi implementasinya. Pada evaluasi area ini, responden akan diberikan kuisioner yang berisi serangkaian pertanyaan berhubungan dengan kerangka kerja keamanan informasi dengan metode *checklist* untuk mendukung kondisi yang terjadi sebenarnya pada instansi dengan hasil kuisioner yang diberikan. Pemberian *checklist* hanya pada pilihan kolom status "Dalam penerapan atau Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh". Lalu berikutnya setelah melakukan pemberian *checklist* adalah pemberian tingkat kematangan area kerangka kerja keamanan informasi berdasarkan hasil kuisioner.

Tabel 4.7 Hasil data penilaian pada Kerangka Kerja Keamanan Informasi

Bagian IV: Kerangka Keamanan Informasi							
Jumlah Pertanyaan	KP 1		KP 2		KP 3		Total
	12		10		7		29
Status Pengamanan	Kategori Pengamanan						
	KP 1	Skor KP 1	KP 2	Skor KP 2	KP 3	Skor KP 3	Total
Tidak dilakukan	0	0	0	0	0	0	0
Dalam perencanaan	6	1	9	2	7	3	24
Dalam penerapan atau	6	2	1	4	0	6	16

diterapkan sebagian							
Diterapkan secara menyeluruh	0	3	0	6	0	9	0
						Total Skor	40

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Tabel 4.7 diatas merupakan hasil penilaian data pada Kerangka Kerja Keamanan Informasi berupa instrument penelitian kuisioner terkait kesiapan dan kelengkapan berupa kebijakan dan prosedur dalam pengelolaan keamanan informasi beserta penerapannya. Area Kerangka Kerja Keamanan Informasi ini terdapat 12 pertanyaan yang berkaitan dengan kategori pengamanan 1 atau yang disingkat dengan KP 1, lalu 10 pertanyaan yang berkaitan dengan kategori pengamanan 2 yang disingkat menjadi KP 2, dan 7 pertanyaan yang berkaitan dengan kategori pengamanan 3 yang lalu disingkat menjadi KP 3 sehingga jika seluruh kategori pengamanan ini dijumlah akan menghasilkan 29 pertanyaan.

Dalam melakukan pengambilan data, responden menjawab pertanyaan berdasarkan opsi pilihan yang telah tersedia yaitu "Tidak dilakukan","Dalam perencanaan","Dalam penerapan / diterapkan sebagian", dan "Diterapkan secara menyeluruh" yang masing-masing opsi pilihan tersebut telah memliki nilainya masing-masing berdasarkan kategori pengamanan. Pada kuisioner bagian Kerangka Kerja Keamanan informasi yang diberikan didapatkan hasil opsi "Tidak dilakukan" sebanyak 0. Lalu didapatkan hasil opsi "Dalam perencanaan" pada kategori pengamanan 1 sebanyak 6, pada kategori pengamanan 2 sebanyak 9, dan pada kategori pengamanan 3 sebanyak 7 sehingga jika dijumlah akan menghasilkan 23 jawaban opsi "Dalam perencanaan" dengan total skor yang diperoleh yaitu 24. Pada opsi "Dalam penerapan atau diterapkan sebagian" didapakan hasil jawaban pada kategori pengamanan 1 sebanyak 6, lalu pada kategori pengamanan 2 sebanyak 1 dan pada kategori pengamanan 3 sebanyak 0 sehingga jika dijumlah akan menghasilkan 7 jawaban opsi "Dalam penerapan atau diterapkan sebagian" dengan total skor 16. Dan pada opsi "Diterapkan secara menyeluruh" didapatkan hasil jawaban 0 dengan total skor 0. Jika seluruh skor digabung akan menghasilkan total skor 40 pada bagian Kerangka Kerja Keamanan Informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Tabel 4.8 Data Penilaian Kematangan Kerangka Kerja Keamanan Informasi

Jumlah Pertanyaan Tingkat Pertanyaan	II	III	IV	V	Total
	11	13	3	2	29
Status Pengamanan	Tingkat Kematangan				
	II	III	IV	V	Total
Tidak dilakukan	0	0	0	0	0
Dalam perencanaan	4	13	3	2	22
Dalam penerapan / diterapkan sebagian	7	0	0	0	7

Diterapkan secara menyeluruh	0	0	0	0	0
Total	11	13	3	2	29

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Tabel 4.8 menunjukkan data hasil penilaian pada aspek kematangan pada area kerangka kerja keamanan informasi yang sudah dilakukan pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Pada tingkat kematangan II terdiri dari 11 pertanyaan pada area kerangka kerja keamanan informasi dimana sebanyak 0 pertanyaan dengan opsi pilihan "Tidak dilakukan", 4 pertanyaan dengan opsi pilihan "Dalam perencanaan", 7 pertanyaan dengan opsi pilihan "Dalam penerapan / diterapkan sebagian", dan 0 jawaban dengan opsi pilihan "Diterapkan secara menyeluruh". Lalu pada tingkat selanjutnya yaitu tingkat kematangan III terdiri dari 13 pertanyaan dimana sebanyak 0 pertanyaan dengan opsi pilihan "Tidak dilakukan", 13 pertanyaan dengan opsi pilihan "Dalam perencanaan", 0 pertanyaan dengan opsi pilihan "Dalam penerapan / diterapkan sebagian", dan 0 jawaban dengan opsi pilihan "Diterapkan secara menyeluruh". Lalu pada tingkat selanjutnya yaitu tingkat kematangan IV terdiri dari 3 pertanyaan dimana sebanyak 0 pertanyaan dengan opsi pilihan "Tidak dilakukan", 3 pertanyaan dengan opsi pilihan "Dalam perencanaan", 0 pertanyaan dengan opsi pilihan "Dalam penerapan / diterapkan sebagian", dan 0 jawaban dengan opsi pilihan "Diterapkan secara menyeluruh". Sedangkan pada area kerangka kerja Keamanan Informasi pada tingkat kematangan V yang terdiri dari 2 pertanyaan dimana sebanyak 2 pertanyaan dengan opsi pilihan "Dalam perencanaan" Sehingga didasarkan pada data tabel diatas, didapatkan hasil penilaian tingkat kematangan yang berhasil dicapai oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur yaitu pada tingkat I+. Tingkat I+ menandakan bahwa Dinas Komunikasi dan Informatika Provinsi Jawa Timur berada pada tahap kondisi awal dimana hal ini berarti instansi ini bersifat reaktif terhadap kerangka kerja keamanan informasi yang dimilikinya.

4.6 Pengelolaan Aset Informasi

Pada bagian ini, area pengelolaan aset informasi akan mengevaluasi kelengkapan keamanan terhadap aset-aset informasi, termasuk keseluruhan *life cycle* penggunaan aset-aset informasi tersebut. Pada evaluasi area ini, responden akan diberikan kuisioner yang berisi serangkaian pertanyaan berhubungan dengan pengelolaan aset informasi dengan metode *checklist* untuk mendukung kondisi yang terjadi sebenarnya pada instansi dengan hasil kuisioner yang diberikan. Pemberian *checklist* hanya pada pilihan kolom status "Dalam penerapan atau Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh". Lalu berikutnya setelah melakukan pemberian *checklist* adalah pemberian tingkat kematangan area pengelolaan aset informasi berdasarkan hasil kuisioner.

Berdasarkan hasil Kuisioner, Dinas Komunikasi dan Informatika Provinsi Jawa Timur mendapatkan total nilai evaluasi pengelolaan aset sebesar 71.

Tabel 4.9 Hasil data penilaian pada Pengelolaan Aset Informasi

Bagian V: Pengelolaan Aset Informasi							
Jumlah Pertanyaan	KP 1		KP 2		KP 3		Total
	24		10		4		38
Status Pengamanan	Kategori Pengamanan						
	KP 1	Skor KP 1	KP 2	Skor KP 2	KP 3	Skor KP 3	Total
Tidak dilakukan	3	0	0	0	0	0	0
Dalam perencanaan	9	1	5	2	4	3	19
Dalam penerapan atau diterapkan sebagian	10	2	2	4	0	6	28
Diterapkan secara menyeluruh	2	3	3	6	0	9	24
						Total Skor	71

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Tabel 4.9 diatas merupakan hasil penilaian data pada Pengelolaan Aset Informasi berupa instrument penelitian kuisioner terkait kesiapan dan keseluruhan siklus penggunaan aset yang dimiliki. Area Pengelolaan Aset Informasi ini terdapat 24 pertanyaan yang berkaitan dengan kategori pengamanan 1 atau yang disingkat dengan KP 1, lalu 10 pertanyaan yang berkaitan dengan kategori pengamanan 2 yang disingkat menjadi KP 2, dan 4 pertanyaan yang berkaitan dengan kategori pengamanan 3 yang lalu disingkat menjadi KP 3 sehingga jika seluruh kategori pengamanan ini dijumlah akan menghasilkan 38 pertanyaan.

Dalam melakukan pengambilan data, responden menjawab pertanyaan berdasarkan opsi pilihan yang telah tersedia yaitu "Tidak dilakukan","Dalam perencanaan","Dalam penerapan / diterapkan sebagian", dan "Diterapkan secara menyeluruh" yang masing-masing opsi pilihan tersebut telah memliki nilainya masing-masing berdasarkan kategori pengamanan. Pada kuisioner bagian Tata Kelola Keamanan informasi yang diberikan didapatkan hasil opsi "Tidak dilakukan" pada kategori sebanyak 3. Lalu didapatkan hasil opsi "Dalam perencanaan" pada kategori pengamanan 1 sebanyak 9, pada kategori pengamanan 2 sebanyak 5, dan pada kategori pengamanan 3 sebanyak 4 sehingga jika dijumlah akan menghasilkan 18 jawaban opsi "Dalam perencanaan" dengan total skor yang diperoleh yaitu 19. Pada opsi "Dalam penerapan atau diterapkan sebagian"

didapakan hasil jawaban pada kategori pengamanan 1 sebanyak 10, lalu pada kategori pengamanan 2 sebanyak 2 dan pada kategori pengamanan 3 sebanyak 0 sehingga jika dijumlah akan menghasilkan 11 jawaban opsi "Dalam penerapan atau diterapkan sebagian" dengan total skor 28. Dan pada opsi "Diterapkan secara menyeluruh" didapatkan hasil jawaban pada kategori pengamanan 1 sebanyak 2, kategori pengamanan 2 sebanyak 3, dan pada kategori pengamanan 3 sebanyak 0 sehingga jika dijumlah akan menghasilkan 5 jawaban opsi "Diterapkan secara menyeluruh" dengan total skor 24. Jika seluruh skor digabung akan menghasilkan total skor 71 pada bagian Pengelolaan Aset Informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Tabel 4.10 Data Penilaian Kematangan Pengelolaan Aset Informasi

Jumlah Pertanyaan Tingkat Pertanyaan	II	III	IV	V	Total
	29	9	0	0	38
Status Pengamanan	Tingkat Kematangan				
	II	III	IV	V	Total
Tidak dilakukan	3	0	0	0	3
Dalam perencanaan	13	5	0	0	18
Dalam penerapan / diterapkan sebagian	11	1	0	0	12
Diterapkan secara menyeluruh	2	3	0	0	5
Total	29	9	0	0	38

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Tabel 4.10 menunjukkan data hasil penilaian pada aspek kematangan pada area pengelolaan aset informasi yang sudah dilakukan pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Pada tingkat kematangan II terdiri dari 29 pertanyaan pada Pengelolaan Aset informasi dimana sebanyak 3 pertanyaan dengan opsi pilihan "Tidak dilakukan", 13 pertanyaan dengan opsi pilihan "Dalam perencanaan", 11 pertanyaan dengan opsi pilihan "Dalam penerapan / diterapkan sebagian", dan 2 jawaban dengan opsi pilihan "Diterapkan secara menyeluruh". Lalu pada tingkat selanjutnya yaitu tingkat kematangan III terdiri dari 9 pertanyaan dimana sebanyak 0 pertanyaan dengan opsi pilihan "Tidak dilakukan", 5 pertanyaan dengan opsi pilihan "Dalam perencanaan", 1 pertanyaan dengan opsi pilihan "Dalam penerapan / diterapkan sebagian", dan 3 jawaban dengan opsi pilihan "Diterapkan secara menyeluruh". Sedangkan pada area Pengelolaan Aset Informasi ini tidak terdapat tingkat kematangan IV dan tingkat kematangan V. Sehingga didasarkan pada data tabel diatas, didapatkan hasil penilaian tingkat kematangan yang berhasil dicapai oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur yaitu pada tingkat I+. Tingkat I+ menandakan bahwa Dinas Komunikasi dan Informatika Provinsi Jawa Timur berada pada tahap kondisi awal dimana hal ini berarti instansi ini bersifat reaktif terhadap pengelolaan aset informasi.

4.7 Teknologi dan Keamanan Informasi

Pada bagian ini, area teknologi dan keamanan informasi akan mengevaluasi kelengkapan, konsistensi dan efektivitas pengunaan teknologi dalam mengamankan aset-aset informasi yang dimiliki. Pada evaluasi area ini, responden akan diberikan kuisioner yang berisi serangkaian pertanyaan berhubungan dengan teknologi dan keamanan informasi dengan metode *checklist* untuk mendukung kondisi yang terjadi sebenarnya pada instansi dengan hasil kuisioner yang diberikan. Pemberian *checklist* hanya pada pilihan kolom status "Dalam penerapan atau Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh". Lalu berikutnya setelah melakukan pemberian *checklist* adalah pemberian tingkat kematangan area teknologi dan keamanan informasi berdasarkan hasil kuisioner.

Berdasarkan Hasil Kuisioner, Area teknologi dan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa timur memperoleh nilai evaluasi sebesar 35.

Tabel 4.11 Hasil data penilaian pada Teknologi dan Keamanan Informasi

Bagian VI: Teknologi dan Keamanan Informasi							
Jumlah Pertanyaan	KP 1		KP 2		KP 3		Total
	14		10		2		26
Status Pengamanan	Kategori Pengamanan						
	KP 1	Skor KP 1	KP 2	Skor KP 2	KP 3	Skor KP 3	Total
Tidak dilakukan	0	0	1	0	0	0	0
Dalam perencanaan	14	1	9	2	2	3	35
Dalam penerapan atau diterapkan sebagian	0	2	0	4	0	6	0
Diterapkan secara menyeluruh	0	3	0	6	0	9	0
						Total Skor	35

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Tabel 4.7 diatas merupakan hasil penilaian data pada Teknologi dan Keamanan Informasi berupa instrument penelitian kuisioner terkait kesiapan, kelengkapan, dan konsistensi penggunaan teknologi. Area Teknologi dan Keamanan Informasi ini terdapat 14 pertanyaan yang berkaitan dengan kategori

pengamanan 1 atau yang disingkat dengan KP 1, lalu 10 pertanyaan yang berkaitan dengan kategori pengamanan 2 yang disingkat menjadi KP 2, dan 2 pertanyaan yang berkaitan dengan kategori pengamanan 3 yang lalu disingkat menjadi KP 3 sehingga jika seluruh kategori pengamanan ini dijumlah akan menghasilkan 26 pertanyaan.

Dalam melakukan pengambilan data, responden menjawab pertanyaan berdasarkan opsi pilihan yang telah tersedia yaitu "Tidak dilakukan","Dalam perencanaan","Dalam penerapan / diterapkan sebagian", dan "Diterapkan secara menyeluruh" yang masing-masing opsi pilihan tersebut telah memliki nilainya masing-masing berdasarkan kategori pengamanan. Pada kuisioner bagian Teknologi dan Keamanan informasi yang diberikan didapatkan hasil opsi "Tidak dilakukan" pada kategori pengamanan 2 sebanyak 1. Lalu didapatkan hasil opsi "Dalam perencanaan" pada kategori pengamanan 1 sebanyak 14, pada kategori pengamanan 2 sebanyak 9, dan pada kategori pengamanan 3 sebanyak 2 sehingga jika dijumlah akan menghasilkan 25 jawaban opsi "Dalam perencanaan" dengan total skor yang diperoleh yaitu 35. Pada opsi "Dalam penerapan atau diterapkan sebagian" didapakan hasil jawaban sebanyak 0. Dan pada opsi "Diterapkan secara menyeluruh" didapatkan hasil jawaban sebanyak 0. Jika seluruh skor digabung akan menghasilkan total skor 35 pada bagian Teknologi dan Keamanan Informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Tabel 4.12 Data Penilaian Kematangan Teknologi dan Keamanan Informasi

Jumlah Pertanyaan Tingkat	II	III	IV	V	Total
Pertanyaan	14	11	1	0	26
Status Pengamanan	Tingkat Kematangan				
	II	III	IV	V	Total
Tidak dilakukan	0	1	0	0	1
Dalam perencanaan	14	10	1	0	25
Dalam penerapan / diterapkan sebagian	0	0	0	0	0
Diterapkan secara menyeluruh	0	0	0	0	0
Total	14	11	1	0	26

Sumber: Indeks Keamanan Informasi (KAMI) Versi 4.0 (2019)

Tabel 4.12 menunjukkan data hasil penilaian pada aspek kematangan pada area teknologi dan keamanan informasi yang sudah dilakukan pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Pada tingkat kematangan II terdiri dari 14 pertanyaan pada area tata kelola keamanan informasi dimana sebanyak 0 pertanyaan dengan opsi pilihan "Tidak dilakukan", 14 pertanyaan dengan opsi pilihan "Dalam perencanaan", 0 pertanyaan dengan opsi pilihan "Dalam penerapan / diterapkan sebagian", dan 0 jawaban dengan opsi pilihan "Diterapkan secara menyeluruh". Lalu pada tingkat selanjutnya yaitu tingkat kematangan III terdiri dari 11 pertanyaan dimana sebanyak 1 pertanyaan dengan opsi pilihan "Tidak dilakukan", 10 pertanyaan dengan opsi pilihan "Dalam perencanaan", 0 pertanyaan dengan opsi pilihan "Dalam penerapan / diterapkan sebagian", dan 0 jawaban dengan opsi pilihan

"Diterapkan secara menyeluruh". Lalu pada tingkat selanjutnya yaitu tingkat kematangan IV terdiri dari 1 pertanyaan dimana sebanyak 0 pertanyaan dengan opsi pilihan "Tidak dilakukan", 1 pertanyaan dengan opsi pilihan "Dalam perencanaan", 0 pertanyaan dengan opsi pilihan "Dalam penerapan / diterapkan sebagian", dan 0 jawaban dengan opsi pilihan "Diterapkan secara menyeluruh". Sedangkan pada area Teknologi dan Keamanan Informasi ini tidak terdapat tingkat kematangan V. Sehingga didasarkan pada data tabel diatas, didapatkan hasil penilaian tingkat kematangan yang berhasil dicapai oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur yaitu pada tingkat I. Tingkat I menandakan bahwa Dinas Komunikasi dan Informatika Provinsi Jawa Timur berada pada tahap kondisi awal dimana hal ini berarti instansi ini bersifat reaktif terhadap teknologi dan keamanan informasi.

4.8 Suplemen

pola bisnis yang dinamis menyebabkan munculnya beberapa risiko keamanan informasi baru. Keterlibatan pihak ketiga dalam *supply chain* layanan suatu instansi menimbulkan risiko terkait keterlibatan pihak yang berasal dari luar instansi tersebut. Layanan berbasis infrastruktur awan atau yang lebih sering dikenal sebagai *cloud* dapat memberikan peluang efisiensi dan peningkatan kinerja maupun efektifitas yang sangat signifikan bagi instansi. Namun, risiko terkait data yang berada pada pengendalian pihak ketiga dalam hal ini yaitu penyelenggara layanan berbasis *cloud* perlu dimitigasi. Dengan disahkannya peraturan terkait perlindungan data pribadi oleh banyak negara memerlukan kerangka kerja yang secara spesifik membahas bagaimana data pribadi yang dimiliki instansi sudah diamankan sesuai dengan persyaratan hukum.

Pada bagian ini, area suplemen akan mengevaluasi kelengkapan, konsistensi dan efektivitas pengunaan teknologi dalam mengamankan aset-aset informasi yang dimiliki khususnya pada bidang pengamanan keterlibatan pihak ketiga penyedia layanan, bidang pengamanan layanan infrastruktur awan (*cloud service)*, dan pada bidang perlindungan data diri. Pada evaluasi area ini, responden akan diberikan kuisioner yang berisi serangkaian pertanyaan berhubungan dengan teknologi dan keamanan informasi dengan metode *checklist* untuk mendukung kondisi yang terjadi sebenarnya pada instansi dengan hasil kuisioner yang diberikan. Pemberian *checklist* hanya pada pilihan kolom status "Dalam penerapan atau Diterapkan Sebagian" dan "Diterapkan Secara Menyeluruh". Pada area ini, tidak menghasilkan tingkat kematangan namun akan menghasilkan nilai dalam bentuk presentase dengan obyektif atau sasaran pencapaian maksimal.

Tabel 4.13 Data Penilaian Suplemen

Bagian VII: Suplemen		
Jumlah Pertanyaan	KP 1	
	53	
Status Pengamanan	Kategori Pengamanan	
	KP 1	Skor KP 1
Tidak dilakukan	0	0
Dalam perencanaan	0	1
Dalam penerapan atau diterapkan sebagian	0	2
Diterapkan secara menyeluruh	0	3

4.9 Hasil Data Kuisioner

Hasil perhitungan data kuisioner pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur nantinya akan menghasilkan 2 penilaian akhir yaitu tingkat kelengkapan dan penerapan keamanan informasi serta tingkat kematangan informasi.

4.9.1 Tingkat Keamanan Informasi

Berdasarkan hasil penilaian kuisioner yang diperoleh maka dapat diketahui tingkat kematangan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur adalah tingkat I s/d II dan skor kategori sistem elektronik termasuk dalam kategori tinggi yang ditunjukkan dengan gambar dibawah ini :

Gambar 4.1 Hasil Tingkat Keamanan Informasi

Sumber: Indeks KAMI versi 4.0 (2019)

Tabel 4.14 Persentase Hasil Tingkat Keamanan Informasi

	Tata Kelola Keamanan Informasi	Pengelolaan Risiko Keamanan Informasi	Kerangka Kerja Pengelolaan Keamanan Informasi	Pengelolaan Aset Informasi	Teknologi dan Keamanan Informasi
Skor Responden	88	24	40	71	35
Skor Maksimal	127	72	159	168	120
Persentase	69,29%	33,33%	25,16%	42,26%	29,17%

4.9.2 Tingkat Kelengkapan Penerapan Keamanan Informasi

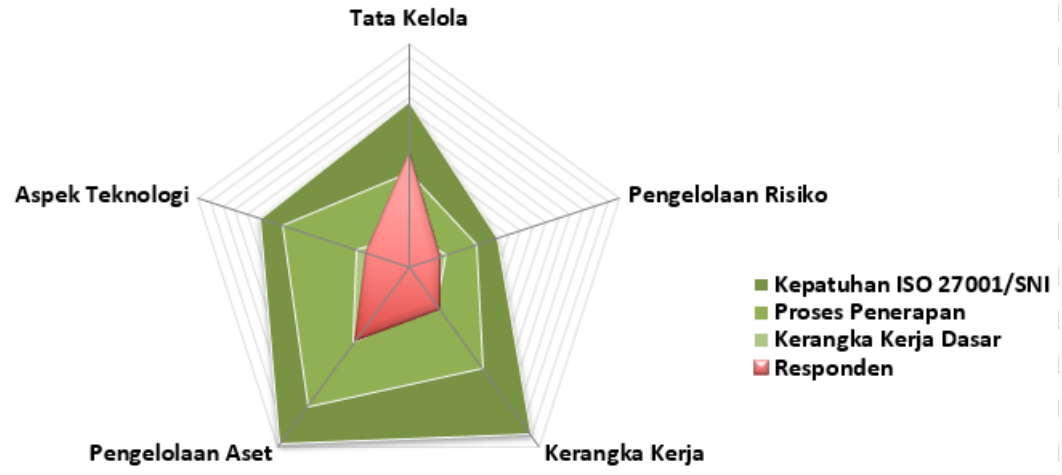
Berdasarkan hasil penilaian yang diperoleh dari kuisioner dapat diketahui tingkat kelengkapan penerapan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur dapat ditarik hasil bahwa hasil evaluasi akhir adalah tidak layak dan pada tangkat kelengkapan penerapan Standar ISO27001 sesuai kategori sistem elektronik adalah senilai 258 dalam bentuk *bar chart* dibawah ini:

Gambar 4.2 Hasil Evaluasi tingkat kelengkapan penerapan Keamanan informasi

Sumber: Indeks KAMI versi 4.0 (2019)

4.9.3 Radar Chart

Berdasarkan hasil penilaian yang diperoleh dari kuisioner, dihasilkan *radar chart* sebagai tolak ukur pengukuran kesiapan dan kepatuhan terhadap ISO 27001/SNI, Proses penerapan, dan kerangka kerja dasar pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada gambar dibawah ini :



Gambar 4.3 Hasil *Radar Chart*

Sumber: Indeks KAMI versi 4.0 (2019)

4.9.4 Dokumen atau Bukti Pendukung

Pada kuisioner penilaian diberikan kolom tambahan berupa kolom bukti sebagai dasar dalam menjawab setiap poin pertanyaan yang diberikan. Untuk setiap pertanyaan dengan jawaban "Dalam Penerapan / Diterapkan Sebagian" atau "Diterapkan secara menyeluruh", kolom bukti akan diisi dengan dokumen atau bukti bukti pendukung. Pada beberapa pertanyaan dengan jawaban "Dalam Perencanaan" terdapat beberapa dokumen pendukung, dan pada pertanyaan dengan jawaban "Tidak dilakukan", tidak disertakan bukti maupun dokumen pendukung. Beberapa bukti maupun dokumen yang dilampirkan bersifat rahasia, sehingga tidak dapat ditunjukkan isi dari dokumen maupun bukti tersebut. Lampiran bukti akan dilampirkan pada bagian lampiran dibagian akhir.

Tabel 4.15 Dokumen Bukti Area Tata Kelola Keamanan Informasi

Nomor Pertanyaan	Bukti atau Dokumen		Keterangan
	Tersedia	Tidak Tersedia	
2.1	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013, Pergub Jatim No. 80 Tahun 2016
2.2	✓		Pergub Jatim No. 80 Tahun 2016
2.3	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013, Pergub Jatim No. 80 Tahun 2016

2.4	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013, Pergub Jatim No. 80 Tahun 2016
2.5	✓		Dokumen SOA ISO27001:2013
2.6		✓	-
2.7	✓		Sertifikat Pelatihan dan kompetensi teknis berstandar Nasional/Internasional dan Ijazah Pendidikan masing2 Pelaksana
2.8	✓		DPA (Daftar Pelaksanaan Anggaran) Seksi Persandian dan Keamanan Informasi tiap Tahun
2.9	✓		DPA (Daftar Pelaksanaan Anggaran) Seksi Persandian dan Keamanan Informasi tiap Tahun
2.10	✓		Dokumen SOA ISO 27001:2013
2.11		✓	-
2.12	✓		Dokumen Kebijakan dan Pedoman Pengamanan Pihak Ketiga ISO 27001:2013; Dokumen Kebijakan Keamanan Informasi ISO 27001:2013
2.13	✓		Dokumen Kebijakan dan Pedoman Kepatuhan Keamanan Informasi ISO 27001:2013; Dokumen Kebijakan Keamanan Informasi ISO 27001:2013
2.14	✓		Dokumen Kebijakan dan Pedoman Keberlanjutan Bisnis dan Keamanan Informasi ISO 27001:2013
2.15	✓		Dokumen Kebijakan dan Pedoman Kepatuhan Keamanan Informasi ISO 27001:2013; Dokumen Kebijakan Keamanan Informasi ISO 27001:2013
2.16	✓		Dokumen Kebijakan Keamanan Informasi ISO 27001:2013
2.17	✓		Kebijakan dan Pedoman Pengamanan dan Pengelolaan Aset ISO 27001:2013
2.18	✓		Kebijakan dan Prosedur Pengukuran SMKI ISO 27001:2013
2.19	✓		Dokumen Kebijakan dan Prosedur Peningkatan Pemahaman Kesadaran (Awareness) dan Komunikasi Sistem

			Manajemen Keamanan Informasi ISO 27001:2013
2.20		✓	-
2.21		✓	-
2.22	✓		Dokumen Kebijakan dan Pedoman Pengelolaan Insiden Keamanan Informasi ISO 27001:2013

Tabel 4.16 Dokumen Bukti Area Pengelolaan Risiko Keamanan Informasi

Nomor Pertanyaan	Bukti atau Dokumen		Keterangan
	Tersedia	Tidak Tersedia	
3.1	✓		Dokumen Kebijakan dan Pedoman Manajemen Risiko SMKI ISO 27001:2013
3.2		✓	-
3.3	✓		Dokumen Kebijakan dan Pedoman Manajemen Risiko SMKI ISO 27001:2013
3.4	✓		Dokumen Kebijakan dan Pedoman Manajemen Risiko SMKI ISO 27001:2013
3.5	✓		Dokumen Kebijakan dan Pedoman Manajemen Risiko SMKI ISO 27001:2013
3.6	✓		Dokumen Kebijakan dan Pedoman Pengendalian Akses ISO 27001:2013; Daftar Pemilik Aplikasi dan Perangkat Server Colocation
3.7		✓	-
3.8		✓	-
3.9		✓	-
3.10		✓	-
3.11		✓	-
3.12		✓	-
3.13		✓	-
3.14		✓	-
3.15		✓	-
3.16		✓	-

Tabel 4.17 Dokumen Bukti Kerangka Kerja Pengelolaan Keamanan Informasi

Nomor Pertanyaan	Bukti atau Dokumen		Keterangan
	Tersedia	Tidak Tersedia	
4.1	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013
4.2	✓		Bukti Kehadiran sosialisasi ISO 27001 Data center pada 28 Juni 2018
4.3	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013
4.4	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013
4.5		✓	-
4.6	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013; SOP Penanganan Insiden Keamanan Informasi
4.7	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013
4.8	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013
4.9		✓	-
4.10		✓	-
4.11		✓	-
4.12		✓	-
4.13		✓	-
4.14		✓	-
4.15		✓	-
4.16		✓	-
4.17		✓	-
4.18		✓	-
4.19		✓	-
4.20		✓	-
4.21		✓	-

4.22		✓	-
4.23		✓	-
4.24		✓	-
4.25		✓	-
4.26		✓	-
4.27		✓	-
4.28		✓	-
4.29		✓	-

Tabel 4.18 Dokumen Bukti Pengelolaan Aset Informasi

Nomor Pertanyaan	Bukti atau Dokumen		Keterangan
	Tersedia	Tidak Tersedia	
5.1	✓		Daftar Inventaris Barang Milik Negara Diskominfo dan Daftar Inventaris Barang di Data Center, Dokumen Kebijakan dan Pedoman Pengamanan dan Pengelolaan Aset ISO 27001:2013
5.2	✓		Kebijakan dan Pedoman Pengamanan dan Pengelolaan Aset
5.3	✓		Kebijakan dan Pedoman Pengamanan dan Pengelolaan Aset
5.4		✓	-
5.5	✓		Kebijakan dan Pedoman Manajemen Perubahan Fasilitas DC
5.6	✓		-
5.7	✓		Dokumen Kebijakan dan Pedoman Instalasi Perangkat Lunak ISO 27001:2013, Dokumen dan Pedoman Manajemen Perubahan Fasilitas Data Center ISO 27001:2013
5.8	✓		SK Struktur Organisasi SMKI, Dokumen Kebijakan Keamanan Informasi ISO 27001:2013
5.9	✓		Dokumen Kebijakan dan Pedoman Pengamanan dan Pengelolaan Aset ISO 27001:2013

5.10	✓		Kebijakan Keamanan Informasi (Hal 114)
5.11	✓		Kebijakan Keamanan Informasi (Hal 70 & 73)
5.12		✓	-
5.13	✓		Kebijakan Keamanan Informasi (Hal 34)
5.14	✓		Kebijakan Keamanan Informasi (Hal 34)
5.15		✓	
5.16	✓		Kebijakan Keamanan Informasi (Hal 79)
5.17	✓		Kebijakan Keamanan Informasi (Hal 101)
5.18	✓		Kebijakan Keamanan Informasi (Hal 65); Berita Acara - Simulasi BCP
5.19	✓		Kebijakan Keamanan Informasi (Hal 45)
5.20	✓		Kebijakan Keamanan Informasi (Hal 15)
5.21	✓		Kebijakan Keamanan Informasi (Hal 12)
5.22	✓		Kebijakan Keamanan Informasi (Hal 26)
5.23	✓		Kebijakan Keamanan Informasi (Hal 34)
5.24	✓		Kebijakan Keamanan Informasi (Hal 37)
5.25		✓	-
5.26		✓	-
5.27		✓	-
5.28	✓		Kebijakan Keamanan Informasi (Hal 45)
5.29	✓		Kebijakan Keamanan Informasi (Hal 45)
5.30	✓		Kebijakan Keamanan Informasi (Hal 47)
5.31	✓		Kebijakan Keamanan Informasi (Hal 51)
5.32	✓		Kebijakan Keamanan Informasi (Hal 55)
5.33	✓		Kebijakan Keamanan Informasi (Hal 54)
5.34	✓		Kebijakan Keamanan Informasi (Hal 47)
5.35	✓		Kebijakan Keamanan Informasi (Hal 47)
5.36		✓	-
5.37		✓	-
5.38		✓	-

Tabel 4.19 Dokumen Bukti Area Teknologi dan Keamanan Informasi

Nomor Pertanyaan	Bukti atau Dokumen		Keterangan
	Tersedia	Tidak Tersedia	
6.1		✓	-
6.2		✓	-
6.3		✓	-
6.4		✓	-
6.5		✓	-
6.6		✓	-
6.7		✓	-
6.8		✓	-
6.9		✓	-
6.10		✓	-
6.11		✓	-
6.12		✓	-
6.13		✓	-
6.14		✓	-
6.15		✓	-
6.16		✓	-
6.17		✓	-
6.18		✓	-
6.19		✓	-
6.20		✓	-
6.21		✓	-
6.22		✓	-
6.23		✓	-
6.24		✓	-
6.25		✓	-
6.26		✓	-

Tabel 4.20 Dokumen Bukti Area Suplemen

Nomor Pertanyaan	Bukti atau Dokumen		Keterangan
	Tersedia	Tidak Tersedia	
7.1.1.1		✓	-
7.1.1.2		✓	-
7.1.1.3		✓	-
7.1.1.4		✓	-
7.1.1.5		✓	-
7.1.1.6		✓	-
7.1.1.7		✓	-
7.1.2.1		✓	-
7.1.2.2		✓	-
7.1.2.3		✓	-
7.1.3.1		✓	-
7.1.3.2		✓	-
7.1.3.3		✓	-
7.1.3.4		✓	-
7.1.3.5		✓	-
7.1.3.6		✓	-
7.1.3.7		✓	-
7.1.3.8		✓	-
7.1.4.1		✓	-
7.1.4.2		✓	-
7.1.5.1		✓	-
7.1.5.2		✓	-
7.1.6.1		✓	-
7.1.6.2		✓	-
7.1.7.1		✓	-
7.1.7.2		✓	-
7.1.7.3		✓	-

7.2.1		✓	-
7.2.2		✓	-
7.2.3		✓	-
7.2.4		✓	-
7.2.5		✓	-
7.2.6		✓	-
7.2.7		✓	-
7.2.8		✓	-
7.2.9		✓	-
7.2.10		✓	-
7.3.1		✓	-
7.3.2		✓	-
7.3.3		✓	-
7.3.4		✓	-
7.3.5		✓	-
7.3.6		✓	-
7.3.7		✓	-
7.3.8		✓	-
7.3.9		✓	-
7.3.10		✓	-
7.3.11		✓	-
7.3.12		✓	-
7.3.13		✓	-
7.3.14		✓	-
7.3.15		✓	-
7.3.16		✓	-

BAB 5 PEMBAHASAN

Dengan didasari oleh penilaian berupa kuisioner yang dilakukan oleh penulis kepada Objek penelitian ini yaitu Dinas Komunikasi dan Informatika Provinsi Jawa Timur, pada hasil tingkat kelengkapan penerapan keamanan informasi berada pada zona "merah" dimana zona ini menunjukkan bahwa sistem manajemen keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur tidak layak sehingga diperlukan beberapa perbaikan pada masing-masing area yang dinilai untuk meningkatkan efektivitas manajemen sistem keamanan informasi. Perbaikan berupa rekomendasi diberikan berdasarkan hasil kuisioner dimana rekomendasi hanya diberikan pada butir pertanyaan yang memiliki jawaban "dalam perencanaan" pada setiap area penilaian. Rekomendasi ini juga berdasarkan dengan kontrol Annex A ISO/IEC 27001:2013, dimulai dari urgensi area dengan nilai persentase terendah yaitu area Pengelolaan Risiko Keamanan Informasi, area Teknologi dan Keamanan Informasi, area Kerangka Kerja Pengelolaan Keamanan Informasi, area Pengelolaan Aset Informasi, dan area Tata Kelola Keamanan Informasi.

5.1 Area Tata Kelola Keamanan Informasi

Pada area Tata Kelola Keamanan Informasi, Dinas Komunikasi dan Informatika Provinsi Jawa Timur mendapatkan skor sebesar 88 dari keseluruhan nilai area tata kelola keamanan informasi sebesar 127, sehingga apabila dibuat dalam persentase, Dinas Komunikasi dan Informatika Provinsi Jawa Timur mencapai persentase sebesar 69,29%. Dari persentase tersebut, masih terdapat beberapa aspek yang belum diterapkan seluruhnya atau baru diterapkan sebagian. Beberapa aspek pada tata kelola kemanan informasi masih dalam perencanaan atau belum dilakukan sehingga perlu dilakukan perbaikan berupa rekomendasi usulan berdasarkan kontrol *Annex* A ISO/IEC 27001:2013. Penilaian tata kelola keamanan informasi menggunakan Indeks KAMI 4.0 menghasilkan 4 rekomendasi yang diusulkan untuk memenuhi kelengkapan penilaian Indeks KAMI yang belum atau tidak dilakukan atau dalam perencanaan oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Berdasarkan hasil penilaian dan skor pada Area Tata Kelola Keamanan Informasi tersebut, secara garis besar Dinas Komunikasi dan Informatika Provinsi Jawa Timur perlu melakukan perencanaan, kajian dan melakukan identifikasi terkait peraturan dan legislasi keamanan informasi lalu melakukan dokumentasi terkait kebijakan tata Kelola keamanan informasi yang telah direncanakan dan dibuat yang nantinya akan diterapkan. Lalu, pada setiap informasi yang dimiliki harus jelas terkait kepemilikanya sehingga hanya yang berwenang bisa mengakses informasi pada saat proses tata kelola keamanan informasi.

Pada kondisi saat ini, Dinas Komunikasi dan Informatika Provinsi Jawa Timur masih dalam tahap perencanaan tata kelola keamanan infromasi yang mencakup tentang mendefinisikan persyaratan / standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi. Kondisi yang terjadi ini telah sesuai

dengan kontrol Annex A ISO/IEX 27001:2013 dengan kode kontrol A.7.1.1 yang mencakup tentang verifikasi dan pemeriksaan kompetensi pada semua pelaksana pengelolaan keamanan informasi. Rekomendasi yang dianjurkan untuk memperbaiki kondisi ini adalah dengan cara membuat dokumen *requirements,* identifikasi hasil kerja, dan dokumen peninjauan hasil kerja terhadap standar kompetensi pelaksana keamanan informasi yang harus sesuai dengan undang-undang, dan proporsional dengan persyaratan instansi.

Lalu Dinas Komunikasi dan Informatika Provinsi Jawa Timur juga masih dalam tahap merencanakan tata kelola keamanan informasi yang mencakup tentang identifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku. Kondisi yang terjadi ini telah sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.18.1.4 yaitu tentang Privasi dan perlindungan informasi identitas pribadi. Seluruh data pribadi yang digunakan harus jelas siapa pemiliknya, apakah data pribadi atau data perusahaan sehingga jelas siapa yang bisa mengaksesnya, sehingga rekomendasi yang dianjurkan adalah privasi dan perlindungan informasi identitas pribadi harus dipastikan sebagaimana disyaratkan dalam undang-undang dan peraturan yang relevan jika berlaku lalu mengidentifikasi data pribadi yang dimiliki agar jelas siapa yang boleh dan bisa mengaksesnya.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap merencanakan tata kelola keamanan informasi yang mencakup tentang penerapan 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. Kondisi yang terjadi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur telah sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.5.1.1 yang mengenai tentang kebijakan untuk Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Sehingga rekomendasi yang sesuai dengan kondisi ini adalah kebijakan-kebijakan keamanan informasi yang dibuat harus didefinisikan terlebih dahulu sebelum diterbitkan dan kebijakan-kebijakan yang telah diterbitkan harus segera dikomunikasikan dengan karyawan dan *stakeholder* yang terkait.

Pada saat ini, Dinas Komunikasi dan Informatika Provinsi Jawa Timur masih dalam tahap perencanaan tata kelola keamanan informasi yang mencakup tentang identifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya. Kondisi yang terjadi ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.18.1.1, dimana kode kontrol ini tentang identifikasi peraturan dan legislasi yang berlaku beserta persyaratan kontraknya. Sehingga rekomendasi yang diajukan adalah seluruh kebijakan-kebijakan yang telah diidentifikasi dan dibuat, perlu ada dokumentasi dan selalu diperbarui sesuai dengan situasi dan kondisi yang berlaku saat itu sehingga kebijakan yang ada bersifat ketat namun fleksibel.

5.2 Area Pengelolaan Risiko Keamanan Informasi

Pada area Pengelolaan Risiko Keamanan Informasi, Dinas Komunikasi dan Informatika Provinsi Jawa Timur mendapatkan skor sebesar 24 dari keseluruhan nilai area pengelolaan risiko keamanan informasi sebesar 72, sehingga apabila dibuat dalam persentase, Dinas Komunikasi dan Informatika Provinsi Jawa Timur mencapai persentase sebesar 33,33%. Dari persentase tersebut, masih terdapat beberapa aspek yang belum diterapkan seluruhnya atau baru diterapkan sebagian. Beberapa aspek pada pengelolaan risiko kemanan informasi masih dalam perencanaan atau belum dilakukan sehingga perlu dilakukan perbaikan berupa rekomendasi usulan berdasarkan kontrol *Annex* A ISO/IEC 27001:2013. Penilaian pengelolaan risiko keamanan informasi menggunakan Indeks KAMI 4.0 menghasilkan 11 rekomendasi yang diusulkan untuk memenuhi kelengkapan penilaian Indeks KAMI yang belum atau tidak dilakukan atau dalam perencanaan oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Berdasarkan hasil penilaian dan skor pada Area Pengelolaan Risiko Keamanan Informasi tersebut secara garis besar Dinas Komunikasi dan Informatika Provinsi Jawa Timur perlu melakukan perencanaan, kajian, dan penetapan tugas, fungsi, dan tanggung jawab pengelola keamanan informasi dan melakukan dokumentasi terkait kebijakan pengelolaan risiko keamanan informasi yang telah direncanakan dan dibuat yang nantinya akan diterapkan. Lalu, melakukan identifikasi terkait penanganan aset informasi yang dimiliki, menyiapkan dan mengkaji secara berkala mitigasi risiko terhadap penanganan aset informasi yang dimiliki. Selain itu, perlu juga melakukan peninjauan yang bersifat independent terhadap risiko dan kontrol keamanan untuk memastikan objektifitas dan manfaat dari pengelolaan mitigasi risiko ini.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi yang mencakup tentang menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.6.1.1 tentang tugas, fungsi, dan tanggung jawab keamanan informasi. Sehingga dengan kondisi ini, adapun rekomendasi yang dapat diberikan adalah dengan mendefinisikan, mengalokasikan, dan mendokumentasikan seluruh tanggung jawab keamanan informasi mulai dari yang bersifat umum seperti melindungi informasi hingga tanggung jawab yang bersifat spesifik atau khusus seperti tanggung jawab dalam memberikan wewenang atau izin dalam akses data atau informasi kepada setiap *stakeholder* yang terkait dengan keamanan informasi ke dalam *requirement* pekerjaan,kebijakan-kebijakan terkait tupoksi dan kontrak kerja secara jelas.

Lalu Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini juga masih dalam tahap melakukan perencanaan pengelolaan risiko keamanan informasi yang mencakup tentang identifikasi ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode

kontrol A.8.2.3 yang membahas tentang penanganan terhadap aset. Sehingga dengan kondisi dan kontrol kode ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat prosedur-prosedur terhadap penanganan aset informasi yang dimiliki oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur lalu prosedur yang telah dibuat, dikembangkan dan diterapkan sesuai dengan skema klasifikasi informasi seperti pembatasan hak akses, pemberian wewenang terhadap aset informasi.

Pada saat ini, Dinas Komunikasi dan Informatika Provinsi Jawa Timur masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait dampak kerugian yang terkait dengan hilangnya atau terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada. Kondisi ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.16.1.3 yang terkait tentang pelaporan tentang kelemahan keamanan informasi. Sehingga, sesuai dengan kondisi tersebut rekomendasi yang dapat diberikan adalah dengan membuat dokumen laporan terhadap kelemahan-kelemahan yang ditemukan sehingga dengan dokumen ini mampu dilakukan tindakan mitigasi dari kelemahan dan ancaman terhadap set informasi yang ditemukan.

Pada saat ini, Dinas Komunikasi dan Informatika Provinsi Jawa Timur masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait menjalankan inisiatif analisa atau kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada yang nantinya digunakan sebagai langkah mitigasi dalam identifikasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi. Kondisi ini sesuai dengan kontrol Annex A ISO/IEC27001:2013 dengan kode kontrol A.5.1.1 yang terkait tentang kebijakan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Sehingga, dengan kondisi dan kontrol kode ini menghasilkan rekomendasi yang dapat diberikan adalah adalah kebijakan-kebijakan keamanan informasi yang dibuat harus didefinisikan terlebih dahulu sebelum diterbitkan dan kebijakan-kebijakan yang telah diterbitkan harus segera dikomunikasikan dengan karyawan dan *stakeholder* yang terkait. Dalam kasus ini kebijakan yang dimaksud adalah dokumen terkait identifikasi risiko, tingkat risiko, serta mitigasi yang dapat dilakukan untuk menanggulangi risiko tersebut.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait penyusunan langkah mitigasi dan penanggulan risiko yang ada. Kondisi ini sesuai dengan kontrol Annex A ISO/IEC27001:2013 dengan kontrol kode A.8.2.3 yang terkait tentang penanganan terhadap aset informasi. Sehingga, dengan kondisi dan kontrol kode saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat prosedur-prosedur terhadap penanganan aset informasi yang dimiliki oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur lalu prosedur yang telah dibuat, dikembangkan dan diterapkan sesuai dengan skema klasifikasi informasi seperti pembatasan hak akses, pemberian wewenang terhadap aset informasi. lalu perlu dilakukan juga dokumentasi terhadap prosedur yang telah dibuat tersebut.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait langkah mitigasi risiko yang disusun sesuai dengan tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya. Kondisi ini sesuai dengan kontrol Annex A ISO/IEC27001:2013 dengan kontrol kode A.16.1.1 yang terkait tentang tanggung jawab dan prosedur. Dengan kondisi dan kontrol kode saat ini, menghasilkan rekomendasi yang dapat diberikan adalah dengan Membuat prosedur dan dokumen terkait Langkah mitigasi risiko-risiko yang mungkin terjadi dalam keamanan informasi dan menentukan target atau tujuan yang perlu dicapai dalam memitigasi risiko yang kemudian disusun sesuai dengan prioritas serta menentukan siapa yang bertanggung jawab pada mitigasi risiko tersebut.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait status penyelesaian langkah mitigasi risiko yang dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya. Kondisi ini sesuai dengan kontrol Annex A ISO/IEC27001:2013 dengan kontrol kode A.18.1.4 yang Mencakup tentang kepatuhan terhadap tinjauan independen atas keamanan informasi. Dengan kondisi dan kontrol kode saat ini, menghasilkan rekomendasi yang dapat diberikan adalah dengan Melakukan peninjauan yang bersifat independent terhadap risiko dan kontrol keamanan untuk memastikan objektifitas dan manfaat dari pengelolaan mitigasi risiko ini. Tinjauan independent ini tidak harus melalui pihak eksternal, namun bisa menggunakan rencana mitigasi yang dimiliki oleh rekan-rekan kerja.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait penyelesaian langkah mitigasi yang sudah diterapkan dan dievaluasi. Langkah mitigasi tersebut diterapkan dan dievaluasi melalui proses yang obyektif atau terukur untuk memastikan konsistensi dan efektifitasnya. Kondisi ini sesuasi dengan kontrol Annex A ISO/IEC27001:2013 dengan kontrol kode A.18.2.1 terkait tentang kepatuhan terhadap tinjauan independen atas keamanan informasi. Sehingga, kondisi dan kontrol saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan melakukan peninjauan yang bersifat independent terhadap risiko dan kontrol keamanan untuk memastikan objektifitas dan manfaat dari pengelolaan mitigasi risiko ini. Tinjauan independent ini tidak harus melalui pihak eksternal, namun bisa menggunakan rencana mitigasi yang dimiliki oleh rekan-rekan kerja.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait 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. Kondisi ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kontrol kode A.18.2.1 kepatuhan terhadap peninjauan kembali yang bersifat independent pada keamanan informasi. Sehingga, kontrol dan kondisi ini menghasilkan

rekomendasi yang dapat diberikan yaitu dengan melakukan peninjauan yang bersifat independent terhadap risiko dan kontrol keamanan untuk memastikan objektifitas dan manfaat dari pengelolaan mitigasi risiko ini. Tinjauan independent ini tidak harus melalui pihak eksternal, namun bisa menggunakan rencana mitigasi yang dimiliki oleh rekan-rekan kerja.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan atau meningkatkan efektifitasnya. Kondisi ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kontrol kode A.5.1.2 yang terkait tentang tinjauan terhadap kebijakan-kebijakan untuk keamanan informasi. Sehingga, kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan melakukan penjadwalan secara berkala dalam melakukan peninjauan kembali atau melakukan pembaruan atas kebijakan-kebijakan pengelolaan risiko yang ada, apakah kebijakan-kebijakan terkait risiko tersebut masih revelan dan sesuai dengan kondisi saat itu, kecukupan dan efektifitasnya.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan. Kondisi ini sesuai dengan kontrol Annex A ISO/IEC27001:2013 dengan kode A.16.1.6 yang terkait tentang pembelajaran terhadap insiden keamanan informasi. Sehingga, dengan kontrol dan kondisi ini menghasilkan rekomendasi yang dapat diberikan yaitu dengan melakukan dokumentasi terhadap langkah atau metode yang digunakan jika terjadi insiden keamanan informasi, sehingga ketika sebuah insiden terjadi, dokumentasi ini dapat membantu menganalisis dan menyelesaikan insiden tersebut dan dapat membantu untuk mengurangi kemungkinan atau dampak dari setiap insiden yang akan terjadi di masa depan.

5.3 Area Kerangka Kerja Pengelolaan Keamanan Informasi

Pada area Kerangka Kerja Pengelolaan Keamanan Informasi, Dinas Komunikasi dan Informatika Provinsi Jawa Timur mendapatkan skor sebesar 40 dari keseluruhan nilai area kerangka kerja pengelolaan keamanan informasi sebesar 159, sehingga apabila dibuat dalam persentase, Dinas Komunikasi dan Informatika Provinsi Jawa Timur mencapai persentase sebesar 25.16%. Dari persentase tersebut, masih terdapat beberapa aspek yang belum diterapkan seluruhnya atau baru diterapkan sebagian. Beberapa aspek pada kerangka kerja pengelolaan kemanan informasi masih dalam perencanaan atau belum dilakukan sehingga perlu dilakukan perbaikan berupa rekomendasi usulan berdasarkan kontrol *Annex* A ISO/IEC 27001:2013. Penilaian kerangka kerja pengelolaan keamanan informasi menggunakan Indeks KAMI 4.0 menghasilkan 22 rekomendasi yang diusulkan untuk memenuhi kelengkapan penilaian Indeks KAMI yang belum atau tidak dilakukan atau dalam perencanaan oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Berdasarkan hasil penilaian dan skor pada Area Tata Kelola Keamanan Informasi tersebut secara garis besar Dinas Komunikasi dan Informatika Provinsi Jawa Timur perlu melakukan perencanaan, kajian, identifikasi risiko, mitigasi risiko dan melakukan dokumentasi terkait kebijakan kerangka kerja keamanan informasi yang telah direncanakan dan dibuat yang nantinya akan diterapkan. Lalu menerapkan sistem *secure* SDLC *(Software Developtment Life Cycle)* pada setiap pengembangan sistem yang dibuat dengan cara membuat pertimbangan seperti *checklist* pada kerangka kerja keamanan informasi yang dimiliki bahwa keamanan informasi sudah dipertimbangkan dalam penerapan dan pengembangan sistem. Selain itu perlu juga membuat aturan dan prosedur dalam pengembangan sistem seperti dengan mempertimbangkan keamanan repositori, pengetahuan terhadap keamanan sistem, dan membuat dokumen manajemen risiko terhadap keamanan informasi pada saat melakukan pengembangan sistem. Dan yang terakhir adalah melakukan penjadwalan secara berkala dalam melakukan peninjauan kembali atau melakukan pembaruan atas kebijakan-kebijakan dan prosedur yang ada, apakah kebijakan-kebijakan terkait keamanan informasi tersebut masih revelan dan sesuai dengan kondisi saat ini, kecukupan dan efektifitasnya.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan kerangka kerja pengelolaan keamanan informasi yang mencakup tentang kebijakan dan prosedur keamanan informasi yang ada, sudah merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran atau objektif tertentu. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.5.1.1 yang mencakup tentang kebijakan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah kebijakan-kebijakan keamanan informasi yang dibuat harus didefinisikan terlebih dahulu sebelum diterbitkan dan kebijakan-kebijakan yang telah diterbitkan harus segera dikomunikasikan dengan karyawan dan *stakeholder* yang terkait. Dalam kasus ini kebijakan yang dimaksud adalah dokumen terkait identifikasi risiko, tingkat risiko, serta mitigasi yang dapat dilakukan untuk menanggulangi risiko tersebut.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan kerangka kerja pengelolaan keamanan informasi yang mencakup tentang ketersediaan prosedur resmi dalam pengelolan suatu pengecualian terhadap penerapan keamanan informasi dan prosedur tindak lanjut terhadap kondisi tersebut. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.5.1.1 yang mencakup tentang kebijakan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah kebijakan-kebijakan keamanan informasi yang dibuat harus didefinisikan terlebih dahulu sebelum diterbitkan dan kebijakan-kebijakan yang telah diterbitkan harus segera dikomunikasikan dengan karyawan dan *stakeholder* yang terkait. Dalam kasus ini kebijakan yang dimaksud

adalah dokumen terkait identifikasi risiko, tingkat risiko, serta mitigasi yang dapat dilakukan untuk menanggulangi risiko tersebut.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang penerapan kebijakan dan prosedur operasional dalam pengelolaan *security patch,* dan pengawasan tanggung jawab dengan adanya rilis *security patch* baru, serta memastikan dan melakukan pelaporan. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.5.1.1 yang mencakup tentang kebijakan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah kebijakan-kebijakan keamanan informasi yang dibuat harus didefinisikan terlebih dahulu sebelum diterbitkan dan kebijakan-kebijakan yang telah diterbitkan harus segera dikomunikasikan dengan karyawan dan *stakeholder* yang terkait. Dalam kasus ini kebijakan yang dimaksud adalah dokumen terkait identifikasi risiko, tingkat risiko, serta mitigasi yang dapat dilakukan untuk menanggulangi risiko tersebut.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang aspek keamanan informasi dalam manajemen proyek. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.6.1.5 yang mencakup tentang keamanan informasi pada manajemen proyek. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan memastikan setiap kerangka kerja yang digunakan membuat *checklist* apakah keamanan informasi sudah dipertimbangkan dalam penerapannya.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang penerapan proses dalam evaluasi risiko terkait rencana pembelian atau implementasi sistem baru dan penanggulanagan masalah yang mungkin muncul. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.14.2.3 yang mencakup tentang peninjauan secara teknis setelah melakukan perubahan terhadap sistem. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat prosedur untuk kontrol dan pengujian terhadap perubahan sistem dengan mengikuti standar kontrol manajemen perubahan yang tersedia.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang penerapan proses pengembangan sistem yang aman . Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.14.2.1 yang mencakup tentang prosedur pengembangan yang aman. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat aturan dan prosedur dalam pengembangan sistem seperti dengan mempertimbangkan keamanan repositori, pengetahuan

terhadap keamanan sistem, dan membuat dokumen manajemen risiko terhadap keamanan informasi pada saat melakukan pengembangan sistem.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang risiko penerapan penanggulangan terhadap suatu sistem ketika terjadinya ketidakpatuhan terhadap kebijakan yang ada. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.14.2.1 yang mencakup tentang prosedur pengembangan yang aman. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat aturan dan prosedur dalam pengembangan sistem seperti dengan mempertimbangkan keamanan repositori, pengetahuan terhadap keamanan sistem, dan membuat dokumen manajemen risiko terhadap keamanan informasi pada saat melakukan pengembangan sistem.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang ketersediaan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan terkait keamanan informasi. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.17.1.1 yang mencakup tentang perencanaan kontinuitas keamanan informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat dokumen terkait persyaratan keamanan informasi dan hubungan terhadap manajemen keamanan informasi dalam situasi tertentu seperti krisis atau bencana.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang mendefinisikan komposisi, peran, wewenang, dan tanggung jawab terhadap perencanaan pemulihan dari bencana terhadap layanan TIK (*disaster recovery plan*). Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.16.1.1 yang mencakup tentang tanggung jawab dan prosedur. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat prosedur dan dokumen terkait deskripsi, wewenang, tanggung jawab yang jelas dari setiap posisi yang ada pada Dinas Komunikasi dan Informatikan Provinsi Jawa Timur khususnya pada divisi keamanan informasi untuk memastikan respon yang cepat, efektif dan teratur dalam menangani insiden atau bencana yang terjadi pada layanan TIK.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang jadwal uji coba perencanaan pemulihan bencana terhadap layan TIK. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.17.1.1 yang mencakup tentang perencanaan kontinuitas keamanan informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat dokumen terkait persyaratan keamanan informasi dan perencanaan dalam segi

waktu terhadap manajemen keamanan informasi dalam situasi tertentu seperti krisis atau bencana.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang hasil evaluasi perencanaan pemulihan bencana terhadap layanan TIK. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.16.1.4 yang mencakup tentang penilaian dan keputusan terhadap permasalahan keamanan informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat dokumen manajemen risiko dan membuat dokumen permasalahan keamanan informasi yang telah terjadi sehingga bisa dilakukan peninjauan dan *monitoring* secara berkala terkait mitigasi dari permasalahan yang terjadi.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang evaluasi kelayakan secara berkala terhadap kebijakan dan prosedur keamanan informasi. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.5.1.2 yang mencakup tentang tinjauan terhadap kebijakan-kebijakan untuk keamanan informasi. Sehingga, kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan melakukan penjadwalan secara berkala dalam melakukan peninjauan kembali atau melakukan pembaruan atas kebijakan-kebijakan pengelolaan risiko yang ada, apakah kebijakan-kebijakan terkait keamanan informasi tersebut masih revelan dan sesuai dengan kondisi saat ini, kecukupan dan efektifitasnya.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang strategi penerapan keamanan informasi yang sesuai dengan hasil Analisa risiko yang dimana penerapannya dilakukan sebagai bagian dari rencana kerja. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.12.7.1 yang mencakup tentang audit kontrol sistem informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan melakukan analisa audit secara berkala terhadap keamanan informasi dan hasil audit ini dapat digunakan sebabagai acuan dalam membuat dokumen manajemen risiko terhadap kerangka kerja keamanan informasi sehingga bisa digunakan sebagai strategi dalam rencana kerja Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang strategi penggunaan teknologi keamanan informasi yang penerapannya sesuai dengan kebutuhan. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.6.1.5 yang mencakup tentang tentang keamanan informasi pada manajemen proyek. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan memastikan setiap kerangka kerja yang digunakan

membuat *checklist* apakah keamanan informasi sudah dipertimbangkan dalam penerapannya.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang strategi penerapan keamanan informasi telah direalisasikan sebagai bagian dari pelaksanaan program kerja. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.6.1.5 yang mencakup tentang tentang keamanan informasi pada manajemen proyek. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan memastikan setiap kerangka kerja yang digunakan membuat *checklist* apakah keamanan informasi sudah dipertimbangkan dalam penerapannya.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang pelaksanaan program audit internal yang dilakukan oleh pihak independen. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.18.2.1 yang mencakup tentang *review* independen terhadap keamanan informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah melakukan audit independen secara berkala agar hasil dari audit independen tersebut bersifat obyektif.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang substansi evaluasi audit internal seperti pengukuran tingkat kepatuhan, konsistensi, dan efektifitas penerapan keamanan informasi. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.18.2.1 yang mencakup tentang *review* independen terhadap keamanan informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah melakukan audit independen secara berkala agar hasil dari audit independen tersebut bersifat obyektif.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang hasil audit internal. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode A.18.2.1 yang mencakup tentang *review* independen terhadap keamanan informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah melakukan audit independen secara berkala agar hasil dari audit independen tersebut bersifat obyektif dan hasil dari audit tersebut dapat digunakan sebagai acuan dalam melakukan pembuatan prosedur dan dokumen-dokumen yang berkaitan dengan keamanan informasi.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang melaporkan hasil audit internal kepaada pimpinan organisasi. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.18.2.1 yang mencakup tentang *review* independen

terhadap keamanan informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah melakukan audit independen secara berkala agar hasil dari audit independen tersebut bersifat obyektif dan melakukan dokumentasi terhadap audit independent yang dilakukan secara berkala.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang Analisa aspek finansial atau perubahan terhadap infrastruktur dalam keperluan untuk revisi kebijakan prosedur yang berlaku. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.5.1.2 yang mencakup tentang tinjauan terhadap kebijakan-kebijakan dan prosedur untuk keamanan informasi. Sehingga, kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan melakukan penjadwalan secara berkala dalam melakukan peninjauan kembali atau melakukan pembaruan atas kebijakan-kebijakan dan prosedur yang ada dari segi finansial, apakah kebijakan-kebijakan terkait keamanan informasi tersebut masih revelan dan sesuai dengan kondisi saat ini, kecukupan dan efektifitasnya.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang pengujian dan evaluasi secara periodik terhadap tingkat kepatuhan program keamanan informasi yang ada. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.18.2.1 yang mencakup tentang peninjauan independen terhadap keamanan informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah melakukan audit independen secara berkala terhadap tingkat kepatuhan program keamanan informasi sehingga hasil dari audit ini bersifat obyektif dan memberikan rekomendasi perbaikan dan pembenahan yang bersifat obyektif.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang rencana dan program peningkatan keamanan informasi untuk jangka menengah atau panjang. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.5.1.1 yang mencakup tentang kebijakan untuk keamanan informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat dokumen terkait rencana dan kebijakan terkait peningkatan keamanan informasi yang sifatnya jangka menengah atau Panjang (1/3/5 tahun).

5.4 Area Pengelolaan Aset Informasi

Pada area Pengelolaan Aset Informasi, Dinas Komunikasi dan Informatika Provinsi Jawa Timur mendapatkan skor sebesar 71 dari keseluruhan nilai area tata kelola keamanan informasi sebesar 168, sehingga apabila dibuat dalam persentase, Dinas Komunikasi dan Informatika Provinsi Jawa Timur mencapai persentase sebesar 42,26%. Dari persentase tersebut, masih terdapat beberapa aspek yang belum diterapkan seluruhnya atau baru diterapkan sebagian.

Beberapa aspek pada pengelolaan aset informasi masih dalam perencanaan atau belum dilakukan sehingga perlu dilakukan perbaikan berupa rekomendasi usulan berdasarkan kontrol *Annex* A ISO/IEC 27001:2013. Penilaian pengelolaan aset informasi menggunakan Indeks KAMI 4.0 menghasilkan 21 rekomendasi yang diusulkan untuk memenuhi kelengkapan penilaian Indeks KAMI yang belum atau tidak dilakukan atau dalam perencanaan oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Berdasarkan hasil penilaian dan skor pada Area Tata Kelola Keamanan Informasi tersebut secara garis besar Dinas Komunikasi dan Informatika Provinsi Jawa Timur perlu melakukan perencanaan, kajian, dan klasifikasi aset informasi dan melakukan dokumentasi terkait kebijakan pengelolaan aset informasi yang telah direncanakan dan dibuat yang nantinya akan diterapkan. Lalu, melakukan rencana *back-up* aset informasi secara berkala dan menyiapkan arsitektur atau sistem *back-up* dan manajemen cadangan terhadap risiko kehilangan aset informasi dengan cara melakukan *restore data.* Rekomendasi lainnya yaitu membuat rencana dan program pengamanan informasi terkait aset informasi jangka menengah maupun panjang, lalu membuat dokumen terkait kebijakan dan prosedur terkait sortir waktu penyimpanan data yang ada dan membuat dokumen syarat-syarat penghancuran data dan melakukan dokumentasi terhadap setiap kegiatan penghancuran data.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap belum melakukan pengelolaan aset informasi yang mencakup tentang pendefinisian tingkatan akses dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.8.2.1 yang mencakup tentang klasifikasi informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat dokumen kebijakan klasifikasi informasi dan dokumen prosedur panduan dalam menangani informasi yang sesuai dengan klasifikasinya.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang proses pengelolaan konfigurasi yang diterapkan secara konsisten. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.12.1.1 yang mencakup tentang dokumentasi prosedur operasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan melakukan dokumentasi seluruh prosedur operasi hingga konfigurasi sistem terkait teknologi informasi.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap belum melakukan pengelolaan aset informasi yang mencakup tentang peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.8.1.3 yang mencakup tentang penggunaan aset informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat

dokumen persetujuan atau "*agreements*" pengguna dan pemberi informasi terkait.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang pengelolaan identitas elektronik dan proses otentikasi. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.8.2.3 yang mencakup tentang penanganan aset. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat dokumen kebijakan klasifikasi, dan prosedur pengolahan aset informasi dan membuat prosedur proses otentikasi beserta kebijakan terhadap risiko-risko pelanggaran yang dapat terjadi.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap belum melakukan pengelolaan aset informasi yang mencakup tentang penetapan terkait waktu penyimpanan klasifikasi data yang ada dan syarat untuk penghancuran data. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.8.3.2 yang mencakup tentang penghancuran atau pemusnahan informasi atau data. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat dokumen terkait kebijakan dan prosedur terkait waktu penyimpanan data yang ada dan membuat dokumen syarat-syarat penghancuran data dan melakukan dokumentasi terhadap setiap kegiatan penghancuran data.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang prosedur *back-up* dan *restrore* data secara berkala. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.12.3.1 yang mencakup tentang prosedur *back-up* informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat rencana terkait *back-up* informasi secara berkala, menyiapkan arsitektur untuk *back-up,* jadwal, dan membuat sistem manajemen cadangan terhadap risiko *restore data.*

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang prosedur untuk user atau tenaga kontrak yang telah usai masa kerjanya. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.7.3.1 yang mencakup tentang pemberhentian dan pergantian tanggung jawab pegawai. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat kebijakan, prosedur, dan aturan dalam proses pemberhentian atau pergantian tanggung jawab terhadap pegawai atau tenaga kontrak.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang daftar data atau informasi yang harus di *back-up* dan pelaporan Analisa kepatuhan terhadap prosedurnya. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex

A ISO/IEC 27001:2013 dengan kode kontrol A.12.3.1 yang mencakup tentang prosedur *back-up* informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat rencana terkait *back-up* informasi secara berkala, menyiapkan arsitektur untuk *back-up,* jadwal, dan membuat laporan *back-up* berkala.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasi. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.8.2.3 yang mencakup tentang penanganan aset informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat daftar rekaman pelaksanaan keamanan informasi yang sesuai dengan klasifikasi informasinya.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang prosedur penggunaan prosedur penggunaan perangkat pengolah informasi yang dimiliki oleh pihak ketiga dengan memastikan aspek HAKI (Hak Atas Kekayaan Intelektual) dan pengamanan akses. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.18.1.2 yang mencakup tentang kepatuhan terhadap hak kekayaan intelektual. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan mengidentifikasi dan analisis terhadap perangkat pengolah informasi yang dibutuhkan serta syarat dan kewajibannya terhadap proses bisnis Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang penerapan pengamanan fasilitas fisik yang sesuai dengan kepentingan aset informasi. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.11.1.3 yang mencakup tentang pengamanan kantor, ruangan, dan fasilitas terkait keamanan informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat ruangan atau fasilitas khusus bagi aset-aset informasi yang berwujud fisik seperti server dan memberikan bantuan keamanan tambahan seperti pengamanan dari pihak ketiga bagi aset-aset informasi yang berwujud perangkat bergerak seperti laptop.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang proses dalam mengelola alokasi kunci masuk baik itu dalam bentuk fisik maupun elektronik ke fasilitas fisik. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.11.1.3 yang mencakup tentang pengamanan kantor, ruangan, dan fasilitas. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat ruangan atau fasilitas khusus bagi aset-aset informasi yang berwujud

fisik seperti server dan membuat kebijakan terhadap siapa saja yang bisa mengakses fasilitas fisik yang ada baik itu akses secara fisik maupun secara elektronik.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang perlindungan infrastruktur komputasi dari dampak lingkungan atau api dan berada dalam kondisi yang sesuai dengan prasyarat pabrikannya. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.11.1.4 yang mencakup tentang perlindungan terhadap ancaman eksternal dan ancaman lingkungan. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan melakukan identifikasi, penilaian risiko, dan penanganan terhadap risiko ancaman eksternal maupun ancaman lingkungan seperti kebakaran.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang perlindungan infrastruktur komputasi yang terpasang dari gangguan pasokan listrik atau petir. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.11.1.4 yang mencakup tentang perlindungan terhadap ancaman eksternal dan ancaman lingkungan. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan melakukan identifikasi, penilaian risiko, dan penanganan terhadap risiko ancaman eksternal maupun ancaman lingkungan seperti petir dan pemadaman listrik.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang peraturan pengamanan perangkat komputasi milik instansi apabila digunakan diluar lokasi kerja resmi atau kantor. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.11.1.1 yang mencakup tentang perlindungan batas keamanan fisik. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan melakukan identifikasi, penilaian risiko, dan penanganan terhadap risiko ancaman seperti penggunaan perangkat milik instansi diluar kondisi ideal atau diluar lingkungan kerja resmi.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang proses untuk memindahkan aset TIK dari lokasi yang sudah ditetapkan. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.11.1.1 yang mencakup tentang batas keamanan fisik. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat dokumentasi proses dan identifikasi, penilaian dan penanganan terhadap risiko terhadap pemindahan aset TIK.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang

konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung seperti pemadam api dan alat deteksi asap. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.11.1.4 yang mencakup tentang perlindungan terhadap ancaman eksternal dan ancaman lingkungan. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan melakukan identifikasi, penilaian risiko, dan penanganan terhadap risiko ancaman eksternal maupun ancaman lingkungan seperti kebakaran dan membuat daftar fasilitas pendukung.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang proses untuk inspeksi dan perawatan perangkat dan fasilitas pendukungnya, dan kelayakan keamanan lokasi kerja dalam penempatan aset informasi. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.11.2.4 yang mencakup tentang pengelolaan perangkat. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat jadwal pemeliharaan atau inspeksi terhadap perangkat dan fasilitas keamanan informasi yang ada secara rutin dan melakukan dokumentasi terhadap proses pengelolaan dan pemeliharaan fasilitas dan perangkat yang dimiliki.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang mekanisme pengamanan dalam pengiriman aset informasi yang melibatkan pihak ketiga. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.13.2.2 yang mencakup tentang kesepakatan pada pengiriman informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat prosedur dan kebijakan keamanan terkait pengiriman aset informasi yang diimplementasikan, dijalankan, dan dilakukan pengawasan.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang peraturan untuk mengamankan lokasi kerja penting seperti ruang server dari risiko perangkat atau bahan yang dapat membahayakan aset informasi. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.11.1.3 yang mencakup tentang pengamanan kantor, ruangan dan fasilitas. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan Membuat peraturan dan kebijakan pengamanan lokasi kantor, ruangan dan fasilitas yang dimiliki dari berbagai macam risiko dan merancang atau membuat ruangan dan fasilitas yang aman dari ancaman risiko fisik.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang proses untuk mengamankan lokasi kerja dari keberadaan pihak ketiga yang

bekerja bagi Dinas Komunikasi dan Informatika Provinsi Jawa Timur. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.11.1.4 yang mencakup tentang perlindungan terhadap ancaman eksternal dan ancaman lingkungan. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah melakukan identifikasi, penilaian risiko, dan penanganan terhadap risiko ancaman eksternal seperti keberadaan pihak ketiga.

5.5 Area Teknologi dan Keamanan Informasi

Pada area Area Teknologi dan Keamanan Informasi, Dinas Komunikasi dan Informatika Provinsi Jawa Timur mendapatkan skor sebesar 35 dari keseluruhan nilai area Teknologi dan keamanan informasi sebesar 120, sehingga apabila dibuat dalam persentase, Dinas Komunikasi dan Informatika Provinsi Jawa Timur mencapai persentase sebesar 29,17%. Dari persentase tersebut, masih terdapat beberapa aspek yang belum diterapkan seluruhnya atau baru diterapkan sebagian. Beberapa aspek pada teknologi dan kemanan informasi masih dalam perencanaan atau belum dilakukan sehingga perlu dilakukan perbaikan berupa rekomendasi usulan berdasarkan kontrol *Annex* A ISO/IEC 27001:2013. Penilaian teknologi dan keamanan informasi menggunakan Indeks KAMI 4.0 menghasilkan 26 rekomendasi yang diusulkan untuk memenuhi kelengkapan penilaian Indeks KAMI yang belum atau tidak dilakukan atau dalam perencanaan oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

Berdasarkan hasil penilaian dan skor pada Area Tata Kelola Keamanan Informasi tersebut secara garis besar Dinas Komunikasi dan Informatika Provinsi Jawa Timur perlu melakukan perencanaan, kajian, dan menyiapkan konfigurasi standar terkait keamanan informasi dan melakukan dokumentasi terkait kebijakan teknologi & keamanan informasi yang telah direncanakan dan dibuat yang nantinya akan diterapkan. Selain itu perlu membuat prosedur terhadap penanganan jaringan, sistem dan aplikasi yang telah dibuat, dikembangkan dan diterapkan sesuai dengan skema klasifikasi informasi seperti pembatasan hak akses, pemberian wewenang terhadap aset informasi dan melakukan proteksi lebih dari satu lapis agar aset informasi telindungi. lalu perlu dilakukan juga dokumentasi terhadap prosedur yang telah dibuat tersebut dan dievaluasi secara rutin. Rekomendasi lainnya adalah melakukan peninjauan secara rutin terhadap kebijakan dan prosedur konfigurasi standar melalui audit independen. Selain itu perlu juga membuat, lalu dikembangkan, dan diimplementasikan kebijakan terkait penggunaan kriptografi demi melindungi data dan informasi dengan pertimbangan menggunakan bentuk pengamanan khusus berlapis.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang layanan TIK yang menggunakan internet dan sudah dilindungi dengan lebih dari satu lapis pengamanan. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.13.1.1 yang mencakup tentang kontrol jaringan. Sehingga dengan kontrol dan kondisi saat ini

menghasilkan rekomendasi yang dapat diberikan adalah mengelola layanan TIK menggunakan keamanan lebih dari satu lapis agar aset informasi terlindungi.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang jaringan komunikasi disegmentasi sesuai dengan kepentingannya. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.13.1.3 yang mencakup tentang segregasi jaringan. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah melakukan segregasi dan segmentasi terhadap jaringan komunikasi bisa didasarkan pada domain publik, divisi atau departemen.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang konfigurasi standar untuk keamanan sistem bagi seluruh aset jaringan, sistem, dan aplikasi, yang dimutakhirkan sesuai dengan perkembangan dan kebutuhan. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.14.2.5 yang mencakup tentang Teknik pengembangan sistem yang aman. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan Membuat prosedur-prosedur terhadap Prinsip atau konfigurasi standar untuk sistem keamanan sistem bagi seluruh aset yang dimiliki dan harus ditetapkan, didokumentasikan, dipelihara, dan dikembangkan sesuai dengan kebutuhan.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang analisa kepatuhan penerapan konfigurasi standar secara rutin. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.18.2.2 yang mencakup tentang kepatuhan dengan standar dan kebijakan keamanan. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah melakukan peninjauan secara rutin terhadap kebijakan dan prosedur konfigurasi standar melalui audit independen.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan atau kebutuhan konfigurasi. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.8.2.3 yang mencakup tentang penanganan aset-aset. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat prosedur terhadap penanganan jaringan, sistem dan aplikasi dan telah dibuat, dikembangkan dan diterapkan sesuai dengan skema klasifikasi informasi seperti pembatasan hak akses, pemberian wewenang terhadap aset informasi. lalu perlu dilakukan juga dokumentasi terhadap prosedur yang telah dibuat tersebut dan dijalankan secara rutin.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang infrastruktur, sistem dan aplikasi dimonitor untuk memastikan ketersediaan sesuai kebutuhan atau persyaratan. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.14.1.1 yang mencakup tentang Analisis dan spesifikasi kebutuhan keamanan informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan melakukan analisis dan membuat daftar kebutuhan dan persyaratan infrastruktur, sistem, dan aplikasi. Daftar tersebut dimonitor untuk melakukan manajemen apabila terjadi perubahan kebutuhan dan syarat.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang keseluruhan infrastruktur jaringan, sistem, dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.12.1.3 yang mencakup tentang manajemen kapasitas. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat dokumentasi monitoring pada kapasitas penyimpanan data, dan kapasitas jaringan seperti bandwidth.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang setiap perubahan dalam sistem informasi secara otomatis terekam dalam log. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.12.4.1 yang mencakup tentang *event log* atau *log* kejadian. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat *event log* otomatis seperti log sistem, dan log akses terhadap sistem dan aplikasi, setiap kegiatan yang berhubungan dengan keamanan informasi dan log tersebut harus rutin ditinjau demi menjaga validitas.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang upaya akses oleh yang tidak berhak secara otomatis terekam dalam log. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.12.4.1 yang mencakup tentang *event log* atau *log* kejadian. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat *event log* otomatis seperti log sistem, dan log akses terhadap sistem dan aplikasi termasuk kegiatan upaya akses oleh pihak yang tidak berhak, setiap kegiatan yang berhubungan dengan keamanan informasi dan log tersebut harus rutin ditinjau demi menjaga validitas.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang semua log dianalisa secara berkala untuk memastikan akurasi, validitas, dan kelengkapan isinya bagi kepentingan jejak audit dan forensik. Kondisi

yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.12.4.1 yang mencakup tentang *event logging* atau log kejadian. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat *event log* seperti log sistem, dan log akses terhadap sistem dan aplikasi, setiap kegiatan yang berhubungan dengan keamanan informasi dan log tersebut harus rutin ditinjau demi menjaga validitas.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang penerapan enkripsi untuk melindungi aset informasi penting sesuai dengan kebijakan pengelolaan yang ada. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.10.1.1 yang mencakup tentang kebijakan mengenai penggunaan kontrol kriptografi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat, lalu dikembangkan, dan diimplementasikan kebijakan terkait penggunaan kriptografi demi melindungi data dan informasi yang sesuai dengan kebijakan pengelolaan yang ada seperti peraturan pemerintah.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang standar dalam menggunakan enkripsi. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.10.1.1 yang mencakup tentang kebijakan terkait penggunaan kontrol enkripsi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat, dikembangkan, dan diimplementasikan kebijakan terkait penggunaan kriptografi demi melindungi data dan informasi.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang penerapan pengamanan untuk mengelola kunci enkripsi yang digunakan termasuk siklus penggunaannya. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.10.1.2 yang mencakup tentang management kunci kriptografi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat kebijakan mengenai penggunaan, perlindungan, dan pengembangan kunci kriptografi termasuk penerapan pada seluruh siklus penggunaannya.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang seluruh sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian kata sandi secara otomatis, termasuk menon-aktifkan kata sandi, mengatur kompleksitas atau pajangan dan penggunaan kembali kata sandi lama. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.9.4.3 yang mencakup tentang manajemen sistem kata sandi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat sistem manajemen kata sandi

dan membuat kebijakan dan prosedur terkait pembuatan, kerahasiaan, dan perubahan kata sandi.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang akses yang digunakan untuk mengelola administrasi sistem menggunakan bentuk pengamanan khusus yang berlapis. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.10.1.1 yang mencakup tentang kebijakan terkait penggunaan kontrol kriptografi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat, lalu dikembangkan, dan diimplementasikan kebijakan terkait penggunaan kriptografi demi melindungi data dan informasi dengan pertimbangan menggunakan bentuk pengamanan khusus berlapis.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses, *timeouts, lockouts* setelah kegagalan *login,* dan penarikan hak akses. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.10.1.1 yang mencakup tentang kebijakan terkait penggunaan kontrol kriptografi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah dengan membuat, lalu dikembangkan, dan diimplementasikan kebijakan terkait penggunaan kriptografi seperti otomatisasi proses enkripsi, dan durasi waktu akses demi melindungi data dan informasi.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang penerapan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan termasuk jaringan nirkabel yang tidak resmi. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.13.1.2 yang mencakup tentang keamanan layanan jaringan. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat dan mengidentifikasi mekanisme keamanan dan persyaratan manajemen layanan jaringan termasuk jaringan nirkabel dan dimasukkan kedalam perjanjian layanan jaringan bagaimana dan dimana kondisi jaringan bisa diakses.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang penerapan bentuk pengamanan khusus untuk melindungi akses dari luar. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.13.1.2 yang mencakup tentang keamanan layanan jaringan. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat dan mengidentifikasi mekanisme keamanan dan persyaratan manajemen layanan jaringan termasuk

jaringan nirkabel dan dimasukkan kedalam perjanjian layanan jaringan dan melakukan penerapan pengamanan khusus pada jaringan.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terbaru. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.12.1.2 yang mencakup tentang manajemen perubahan. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat log terkait pemutakhiran sistem operasi pada setiap perangkat desktop dan server yang terintegrasi.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang perlindungan setiap desktop dan server dari penyerangan virus. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.12.2.1 yang mencakup tentang kontrol terhadap *malware*. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah melindungi setiap aset seperti desktop dan server menggunakan pelindung resmi dan berlisensi dan melakukan perbaruan perlindungan anti *malware* secara rutin.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang rekaman dan hasil analisa yang mengkonfirmasi bahwa antivirus telah diperbarui secara rutin dan sistematis. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.12.2.1 yang mencakup tentang kontrol terhadap *malware*. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah melakukan perbaruan perlindungan anti *malware* secara rutin dan didokumentasikan.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang laporan penyerangan virus atau malware yang gagal atau sukses ditindaklanjuti dan diselesaikan. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.12.2.1 yang mencakup tentang kontrol terhadap *malware*. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat laporan terhadap serangan virus atau malware untuk menjadi pedoman apabila terjadi ancaman serangan serupa.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang keseluruhan jaringan, sistem dan aplikasi menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang berlaku. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013

dengan kode kontrol A.12.4.4 yang mencakup tentang sinkroniasi waktu. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah melakukan konfigurasi waktu yang akurat pada seluruh jaringan, sistem dan aplikasi berdasarkan satu referensi atau pedoman.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi atau validasi pada saat proses pengembangan uji-coba. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.14.2.1 yang mencakup tentang kebijakan pengembangan yang aman. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat kebijakan, dan prosedur mengenai kegiatan pengembangan dan akuisisi setiap perangkat lunak dan sistem melalui validasi dan verifikasi fungsi keamanan.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang penerapan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk siklus hidup sistem yang dibangun. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.14.2.6 yang mencakup tentang pengamanan lingkungan pengembangan. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah mendefinisikan dan menetapkan kebijakan dan prosedur terkait perlindungan lingkungan pengembangan yang aman sesuai dengan standar sistem teknologi yang digunakan.

Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang keterlibatan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin. Kondisi yang terjadi saat ini sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.5.1.1 yang mencakup tentang kebijakan untuk keamanan informasi. Sehingga dengan kontrol dan kondisi saat ini menghasilkan rekomendasi yang dapat diberikan adalah membuat kebijakan dan aturan terkait keterlibatan pihak independen.

5.6 Suplemen

Berdasarkan hasil penilaian dan skor pada Area Tata Kelola Keamanan Informasi tersebut secara garis besar Dinas Komunikasi dan Informatika Provinsi Jawa Timur perlu melakukan perencanaan, pengkajian terkait analisis risiko dan evaluasi kredibilitas, serta pembuatan kebijakan terkait keterlibatan pihak ketiga, pengamanan layanan *Cloud Service,* dan perlindungan data diri dan merencanakan serta mengkaji dokumen SLA (*Service Level Agreement*) berisi kesepakatan formal bagi pihak layanan *Cloud Service*. Seluruh hasil perencanaan, kajian dan kebijakan yang dibuat, didokumentasikan.

5.6.1 Pengamanan Keterlibatan Pihak Ketiga Peyedia Layanan

Pada area pengamanan keterlibatan pihak ketiga penyedia layanan, berdasarkan hasil kuisioner yang diberikan dinas Komunikasi dan Informatika Provinsi Jawa Timur berada pada tahap belum menerapkan atau mengadopsi keterlibatan pihak ketiga penyedia layanan pada sistem keamanan informasi yang ada pada dinas Komunikasi dan Informatika Provinsi Jawa Timur sehingga seluruh pengelolaan terkait keterlibatan pihak ketiga masih belum terdokumentasikan. Dinas Komunikasi dan Informatika Provinsi Jawa Timur masih belum menerapkan pengamanan terkait dengan kajian risiko, penetapan data yang disimpan diolah dan dipertukarkan, Langkah pengamanan, kajian kriteria dan aspek hukum, evaluasi keterlibatan pihak ketiga penyedia layanan, standar keamanan teknis penggunaan layanan, dan dokumentasi insiden terhadap risiko keterlibatan pihak ketiga. Kondisi yang terjadi saat ini, secara keseluruhan sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.5.1.1 yang mencakup tentang kebijakan terkait keamanan informasi. Sehingga rekomendasi yang dapat diberikan pada area ini adalah Dinas Komunikasi dan Informatika perlu membuat dan mengkaji kebijakan terkait keterlibatan pihak ketiga sebagai penyedia layanan sebelum melakukan penerapan. Selain itu melakukan kajian analisis terkait risiko, dan evaluasi kredibilitas dari penyedia layanan dan melakukan dokumentasi dari setiap kebijakan yang telah dikaji dan dibuat.

5.6.2 Pengamanan Layanan Infrastuktur Awan (*Cloud Service*)

Pada area pengamanan layanan infrastruktur awan atau *cloud service*, berdasarkan hasil kuisioner yang diberikan dinas Komunikasi dan Informatika Provinsi Jawa Timur berada pada tahap belum menerapkan atau mengadopsi sistem berbasis *cloud service* sehingga seluruh pengelolaan berbasis awan masih belum terdokumentasikan. Dinas Komunikasi dan Informatika Provinsi Jawa Timur masih belum menerapkan pengamanan terkait dengan kajian risiko, penetapan data yang disimpan diolah dan dipertukarkan, Langkah pengamanan, kajian kriteria dan aspek hukum, evaluasi penyelenggara layanan awan, standar keamanan teknis penggunaan layanan, dan dokumentasi insiden terhadap sistem layanan inftastruktur awan. Kondisi yang terjadi saat ini, secara keseluruhan sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.5.1.1 yang mencakup tentang kebijakan terkait keamanan informasi. Sehingga rekomendasi yang dapat diberikan pada area ini adalah Dinas Komunikasi dan Informatika perlu membuat dan mengkaji kebijakan terkait sistem berbasis awan sebelum melakukan penerapan. Selain itu melakukan kajian analisis terkait risiko, dan evaluasi kredibilitas dari penyedia layanan infrastruktur awan dan melakukan dokumentasi dari setiap kebijakan yang telah dikaji dan dibuat. Lalu Membuat dan mengkaji kebijakan persyaratan dan kebutuhan keamanan informasi terkait layanan berbasis awan seperti bagaimana manajemen aset informasi yang ditempatkan pada layanan awan dikelola dan perjanjian hak ijin akses untuk memitigasi risiko yang terjadi, dan yang terakhir yaitu merencanakan dan mengkaji dokumen SLA (*Service Level Agreement*) berisi kesepakatan formal yang mencakup deskripsi layanan, kelebihan dan kendala layanan, prosedur pelaporan,

dan pemantauan kinerja sebelum memilih penyedia layanan infrastuktur awan (*cloud service*).

5.6.3 Perlindungan Data Pribadi

Pada area perlindungan data pribadi, berdasarkan hasil kuisioner yang diberikan dinas Komunikasi dan Informatika Provinsi Jawa Timur berada pada tahap belum menerapkan perlindungan data pribadi sehingga seluruh pengelolaan perlindungan data pribadi masih belum terdokumentasikan. Dinas Komunikasi dan Informatika Provinsi Jawa Timur masih belum menerapkan pengamanan terkait dengan kajian risiko, penetapan data yang disimpan diolah dan dipertukarkan, Langkah pengamanan, kajian kriteria dan aspek hukum, evaluasi perlindungan data pribadi, standar keamanan teknis dalam penerapan perlindungan data pribadi, dan dokumentasi insiden terhadap berbagai risiko yang mungkin terjadi pada perlindungan data pribadi. Kondisi yang terjadi saat ini, secara keseluruhan sesuai dengan kontrol Annex A ISO/IEC 27001:2013 dengan kode kontrol A.5.1.1 yang mencakup tentang kebijakan terkait keamanan informasi. Sehingga rekomendasi yang dapat diberikan pada area ini adalah Dinas Komunikasi dan Informatika perlu membuat dan mengkaji kebijakan terkait perlindungan data pribadi sebelum melakukan penerapan. Selain itu melakukan kajian analisis terkait risiko, dan melakukan dokumentasi dari setiap kebijakan yang telah dikaji dan dibuat.

BAB 6 KESIMPULAN DAN SARAN

6.1 Kesimpulan

1. Evaluasi terhadap Dinas Komunikasi dan Informatika Provinsi Jawa Timur dengan menggunakan penilaian Indeks KAMI 4.0, menghasilkan status tidak layak dengan nilai tingkat kelengkapan penerapan sesuai dengan standar ISO27001 mendapatkan skor 258. Setiap area yang ada pada Indeks KAMI 4.0, pada area tata kelola keamanan informasi tingkat keamanan mencapai tingkat II, area pengelolaan risiko keamanan informasi berada pada tingkat I+, area kerangka kerja keamanan informasi mencapai tingkat I+, area pengelolaan aset informasi mencapai tingkat I+, area teknologi dan keamanan informasi mencapai tingkat I.
2. Berdasarkan hasil evaluasi yang dilakukan menggunakan indeks KAMI 4.0, pada hasil evaluasi akhir, Didapatkan beberapa pertanyaan yang masih pada tahap tidak dilakukan dan pada tahap dalam penerapan. Pada area tata Kelola keamanan informasi sebanyak 4 pertanyaan pada status dalam perencanaan. Pada area pengelolaan risiko keamanan informasi sebanyak 11 pertanyaan pada status dalam perencanaan. Pada area kerangka kerja keamanan informasi sebanyak 22 pertanyaan pada status dalam perencanaan. Pada area pengelolaan aset keamanan informasi sebanyak 3 pertanyaan pada status tidak dilakukan dan 18 pertanyaan pada status dalam perencanaan. Pada area teknologi dan keamanan informasi sebanyak 1 pertanyaan pada status tidak dilakukan dan 25 pertanyaan pada status dalam perencanaan.
3. Berdasarkan hasil analisis yang dilakukan menggunakan indeks KAMI 4.0, terdapat beberapa rekomendasi berdasarkan ISO/IEC 27001:2013 yang dapat dipertimbangkan oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur dalam perbaikan penerapan keamanan informasi dan untuk meningkatkan penilaian indeks KAMI. Pada area tata kelola keamanan informasi tingkat keamanan mencapai sebanyak 4 rekomendasi, area pengelolaan risiko keamanan informasi sebanyak 11 rekomendasi, area kerangka kerja keamanan informasi sebanyak 22 rekomendasi, area pengelolaan aset informasi sebanyak 21 rekomendasi, dan area teknologi dan keamanan informasi sebanyak 26 rekomendasi.

6.2 Saran

1. Dinas Komunikasi dan Informatika Provinsi Jawa Timur sebaiknya diharapkan melaksanakan atau menerapkan rekomendasi-rekomendasi yang diberikan pada penelitian ini.
2. Pada penelitian selanjutnya sebaiknya melakukan evaluasi dan analisis menggunakan kerangka kerja selain Indeks KAMI 4.0 yang juga memiliki keterkaitan dengan keamanan informasi didalamnya seperti kerangka

kerja COBIT (*Control Objective for Information and related Technology*) dan ITIL (*Information Technology Infrastucture Library*).

3. Dinas Komunikasi dan Informatika Provinsi Jawa Timur perlu melakukan tinjauan ulang terkait kesiapan keamanan informasi dan mengukur keberhasilan rekomendasi perbaikan yang telah dilaksanakan setidaknya 2 kali dalam setahun menggunakan Indeks KAMI berdasarkan anjuran oleh Badan Siber dan Sandi Negara.

DAFTAR REFERENSI

Davis, B, Gordon .1991. Sistem informasi manajemen**.** Jakarta : PT Pustaka Binaman Pressindo.

Firmana Roodhin, Hidayanto dan Hanim, Bekti Cahyo dan Astuti, Hanim Maria, 2013. Penggunaan Indeks Keamanan Informasi (KAMI) Sebagai Evaluasi Keamanan Informasi Pada PT. PLN Distribusi JATIM. Jurnal Teknik POMITS, 1(1),pp. 1-5.

Indah, S., Octaviani, D., Herlambang, A. D., Studi, P., Informasi, S., Komputer, F. I., & Brawijaya, U. (2017). Evaluasi Kesiapan Kerangka Kerja Keamanan Informasi Pada Dinas Komunikasi Dan Informatika Kota Batu Dengan Menggunakan Indeks, *1*(1), 1–5.

ISO/IEC. (2013). ISO/IEC 27001:2013(E) Information technology — Security techniques — Information security management systems — Requirements.

Kementerian Komunikasi dan Informatika. (2016). Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi, 29

O'brien, J. A. & Marakas, G. M., 2010. *Introduction to Information System.* New York: McGraw.

Pratama, E.R., Suprapto dan Perdanakusuma, A.R., 2018. Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur). Jurnal Pengembangan Teknologi Informasidan Ilmu Komputer, 2(11), pp. 5911-5920.

Raharjo B., 2005, Keamanan Sistem Informasi Berbasis Internet.

Satria Sujalma, Ferdian & Ambarwati, Awalludiyah & Damastuti, Natalia. (2017). EVALUASI KEAMANAN INFORMASI PADA PT. MA-RI MENGGUNAKAN INDEKS KAMI.

Sutabri, T., 2012. *Konsep Sistem Informasi*. *Perpustakaan Nasional: Katalog dalam Terbitan*, Yokyakarta: CV ANDI OFFSET.

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

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

LAMPIRAN A TRANSKRIP WAWANCARA

Nama Responden : Aulia Bahar Pernama, S.Kom, M.ISM

Jabaran Responden : Kepala Seksi Persandian dan Keamanan Informasi

Hari / Tanggal : Kamis, 7 November 2019

Tempat / Waktu : Dinas KOMINFO Provinsi Jawa Timur, 14.00 WIB

No	
1	Pertanyaan
	Bagaimana kondisi keamanan informasi secara umum pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur?
	Jawaban
	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini memberikan layanan keamanan informasi pada lingkup dinas di Provinsi Jawa Timur untuk sementara ini, dan memang kadang kita juga memberi layanan pada kabupaten dan kota se-Provinsi Jawa Timur, jadi di Provinsi kita sebagai Pembina dari kabupaten dan kota jadi Ketika mereka mengalami kesulitan dalam pengelolaan keamanan informasi, Dinas Komunikasi dan Informatika Provinsi Jawa Timur bisa membantu mereka.
2	Pertanyaan
	Apakah Dinas Komunikasi dan Informatika Provinsi Jawa Timur pernah melakukan evaluasi khusus terkait keamanan informasi?
	Jawaban
	Pernah melakukan evaluasi terkait teknologi informasi dan rencananya Dinas Komunikasi dan Informatika Provinsi Jawa Timur akan melakukan evaluasi terkait keamanan informasi dengan Badan Siber dan Sandi Negara (BSSN).
3	Pertanyaan
	Apakah terdapat SOP (Standar Operasional) terkait keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur?
	Jawaban
	Ada beberapa bentuk Standar Operasional yang dimiliki dan beberapa kegiatan terkait keamanan informasi sudah memiliki Standar Operasionalnya. Mulai dari penanggulangan insiden, cara penyimpanan data dan lain sebagainya.
4	Pertanyaan
	Bagaimana kondisi terkait infrastruktur keamanan informasi yang ada pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur?
	Jawaban

	Sudah memiliki infrastruktur dasar seperti *firewall, email spam guard, dan juga data leak prevention* dan untuk beberapa aplikasi yang dimiliki dibuat atau di *build* oleh pihak ketiga dan oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur sendiri.
	Pertanyaan
5	Apakah ada kendala maupun pernah terjadi insiden terkait keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur?
	Jawaban
	Untuk insiden terkait keamanan informasi sering terjadi, seperti terkena serangan *deface, hack,* dan lain sebagainya. Namun untuk insiden yang sering terjadi adalah serangan *deface*.

LAMPIRAN B HASIL KUISIONER

Bagian II : Tata Kelola Keamanan Informasi					Bukti	
					Ada	Tidak
#	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?	Diterapkan Secara Menyeluruh	✓	
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?	Diterapkan Secara Menyeluruh	✓	
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	✓	
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	✓	
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Dalam Penerapan / Diterapkan Sebagian	✓	
2.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Dalam Perencanaan		✓
2.7	II	1	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Dalam Penerapan / Diterapkan Sebagian	✓	
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?	Diterapkan Secara Menyeluruh	✓	
2.9	II	2	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	✓	
2.10	II	2	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Dalam Penerapan / Diterapkan Sebagian	✓	
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?	Dalam Perencanaan		✓

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?	Diterapkan Secara Menyeluruh	✓	
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?	Diterapkan Secara Menyeluruh	✓	
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?	Diterapkan Secara Menyeluruh	✓	
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?	Dalam Penerapan / Diterapkan Sebagian	✓	
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?	Dalam Penerapan / Diterapkan Sebagian	✓	
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?	Dalam Penerapan / Diterapkan Sebagian	✓	
2.18	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Diterapkan Secara Menyeluruh	✓	
2.19	IV	3	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Dalam Penerapan / Diterapkan Sebagian	✓	
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?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
2.22	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Dalam Penerapan / Diterapkan Sebagian	✓	

Bagian III : Pengelolaan Risiko Keamanan Informasi					Bukti	
					Ada	Tidak
#	Kajian Risiko Keamanan Informasi					
3.1	II	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Dalam Penerapan / Diterapkan Sebagian	✓	
3.2	II	1	Apakah Instansi anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?	Dalam Perencanaan		✓
3.3	II	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Diterapkan Secara Menyeluruh	✓	
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 anda?	Dalam Penerapan / Diterapkan Sebagian	✓	
3.5	II	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Dalam Penerapan / Diterapkan Sebagian	✓	
3.6	II	1	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	Dalam Penerapan / Diterapkan Sebagian	✓	
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Dalam Perencanaan		✓
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Dalam Perencanaan		✓
3.9	II	1	Apakah Instansi 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)?	Dalam Perencanaan		✓
3.10	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Dalam Perencanaan		✓

3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Dalam Perencanaan		✓
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Dalam Perencanaan		✓

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi					Bukti	
					Ada	Tidak
#			**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?	Dalam Penerapan / Diterapkan Sebagian	✓	
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?	Dalam Penerapan / Diterapkan Sebagian	✓	
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?	Dalam Penerapan / Diterapkan Sebagian	✓	
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?	Dalam Penerapan / Diterapkan Sebagian	✓	
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?	Dalam Perencanaan		✓
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?	Dalam Penerapan / Diterapkan Sebagian	✓	
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?	Dalam Penerapan / Diterapkan Sebagian	✓	
4.8	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Dalam Penerapan / Diterapkan Sebagian	✓	

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?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
4.11	III	2	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
4.16	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Dalam Perencanaan		✓
4.17	III	3	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
4.19	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Dalam Perencanaan		✓
#	**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?	Dalam Perencanaan		✓
4.21	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Dalam Perencanaan		✓
4.22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Dalam Perencanaan		✓
4.23	III	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan	Dalam Perencanaan		✓

			keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?			
4.24	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?	Dalam Perencanaan		✓
4.25	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Dalam Perencanaan		✓
4.26	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓

Bagian V: Pengelolaan Aset Informasi					Bukti	
					Ada	Tidak
#			**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)	Dalam Penerapan / Diterapkan Sebagian	✓	
5.2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Diterapkan Secara Menyeluruh	✓	
5.3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	Diterapkan Secara Menyeluruh	✓	
5.4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut?	Tidak Dilakukan		✓
5.5	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	Dalam Penerapan / Diterapkan Sebagian	✓	
5.6	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Dalam Perencanaan		✓

5.7	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Dalam Penerapan / Diterapkan Sebagian	✓	
			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	Dalam Penerapan / Diterapkan Sebagian	✓	
5.9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Dalam Penerapan / Diterapkan Sebagian	✓	
5.10	II	1	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	Dalam Penerapan / Diterapkan Sebagian	✓	
5.11	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	Dalam Penerapan / Diterapkan Sebagian	✓	
5.12	II	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi	Tidak Dilakukan		✓
5.13	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	Dalam Perencanaan	✓	
5.14	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Dalam Penerapan / Diterapkan Sebagian	✓	
5.15	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	Tidak Dilakukan		✓
5.16	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Dalam Penerapan / Diterapkan Sebagian	✓	
5.17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dalam Penerapan / Diterapkan Sebagian	✓	
5.18	II	1	Prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala	Dalam Perencanaan	✓	
5.19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Dalam Penerapan / Diterapkan Sebagian	✓	

5.20	III	2	Proses pengecekan latar belakang SDM	Diterapkan Secara Menyeluruh	✓	
5.21	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Diterapkan Secara Menyeluruh	✓	
5.22	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Diterapkan Secara Menyeluruh	✓	
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	Dalam Penerapan / Diterapkan Sebagian	✓	
5.24	III	2	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	Dalam Perencanaan	✓	
5.25	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Dalam Perencanaan		✓
5.26	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
#	**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?	Dalam Perencanaan	✓	
5.29	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Dalam Perencanaan	✓	
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?	Dalam Perencanaan	✓	
5.31	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Dalam Perencanaan	✓	
5.32	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Dalam Perencanaan	✓	
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)?	Dalam Perencanaan	✓	
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?	Dalam Perencanaan	✓	

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?	Dalam Perencanaan	✓	
5.36	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Dalam Perencanaan		✓
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)	Dalam Perencanaan		✓
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?	Dalam Perencanaan		✓

Bagian VI: Teknologi dan Keamanan Informasi					Bukti	
					Ada	Tidak
#			**Pengamanan Teknologi**			
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Dalam Perencanaan		✓
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
6.4	II	1	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Dalam Perencanaan		✓
6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	Dalam Perencanaan		✓
6.6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Dalam Perencanaan		✓
6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Dalam Perencanaan		✓
6.8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Dalam Perencanaan		✓
6.9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Dalam Perencanaan		✓
6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Dalam Perencanaan		✓
6.11	II	1	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Dalam Perencanaan		✓

6.12	III	2	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?	Dalam Perencanaan		✓
6.13	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
6.17	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Dalam Perencanaan		✓
6.18	II	1	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?	Dalam Perencanaan		✓
6.19	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Perencanaan		✓
6.20	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Dalam Perencanaan		✓
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?	Dalam Perencanaan		✓
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Dalam Perencanaan		✓
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Dalam Perencanaan		✓
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?	Tidak Dilakukan		✓
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 yng dibangun?	Dalam Perencanaan		✓
6.26	IV	3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Dalam Perencanaan		✓

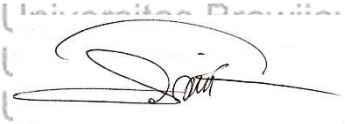
Bagian VII: Suplemen					Bukti	
					Ada	Tidak
#	Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan					
7.1.1	**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**					
7.1.1.1		1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?	Tidak Dilakukan		✓
7.1.1.2		1	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?	Tidak Dilakukan		✓
7.1.1.3		1	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?	Tidak Dilakukan		✓
7.1.1.4		1	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓
7.1.1.7		1	Apakah hak audit TI secara berkala ke 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?	Tidak Dilakukan		✓
7.1.1	**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?	Tidak Dilakukan		✓
7.1.2.2		1	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓

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?	Tidak Dilakukan		✓
7.1.3.3		1	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?	Tidak Dilakukan		✓
7.1.3.4		1	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓
7.1.3.6		1	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓
7.1.4.2		1	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓
7.1.5.2		1	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓
7.1.6.2		1	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓

7.1.7.2		1	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?	Tidak Dilakukan		✓
7.1.7.3		1	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓
7.2.2		1	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*?	Tidak Dilakukan		✓
7.2.3		1	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan *cloud*?	Tidak Dilakukan		✓
7.2.4		1	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*?	Tidak Dilakukan		✓
7.2.5		1	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan *cloud* terkait reputasi penyelenggaranya?	Tidak Dilakukan		✓
7.2.6		1	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan *cloud,* termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?	Tidak Dilakukan		✓
7.2.7		1	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓
7.2.9		1	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan *cloud*?	Tidak Dilakukan		✓
7.2.10		1	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan *cloud,* termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓
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?	Tidak Dilakukan		✓
7.3.3		1	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?	Tidak Dilakukan		✓
7.3.4		1	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?	Tidak Dilakukan		✓
7.3.5		1	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (*Data Protection Officer, Data Controller, Data Processor*) yang	Tidak Dilakukan		✓

			bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?				
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?	Tidak Dilakukan			✓
7.3.7		1	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?	Tidak Dilakukan			✓
7.3.8		1	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?	Tidak Dilakukan			✓
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?	Tidak Dilakukan			✓
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 ?	Tidak Dilakukan			✓
7.3.11		1	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?	Tidak Dilakukan			✓
7.3.12		1	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?	Tidak Dilakukan			✓
7.3.13		1	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?	Tidak Dilakukan			✓
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?	Tidak Dilakukan			✓
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?	Tidak Dilakukan			✓
7.3.16		1	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?	Tidak Dilakukan			✓

Mengetahui,
Responden



Ali Firman Herlambang, S.T

LAMPIRAN C *CHECKLIST* BUKTI

Bagian II : Tata Kelola Keamanan Informasi				Bukti		Keterangan
				Ada	Tidak	
#			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?	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013, Pergub Jatim No. 80 Tahun 2016
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?	✓		Pergub Jatim No. 80 Tahun 2016
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013, Pergub Jatim No. 80 Tahun 2016
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013, Pergub Jatim No. 80 Tahun 2016
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	✓		Dokumen SOA ISO27001:2013
2.6	II	1	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?		✓	
2.7	II	1	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	✓		Sertifikat Pelatihan dan kompetensi teknis berstandar Nasional/Internasional dan Ijazah Pendidikan masing2 Pelaksana
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?	✓		DPA (Daftar Pelaksanaan Anggaran) Seksi Persandian dan Keamanan Informasi tiap Tahun

2.9	II	2	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	✓		DPA (Daftar Pelaksanaan Anggaran) Seksi Persandian dan Keamanan Informasi tiap Tahun
2.10	II	2	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	✓		Dokumen SOA ISO 27001:2013
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?		✓	
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?	✓		Dokumen Kebijakan dan Pedoman Pengamanan Pihak Ketiga ISO 27001:2013; Dokumen Kebijakan Keamanan Informasi ISO 27001:2013
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?	✓		Dokumen Kebijakan dan Pedoman Kepatuhan Keamanan Informasi ISO 27001:2013; Dokumen Kebijakan Keamanan Informasi ISO 27001:2013
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?	✓		Dokumen Kebijakan dan Pedoman Keberlanjutan Bisnis dan Keamanan Informasi ISO 27001:2013
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?	✓		Dokumen Kebijakan dan Pedoman Kepatuhan Keamanan Informasi ISO 27001:2013; Dokumen Kebijakan Keamanan Informasi ISO 27001:2013
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?	✓		Dokumen Kebijakan Keamanan Informasi ISO 27001:2013
2.17	IV	3	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi,	✓		Kebijakan dan Pedoman Pengamanan dan

			khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?			Pengelolaan Aset ISO 27001:2013
2.18	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	✓		Kebijakan dan Prosedur Pengukuran SMKI ISO 27001:2013
2.19	IV	3	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	✓		Dokumen Kebijakan dan Prosedur Peningkatan Pemahaman Kesadaran (Awareness) dan Komunikasi Sistem Manajemen Keamanan Informasi ISO 27001:2013
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?		✓	
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?		✓	
2.22	IV	3	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	✓		Dokumen Kebijakan dan Pedoman Pengelolaan Insiden Keamanan Informasi ISO 27001:2013

Bagian III : Pengelolaan Risiko Keamanan Informasi				Bukti		Keterangan
				Ada	Tidak	
#	**Kajian Risiko Keamanan Informasi**					
3.1	II	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	✓		Dokumen Kebijakan dan Pedoman Manajemen Risiko SMKI ISO 27001:2013
3.2	II	1	Apakah Instansi anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?		✓	

3.3	II	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	✓		Dokumen Kebijakan dan Pedoman Manajemen Risiko SMKI ISO 27001:2013
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 anda?	✓		Dokumen Kebijakan dan Pedoman Manajemen Risiko SMKI ISO 27001:2013
3.5	II	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	✓		Dokumen Kebijakan dan Pedoman Manajemen Risiko SMKI ISO 27001:2013
3.6	II	1	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	✓		Dokumen Kebijakan dan Pedoman Pengendalian Akses ISO 27001:2013; Daftar Pemilik Aplikasi dan Perangkat Server Colocation
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?		✓	
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?		✓	
3.9	II	1	Apakah Instansi 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)?		✓	
3.10	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?		✓	
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?		✓	
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?		✓	

3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?		✓	
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?		✓	
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?		✓	
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?		✓	

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi				Bukti		Keterangan
				Ada	Tidak	
#	**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?	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013
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?	✓		Bukti Kehadiran sosialisasi ISO 27001 Data center pada 28 Juni 2018
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?	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013
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?	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan		✓	

			informasi, maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?			
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?	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013; SOP Penanganan Insiden Keamanan Informasi
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?	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013
4.8	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	✓		Dokumen Kebijakan dan Kepatuhan Keamanan Informasi ISO27001:2013
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?		✓	
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?		✓	
4.11	III	2	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?		✓	
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?		✓	
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?		✓	
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?		✓	
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?			
4.16	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?		✓	
4.17	III	3	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?		✓	
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?		✓	
4.19	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?		✓	
#	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?		✓	
4.21	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?		✓	
4.22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?		✓	
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 (atau sesuai dengan standar yang berlaku)?		✓	
4.24	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?		✓	
4.25	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?		✓	

4.26	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?		✓	
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?		✓	
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?		✓	
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?		✓	

Bagian V: Pengelolaan Aset Informasi				Bukti		Keterangan
				Ada	Tidak	
#			**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)	✓		Daftar Inventaris Barang Milik Negara Diskominfo dan Daftar Inventaris Barang di Data Center, Dokumen Kebijakan dan Pedoman Pengamanan dan Pengelolaan Aset ISO 27001:2013
5.2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	✓		Kebijakan dan Pedoman Pengamanan dan Pengelolaan Aset
5.3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?	✓		Kebijakan dan Pedoman Pengamanan dan Pengelolaan Aset
5.4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut?		✓	

5.5	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?	✓		Kebijakan dan Pedoman Manajemen Perubahan Fasilitas DC
5.6	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?		✓	
5.7	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	✓		Dokumen Kebijakan dan Pedoman Instalasi Perangkat Lunak ISO 27001:2013, Dokumen dan Pedoman Manajemen Perubahan Fasilitas Data Center ISO 27001:2013
			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	✓		SK Struktur Organisasi SMKI, Dokumen Kebijakan Keamanan Informasi ISO 27001:2013
5.9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	✓		Dokumen Kebijakan dan Pedoman Pengamanan dan Pengelolaan Aset ISO 27001:2013
5.10	II	1	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI	✓		Kebijakan Keamanan Informasi (Hal 114)
5.11	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan	✓		Kebijakan Keamanan Informasi (Hal 70 & 73)
5.12	II	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi		✓	
5.13	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	✓		Kebijakan Keamanan Informasi (Hal 34)
5.14	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	✓		Kebijakan Keamanan Informasi (Hal 34)
5.15	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data		✓	

5.16	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	✓		Kebijakan Keamanan Informasi (Hal 79)
5.17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	✓		Kebijakan Keamanan Informasi (Hal 101)
5.18	II	1	Prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala	✓		Kebijakan Keamanan Informasi (Hal 65); Berita Acara - Simulasi BCP
5.19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	✓		Kebijakan Keamanan Informasi (Hal 45)
5.20	III	2	Proses pengecekan latar belakang SDM	✓		Kebijakan Keamanan Informasi (Hal 15)
5.21	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	✓		Kebijakan Keamanan Informasi (Hal 12)
5.22	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	✓		Kebijakan Keamanan Informasi (Hal 26)
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	✓		Kebijakan Keamanan Informasi (Hal 34)
5.24	III	2	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	✓		Kebijakan Keamanan Informasi (Hal 37)
5.25	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?		✓	
5.26	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?		✓	
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?		✓	
#			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?	✓		Kebijakan Keamanan Informasi (Hal 45)
5.29	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	✓		Kebijakan Keamanan Informasi (Hal 45)

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?	✓		Kebijakan Keamanan Informasi (Hal 47)
5.31	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	✓		Kebijakan Keamanan Informasi (Hal 51)
5.32	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?	✓		Kebijakan Keamanan Informasi (Hal 55)
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)?	✓		Kebijakan Keamanan Informasi (Hal 54)
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?	✓		Kebijakan Keamanan Informasi (Hal 47)
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?	✓		Kebijakan Keamanan Informasi (Hal 47)
5.36	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?		✓	
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)		✓	
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?		✓	

Bagian VI: Teknologi dan Keamanan Informasi				Bukti		Keterangan
				Ada	Tidak	
#			Pengamanan Teknologi			
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?		✓	
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?		✓	
6.3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?		✓	
6.4	II	1	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?		✓	
6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?		✓	
6.6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?		✓	
6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?		✓	
6.8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?		✓	
6.9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?		✓	
6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?		✓	
6.11	II	1	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?		✓	
6.12	III	2	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?		✓	

6.13	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?		✓	
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?		✓	
6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?		✓	
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?		✓	
6.17	III	2	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?		✓	
6.18	II	1	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?		✓	
6.19	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?		✓	
6.20	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?		✓	
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?		✓	
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?		✓	
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?		✓	
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?		✓	
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 yng dibangun?			
6.26	IV	3	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?		✓	

Bagian VII: Suplemen				Bukti		Keterangan
				Ada	Tidak	
#			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?		✓	
7.1.1.2		1	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?		✓	
7.1.1.3		1	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?		✓	
7.1.1.4		1	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?		✓	
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?		✓	
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?		✓	
7.1.1.7		1	Apakah hak audit TI secara berkala ke 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?		✓	

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?		✓	
7.1.2.2		1	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?		✓	
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?		✓	
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 instanasi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?		✓	
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?		✓	
7.1.3.3		1	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?		✓	
7.1.3.4		1	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?		✓	
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?		✓	
7.1.3.6		1	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?		✓	

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?		✓	
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?		✓	
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?		✓	
7.1.4.2		1	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?		✓	
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?		✓	
7.1.5.2		1	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?		✓	
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?		✓	
7.1.6.2		1	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?		✓	
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?		✓	
7.1.7.2		1	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba,		✓	

			didokumentasikan hasilnya dan dievaluasi efektivitasnya?			
7.1.7.3		1	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?		✓	
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?		✓	
7.2.2		1	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*?		✓	
7.2.3		1	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan *cloud*?		✓	
7.2.4		1	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*?		✓	
7.2.5		1	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan *cloud* terkait reputasi penyelenggaranya?		✓	
7.2.6		1	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan *cloud,* termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?		✓	
7.2.7		1	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?		✓	
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?		✓	
7.2.9		1	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan *cloud*?		✓	
7.2.10		1	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan *cloud,* termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?		✓	

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?		✓	
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?		✓	
7.3.3		1	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?		✓	
7.3.4		1	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?		✓	
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?		✓	
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?		✓	
7.3.7		1	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?		✓	
7.3.8		1	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?		✓	
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?		✓	
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 ?		✓	
7.3.11		1	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?		✓	

7.3.12		1	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?		✓	
7.3.13		1	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?		✓	
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?		✓	
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?		✓	
7.3.16		1	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?		✓	

Mengetahui,
Responden

Ali Firman Herlambang, S.T

LAMPIRAN D KONTROL ANNEX A ISO 27001:2013

No Kode	Keterangan	Rekomendasi
A.5 Kebijakan Keamanan Informasi		
A.5.1 Manajemen Keamanan Informasi		
Tujuan : memberikan arahan dan dukungan bagi keamanan informasi agar sesuai dengan kebutuhan organisasi dan sesuai dengan hukum dan regulasi yang berlaku		
A.5.1.1	Kebijakan untuk keamanan informasi	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	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 Kebijakan 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	Semua tanggung jawab keamanan informasi harus ditentukan dan dialokasikan.
A.6.1.2	Pemisahan tugas	Kontak yang sesuai dengan otoritas yang relevan harus dijaga
A.6.1.3	Kontak dengan pihak berwenang	Kontak yang sesuai dengan otoritas yang relevan harus dijaga.
A.6.1.4	Kontak dengan kelompok minat khusus	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	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	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	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	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	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	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	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	Aset yang dipelihara dalam inventaris harus dimiliki.
A.8.1.3	Penggunaan aset yang dapat diterima	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	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	Informasi harus diklasifikasikan dalam persyaratan hukum, nilai, kekritisan dan kepekaan terhadap pengungkapan atau modifikasi yang tidak sah
A.8.2.2	Pemberian label informasi	Prosedur untuk menangani aset harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.
A.8.2.3	Penanganan aset	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	Prosedur harus diterapkan untuk manajemen media yang dapat dipindahkan sesuai dengan skema klasifikasi yang diadopsi oleh organisasi
A.8.3.2	Pembuangan media	Media harus dibuang dengan aman ketika tidak lagi diperlukan, menggunakan prosedur formal
A.8.3.3	Transfer media fisik	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	Kebijakan kontrol akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan bisnis dan informasi
A.9.1.2	Akses ke jaringan dan layanan jaringan	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	Proses pendaftaran dan de-registrasi pengguna formal harus dilaksanakan untuk memungkinkan penugasan hak akses.

A.9.2.2	Provisioning akses pengguna	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	Alokasi dan penggunaan hak akses istimewa harus dibatasi dan dikendalikan.
A.9.2.4	Pengelolaan informasi otentikasi rahasia pengguna	Alokasi informasi otentikasi rahasia harus dikontrol melalui proses manajemen formal
A.9.2.5	Tinjauan hak akses pengguna	Pemilik aset harus meninjau hak akses pengguna secara berkala.
A.9.2.6	Penghapusan atau penyesuaian hak akses	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	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	Akses ke informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan kontrol akses
A.9.4.2	Prosedur log-on yang aman	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	Sistem manajemen kata sandi harus interaktif dan harus memastikan kata sandi berkualitas.
A.9.4.4	Penggunaan program utilitas istimewa	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	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	Kebijakan tentang penggunaan kontrol kriptografi untuk perlindungan informasi harus dikembangkan dan diimplementasikan

A.10.1.2	Pengelolaan kunci	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	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	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	Keamanan fisik untuk kantor, kamar dan fasilitas harus dirancang dan diterapkan
A.11.1.4	Melindungi terhadap ancaman eksternal dan lingkungan	Perlindungan fisik terhadap bencana alam, serangan atau kecelakaan jahat harus dirancang dan diterapkan
A.11.1.5	Bekerja di area yang aman	Prosedur untuk bekerja di area aman harus dirancang dan diterapkan
A.11.1.6	Area pengiriman dan pemuatan	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	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	Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam mendukung utilitas
A.11.2.3	Keamanan kabel	Kabel daya dan telekomunikasi yang membawa data atau layanan informasi pendukung harus dilindungi dari gangguan, gangguan atau kerusakan
A.11.2.4	Pemeliharaan peralatan	Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan
A.11.2.5	Penghapusan aset	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	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	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	Pengguna harus memastikan bahwa peralatan yang tidak dijaga memiliki perlindungan yang tepat
A.11.2.9	Meja yang jelas dan kebijakan layar yang jelas	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	Prosedur operasi harus didokumentasikan dan tersedia bagi semua pengguna yang membutuhkannya.
A.12.1.2	Manajemen perubahan	Perubahan pada organisasi, proses bisnis, fasilitas pemrosesan informasi dan sistem yang mempengaruhi keamanan informasi harus dikontrol
A.12.1.3	Manajemen kapasitas	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	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 dilindungi terhadap malware.		
A.12.2.1	Kontrol terhadap Kontrol malware	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	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	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	Fasilitas logging dan informasi log harus dilindungi terhadap gangguan dan akses yang tidak sah.
A.12.4.3	Log administrator dan operator	Administrator sistem dan kegiatan operator sistem harus dicatat dan log dilindungi dan ditinjau secara berkala
A.12.4.4	Sinkronisasi jam	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	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	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	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	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 pemrosesan informasi pendukungnya		
A.13.1.1	Kontrol jaringan	Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi
A.13.1.2	Keamanan layanan jaringan	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	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 dengan entitas eksternal apa pun		
A.13.2.1	Kebijakan dan prosedur pengalihan informasi	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	Perjanjian harus menangani transfer aman informasi bisnis antara organisasi dan pihak eksternal.
A.13.2.3	Pesan elektronik	Informasi yang terlibat dalam pesan elektronik harus dilindungi dengan tepat
A.13.2.4	Perjanjian kerahasiaan atau nondisclosure	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	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	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	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 siklus pengembangan sistem informasi		
A.14.2.1	Kebijakan pembangunan yang aman	Aturan untuk pengembangan perangkat lunak dan sistem harus ditetapkan dan diterapkan untuk perkembangan dalam organisasi.
A.14.2.2	Prosedur kontrol perubahan sistem	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	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	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	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	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	Organisasi harus mengawasi dan memantau aktivitas pengembangan sistem yang dialihdayakan
A.14.2.8	Pengujian keamanan sistem	Pengujian fungsi keamanan harus dilakukan selama pengembangan.
A.14.2.9	Pengujian penerimaan sistem	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	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	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	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	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 disepakati sesuai dengan perjanjian pemasok.		

A.15.2.1	Pemantauan dan peninjauan layanan pemasok	Organisasi harus secara teratur memantau, meninjau, dan mengaudit layanan pemasok
A.15.2.2	Mengelola perubahan pada layanan pemasok	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	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	Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang tepat secepat mungkin
A.16.1.3	Melaporkan kelemahan keamanan informasi	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	Kejadian keamanan informasi harus dinilai dan diputuskan apakah akan diklasifikasikan sebagai insiden keamanan informasi
A.16.1.5	Tanggapan terhadap insiden keamanan informasi	Insiden keamanan informasi harus direspons sesuai dengan prosedur terdokumentasi
A.16.1.6	Belajar dari insiden keamanan informasi	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	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		
Tujuan : Keberlanjutan keamanan informasi harus disematkan dalam sistem manajemen kesinambungan bisnis organisasi.		
A.17.1.1	Merencanakan keberlanjutan keamanan informasi	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	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	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	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	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	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	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	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 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	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	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	Sistem informasi harus ditinjau secara berkala untuk kepatuhan terhadap kebijakan dan standar keamanan informasi organisasi.

LAMPIRAN E REKOMENDASI

No Pertanyaan	Permasalahan	Kode Kontrol Annex A	Keterangan	Rekomendasi
TATA KELOLA KEAMANAN INFORMASI				
2.6	Dinas Komunikasi dan Informatika Provinsi Jawa Timur masih dalam tahap perencanaan tata 126elola keamanan infromasi yang mencakup tentang mendefinisikan persyaratan / standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi	A.7.1.1	Mencakup tentang verifikasi dan pemeriksaan kompetensi pada semua pelaksana pengelolaan keamanan informasi	Membuat dokumen *requirements,* identifikasi hasil kerja, dan dokumen peninjauan hasil kerja terhadap standar kompetensi pelaksana keamanan informasi yang harus sesuai dengan undang-undang, dan proporsional dengan persyaratan instansi.
2.11	Dinas Komunikasi dan Informatika Provinsi Jawa Timur masih dalam tahap merencanakan tata kelola keamanan informasi yang mencakup tentang identifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku.	A.18.1.4	Mencakup tentang Privasi dan perlindungan informasi identitas pribadi	Privasi dan perlindungan informasi identitas pribadi harus dipastikan sebagaimana disyaratkan dalam undang-undang dan peraturan yang relevan berlaku lalu mengidentifikasi data pribadi yang dimiliki agar jelas siapa yang boleh dan bisa mengaksesnya.
2.20	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap merencanakan tata 126elola keamanan informasi yang mencakup tentang penerapan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan 126elola126 perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi	A.5.1.1	Mencakup tentang kebijakan untuk Dinas Komunikasi dan Informatika Provinsi Jawa Timur	Kebijakan-kebijakan keamanan informasi yang dibuat harus didefinisikan terlebih dahulu sebelum diterbitkan dan kebijakan-kebijakan yang telah diterbitkan harus segera dikomunikasikan dengan karyawan dan *stakeholder* yang terkait.
2.22	Dinas Komunikasi dan Informatika Provinsi Jawa Timur masih dalam tahap perencanaan tata 126elola keamanan informasi yang mencakup tentang identifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi	A.18.1.1	Mencakup tentang identifikasi peraturan dan legislasi yang berlaku beserta	Seluruh kebijakan-kebijakan yang telah diidentifikasi dan dibuat, perlu ada dokumentasi dan selalu diperbarui sesuai dengan situasi dan kondisi yang berlaku saat itu sehingga kebijakan yang ada bersifat ketat namun fleksibel.

	yang harus dipatuhi dan menganalisa tingkat kepatuhannya		persyaratan kontraknya	
	PENGELOLAAN RISIKO KEAMANAN INFORMASI			
3.2	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan tentang menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan.	A.6.1.1	Mencakup tentang tugas, fungsi, dan tanggung jawab keamanan informasi.	Mendefinisikan, mengalokasikan, dan mendokumentasikan seluruh tanggung jawab keamanan informasi mulai dari yang bersifat umum seperti melindungi informasi hingga tanggung jawab yang bersifat spesifik atau khusus seperti tanggung jawab dalam memberikan wewenang atau izin dalam akses data atau informasi kepada setiap *stakeholder* yang terkait dengan keamanan informasi ke dalam *requirement* pekerjaan,kebijakan-kebijakan terkait tupoksi dan kontrak kerja secara jelas.
3.7	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap melakukan perencanaan tentang identifikasi ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama.	A.8.2.3	Mencakup tentang penanganan terhadap aset.	Membuat prosedur-prosedur terhadap penanganan aset informasi yang dimiliki oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur lalu prosedur yang telah dibuat, dikembangkan dan diterapkan sesuai dengan skema klasifikasi informasi seperti pembatasan hak akses, pemberian wewenang terhadap aset informasi.
3.8	Dinas Komunikasi dan Informatika Provinsi Jawa Timur masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada	A.16.1.3	Mencakup tentang pelaporan tentang kelemahan keamanan informasi.	Membuat dokumen laporan terhadap kelemahan-kelemahan yang ditemukan sehingga dengan dokumen ini mampu dilakukan tindakan mitigasi dari kelemahan dan ancaman terhadap set informasi yang ditemukan.
3.9	Dinas Komunikasi dan Informatika Provinsi Jawa Timur masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada yang nantinya digunakan sebagai langkah mitigasi dalam identifikasi atau penanggulangan	A.5.1.1	Mencakup tentang kebijakan keamanan informasi pada Dinas Komunikasi dan Informatika	Kebijakan-kebijakan keamanan informasi yang dibuat harus didefinisikan terlebih dahulu sebelum diterbitkan dan kebijakan-kebijakan yang telah diterbitkan harus segera dikomunikasikan dengan karyawan dan *stakeholder* yang terkait. Dalam kasus ini kebijakan yang dimaksud adalah dokumen terkait identifikasi risiko,

	yang menjadi bagian dari program pengelolaan keamanan informasi.		Provinsi Jawa Timur.	tingkat risiko, serta mitigasi yang dapat dilakukan untuk menanggulangi risiko tersebut.
3.10	Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait penyusunan langkah mitigasi dan penanggulan risiko yang ada.	A.8.2.3	Mencakup tentang penanganan terhadap aset informasi.	Membuat prosedur-prosedur terhadap penanganan aset informasi yang dimiliki oleh Dinas Komunikasi dan Informatika Provinsi Jawa Timur lalu prosedur yang telah dibuat, dikembangkan dan diterapkan sesuai dengan skema klasifikasi informasi seperti pembatasan hak akses, pemberian wewenang terhadap aset informasi. lalu perlu dilakukan juga dokumentasi terhadap prosedur yang telah dibuat tersebut.
3.12	Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait langkah mitigasi risiko yang disusun sesuai dengan tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya	A.16.1.1	Mencakup tentang tanggung jawab dan prosedur	Membuat prosedur dan dokumen terkait Langkah mitigasi risiko-risiko yang mungkin terjadi dalam keamanan informasi dan menentukan target atau tujuan yang perlu dicapai dalam memitigasi risiko yang kemudian disusun sesuai dengan prioritas serta menentukan siapa yang bertanggung jawab pada mitigasi risiko tersebut.
3.13	Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait status penyelesaian langkah mitigasi risiko yang dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya	A.18.2.1	Mencakup tentang kepatuhan terhadap tinjauan independen atas keamanan informasi.	Melakukan peninjauan yang bersifat independent terhadap risiko dan kontrol keamanan untuk memastikan objektifitas dan manfaat dari pengelolaan mitigasi risiko ini. Tinjauan independent ini tidak harus melalui pihak eksternal, namun bisa menggunakan rencana mitigasi yang dimiliki oleh rekan-rekan kerja.
3.14	Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait penyelesaian langkah mitigasi yang sudah diterapkan dan dievaluasi	A.18.2.1	Mencakup tentang kepatuhan terhadap tinjauan independen atas keamanan informasi.	Melakukan peninjauan yang bersifat independent terhadap risiko dan kontrol keamanan untuk memastikan objektifitas dan manfaat dari pengelolaan mitigasi risiko ini. Tinjauan independent ini tidak harus melalui pihak eksternal, namun bisa menggunakan rencana

				mitigasi yang dimiliki oleh rekan-rekan kerja.
3.15	Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait 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.18.2.1	Mencakup tentang kepatuhan terhadap tinjauan independen atas keamanan informasi.	Melakukan peninjauan yang bersifat independent terhadap risiko dan kontrol keamanan untuk memastikan objektifitas dan manfaat dari pengelolaan mitigasi risiko ini. Tinjauan independent ini tidak harus melalui pihak eksternal, namun bisa menggunakan rencana mitigasi yang dimiliki oleh rekan-rekan kerja.
3.16	Dinas Komunikasi dan Informatika Provinsi Jawa Timur pada saat ini masih dalam tahap perencanaan pengelolaan risiko keamanan informasi terkait kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan /meningkatkan efektifitasnya.	A.5.1.2	Mencakup tentang tinjauan terhadap kebijakan-kebijakan untuk keamanan informasi.	Melakukan penjadwalan secara berkala dalam melakukan peninjauan kembali atau melakukan pembaruan atas kebijakan-kebijakan pengelolaan risiko yang ada, apakah kebijakan-kebijakan terkait risiko tersebut masih revelan dan sesuai dengan kondisi saat itu, kecukupan dan efektifitasnya.
KERANGKA KERJA PENGELOLAAN KEAMANAN INFORMASI				
4.5	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan kerangka kerja pengelolaan keamanan informasi yang mencakup tentang kebijakan dan prosedur keamanan informasi yang ada, sudah merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran atau objektif tertentu.	A.5.1.1	Mencakup tentang kebijakan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.	Kebijakan-kebijakan keamanan informasi yang dibuat harus didefinisikan terlebih dahulu sebelum diterbitkan dan kebijakan-kebijakan yang telah diterbitkan harus segera dikomunikasikan dengan karyawan dan *stakeholder* yang terkait. Dalam kasus ini kebijakan yang dimaksud adalah dokumen terkait identifikasi risiko, tingkat risiko, serta mitigasi yang dapat dilakukan untuk menanggulangi risiko tersebut.

4.9	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan kerangka kerja pengelolaan keamanan informasi yang mencakup tentang ketersediaan prosedur resmi dalam pengelolan suatu pengecualian terhadap penerapan keamanan informasi dan prosedur tindak lanjut terhadap kondisi tersebut .	A.5.1.1	Mencakup tentang kebijakan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.	Kebijakan-kebijakan keamanan informasi yang dibuat harus didefinisikan terlebih dahulu sebelum diterbitkan dan kebijakan-kebijakan yang telah diterbitkan harus segera dikomunikasikan dengan karyawan dan *stakeholder* yang terkait. Dalam kasus ini kebijakan yang dimaksud adalah dokumen terkait identifikasi risiko, tingkat risiko, serta mitigasi yang dapat dilakukan untuk menanggulangi risiko tersebut.
4.10	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang penerapan kebijakan dan prosedur operasional dalam pengelolaan *security patch,* dan pengawasan tanggung jawab dengan adanya rilis *security patch* baru, serta memastikan dan melakukan pelaporan.	A.5.1.1	Mencakup tentang kebijakan keamanan informasi pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur.	Kebijakan-kebijakan keamanan informasi yang dibuat harus didefinisikan terlebih dahulu sebelum diterbitkan dan kebijakan-kebijakan yang telah diterbitkan harus segera dikomunikasikan dengan karyawan dan *stakeholder* yang terkait. Dalam kasus ini kebijakan yang dimaksud adalah dokumen terkait identifikasi risiko, tingkat risiko, serta mitigasi yang dapat dilakukan untuk menanggulangi risiko tersebut.
4.11	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang aspek keamanan informasi dalam manajemen proyek.	A.6.1.5	Mencakup tentang keamanan informasi pada manajemen proyek.	Memastikan setiap kerangka kerja yang digunakan membuat *checklist* apakah keamanan informasi sudah dipertimbangkan dalam penerapannya.
4.12	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang penerapan proses dalam evaluasi risiko terkait rencana pembelian atau implementasi sistem baru dan penanggulanagan masalah yang mungkin muncul.	A.14.2.3	Mencakup tentang peninjauan secara teknis setelah melakukan perubahan terhadap sistem.	Membuat prosedur untuk kontrol dan pengujian terhadap perubahan sistem dengan mengikuti standar kontrol manajemen perubahan yang tersedia.
4.13	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang	A.14.2.1	Mencakup tentang prosedur	Membuat aturan dan prosedur dalam pengembangan sistem seperti dengan mempertimbangkan keamanan repositori, pengetahuan terhadap

	penerapan proses pengembangan sistem yang aman		pengembangan yang aman	keamanan sistem, dan membuat dokumen manajemen risiko terhadap keamanan informasi pada saat melakukan pengembangan sistem.
4.14	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang risiko penerapan penanggulangan terhadap suatu sistem ketika terjadinya ketidakpatuhan terhadap kebijakan yang ada.	A.14.2.1	Mencakup tentang prosedur pengembangan yang aman	Membuat aturan dan prosedur dalam pengembangan sistem seperti dengan mempertimbangkan keamanan repositori, pengetahuan terhadap keamanan sistem, dan membuat dokumen manajemen risiko terhadap keamanan informasi pada saat melakukan pengembangan sistem.
4.15	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang ketersediaan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan terkait keamanan informasi	A.17.1.1	Mencakup tentang perencanaan kontinuitas keamanan informasi	Membuat dokumen terkait persyaratan keamanan informasi dan hubungan terhadap manajemen keamanan informasi dalam situasi tertentu seperti krisis atau bencana.
4.16	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang mendefinisikan komposisi, peran, wewenang, dan tanggung jawab terhadap perencanaan pemulihan dari bencana terhadap layanan TIK (*disaster recovery plan*).	A.16.1.1	Mencakup tentang tanggung jawab dan prosedur	Membuat prosedur dan dokumen terkait deskripsi, wewenang, tanggung jawab yang jelas dari setiap posisi yang ada pada Dinas Komunikasi dan Informatikan Provinsi Jawa Timur khususnya pada divisi keamanan informasi untuk memastikan respon yang cepat, efektif dan teratur dalam menangani insiden atau bencana yang terjadi pada layanan TIK.
4.17	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang jadwal uji coba perencanaan pemulihan bencana terhadap layan TIK	A.17.1.1	Mencakup tentang perencanaan kontinuitas keamanan informasi.	Membuat dokumen terkait persyaratan keamanan informasi dan perencanaan dalam segi waktu terhadap manajemen keamanan informasi dalam situasi tertentu seperti krisis atau bencana.
4.18	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih	A.16.1.4	Mencakup tentang	Membuat dokumen manajemen risiko dan membuat dokumen

	dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang hasil evaluasi perencanaan pemulihan bencana terhadap layanan TIK.		penilaian dan keputusan terhadap permasalahan keamanan informasi.	permasalahan keamanan informasi yang telah terjadi sehingga bisa dilakukan peninjauan dan *monitoring* secara berkala terkait mitigasi dari permasalahan yang terjadi.
4.19	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang evaluasi kelayakan secara berkala terhadap kebijakan dan prosedur keamanan informasi.	A.5.1.2	Mencakup tentang tinjauan terhadap kebijakan-kebijakan untuk keamanan informasi.	Melakukan penjadwalan secara berkala dalam melakukan peninjauan kembali atau melakukan pembaruan atas kebijakan-kebijakan pengelolaan risiko yang ada, apakah kebijakan-kebijakan terkait keamanan informasi tersebut masih revelan dan sesuai dengan kondisi saat ini, kecukupan dan efektifitasnya.
4.20	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang strategi penerapan keamanan informasi yang sesuai dengan hasil Analisa risiko yang dimana penerapannya dilakukan sebagai bagian dari rencana kerja.	A.12.7.1	Mencakup tentang audit kontrol sistem informasi.	Melakukan analisa audit secara berkala terhadap keamanan informasi dan hasil audit ini dapat digunakan sebabagai acuan dalam membuat dokumen manajemen risiko terhadap kerangka kerja keamanan informasi sehingga bisa digunakan sebagai strategi dalam rencana kerja Dinas Komunikasi dan Informatika Provinsi Jawa Timur.
4.21	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang strategi penggunaan teknologi keamanan informasi yang penerapannya sesuai dengan kebutuhan.	A.6.1.5	Mencakup tentang tentang keamanan informasi pada manajemen proyek	Memastikan setiap kerangka kerja yang digunakan membuat *checklist* apakah keamanan informasi sudah dipertimbangkan dalam penerapannya.
4.22	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang strategi penerapan keamanan informasi telah direalisasikan sebagai bagian dari pelaksanaan program kerja	A.6.1.5	Mencakup tentang tentang keamanan informasi pada manajemen proyek	Memastikan setiap kerangka kerja yang digunakan membuat *checklist* apakah keamanan informasi sudah dipertimbangkan dalam penerapannya.
4.23	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan	A.18.2.1	Mencakup tentang *review* independen	Melakukan audit independen secara berkala agar hasil dari audit

	pengelolaan kerangka keamanan informasi yang mencakup tentang pelaksanaan program audit internal yang dilakukan oleh pihak independen		terhadap keamanan informasi.	independen tersebut bersifat obyektif.
4.24	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang substansi evaluasi audit internal seperti pengukuran tingkat kepatuhan, konsistensi, dan efektifitas penerapan keamanan informasi	A.18.2.1	Mencakup tentang *review* independen terhadap keamanan informasi.	Melakukan audit independen secara berkala agar hasil dari audit independen tersebut bersifat obyektif.
4.25	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang hasil audit internal.	A.18.2.1	Mencakup tentang *review* independen terhadap keamanan informasi.	melakukan audit independen secara berkala agar hasil dari audit independen tersebut bersifat obyektif dan hasil dari audit tersebut dapat digunakan sebagai acuan dalam melakukan pembuatan prosedur dan dokumen-dokumen yang berkaitan dengan keamanan informasi.
4.26	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang melaporkan hasil audit internal kepaada pimpinan organisasi	A.18.2.1	Mencakup tentang *review* independen terhadap keamanan informasi.	Melakukan audit independen secara berkala agar hasil dari audit independen tersebut bersifat obyektif dan melakukan dokumentasi terhadap audit independent yang dilakukan secara berkala.
4.27	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang Analisa aspek finansial atau perubahan terhadap infrastruktur dalam keperluan untuk revisi kebijakan prosedur yang berlaku	A.5.1.2	Mencakup tentang tinjauan terhadap kebijakan-kebijakan dan prosedur untuk keamanan informasi	Melakukan penjadwalan secara berkala dalam melakukan peninjauan kembali atau melakukan pembaruan atas kebijakan-kebijakan dan prosedur yang ada dari segi finansial, apakah kebijakan-kebijakan terkait keamanan informasi tersebut masih revelan dan sesuai dengan kondisi saat ini, kecukupan dan efektifitasnya.

4.28	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang pengujian dan evaluasi secara periodik terhadap tingkat kepatuhan program keamanan informasi yang ada	A.18.2.1	Mencakup tentang peninjauan independen terhadap keamanan informasi	Melakukan audit independen secara berkala terhadap tingkat kepatuhan program keamanan informasi sehingga hasil dari audit ini bersifat obyektif dan memberikan rekomendasi perbaikan dan pembenahan yang bersifat obyektif.
4.29	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan kerangka keamanan informasi yang mencakup tentang rencana dan program peningkatan keamanan informasi untuk jangka menengah atau panjang.	A.5.1.1	Mencakup tentang kebijakan untuk keamanan informasi.	Membuat dokumen terkait rencana dan kebijakan terkait peningkatan keamanan informasi yang sifatnya jangka menengah atau Panjang (1/3/5 tahun).
PENGELOLAAN ASET INFORMASI				
5.4	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap belum melakukan pengelolaan aset informasi yang mencakup tentang pendefinisian tingkatan akses dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut	A.8.2.1	Mencakup tentang klasifikasi informasi	Membuat dokumen kebijakan klasifikasi informasi dan dokumen prosedur panduan dalam menangani informasi yang sesuai dengan klasifikasinya.
5.6	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang proses pengelolaan konfigurasi yang diterapkan secara konsisten	A.12.1.1	Mencakup tentang dokumentasi prosedur operasi	Melakukan dokumentasi seluruh prosedur operasi hingga konfigurasi sistem terkait teknologi informasi.
5.12	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap belum melakukan pengelolaan aset informasi yang mencakup tentang peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data	A.8.1.3	Mencakup tentang penggunaan aset informasi	Membuat dokumen persetujuan atau "*agreements*" pengguna dan pemberi informasi terkait.
5.13	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang pengelolaan	A.8.2.3	Mencakup tentang penanganan aset	Membuat dokumen kebijakan klasifikasi, dan prosedur pengolahan aset informasi dan membuat prosedur proses otentikasi beserta kebijakan

	identitas elektronik dan proses otentikasi			terhadap risiko-risko pelanggaran yang dapat terjadi.
5.15	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap belum melakukan pengelolaan aset informasi yang mencakup tentang penetapan terkait waktu penyimpanan klasifikasi data yang ada dan syarat untuk penghancuran data	A.8.3.2	Mencakup tentang penghancuran atau pemusnahan informasi atau data	Membuat dokumen terkait kebijakan dan prosedur terkait waktu penyimpanan data yang ada dan membuat dokumen syarat-syarat penghancuran data dan melakukan dokumentasi terhadap setiap kegiatan penghancuran data.
5.18	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang prosedur *back-up* dan *restrore* data secara berkala	A.12.3.1	Mencakup tentang prosedur *back-up* informasi	Membuat rencana terkait *back-up* informasi secara berkala, menyiapkan arsitektur untuk *back-up,* jadwal, dan membuat sistem manajemen cadangan terhadap risiko *restore data.*
5.24	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang prosedur untuk user atau tenaga kontrak yang telah usai masa kerjanya	A.7.3.1	Mencakup tentang pemberhentian dan pergantian tanggung jawab pegawai	Membuat kebijakan, prosedur, dan aturan dalam proses pemberhentian atau pergantian tanggung jawab terhadap pegawai atau tenaga kontrak.
5.25	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang daftar data atau informasi yang harus di *back-up* dan pelaporan Analisa kepatuhan terhadap prosedurnya	A.12.3.1	Mencakup tentang prosedur *back-up* informasi.	Membuat rencana terkait *back-up* informasi secara berkala, menyiapkan arsitektur untuk *back-up,* jadwal, dan membuat laporan *back-up* berkala.
5.26	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasi	A.8.2.3	Mencakup tentang penanganan aset informasi.	Membuat daftar rekaman pelaksanaan keamanan informasi yang sesuai dengan klasifikasi informasinya.
5.27	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang prosedur penggunaan prosedur penggunaan perangkat pengolah informasi yang dimiliki oleh pihak ketiga dengan	A.18.1.2	Mencakup tentang kepatuhan terhadap hak kekayaan intelektual	Mengidentifikasi dan analisis terhadap perangkat pengolah informasi yang dibutuhkan serta syarat dan kewajibannya terhadap proses bisnis Dinas Komunikasi dan Informatika Provinsi Jawa Timur.

	memastikan aspek HAKI (Hak Atas Kekayaan Intelektual) dan pengamanan akses			
5.28	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang penerapan pengamanan fasilitas fisik yang sesuai dengan kepentingan aset informasi.	A.11.1.3	Mencakup tentang pengamanan kantor, ruangan, dan fasilitas terkait keamanan informasi	Membuat ruangan atau fasilitas khusus bagi aset-aset informasi yang berwujud fisik seperti server dan memberikan bantuan keamanan tambahan seperti pengamanan dari pihak ketiga bagi aset-aset informasi yang berwujud perangkat bergerak seperti laptop.
5.29	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang proses dalam mengelola alokasi kunci masuk baik itu dalam bentuk fisik maupun elektronik ke fasilitas fisik.	A.11.1.3	Mencakup tentang pengamanan kantor, ruangan, dan fasilitas	Membuat ruangan atau fasilitas khusus bagi aset-aset informasi yang berwujud fisik seperti server dan membuat kebijakan terhadap siapa saja yang bisa mengakses fasilitas fisik yang ada baik itu akses secara fisik maupun secara elektronik.
5.30	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang perlindungan infrastruktur komputasi dari dampak lingkungan atau api dan berada dalam kondisi yang sesuai dengan prasyarat pabrikannya	A.11.1.4	Mencakup tentang perlindungan terhadap ancaman eksternal dan ancaman lingkungan	Melakukan identifikasi, penilaian risiko, dan penanganan terhadap risiko ancaman eksternal maupun ancaman lingkungan seperti kebakaran.
5.31	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang perlindungan infrastruktur komputasi yang terpasang dari gangguan pasokan listrik atau petir	A.11.1.4	Mencakup tentang perlindungan terhadap ancaman eksternal dan ancaman lingkungan	Melakukan identifikasi, penilaian risiko, dan penanganan terhadap risiko ancaman eksternal maupun ancaman lingkungan seperti petir dan pemadaman listrik.
5.32	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang peraturan pengamanan perangkat komputasi milik instansi apabila digunakan diluar lokasi kerja resmi atau kantor	A.11.1.1	Mencakup tentang perlindungan batas keamanan fisik	Melakukan identifikasi, penilaian risiko, dan penanganan terhadap risiko ancaman seperti penggunaan perangkat milik instansi diluar kondisi ideal atau diluar lingkungan kerja resmi.
5.33	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan	A.11.1.1	Mencakup tentang perlindungan	Membuat dokumentasi proses dan identifikasi, penilaian dan

	pengelolaan aset informasi yang mencakup tentang proses untuk memindahkan aset TIK dari lokasi yang sudah ditetapkan		batas keamanan fisik	penanganan terhadap risiko terhadap pemindahan aset TIK.
5.34	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung seperti pemadam api dan alat deteksi asap	A.11.1.4	Mencakup tentang perlindungan terhadap ancaman eksternal dan ancaman lingkungan	Melakukan identifikasi, penilaian risiko, dan penanganan terhadap risiko ancaman eksternal maupun ancaman lingkungan seperti kebakaran dan membuat daftar fasilitas pendukung.
5.35	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang proses untuk inspeksi dan perawatan perangkat dan fasilitas pendukungnya, dan kelayakan keamanan lokasi kerja dalam penempatan aset informasi	A.11.2.4	Mencakup tentang pengelolaan perangkat	Membuat jadwal pemeliharaan atau inspeksi terhadap perangkat dan fasilitas keamanan informasi yang ada secara rutin dan melakukan dokumentasi terhadap proses pengelolaan dan pemeliharaan fasilitas dan perangkat yang dimiliki.
5.36	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang mekanisme pengamanan dalam pengiriman aset informasi yang melibatkan pihak ketiga	A.13.2.2	Mencakup tentang kesepakatan pada pengiriman informasi	Membuat prosedur dan kebijakan keamanan terkait pengiriman aset informasi yang diimplementasikan, dijalankan, dan dilakukan pengawasan.
5.37	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang peraturan untuk mengamankan lokasi kerja penting seperti ruang server dari risiko perangkat atau bahan yang dapat membahayakan aset informasi	A.11.1.3	Mencakup tentang pengamanan kantor, ruangan dan fasilitas	Membuat peraturan dan kebijakan pengamanan lokasi kantor, ruangan dan fasilitas yang dimiliki dari berbagai macam risiko dan merancang atau membuat ruangan dan fasilitas yang aman dari ancaman risiko fisik.

5.38	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan pengelolaan aset informasi yang mencakup tentang proses untuk mengamankan lokasi kerja dari keberadaan pihak ketiga yang bekerja bagi Dinas Komunikasi dan Informatika Provinsi Jawa Timur	A.11.1.4	Mencakup tentang perlindungan terhadap ancaman eksternal dan ancaman lingkungan	Melakukan identifikasi, penilaian risiko, dan penanganan terhadap risiko ancaman eksternal seperti keberadaan pihak ketiga.
TEKNOLOGI DAN KEAMANAN INFORMASI				
6.1	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang layanan TIK yang menggunakan internet dan sudah dilindungi dengan lebih dari satu lapis pengamanan	A.13.1.1	Mencakup tentang kontrol jaringan	Mengelola layanan TIK menggunakan keamanan lebih dari satu lapis agar aset informasi terlindungi.
6.2	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang jaringan komunikasi disegmentasi sesuai dengan kepentingannya.	A.13.1.3	Mencakup tentang segregasi jaringan	Melakukan segregasi dan segmentasi terhadap jaringan komunikasi bisa didasarkan pada domain publik, divisi atau departemen.
6.3	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang konfigurasi standar untuk keamanan sistem bagi seluruh aset jaringan, sistem, dan aplikasi, yang dimutakhirkan sesuai dengan perkembangan dan kebutuhan	A.14.2.5	Mencakup tentang teknik pengembangan sistem yang aman	Membuat prosedur-prosedur terhadap Prinsip atau konfigurasi standar untuk sistem keamanan sistem bagi seluruh aset yang dimiliki dan harus ditetapkan, didokumentasikan, dipelihara, dan dikembangkan sesuai dengan kebutuhan.
6.4	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area	A.18.2.2	Mencakup tentang kepatuhan	Melakukan peninjauan secara rutin terhadap kebijakan dan prosedur

	Teknologi dan Keamanan Informasi yang mencakup tentang analisa kepatuhan penerapan konfigurasi standar secara rutin		dengan standar dan kebijakan keamanan	konfigurasi standar melalui audit independen.
6.5	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang jaringan,sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan atau kebutuhan konfigurasi	A.8.2.3	Mencakup tentang penanganan aset-aset	Membuat prosedur terhadap penanganan jaringan, sistem dan aplikasi dan telah dibuat, dikembangkan dan diterapkan sesuai dengan skema klasifikasi informasi seperti pembatasan hak akses, pemberian wewenang terhadap aset informasi. lalu perlu dilakukan juga dokumentasi terhadap prosedur yang telah dibuat tersebut dan dijalankan secara rutin.
6.6	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang infrastruktur, sistem dan aplikasi dimonitor untuk memastikan ketersediaan sesuai kebutuhan atau persyaratan	A.14.1.1	Mencakup tentang Analisis dan spesifikasi kebutuhan keamanan informasi	Melakukan analisis dan membuat daftar kebutuhan dan persyaratan infrastruktur, sistem, dan aplikasi. Daftar tersebut dimonitor untuk melakukan manajemen apabila terjadi perubahan kebutuhan dan syarat.
6.7	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang keseluruhan infrastruktur jaringan, sistem, dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan	A.12.1.3	Mencakup tentang manajemen kapasitas	Membuat dokumentasi monitoring pada kapasitas penyimpanan data, dan kapasitas jaringan seperti bandwidth.
6.8	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang setiap perubahan dalam sistem informasi secara otomatis terekam dalam log	A.12.4.1	Mencakup tentang *event log* atau *log* kejadian	Membuat *event log* otomatis seperti log sistem, dan log akses terhadap sistem dan aplikasi, setiap kegiatan yang berhubungan dengan keamanan informasi dan log tersebut harus rutin ditinjau demi menjaga validitas.

6.9	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang upaya akses oleh yang tidak berhak secara otomatis terekam dalam log	A.12.4.1	Mencakup tentang *event log* atau *log* kejadian.	Membuat *event log* otomatis seperti log sistem, dan log akses terhadap sistem dan aplikasi termasuk kegiatan upaya akses oleh pihak yang tidak berhak , setiap kegiatan yang berhubungan dengan keamanan informasi dan log tersebut harus rutin ditinjau demi menjaga validitas.
6.10	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang semua log dianalisa secara berkala untuk memastikan akurasi, validitas, dan kelengkapan isinya bagi kepentingan jejak audit dan forensik	A.12.4.1	Mencakup tentang *event logging* atau log kejadian.	Membuat *event log* seperti log sistem, dan log akses terhadap sistem dan aplikasi, setiap kegiatan yang berhubungan dengan keamanan informasi dan log tersebut harus rutin ditinjau demi menjaga validitas.
6.11	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang penerapan enkripsi untuk melindungi aset informasi penting sesuai dengan kebijakan pengelolaan yang ada	A.10.1.1	Mencakup tentang kebijakan mengenai penggunaan kontrol kriptografi.	Membuat, lalu dikembangkan, dan diimplementasikan kebijakan terkait penggunaan kriptografi demi melindungi data dan informasi yang sesuai dengan kebijakan pengelolaan yang ada seperti peraturan pemerintah.
6.12	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang standar dalam menggunakan enkripsi	A.10.1.1	Mencakup tentang kebijakan terkait penggunaan kontrol enkripsi	Membuat, dikembangkan, dan diimplementasikan kebijakan terkait penggunaan kriptografi demi melindungi data dan informasi.
6.13	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang penerapan pengamanan untuk mengelola kunci enkripsi yang digunakan termasuk siklus penggunaannya	A.10.1.2	Mencakup tentang management kunci kriptografi	Membuat kebijakan mengenai penggunaan, perlindungan, dan pengembangan kunci kriptografi termasuk penerapan pada seluruh siklus penggunaannya.
6.14	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang seluruh sistem dan aplikasi secara otomatis mendukung dan menerapkan	A.9.4.3	Mencakup tentang manajemen sistem kata sandi	Membuat sistem manajemen kata sandi dan membuat kebijakan dan prosedur terkait pembuatan, kerahasiaan, dan perubahan kata sandi.

	penggantian kata sandi secara otomatis, termasuk menon-aktifkan kata sandi, mengatur kompleksitas atau pajangan dan penggunaan kembali kata sandi lama			
6.15	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang akses yang digunakan untuk mengelola administrasi sistem menggunakan bentuk pengamanan khusus yang berlapis	A.10.1.1	Mencakup tentang kebijakan terkait penggunaan kontrol kriptografi	Membuat, lalu dikembangkan, dan diimplementasikan kebijakan terkait penggunaan kriptografi demi melindungi data dan informasi dengan pertimbangan menggunakan bentuk pengamanan khusus berlapis.
6.16	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses, *timeouts, lockouts* setelah kegagalan *login,* dan penarikan hak akses	A.10.1.1	Mencakup tentang kebijakan terkait penggunaan kontrol kriptografi	Membuat, lalu dikembangkan, dan diimplementasikan kebijakan terkait penggunaan kriptografi seperti otomatisasi proses enkripsi, dan durasi waktu akses demi melindungi data dan informasi.
6.17	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang penerapan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan termasuk jaringan nirkabel yang tidak resmi	A.13.1.2	Mencakup tentang keamanan layanan jaringan	Membuat dan mengidentifikasi mekanisme keamanan dan persyaratan manajemen layanan jaringan termasuk jaringan nirkabel dan dimasukkan kedalam perjanjian layanan jaringan bagaimana dan dimana kondisi jaringan bisa diakses.
6.18	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang penerapan bentuk pengamanan khusus untuk melindungi akses dari luar	A.13.1.2	Mencakup tentang keamanan layanan jaringan	Membuat dan mengidentifikasi mekanisme keamanan dan persyaratan manajemen layanan jaringan termasuk jaringan nirkabel dan dimasukkan kedalam perjanjian layanan jaringan dan melakukan penerapan pengamanan khusus pada jaringan.
6.19	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang sistem operasi untuk setiap perangkat	A.12.1.2	Mencakup tentang manajemen perubahan	membuat log terkait pemutakhiran sistem operasi pada setiap perangkat desktop dan server yang terintegrasi.

	desktop dan server dimutakhirkan dengan versi terbaru			
6.20	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang perlindungan setiap desktop dan server dari penyerangan virus	A.12.2.1	Mencakup tentang kontrol terhadap *malware*	Melindungi setiap aset seperti desktop dan server menggunakan pelindung resmi dan berlisensi dan melakukan perbaruan perlindungan anti *malware* secara rutin.
6.21	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang rekaman dan hasil analisa yang mengkonfirmasi bahwa antivirus telah diperbarui secara rutin dan sistematis	A.12.2.1	Mencakup tentang kontrol terhadap *malware*	Melakukan perbaruan perlindungan anti *malware* secara rutin dan didokumentasikan.
6.22	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang laporan penyerangan virus atau malware yang gagal atau sukses ditindaklanjuti dan diselesaikan	A.12.2.1	Mencakup tentang kontrol terhadap *malware*	Membuat laporan terhadap serangan virus atau malware untuk menjadi pedoman apabila terjadi ancaman serangan serupa.
6.23	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang keseluruhan jaringan, sistem dan aplikasi menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang berlaku	A.12.4.4	Mencakup tentang sinkroniasi waktu	Melakukan konfigurasi waktu yang akurat pada seluruh jaringan, sistem dan aplikasi berdasarkan satu referensi atau pedoman.
6.24	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi atau validasi pada saat proses pengembangan uji-coba	A.14.2.1	Mencakup tentang kebijakan pengembangan yang aman.	Membuat kebijakan, dan prosedur mengenai kegiatan pengembangan dan akuisisi setiap perangkat lunak dan sistem melalui validasi dan verifikasi fungsi keamanan.
6.25	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area	A.14.2.6	Mencakup tentang pengamanan	Mendefinisikan dan menetapkan kebijakan dan prosedur terkait perlindungan lingkungan

	Teknologi dan Keamanan Informasi yang mencakup tentang penerapan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk siklus hidup sistem yang dibangun		lingkungan pengembangan	pengembangan yang aman sesuai dengan standar sistem teknologi yang digunakan.
6.26	Dinas Komunikasi dan Informatika Provinsi Jawa Timur saat ini masih dalam tahap perencanaan Area Teknologi dan Keamanan Informasi yang mencakup tentang keterlibatan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin	A.5.1.1	Mencakup tentang kebijakan untuk keamanan informasi.	Membuat kebijakan dan aturan terkait keterlibatan pihak independen.
	SUPLEMEN			
7	Pada area pengamanan keterlibatan pihak ketiga penyedia layanan dan Perlindungan Data Pribadi, Dinas Komunikasi dan Informatika Provinsi Jawa Timur berada pada tahap belum menerapkan	A.5.1.1	Mencakup tentang kebijakan terkait keamanan informasi	Membuat dan mengkaji kebijakan terkait perlindungan data pribadi sebelum melakukan penerapan. Selain itu melakukan kajian analisis terkait risiko, dan melakukan dokumentasi dari setiap kebijakan yang telah dikaji dan dibuat.
	Pada area Pengamanan Layanan Infrastruktur Awan (*Cloud Service*) berada pada tahap belum menerapkan Layanan Awan (*Cloud Service*)	A.15.1.1	Mencakup tentang kebijakan keamanan informasi terkait *supplier*	Membuat dan mengkaji kebijakan persyaratan dan kebutuhan keamanan informasi terkait layanan berbasis awan seperti bagaimana manajemen aset informasi yang ditempatkan pada layanan awan dikelola dan perjanjian hak ijin akses untuk memitigasi risiko yang terjadi, dan yang terakhir yaitu merencanakan dan mengkaji dokumen SLA (*Service Level Agreement*) berisi kesepakatan formal yang mencakup deskripsi layanan, kelebihan dan kendala layanan, prosedur pelaporan, dan pemantauan kinerja sebelum memilih penyedia layanan infrastuktur awan (*cloud service*).

LAMPIRAN F GAMBAR BUKTI

GUBERNUR JAWA TIMUR

PERATURAN GUBERNUR JAWA TIMUR
NOMOR 80 TAHUN 2016

TENTANG

KEDUDUKAN, SUSUNAN ORGANISASI, URAIAN TUGAS
DAN FUNGSI SERTA TATA KERJA
DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI JAWA TIMUR

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR JAWA TIMUR

Menimbang : bahwa untuk menyiapkan bahan pelaksanaan ketentuan Pasal 5 Peraturan Daerah Provinsi Jawa Timur Nomor 11 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah, perlu menetapkan Peraturan Gubernur tentang Kedudukan, Susunan Organisasi, Uraian Tugas dan Fungsi serta Tata Kerja Dinas Komunikasi dan Informatika Provinsi Jawa Timur dalam Peraturan Gubernur.

Mengingat :

1. Undang-Undang Nomor 2 Tahun 1950 tentang Pembentukan Propinsi Djawa Timur (Himpunan Peraturan-Peraturan Negara Tahun 1950) sebagaimana telah diubah dengan Undang–Undang Nomor 18 Tahun 1950 tentang Perubahan dalam Undang–Undang Nomor 2 Tahun 1950 (Himpunan Peraturan-Peraturan Negara Tahun 1950);
2. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234);
3. Undang-Undang Nomor 5 Tahun 2014 tentang Aparatur Sipil Negara (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 6, Tambahan Lembaran Negara Republik Indonesia Nomor 5494);

4.Undang

Gambar Peraturan Gubernur Jawa Timur no 80 Tahun 2016

Statement of Applicability

DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA TIMUR 2018

Versi	1.0
Status	FINAL
Nomor Dokumen	706 / 1 / 114 / 2018
Klasifikasi	Internal
Pemilik Dokumen	Perwakilan Manajemen

Statement of Applicability

ISO 27001:2013 CONTROLS

Annex	Control	Applicable / Not Applicable	Annex	Control
A.5 Security Policy				
A.5.1 Management Direction for Information Security				
A.5.1.1.	Policies for information security	Yes	DISKOMINFO PEMPROV JAWA TIMUR membuat pedoman umum mengenai keamanan informasi sebagai arahan dalam menjalankan keamanan informasi	Lampiran peraturan terkait SMKI
A.5.1.2.	Review of the policies for information security	Yes	DISKOMINFO PEMPROV JAWA TIMUR melakukan tinjauan periodik untuk memastikan kesesuaian, kecukupan, dan keefektifan kebijakan keamanan informasi	Lampiran peraturan terkait SMKI
A.6 Organization of Information Security				
A.6.1. Internal Organization				
A.6.1.1.	Information security roles and responsibility;	Yes	DISKOMINFO PEMPROV JAWA TIMUR menetapkan peran dan tanggung jawab untuk memastikan setiap orang menyadari tugas mereka	SK Struktur Organisasi SMKI
A.6.1.2.	Segregation of duties;	Yes	DISKOMINFO PEMPROV JAWA TIMUR memastikan dan memisahkan tanggung jawab masing – masing *user* dan mengurangi risiko penyalahgunaan	Kebijakan dan prosedur peningkatan pemahaman kesadaran dan komunikasi SMKI
A.6.1.3.	Contact with authorities;	Yes	DISKOMINFO PEMPROV JAWA TIMUR memiliki dan menjaga kontak dengan pihak terkait jika terjadi gangguan (tanggap darurat)	Kontak seperti, polisi, rumah sakit, pln, dll

Gambar Dokumen SOA ISO27001:2013

PROVINSI JAWA TIMUR

DOKUMEN PELAKSANAAN ANGGARAN

SATUAN KERJA PERANGKAT DAERAH (DPA-SKPD)

TAHUN ANGGARAN 2019

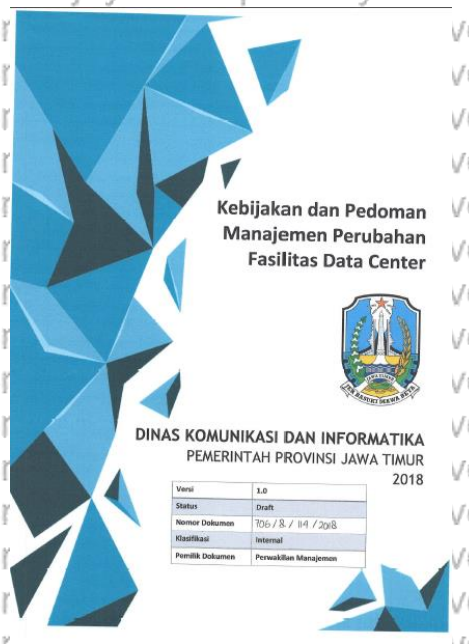
DINAS KOMUNIKASI DAN INFORMATIKA
BIDANG APTIKA

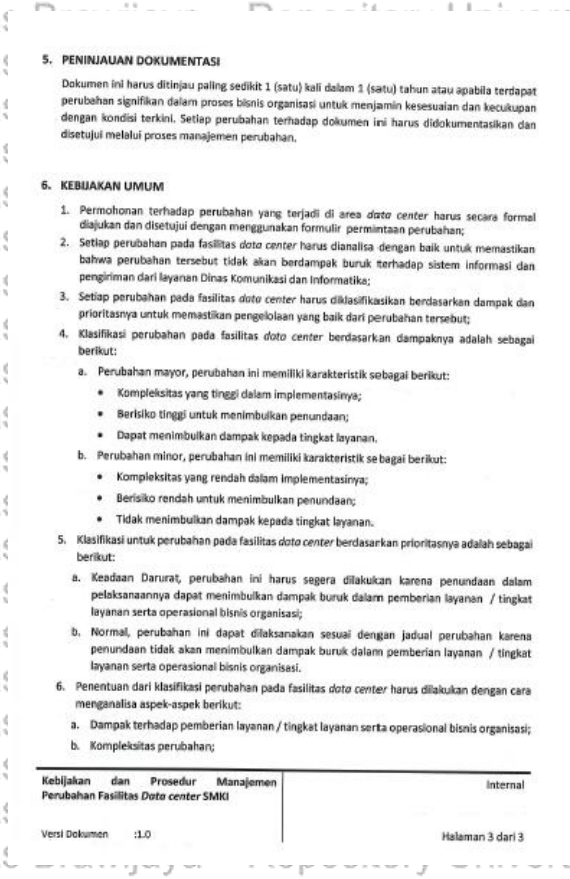
NOMOR DPA Tahun 2019

Peraturan Daerah Provinsi Jawa Timur Nomor 11 Tahun 2018 tentang APBD Tahun Anggaran 2019 (tanggal 28 Desember 2018)
Peraturan Gubernur Jawa Timur Nomor 128 Tahun 2018 tentang Penjabaran APBD Tahun Anggaran 2019 (tanggal 28 Desember 2018)
Keputusan Gubernur Jawa Timur Nomor 903/279/203.2/2018 tentang Penetapan Dokumen Pelaksanaan Anggaran Satuan Kerja Perangkat Daerah (DPA-SKPD) Dinas Komunikasi dan Informatika Provinsi Jawa Timur Tahun Anggaran 2019 (tanggal 31 Desember 2018)

Gambar DPA (Daftar Pelaksanaan Anggaran) Seksi Persandian dan Keamanan Informasi

Gambar Dokumen Kebijakan Keamanan Informasi





5. PENINJAUAN DOKUMENTASI

Dokumen ini harus ditinjau paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau apabila terdapat perubahan signifikan dalam proses bisnis organisasi untuk menjamin kesesuaian dan kecukupan dengan kondisi terkini. Setiap perubahan terhadap dokumen ini harus didokumentasikan dan disetujui melalui proses manajemen perubahan.

6. KEBIJAKAN UMUM

1. Permohonan terhadap perubahan yang terjadi di area *data center* harus secara formal diajukan dan disetujui dengan menggunakan formulir permintaan perubahan;
2. Setiap perubahan pada fasilitas *data center* harus dianalisa dengan baik untuk memastikan bahwa perubahan tersebut tidak akan berdampak buruk terhadap sistem informasi dan pengiriman dari layanan Dinas Komunikasi dan Informatika;
3. Setiap perubahan pada fasilitas *data center* harus diklasifikasikan berdasarkan dampak dan prioritasnya untuk memastikan pengelolaan yang baik dari perubahan tersebut;
4. Klasifikasi perubahan pada fasilitas *data center* berdasarkan dampaknya adalah sebagai berikut:
   a. Perubahan mayor, perubahan ini memiliki karakteristik sebagai berikut:
      - Kompleksitas yang tinggi dalam implementasinya;
      - Berisiko tinggi untuk menimbulkan penundaan;
      - Dapat menimbulkan dampak kepada tingkat layanan.
   b. Perubahan minor, perubahan ini memiliki karakteristik sebagai berikut:
      - Kompleksitas yang rendah dalam implementasinya;
      - Berisiko rendah untuk menimbulkan penundaan;
      - Tidak menimbulkan dampak kepada tingkat layanan.
5. Klasifikasi untuk perubahan pada fasilitas *data center* berdasarkan prioritasnya adalah sebagai berikut:
   a. Keadaan Darurat, perubahan ini harus segera dilakukan karena penundaan dalam pelaksanaannya dapat menimbulkan dampak buruk dalam pemberian layanan / tingkat layanan serta operasional bisnis organisasi;
   b. Normal, perubahan ini dapat dilaksanakan sesuai dengan jadual perubahan karena penundaan tidak akan menimbulkan dampak buruk dalam pemberian layanan / tingkat layanan serta operasional bisnis organisasi.
6. Penentuan dari klasifikasi perubahan pada fasilitas *data center* harus dilakukan dengan cara menganalisa aspek-aspek berikut:
   a. Dampak terhadap pemberian layanan / tingkat layanan serta operasional bisnis organisasi;
   b. Kompleksitas perubahan;

Kebijakan dan Prosedur Manajemen Perubahan Fasilitas *Data center* SMKI	Internal
Versi Dokumen :1.0	Halaman 3 dari 3

Gambar Kebijakan dan Pedoman Manajemen Perubahan Fasilitas DC