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

SKRIPSI

Untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun oleh:
Yusriyah Rahmah
NIM: 165150400111002

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

PENGESAHAN

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

SKRIPSI

Diajukan untuk memenuhi sebagian persyaratan
memperoleh gelar Sarjana Komputer

Disusun Oleh :
Yusriyah Rahmah
NIM: 165150400111002

Skripsi ini telah diuji dan dinyatakan lulus pada
5 Mei 2020
Telah diperiksa dan disetujui oleh:

Dosen Pembimbing I	Dosen Pembimbing II
Widhy Hayuhardhika Nugraha Putra, S.Kom., M.Kom.	Admaja Dwi Herlambang, S.Pd., M.Pd.
NIK: 2017128704092001	NIP: 198908022019031007

Mengetahui
Ketua Jurusan Sistem Informasi

Dr. Eng. Herman Tolle, S.T., M.T.
NIP: 19740823 200012 1 001

PERNYATAAN ORISINALITAS

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

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

Malang, 2 Mei 2020

Yusriyah Rahmah

NIM: 165150400111002

ABSTRAK

Yusriyah Rahmah, Evaluasi Tingkat Keamanan Informasi Pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto dengan Menggunakan Indeks KAMI

Pembimbing: Widhy Hayuhardhika Nugraha Putra, S.Kom., M.Kom. dan Adrnaja Dwi Herlambang S.Pd., M.Pd.

Dinas Komunikasi dan Informatika Kabupaten Mojokerto merupakan instansi pemerintahan yang mengimplementasikan perkembangan teknologi informasi, namun dalam hal memonitor hak akses ilegal belum dilakukan pencatatan atau pendokumentasiannya. Seringkali hanya dilakukan penanganan ketika telah terjadi kebobolan pada sistem, sehingga perlu memperhatikan keamanan informasi untuk mengamankan segala informasi yang dikelola. Tujuan penelitian ini adalah untuk mengetahui sejauh mana tingkat keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto dengan menggunakan Indeks KAMI versi 3.1 sesuai dengan standar penerapan ISO/IEC 27001:2013. Hasil evaluasi keamanan informasi pada tingkat kelengkapan sebesar 109 dan tingkat kematangan setiap area keamanan informasi berada pada level I hingga level I+. Hal tersebut menunjukkan bahwa keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto masih perlu ditingkatkan. Terdapat tiga belas rekomendasi pada area tata kelola keamanan informasi, delapan rekomendasi pada area pengelolaan risiko keamanan informasi, lima belas rekomendasi pada area kerangka kerja pengelolaan keamanan informasi, dua puluh empat rekomendasi pada area pengelolaan aset informasi, dan empat belas rekomendasi pada area teknologi dan keamanan informasi. Salah satu rekomendasi perbaikan yakni dengan membuat kebijakan dan prosedur organisasi mengenai keamanan sistem menggunakan kerangka kerja ITIL versi 4 praktik IT asset management.

Kata kunci: Evaluasi, Indeks, Keamanan, Informasi, SNI/ISO 27001:2013

ABSTRACT

Yusriyah Rahmah, Evaluasi Tingkat Keamanan Informasi Pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto dengan Menggunakan Indeks KAMI

Supervisors: Widhy Hayuhardhika Nugraha Putra, S.Kom., M.Kom. and Admaja Dwi Herlambang S.Pd., M.Pd.

Dinas Komunikasi dan Informatika Kabupaten Mojokerto is a government agency that implements the development of information technology, but in the case of monitoring illegal access rights no record or documentation has been made. It is only handled when there has been a breakdown in the system, they have to pay concern about the safety of government information. In this research we try to measure information security management at Dinas Komunikasi dan Informatika Kabupaten Mojokerto using KAMI Index version 3.1 according to the standard of ISO / IEC 27001:2013. The evaluation result of information security completeness level is 109 and maturity level of each area of information security at the level I to level I +. It shows that information security at Dinas Komunikasi dan Informatika Kabupaten Mojokerto need to be improved. There are thirteen recommendations in the areas of information security governance, eight recommendations on the area of information security risk management, fifteen recommenaations on areas of information security management framework, twenty four recommendations on the asset management area information, and the fourteen recommendations in the area of technology and information security. One of the recommendations for improvements by create organizational policies and procedures regarding information security using ITIL framework version 4 IT asset management practices.

Keywords: Evaluation, Index, Security, Information, ISO/IEC 27001:2013

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB 1 PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi (TI) saat ini terus berkembang, banyak organisasi yang mengembangkan teknologi informasi untuk memudahkan menghasilkan dan memperoleh data dan informasi. Menurut Purnama (2016), teknologi informasi merupakan suatu kebutuhan yang dapat membantu kinerja suatu organisasi atau individu. Teknologi informasi pula sebagai seperangkat alat untuk melakukan tugas pemrosesan informasi (Fatmah, 2020). Data dan informasi yang dihasilkan oleh suatu organisasi merupakan aset yang sangat berharga. Sebagaimana yang dikemukakan Saputra (2018), bahwa data dan informasi merupakan sesuatu yang sangat berharga sebab diperlukan banyak sumber daya untuk menghasilkannya. Data serta informasi pada sebuah organisasi biasanya merupakan sebuah produk yang memiliki nilai jual dan dapat mempengaruhi reputasi organisasi.

Instansi pemerintahan di Indonesia mulai mengimplementasikan perkembangan teknologi informasi sebagai alat bantu untuk mengerjakan tugas dan memberikan layanan kepada masyarakat. Instruksi Presiden Nomor 3 tahun 2003 tentang Kebijaksanaan dan Strategi Nasional Pengembangan E-Government, menjadi salah satu inspirasi pengembangan layanan publik berbasis pemerintahan elektronik di seluruh Indonesia. Berdasarkan kebijakan untuk mengimplementasikan layanan e-government di lingkungan pemerintahan, layanan ini dipercaya mampu memberikan banyak keuntungan, baik dari sisi peningkatan layanan publik maupun dalam meningkatkan kualitas kinerja di lingkungan pemerintahan. Purnama (2016) juga mengemukan bahwa penggunaan teknologi informasi merupakan komponen vital dari kinerja bisnis

Selain penerapan layanan teknologi informasi, suatu organisasi perlu memperhatikan sisi keamanan informasinya agar terhindar dari adanya pencurian data dan hilangnya data yang tidak untuk dipublikasikan secara sengaja maupun tidak sengaja, serta agar tidak bisa diakses dan dicuri oleh orang yang tidak berhak. Berdasarkan peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi, dijelaskan bahwa setiap penyelenggaraan sistem elektronik harus melakukan keamanan terhadap informasi dalam kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara atau pertahanan dan keamanan negara. Maka dari itu, Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Mojokerto selaku organisasi perangkat daerah perlu menerapkan dan memperhatikan keamanan informasi untuk mengamankan segala informasi yang dikelolanya.

Berdasarkan hasil wawancara yang telah dilakukan peneliti pada Lampiran A, narasumber menjelaskan bahwa dalam hal memonitor hak akses ilegal pada web mojokertokab.go.id belum dilakukan pencatatan atau pendokumentasinya,

hanya penanganan ketika telah terjadi kebobolan pada sistem. Hak akses ilegal berupa perubahan tampilan pada web Diskominfo Kabupaten Mojokerto dan mempengaruhi keamanan segala informasi yang dikelola. Sedangkan untuk mengatur semua prosedur pengelolaan keamanan sistem, belum terdapat *Standart Operational Procedure* (SOP) pada Diskominfo Kabupaten Mojokerto. Maka dari permasalahan tersebut diperlukan adanya sebuah evaluasi keamanan informasi pada Diskominfo Kabupaten Mojokerto.

Pada artikel yang diterbitkan oleh Badan Siber dan Sandi Negara (BSSN), tertulis bahwa BSSN mengadakan pelatihan yang bertujuan agar terlaksananya penerapan Sistem Manajemen Keamanan Informasi berbasis Indeks KAMI dan mendorong dilakukannya penilaian mandiri atau *self assessment* sebagai bahan pemetaan awal tentang kondisi keamanan informasi pemerintah daerah. Pada Rencana Strategi Diskominfo Kabupaten Mojokerto tahun 2016-2021 juga terdapat program kerja mengenai audit keamanan informasi, oleh karena itu penelitian ini dapat berguna untuk mendukung kebijakan evaluasi keamanan informasi dengan melakukan penilaian mandiri sebelum adanya visitasi auditor resmi. Selain itu, evaluasi diperlukan untuk mengamati kesiapan hal – hal yang telah dilakukan organisasi dalam melakukan tindakan pengamanan informasi.

Evaluasi tingkat keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto akan dilakukan dengan menggunakan Indeks KAMI versi 3.1. Indeks KAMI versi 3.1 merupakan suatu aplikasi untuk mengevaluasi tingkat kematangan, tingkat kelengkapan penerapan standar ISO/IEC 27001, dan peta area tata kelola keamanan sistem informasi pada suatu instansi pemerintah. Evaluasi menggunakan Indeks KAMI versi 3.1 terdiri dari 5 (lima) area keamanan informasi, yakni tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja pengelolaan keamanan informasi, pengelolaan aset informasi, dan teknologi dan keamanan informasi. Dalam perkembangannya, evaluasi pengelolaan keamanan informasi bagi penyelenggara pelayanan didasarkan pada Panduan Penerapan Tata Kelola Keamanan Informasi Tahun 2011 dengan alat evaluasi berupa penggunaan Indeks Keamanan Informasi (KAMI) (Siga, 2014).

Penelitian sebelumnya tentang evaluasi manajemen keamanan informasi menggunakan Indeks KAMI berdasarkan ISO/IEC 27001:2013 pernah dilakukan pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya. Hasil yang didapatkan dari evaluasi menggunakan lima area Indeks KAMI menunjukkan tingkat ketergantungan sebesar 26 dan mendapatkan nilai sebesar 249 dari 645. Dari hasil evaluasi DPTSI ITS Surabaya tersebut berada pada kategori belum layak dan akan diberikan rekomendasi berdasarkan kontrol ISO 27001:2013 pada bagian yang dinilai kurang.

Berdasarkan penjabaran diatas, kegiatan evaluasi perlu dilakukan pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto untuk menilai keamanan informasinya. Tujuan diadakannya penelitian ini adalah untuk menilai pengelolaan keamanan informasi, mengetahui tingkat kematangan, dan

menyusun rekomendasi berdasarkan hasil analisis pengelolaan keamanan informasi pada Diskominfo Kabupaten Mojokerto menggunakan standar ISO 27001.

1.2 Rumusan Masalah

Berdasarkan pada penjelasan latar belakang di atas, maka ditentukan beberapa rumusan masalah pada penelitian ini diantaranya:

1. Bagaimana hasil tingkat keamanan informasi Dinas Komunikasi dan Informatika Kabupaten Mojokerto dengan menggunakan Indeks KAMI versi 3.1?
2. Bagaimana rekomendasi untuk meningkatkan keamanan informasi pada Dinas Komunikasi dan Informasi Kabupaten Mojokerto berdasarkan Indeks KAMI versi 3.1?

1.3 Tujuan

Berdasarkan pada penjelasan latar belakang dan rumusan masalah di atas, maka ditentukan beberapa tujuan pada penelitian ini diantaranya:

1. Mengetahui sejauh mana tingkat keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto dari hasil evaluasi menggunakan Indeks KAMI versi 3.1.
2. Memberikan rekomendasi berdasarkan hasil evaluasi untuk meningkatkan keamanan informasi pada Dinas Komunikasi dan informasi Kabupaten Mojokerto.

1.4 Manfaat

Berdasarkan pada penjelasan latar belakang di atas, maka ditentukan beberapa manfaat pada penelitian ini diantaranya:

1. Dapat mengetahui tingkat keamanan informasi pada Dinas Komunikasi dan Informasi Kabupaten Mojokerto.
2. Dapat memberikan hasil rekomendasi terkait pengelolaan keamanan informasi untuk meningkatkan keamanan informasi pada Dinas Komunikasi dan Informasi Kabupaten Mojokerto.

1.5 Batasan Masalah

Berdasarkan pada penjelasan latar belakang di atas, maka ditentukan beberapa batasan masalah pada penelitian ini diantaranya:

1. Penilaian tingkat keamanan informasi dilakukan menggunakan Indeks KAMI dengan 5 area, yaitu tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, serta teknologi dan keamanan informasi.

2. Pemberian rekomendasi untuk hasil evaluasi sesuai dengan standar ISO 27001:2013.

1.6 Sistematika Pembahasan

Sistematika yang diterapkan dalam penelitian ini adalah:

BAB I Pendahuluan

Dalam bab ini berisi latar belakang, rumusan masalah, tujuan, manfaat, batasan masalah, dan sistematika penulisan

BAB II Tinjauan Pustaka

Bab ini berisi penjelasan mengenai referensi pendukung dan mengenai konsep yang diangkat dalam penelitian

BAB III Metode Penelitian

Bab ini membahas langkah – langkah yang dilakukan melakukan penelitian

BAB IV Pengumpulan dan Pengolahan Data

Membahas penyajian data

BAB V Analisis Hasil

Berisi analisa hasil penelitian

BAB VI Penutupan

Pada bab ini berisi kesimpulan dan saran penulis yang diperoleh dari proses penelitian yang dilakukan

BAB 2 LANDASAN KEPUSTAKAAN

2.1 Penelitian Terdahulu

Penelitian ini merupakan pengembangan dari beberapa penelitian sebelumnya, penulis melakukan kajian pustaka dari penelitian – penelitian sebelumnya dengan topik evaluasi yang sama sebagai referensi pada penelitian, yakni topik evaluasi keamanan informasi. Metode yang digunakan pada penelitian ini adalah Indeks KAMI, sehingga penelitian ini juga memperoleh teori dalam proses penyelesaian. Terdapat beberapa penelitian sebagai literatur yang berisikan teori – teori yang sesuai dan mendukung penelitian ini. Penulis mengambil referensi penelitian dari jurnal – jurnal lokal dan internasional yang relevan dan dapat mendukung dalam menyelesaikan penelitian yang dilakukan.

Penelitian sebelumnya dilakukan oleh Siga, dkk (2014) mahasiswa Institut TekNologi Sepuluh November pada objek Kantor Wilayah Ditjen Perbendaharaan Negara Jawa Timur untuk mengevaluasi kebijakan dan standar manajemen keamanan informasi (SMKI). Hasil evaluasi dijadikan sebagai acuan untuk melindungi informasi pada Kementerian Keuangan dari berbagai macam ancaman. Hasil penelitian digunakan menghasilkan penilaian, mengetahui tingkat kematangan, dan mendapatkan rekomendasi dari hasil analisis terkait pengelolaan keamanan informasi. Berdasarkan hasil analisisnya, dapat disimpulkan bahwa status kesiapan pengelolaan keamanan informasi yang mencakup 5 area keamanan dinilai masih perlu adanya perbaikan, dengan skor 337 dari nilai maksimal 588.

Selanjutnya pada tahun 2014 pula, penelitian dilakukan oleh Putra, dkk dengan menggunakan Indeks Keamanan Informasi (KAMI) pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk (Telkom). Telkom merupakan perusahaan milik negara yang bergerak dalam bidang penyedia layanan komunikasi di Indonesia. Karena bergerak di bidang komunikasi, diperlukan banyak jaringan yang terhubung dengan kantor pusat Telkom, hal tersebut berdampak munculnya risiko keamanan informasi yang dapat mengancam operasionalnya. Hasil dari penelitian tersebut, Telkom masuk dalam kategori kritis ketergantungan dengan nilai 44 dari total keseluruhan 48, sedangkan analisis dengan kelima area Indeks KAMI mendapatkan nilai sebesar 582 dari 588. Dari hasil tersebut Telkom sudah termasuk kategori optimal dan akan diberikan saran perbaikan pada bagian – bagian yang masih kurang.

Berdasarkan penelitian terdahulu yang membahas tentang keamanan informasi pada suatu instansi atau organisasi, proses evaluasi yang dilakukan menggunakan Indeks KAMI dan hasil pengukuran dari penelitian digunakan sebagai saran perbaikan. Berdasarkan penelitian yang sudah dilakukan tersebut, maka dalam penelitian evaluasi ini juga memilih untuk melakukan evaluasi keamanan informasi pada sebuah instansi dengan menggunakan Indeks KAMI.

Hasil pengukuran pada penelitian ini juga digunakan sebagai saran atau referensi untuk meningkatkan tingkat keamanan informasi.

2.2 Landasan Teori

2.2.1 Evaluasi

Menurut Kamus Besar Bahasa Indonesia (KBBI), evaluasi adalah upaya penilaian secara teknis dan ekonomis terhadap suatu cebakan bahan galian untuk kemungkinan pelaksanaan penambangannya. Menurut Cronholm & Goldkuhl (2003) terdapat tiga strategi untuk mengevaluasi sistem informasi, yaitu *goal-based evaluation*, *goal-free evaluation*, dan *criteria-based evaluation*.

Goal-based evaluation, evaluasi ini berdasarkan suatu tujuan yakni sebagai pengukuran sejauh mana suatu program telah mencapai tujuan yang jelas dan spesifik. Pendekatan strategi ini termasuk dalam kategori deduktif. Untuk melakukan evaluasi diperlukan evaluator yang menguasai tujuan organisasi tersebut dan dapat menggunakan pendekatan kuantitatif maupun kualitatif.

Goal-free evaluation atau yang dimaksud evaluasi bebas dari tujuan merupakan pendekatan yang bersifat interpretative. Evaluasi interpretatif bertujuan untuk mendapatkan pemahaman yang lebih mendalam mengenai sifat apa yang akan dievaluasi dan memahami keadaan atau pengaruh yang ditimbulkan organisasi yang akan dievaluasi. Hasil dari pendekatan ini membutuhkan penafsiran yang lebih dalam secara kualitatif. Pendekatan strategi ini termasuk dalam kategori penelitian induktif, yakni mendeskripsikan dan menyimpulkan keadaan atau menemukan permasalahan berdasarkan hasil pengamatan yang dilakukan selama kegiatan evaluasi dan bersifat bebas.

Criteria-based evaluation, pendekatan berdasarkan kriteria ini merupakan evaluasi yang tidak berdasarkan konteks organisasi tertentu namun pada teori atau perspektif tertentu. Ada beberapa pendekatan berdasarkan kriteria misalnya heuristic, *checklist*, atau prinsip tertentu. Pada pendekatan ini, evaluator perlu menguasai kriteria atau standar yang menjadi tolok-ukur kegiatan evaluasi.

Cronholm & Goldkuhl (2003) mengemukakan bahwa terdapat dua aspek dalam melakukan evaluasi pada sistem informasi, yakni *IS – As Such* dan *IS – In Use*. *IS – As Such* merupakan evaluasi tanpa melibatkan pengguna atau *user*, sedangkan mengevaluasi sistem informasi dengan melibatkan pengguna (*user*) adalah *IS – In Use*. Adapun tahap evaluasi menurut Cronholm & Goldkuhl dibagi menjadi tiga tahap, yakni *Plan the evaluation*, *evaluate according to chosen evaluation type or a combination of*, dan *draw conclusions*.

2.2.2 Teknik Pengambilan Sampel

Teknik sampling atau teknik pengambilan sampel digunakan untuk menentukan sampel yang akan digunakan untuk penelitian. Ada berbagai macam teknik sampling yang dapat digunakan sesuai kebutuhan penelitian. Menurut Sugiyono (2017), teknik sampling dibagi menjadi dua kategori yakni *Probability Sampling* dan *Nonprobability Sampling*. Berikut merupakan macam – macamnya:

- *Probabilility Sampling*

  Probabilility Sampling adalah teknik pengambilan sampel dengan memberikan peluang yang sama pada setiap populasi yang akan dipilih menjadi sampel. Teknik *Probabilility Sampling* dibagi menjadi empat yakni sebagai berikut:

  1. *Simple Random Sampling*

     Teknik pengambilan sampel ini dilakukan secara acak tanpa memperhatikan tingkatan pada populasi dengan menganggap seluruh populasinya homogen.

  2. *Proportionate Stratified Random Sampling*

     Teknik ini digunakan bila populasi memiliki strata (tingkatan), seningga sampel yang diambil meliputi setiap tingkatan yang ada pada populasi secara proporsional.

  3. *Disproportionate Stratified Random Sampling*

     Pengambilan sampel dengan menggunakan teknik ini apabila populasi memiliki strata namun kurang proporsional.

  4. *Area Sampling (Cluster Sampling)*

     Teknik sampling daerah digunakan untuk menentukan sampel apabila sumber data sangat luas, maka pengambilan sampel berdasarkan daerah atau *cluster* populasi yang telah ditetapkan.

- *Nonprobalility Sampling*

  Nonprobalility Sampling adalah teknik pengambilan sampel yang tidak memberi peluang atau kesempatan sama bagi setiap populasi untuk dipilih menjadi sampel.

  1. *Sampling Sistematis*

     Sampling Sistematis merupakan teknik pengambilan sampel berdasarkan urutan dari anggota populasi yang diberi nomor urut. Misal populasi diberi angka urut hingga 10, maka pengambilan sampel dapat dilakukan dengan mengambil angka ganjil saja, genap saja, atau kelipatan tertentu

2. *Sampling Kuota*

Teknik pengumpulan sampel ini untuk menentukan sampel dari populasi yang mempunyai ciri – ciri tertentu sampai mencapai jumlah atau kuota tertentu.

3. *Sampling Incidental*

Teknik penentuan sampel insidental berdasarkan kebetulan, yakni siapa saja yang secara kebetulan bertemu dengan peneliti dan dianggap cocok sebagai sumber data.

4. *Purposive Sampling*

Teknik purposive sampling adalah teknik pengambilan sampel sumber data dengan pertimbangan tertentu. Teknik ini diartikan sebagai pemilihan sampel yang dilakukan berdasarkan tujuan – tujuan tertentu. Misalnya, responden dianggap sebagai orang yang paling tahu tentang tujuan tertentu atau apa yang peneliti harapkan, dan responden tersebut yang akan memudahkan peneliti menelusuri apa yang diteliti.

5. *Sampling Jenuh*

Teknik ini digunakan bila semua populasi digunakan sebagai sampel. Pengambilan sampel ini sering dilakukan apabila jumlah populasi relatif kecil. Istilah lain jenuh adalah sensus, yang mana semua populasi dijadikan sampel

6. *Snowball Sampling*

Snowball sampling adalah teknik penentuan sampel yang awalnya jumlahnya kecil, kemudian membesar. Dalam penentuan sampel ini, pertama – tama dipilih satu orang atau beberapa, kemudian belum dirasa cukup sumber datanya, maka peneliti mencari orang lain.

Teknik pengambilan sampel yang digunakan pada penelitian ini adalah teknik purposive sampling. Pemilihan sampel dengan menggunakan teknik purposive sampling dikarenakan tidak semua sampel memiliki kriteria – kriteria yang sesuai dengan yang ditentukan oleh peneliti. Teknik ini termasuk teknik sampling yang tidak memberikan peluang yang sama pada calon responden untuk dijadikan sampel. Adapun kriteria – kriteria yang dijadikan sebagai sampel penelitian didapatkan dari tujuan atau topik tertentu yang sesuai dengan tema penelitian. Dengan menetapkankan kriteria yang sesuai dengan tujuan penelitian, sehingga dinarapkan dapat menjawab permasalahan dan informasi yang dibutuhkan peneliti.

2.2.3 Keamanan Informasi

Pengertian keamanan informasi menurut Putra, dkk (2014) adalah upaya pengamanan aset informasi dari ancaman yang tidak terduga dan upaya meminimalisir munculnya risiko yang tidak diinginkan. Semakin banyak informasi

yang disimpan pada suatu organisasi maka akan semakin banyak juga risiko yang mungkin terjadi, seperti kerusakan, kehilangan, atau tersebarnya informasi pribadi kepada pihak yang tidak bertanggungjawab. Terdapat lima layanan jaminan keamanan, diantaranya adalah sebagai berikut:

1. *Confidentiality*

   Memastikan bahwa informasi hanya bisa diakses oleh pihak yang berwenang.
2. *Authenticity*

   Menjamin keaslian suatu informasi
3. *Integrity*

   Memastikan bahwa suatu informasi lengkap, tepat, serta sesuai.
4. *Availability*

   Memastikan bahwa informasi dapat diakses oleh orang yang berwenang dan data tersedia ketika dibutuhkan tanpa ada keterlambatan waktu
5. *Non-repudiation*

   Menjamin pihak lain tidak dapat merubah keaslian tanda tangan digital pada suatu dokumen atau jaringan tertentu.

Terdapat pendapat dari Ichsan (2013) bahwa *IT Security* atau keamanan teknologi informasi merupakan bentuk pengamanan pada infrastruktur suatu organisasi dari gangguan berupa jaringan yang tidak diinginkan dan akses tak berwenang atau terlarang, sedangkan keamanan informasi merupakan bentuk pengamanan terhadap data – data dan informasi suatu organisasi.

2.2.4 Dinas Komunikasi dan Informatika Kabupaten Mojokerto

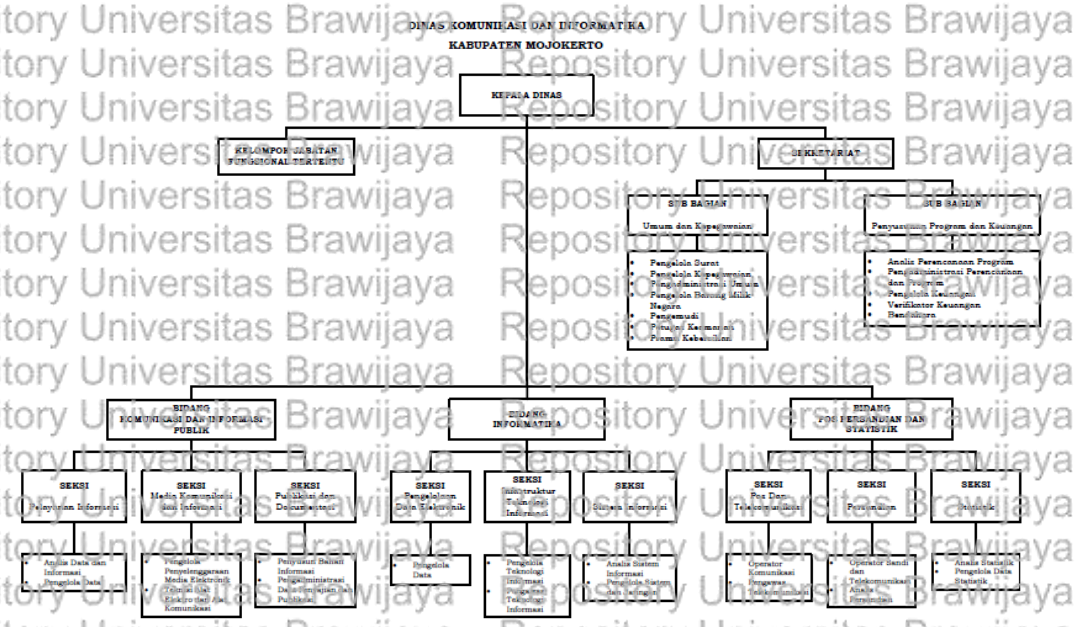
Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Mojokerto merupakan Organisasi Perangkat Daerah (OPD) di wilayah pemerintahan Kabupaten Mojokerto Provinsi Jawa Timur yang didirikan pada awal tahun 2017 dan memiliki tupoksi pada bidang teknologi. Dinas Komunikasi dan Informatika adalah bagian pelaksana kepentingan pemerintahan di wilayah daerah yang berwenang pada bidang komunikasi dan informatika, bidang statistik, dan persandian. Diskominfo Kabupaten Mojokerto memiliki visi terwujudnya masyarakat kabupaten mojokerto yang mandiri, sejahtera dan bermartabat melalui penguatan dan pengembangan basis perekonomian, pendidikan, serta kesehatan.

Tugas dan fungsi Diskominfo Mojokerto tertulis dalam peraturan bupati mojokerto (Perbup) No. 69 Tahun 2016 tentang kedudukan, susunan organisasi, tugas, dan fungsi serta tata kerja Diskominfo mojokerto. Diskominfo Kabupaten Mojokerto memiliki wewenang untuk merumuskan kebijakan, melakukan evaluasi, dan melaksanakan administrasi pada bidang komunikasi dan

informatika, statistik, dan persandian, serta menjalankan tugas dan fungsi lainnya yang diberikan oleh bupati.

Selain itu, Diskominfo Kabupaten Mojokerto juga berwenang dalam membantu Kepala Dinas dalam melaksanakan sebagian tugas meliputi pelayanan informasi, media komunikasi, dan informasi, serta publikasi dan dokumentasi pada bidang komunikasi dan informasi publik. Pada bidang informatika, memiliki tugas dalam pengelolaan data elektronik, infrastruktur teknologi informasi, dan sistem informasi. Sedangkan pada bidang pos, persandian, dan statistik mempunyai tugas terkait pos dan telekomunikasi, persandian, serta statistik.

Berikut adalah struktur organisasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto:



Gambar 2.1 Struktur organisasi Dinas Komunikasi dan Informatika Kabupaten Mojokerto

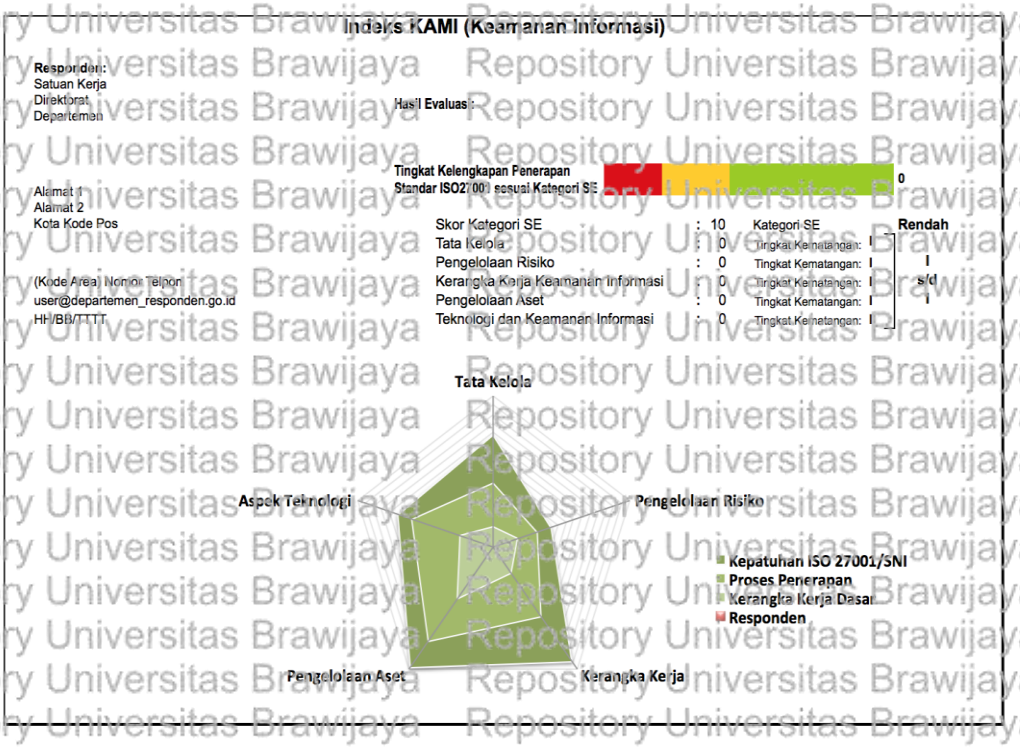
Sumber: diskominfo.mojokertokab.go.id

2.2.5 Indeks KAMI

Indeks Keamanan Informasi atau yang sering disebut Indeks KAMI merupakan alat evaluasi yang digunakan untuk menganalisis tingkat kesiapan keamanan informasi pada suatu instansi pemerintahan. Indeks KAMI tidak digunakan untuk menganalisis keefektifan atau kelayakan suatu pengamanan yang telah diterapkan, melainkan sebagai perangkat yang menghasilkan analisis kesiapan terkait kondisi kematangan dan kelengkapan kerangka kerja keamanan informasi yang diberikan kepada pimpinan instansi. Evaluasi ini dilakukan pada berbagai area yang ditentukan sebagai target penerapan keamanan informasi dengan pembahasan sesuai aspek keamanan pada standar ISO/IEC 27001.

Dasar hukum untuk memiliki dan menerapkan SMKI khususnya indeks KAMI lebih ditekankan kembali bagi pelayanan publik, sebagaimana yang tercantum pada Peraturan Menteri Komunikasi dan Informatika (Permenkominfo) Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (SMPI). Adapun dalam Permenkominfo Nomor 7 Tahun 2018, setiap Penyelenggara Sistem Elektronik (PSE) harus terdaftar di Kominfo. Persyaratan dalam pendaftaran tersebut yaitu PSE harus memiliki sertifikat keamanan informasi. Sertifikat keamanan informasi dapat berupa sertifikat Indeks KAMI maupun sertifikat ISO27001.

Evaluasi pada keamanan informasi berdasarkan Indeks KAMI memiliki dua bagian, yaitu bagian kategori sistem elektronik dan bagian keamanan informasi. Bagian kategori sistem elektronik adalah gambaran umum terkait keadaan sistem elektronik sebagai pendukung proses kerja. Sedangkan bagian keamanan informasi memiliki lima area, yaitu tata kelola keamanan informasi, kerangka kerja keamanan informasi, pengelolaan risiko keamanan informasi, pengelolaan aset informasi, dan teknologi dan keamanan informasi. Hasil dari proses evaluasi Indeks KAMI dapat berupa seperti Gambar 2.2.



Gambar 2.2 Tampilan Hasil Evaluasi Indeks KAMI

Sumber: Pengantar Indeks KAMI Versi 3.1 (2015)

Tercantum pada Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik (2011) bahwa penilaian Indeks KAMI didasarkan dari persyaratan keamanan yang terdapat pada ISO/IEC 27001 dan tersusun ke dalam lima area Indeks KAMI sebagai berikut:

1. Tata Kelola Keamanan Informasi

   Area ini mengevaluasi kesiapan tata kelola keamanan informasi terkait tugas, fungsi, dan tanggungjawab pengelola keamanan informasi.

2. Pengelolaan Risiko Keamanan Informasi

   Area ini mengevaluasi kesiapan pengelolaan risiko sebagai dasar penerapan strategi keamanan informasi.

3. Kerangka Kerja Keamanan Informasi

   Area ini mengevaluasi kesiapan serta kelengkapan kerangka kerja termasuk prosedur dan kebijakan pengelolaan keamanan informasi dan strategi penerapannya.

4. Pengelolaan Aset Informasi

   Area ini mengevaluasi kelengkapan pengamanan pada aset informasi termasuk penggunaannya.

5. Teknologi dan Keamanan Informasi

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

2.2.5.1 Tata Kelola

Dalam rangka menciptakan nilai tambah dan meminimalkan risiko Teknologi Informasi (TI) dibutuhkan manajemen pengelolaan semua sumber daya TI yang efisien dan efektif, antara lain melalui IT Governance (Tata Kelola TI). Sesuai dengan tujuan pengembangan *e-government* di Indonesia berdasarkan Inpres No. 3 Tahun 2003, adalah untuk mengembangkan penyelenggaraan kepemerintahan yang berbasis elektronik dalam rangka meningkatkan kualitas layanan publik secara efektif dan efisien. Usaha dalam memanfaatkan TI akan berjalan seperti yang diharapkan tentunya diperlukan tata kelola TI yang baik. Keberhasilan IT *Governance* (tata kelola TI) sangat ditentukan oleh keselarasan penerapan TI dan tujuan organisasi.

Seluruh instansi pemerintahan di departemen tingkat pusat, provinsi, dan kabupaten/kota dibekali panduan tata kelola TIK Nasional melalui Peraturan Menteri Komunikasi dan Informatika No. 41/PER/MEN.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional. Kemudian diikuti dengan munculnya Panduan Penerapan Tata Kelola Keamanan informasi Bagi Penyelenggara Pelayanan Publik Tahun 2011 yang disusun oleh Tim Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika RI. Hal tersebut diterapkan dalam rangka penyelenggaraan pelayanan publik memerlukan *good governance* yang akan menjamin transparansi, akuntabilitas, efisiensi, dan efektivitas penyelenggaraan pemerintahan.

Dalam konsep tata kelola keamanan informasi, organisasi bertanggungjawab mengelola secara keseluruhan berjalannya keamanan informasi pada organisasi. Menurut Lenawati (2016), tata kelola keamanan informasi didefinisikan sebagai sistem yang mengarahkan dan mengatur aktivitas keamanan informasi di sebuah organisasi. Hasil utama dari tata kelola keamanan informasi meliputi keselarasan strategi keamanan informasi dengan strategi bisnis untuk mendukung tujuan organisasi, manajemen risiko dengan menjalankan langkah yang tepat untuk mengelola dan mengurangi risiko serta dampak potensial terhadap sumber daya informasi, pengelolaan sumber daya dengan memanfaatkan pengetahuan keamanan informasi dan infrastruktur efisien dan efektif, serta pengukuran kinerja dengan memantau dan melaporkan tata kelola keamanan informasi untuk memastikan tujuan organisasi tercapai.

2.2.5.2 Pengelolaan Risiko

Pengelolaan risiko melalui tahapan identifikasi risiko, penilaian risiko, dan pemecahan masalah. Risiko sendiri dapat muncul apabila *Vulnerability* atau kelemahan berbanding lurus dengan *Threat* atau ancaman. Dimana suatu kelemahan seperti celah keamanan terjangkit atau terancam suatu virus, maka akan memunculkan suatu risiko yang dapat mengnambat atau merusak teknologi informasi. Maka dari itu proses pengelolaan manajemen risiko diawali dengan penilaian risiko sebagai pembobotan, kemudian mitigasi risiko sebagai eksekusi nilai tertinggi, dan diakhiri dengan evaluasi risiko untuk membandingkan rencana mitigasi risiko.

Penilaian risiko dapat dilakukan dengan sembilan langkah mensitasi dari buku *risk management guide for information technology systems* yang disusun oleh Stoneburner, dkk (2002) yaitu pertama, Karakteristik Sistem sebagai pengetahuan ruang lingkup permasalahan. Kedua, mengidentifikasi ancaman (*threat*) untuk menelusuri sumber ancaman yang bisa masuk secara *exploid* (sengaja) maupun *triggered* (tidak sengaja). Langkah ketiga yakni mengidentifikasi kelemahan, meliputi kelemahan pada prosedur keamanan, perancangan, implementasi, ataupun pengendalian internal. Kemudian menentukan pengendalian, yakni mencari solusi mengendalikan tanpa harus membenahi kelemahan. Langkah kelima, menentukan tingkat potensi terjadinya risiko (*likelihood*). Setelah itu menganalisis dampak, pengaruh yang terjadi apabila risiko terjadi. Kemudian memilih risiko, menentukan level atau tingkat risiko dalam waktu dekat. Memilih cara pengendalian dengan mengkonfirmasi pengendalian atau rekomendasi. Terakhir yakni menyusun dokumen pengendalian risiko.

Setelah melakukan aktivitas pengidentifikasian risiko meliputi aktivitas identifikasi informasi, identifikasi ancaman dan kelemahan, analisa dampak bisnis, serta penilaian risiko (*risk assessment*), kemudian dilakukan mitigasi risiko. Proses mitigasi risiko yaitu upaya dalam menilai kontrol keamanan yang secara efektif dan efisien dapat menurunkan risiko teknologi informasi yang berpotensi

terjadi. Pada analisis kontrol keamanan akan dilakukan pengidentifikasian, perhitungan nilai prioritas, dan penentuan tingkatan prioritas investasi. Rencana mitigasi tersebut akan dibandingkan dengan evaluasi risiko.

2.2.5.3 Kerangka Kerja

Dalam pengelolaan keamanan informasi, organisasi sebaiknya memiliki kebijakan dan program kerja terkait keamanan informasi. Penerapan kerangka kerja keamanan informasi meliputi *Disaster Recovery Plan* (DRP), *Business Continuity Plan* (BCP), dan *Secure Software Development Life Cycle* (*Secure* SDLC). DRP merupakan rencana pemulihan bencana pada layanan TIK, sedangkan BCP merupakan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK. *Secure* SDLC merupakan proses pengembangan sistem yang aman.

Menurut Putri (2008) *Disaster Recovery Plan* adalah pedoman yang berisi prosedur penanganan hilangnya sumber daya sistem informasi milik organisasi yang disebabkan terjadinya bencana, penyedia operasi cadangan sementara sebagai pengganti sistem utama, pengelolaan proses pemulihan, serta penyelamatan data untuk mengurangi kerugian yang menimpa organisasi. Keuntungan diadakannya DRP yang dipaparkan oleh Yuliad (2016) diantaranya dapat mengurangi kemungkinan terjadinya kerugian secara ekonomi yang disebabkan terjadinya bencana, meningkatkan kestabilan organisasi, merencanakan pemulihan yang teratur dan terukur, menghindari terjadinya ketergantungan terpusat, serta melindungi organisasi termasuk keselamatan personil di dalamnya.

Business Continuity Plan terkait pembuatan rencana atau *framework* sebagai acuan agar proses bisnis terus berjalan meski dalam keadaan bahaya. Berdasarkan penjabaran Solehudin (2005), BCP adalah proses untuk mengurangi ancaman terhadap fungsi organisasi secara otomatis atau manual untuk menjamin kelanjutan layananan operasi yang penting. *Business Continuity Plan* adalah strategi untuk mengurangi efek dari gangguan dan mengupayakan berjalannya kembali proses bisnis suatu organisasi. BRP bermanfaat untuk mengurangi risiko kerugian keuangan dan meningkatkan kemampuan perusahaan untuk memulihkan diri dari bencana atau gangguan secepat mungkin.

2.2.5.4 Pengelolaan Aset

Mensitasi dari *CISA Review Manual 2010 Table of Contents Chapter 5: Protection of Information Assets*, *Information Asset Protection* memiliki 5 aspek, yakni.

1. *Security Managemet*

   Faktor penting dalam melindungi aset informasi dan privasi adalah dengan mendasari manajemen keamanan informasi secara efektif. Tujuan *security management* untuk memenuhi persyaratan bisnis organisasi yakni dengan

memastikan ketersediaan sistem informasi secara berkelanjutan, memastikan integritas informasi yang disimpan, mempertahankan kerahasiaan data sensitif, memastikan kesesuaian dengan hukum, peraturan, dan standar yang berlaku, memastikan kepatuhan terhadap kepercayaan dan kewajiban terkait informasi, serta menjaga kerahasiaan data sensitif.

2. *Logical Access Controls*

Logical Access Controls adalah cara utama yang digunakan untuk mengelola dan melindungi aset informasi. Tujuan kontrol ini adalah mencegah akses tidak sah dan modifikasi ke data sensitif organisasi dan penggunaan fungsi kritis sistem. Untuk mencapai tingkat kontrol ini, diperlukan penerapan kontrol akses di semua lapisan arsitektur sistem informasi organisasi, termasuk jaringan, *platform* atau sistem operasi, basis data, dan sistem aplikasi. Aktivitas yang dilakukan meliputi identifikasi dan otentifikasi, otorisasi akses, memeriksa sumber daya informasi tertentu, dan mencatat serta melaporkan kegiatan pengguna.

3. *Network Security Controls*

Mengontrol jaringan keamanan harus dilakukan oleh operator yang berkualitas teknis. *Network Security Controls* harus membatasi akses operator dari menjalankan fungsi tertentu. *Network Security Controls* harus memelihara jejak audit dari semua aktifitas operator. Jalur audit harus ditinjau secara berkala oleh manajemen operasi untuk mendeteksi aktivitas operasi jaringan yang tidak sah.

4. *Environmental Controls*

Eksposur lingkungan disebabkan oleh peristiwa yang terjadi secara alami, seperti petir, gempa bumi, letusan gunung berapi, angin topan, dan lain sebagainya. Kegagalan yang disebabkan lingkungan tersebut dapat dikontrol dengan panel kontrol alarm, detektor air, alat pemadam api, pendeteksi asap, sistem pencegah kebakaran, alarm kebakaran manual, lokasi ruang komputer yang strategis, ruangan yang tahan api, atau pelindung lonjakan daya listrik.

5. *Physical Security Controls*

Physical Security Controls dapat dilakukan dengan mengadakan *ID Card, ID Card* harus dikenakan oleh semua personil, dengan membedakan warna antara identitas karyawan dan pengunjung. Penjagaan keamanan juga dapat diterapkan sebagai pelengkap kamera video dan penjagaan pintu. Mengontrol akses pengunjung, tidak mengiklankan lokasi fasilitas sensitif, sistem alarm, pengamanan dokumen, dan lain sebagainya.

2.2.5.5 Aspek Teknologi

Aspek teknologi keamanan informasi mengevaluasi kelengkapan, efektifitas, dan konsistensi penggunaan teknologi dalam pengamanan aset informasi. Keamanan informasi dapat dilakukan dengan proteksi peralatan komputer maupun non-komputer, fasilitas, data, dan informasi dari penyalahgunaan oleh pihak yang tidak berwenang. Beberapa proteksi atau pertahanan keamanan yang dapat dilakukan organisasi yakni menggunakan enkripsi, *firewall*, pengawasan surat elektronik, dan pertahanan dari virus atau *malware*.

Penggunaan enkripsi data menjadi sebuah cara untuk melindungi data dengan mentransmisikan data dalam bentuk yang beraturan dan tidak beraturan oleh sistem komputer untuk pengguna terotorisasi. Adapun *firewall* yang bertindak sebagai penjaga yang melindungi jaringan komputer dari penyusupan dengan menyediakan sebuah penyaring dan titik pengiriman yang aman untuk akses dari internet serta jaringan lain. Tempat yang sering menjadi titik serangan oleh peretas untuk menyebarkan virus komputer atau menyusup ke dalam komputer jaringan adalah melalui surat elektronik. Surat elektronik merupakan tempat organisasi melawan pesan yang tidak resmi atau perusakan. Banyak organisasi membangun pertahanan teknologi melawan penyebaran virus dengan memusatkan distribusi dan memperbarui perangkat lunak antivirus sebagai tanggungjawab sistem informasinya.

2.2.6 ISO 27000

Standarisasi ISO telah mengembangkan sejumlah standar tentang sistem manajemen keamanan informasi (SMKI) dalam bentuk persyaratan maupun panduan. Menurut Panduan Penerapan Tata Kelola Keamanan Informasi Tahun 2017, Standar SMKI dikelompokkan sebagai keluarga atau seri ISO 27000 yang terdiri sebagai berikut.

- ISO/IEC 27000:2014 – *ISMS Overview and Vocabulary*

  Standar ISO 27000 memuat prinsip – prinsip dasar *Information Security Management System* (ISMS) atau Sistem Manajemen Keamanan Informasi, mendefinisikan sejumlah istilah penting dan hubungan antar standar keluarga SMKI, baik yang telah diterbitkan maupun yang sedang dalam pengembangan.

- ISO/IEC 27001:2013 – *ISMS Requirements*

  Standar ini berisi persyaratan yang harus dipenuhi untuk membangun Sistem Manajemen Keamanan Informasi (SMKI). ISO/IEC 27001 dirancang untuk menjamin agar kontrol – kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan. Standar ISO 27001:2013 bertujuan untuk menjaga konsistensi, keselarasan, dan kompatibilitas dari sistem manajemen organisasi yang merujuk pada standar – standar yang dikembangkan ISO.

Lampiran yang digunakan sebagai kontrol keamanan (*security control*) untuk mengimplementasikan SMKI pada Standar ISO 27001:2013 disebut Annex A. Lampiran Annex A mencakup 114 kontrol dalam 14 area, yakni kebijakan keamanan informasi, organisasi keamanan informasi, keamanan sumber daya manusia, manajemen aset, akses kontrol, kriptografi, keamanan fisik dan lingkungan, keamanan operasi, keamanan komunikasi, akuisisi, pengembangan dan pemeliharaan sistem, hubungan pemasok, manajemen insiden keamanan informasi, aspek keamanan informasi manajemen kesinambungan bisnis, dan kepatuhan. Lampiran Annex A atau kontrol ISO 27001:2013 disajikan berupa tabel pada Lampiran F.

- ISO/IEC 27002:2013 – *Code of Practice for ISMS*

  Standar ini memuat panduan contoh penerapan keamanan informasi pada kontrol tertentu untuk mencapai sasaran kontrol tersebut. Kontrol yang disediakan mencakup 14 area pengamanan ISO/IEC 27001.

- ISO/IEC 27003:2010 – *ISMS Implementation Guidance*

  Tujuan dari standar ini adalah sebagai panduan untuk perancangan dan penerapan SMKI agar memenuhi persyaratan ISO/IEC 27001. ISO/IEC 27003 mendefinisikan proses pembangunan SMKI terkait persiapan, perancangan, dan pengembangan SMKI sebagai suatu kegiatan proyek.

- ISO/IEC 27004:2009 – *ISMS Measurements*

  ISO/IEC 27004 disediakan untuk memberikan panduan penyusunan dan penggunaan teknik pengukuran untuk mengkaji keefektifan penerapan SMKI sesuai ISO 27001. Standar ISO/IEC 27004 juga berguna untuk mengukur ketercapaian sasaran keamanan yang ditetapkan.

- ISO/IEC 27005:2008 – *Information Security Risk Management*

  Standar ini adalah penvedia panduan untuk kegiatan manajemen risiko keamanan informasi pada suatu organisasi dalam rangka mendukung persyaratan SMKI pada ISO 27001.

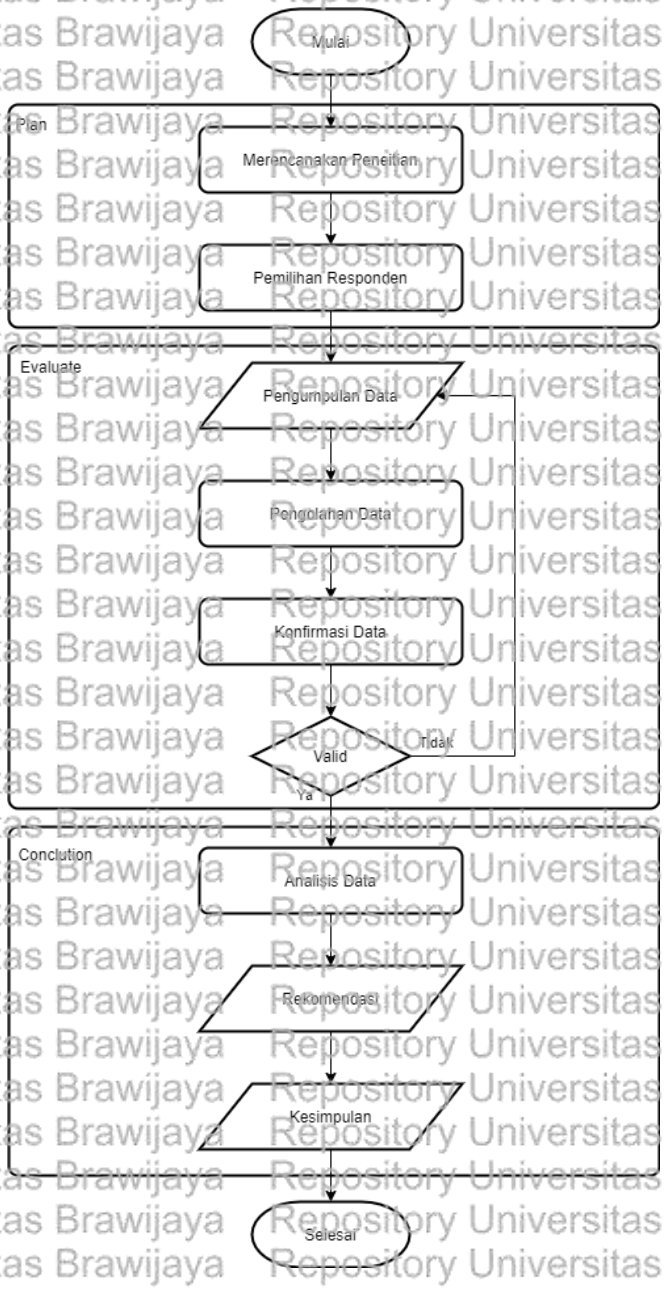
- ISO/IEC 27006 – *Requirements for bodies providing audit and certification of ISMS*

  Standar ISO/IEC 27006 merupakan standar untuk menetapkan persyaratan dan memberikan panduan bagi organisasi yang berwenang melaksanakan audit dan sertifikasi SMKI. ISO/IEC 27006 bertujuan sebagai pendukung proses akreditasi badan sertifikasi ISO 27001.

BAB 3 METODE

3.1 Metode Penelitian

Metode penelitian merupakan tahapan yang akan digunakan untuk melaksanakan penelitian pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto. Metode penelitian ini mensitasi dari jurnal *Strategies for Information Systems Evaluation* yang ditulis oleh Stefan Cronholm & Goran Goldkuhl (2003).



Gambar 3.1 Proses Penelitian

Berikut adalah penjelasan dari Gambar 3.1 alur metode penelitian :

1. Tahap awal yang dilakukan yakni melakukan perencanaan penelitian dengan informasi yang didapat dalam studi literatur. Kemudian menentukan rencana penelitian sesuai dengan panduan metode Indeks Keamanan Informasi (KAMI).
2. Melakukan pemilihan responden untuk mengisi kuesioner Indeks KAMI, responden ditentukan sesuai pada panduan indeks KAMI.
3. Selanjutnya adalah pengumpulan data dengan melakukan pengisian kuesioner.
4. Setelah data kuesioner terkumpul, data diolah ke dalam format Indeks KAMI sesuai panduan.
5. Tahapan selanjutnya yakni konfirmasi data dengan melakukan validasi menggunakan *checklist*. Validasi digunakan untuk verifikasi data yang telah terkumpul dari responden apakah sesuai seperti keadaan sebenarnya.
6. Tahap berikutnya yakni menganalisis data. Langkah ini dilakukan dengan menghitung hasil kuesioner menggunakan formula Indeks KAMI, kemudian dilakukan *checklist* sebagai perbandingan hasil evaluasi dengan kontrol standar ISO 27001.
7. Kemudian membuat rekomendasi dari hasil evaluasi sesuai kontrol dalam standar ISO 27001.
8. Tahapan terakhir yakni memberikan kesimpulan hasil dari analisis data dan saran untuk ke depannya.

3.2 Merencanakan Penelitian

Tahap awal yang dilaksanakan pada penelitian ini adalah melakukan perencanaan penelitian dengan didasari informasi yang didapat dalam studi literatur. Penentuan rencana penelitian sesuai dengan panduan metode Indeks Keamanan Informasi (KAMI). Tahapan ini dilakukan dengan menyiapkan keperluan penelitian sebelum memulai langsung pada organisasi yang akan dievaluasi.

3.3 Pemilihan Responden

Sumber data yang dianggap dapat mendukung penelitian ini adalah yang sesuai dengan kriteria responden berdasarkan Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks KAMI (2017), responden yang memiliki kewenangan dan tanggung jawab dalam pengelolaan keamanan informasi sehingga dapat mengisi kuesioner dan memberikan penjelasan ketika diwawancarai. Pemilihan responden yang tepat dilakukan untuk mengisi kuesioner sesuai Indeks KAMI yang akan diberikan.

3.4 Pengumpulan Data

Metode atau teknik pengumpulan data adalah suatu cara yang ditempuh oleh dalam mencari atau menggali data pada suatu objek. Penelitian dilakukan dengan melakukan studi lapangan dahulu dan meminta persetujuan serta penentuan objek penelitian pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto. Sehubungan dengan penelitian ini, dalam melakukan penggalian data yang dibutuhkan, peneliti menggunakan metode pengumpulan data dengan menggunakan pendekatan metode kuesioner.

Metode Kuesioner merupakan teknik pengumpulan data yang dilakukan dengan cara memberi seperangkat pernyataan tertulis pada responden dan pihak responden dapat memilih pilihan jawaban. Pertanyaan kuesioner diambil sesuai dengan pedoman Indeks KAMI pada Lampiran B. Setiap jawaban akan diberi nilai yang berbeda sesuai kategori pengamanannya atau tahapan penerapannya.

Penyusunan kuesioner sesuai dengan format Indeks KAMI yang diambil dari web BSSN. Indeks KAMI yang digunakan oleh peneliti menggunakan standar Indeks KAMI versi 3.1 yang terdiri dari area kategori sistem informasi dan area keamanan informasi. Kuesioner diberikan oleh peneliti kepada responden yang telah dipilih sesuai kriteria sampel.

Sesuai dengan petunjuk penggunaan alat evaluasi Indeks Keamanan Informasi (Indeks KAMI), kuesioner awal yang harus dikerjakan adalah bagian I kategori sistem elektronik seperti pada Gambar 3.2. Pada kuesioner tersebut menggambarkan terkait bagaimana keadaan sistem elektronik yang digunakan dalam mendukung proses kerja pada instansi. Kategori sistem elektronik memiliki sepuluh pertanyaan yang berguna untuk mengetahui tingkat ketergantungan.

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 Kuesioner Bagian I

Sumber: Indeks KAMI Versi 3.1 (2015)

Gambar 3.2 menggambarkan kuesioner bagian I terkait kategori sistem elektronik. Pengisian dilakukan dengan memilih jawaban A, B, atau C sesuai definisi setiap huruf. Penilaian atau skor akan berubah sesuai pilihan jawaban pada kolom status. Jumlah skor tersebut akan otomatis terakumulasi pada baris terakhir, sebagai penilaian kategori sistem informasi.

Pada area keamanan informasi, terdapat dari lima bagian yang dimulai dari bagian II hingga bagian VI, yakni:

a. Bagian II: Tata Kelola Keamanan Informasi
b. Bagian III: Pengelolaan Risiko Keamanan Informasi
c. Bagian IV: Kerangka Kerja Keamanan Informasi
d. Bagian V: Pengelolaan Aset Informasi
e. Bagian VI: Teknologi dan Keamanan Informasi

Pada setiap pertanyaan terdapat pilihan jawaban sesuai status penerapannya, berikut adalah opsi pada status penerapan:

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

3.5 Pengolahan Data

Setelah data kuesioner terkumpul, data diolah ke dalam format indeks KAMI sesuai panduan. Seluruh data dimasukkan pada file excel sesuai format Indeks KAMI versi 3.1, termasuk identitas responden. Data tersebut dikumpulkan menjadi informasi yang dapat dibaca mengikuti pedoman Indeks KAMI versi 3.1.

Pada area kategori sistem informasi terdapat skor yang dapat menggambarkan tingkat kematangan pada instansi, seperti pada Tabel 3.1. Sedangkan pada area keamanan informasi juga terdapat skor sesuai dengan kategori pengaman dan status penerapannya. Penilaian area keamanan informasi didefinisikan pada Gambar 3.3 yang membentuk matriks nilai antara kategori pengaman dengan status penerapannya.

Tabel 3.1 Definisi Skor Kategori Sistem Elektronik

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

Sumber: Indeks KAMI Versi 3.1 (2015)

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

Gambar 3.3 Matriks Nilai Kategori Pengamanan

Sumber: Indeks KAMI Versi 3.1 (2015)

Gambar 3.3 merupakan matriks nilai area keamanan informasi yang disesuaikan dengan status penerapannya dan kategorinya. Nilai pada kategori awal lebih rendah dari berikutnya. Sedangkan apabila penerapannya berjalan secara menyeluruh maka mendapatkan skor lebih tinggi daripada status penerapan yang lain.

3.6 Konfirmasi Data

Setelah seluruh data yang dibutuhkan terkumpul maka dibutuhkan verifikasi data untuk memastikan kebenaran data. Pada tahapan ini dilakukan *checklist* untuk verifikasi data terhadap hasil kuesioner yang didapatkan sebelumnya melalui kuesioner. Metode ini dilakukan dengan cara tatap muka dengan pihak – pihak yang terkait dalam penanganan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto untuk menggali informasi dan mendapatkan bukti dari data yang telah diisi.

Checklist dilakukan dengan cara pendampingan langsung kepada responden yang sudah ditentukan. Pada tahap ini kuesioner yang membutuhkan bukti adalah pertanyaan yang terjawab dengan status "Dalam Perencanaan/ Diterapkan Sebagian" dan "Diterapkan Menyeluruh".

3.7 Analisis Data

Seluruh data yang terkumpul dan telah divalidasi, akan dilakukan penganalisisan menggunakan Indeks KAMI Versi 3.1. Indeks KAMI Versi 3.1 terdiri dari 5 area yang akan dievaluasi. Data tersebut akan dihitung dan dianalisis untuk menghasilkan rekomendasi. Analisis dilakukan dengan memetakan jawaban responden sesuai dengan tingkat kematangannya dan disajikan dalam bentuk diagram dan tabel Indeks KAMI.

Hasil dari penjumlahan skor pada masing – masing area akan ditampilkan dalam dua bentuk instrumen, yakni:

1. Tabel Nilai

Skor Kategori SE	: 50	Kategori SE	Strategis	
Tata Kelola	: 0	Tk Kematangan :	I	
Pengelolaan Risiko	: 0	Tk Kematangan :	I	I
Kerangka Kerja Keamanan Informasi	: 0	Tk Kematangan :	I	s/d
Pengelolaan Aset	: 0	Tk Kematangan :	I	I
Teknologi dan Keamanan Informasi	: 0	Tk Kematangan :	I	

Gambar 3.4 Tabel Hasil Penilaian

Sumber: Indeks KAMI Versi 3.1 (2015)

Gambar 3.4 merupakan tabel yang menunjukkan perhitungan total nilai dari setiap area pada keamanan informasi, nilai tersebut akan memberikan gambaran tingkat kematangan pada setiap bagian. Adapun korelasi kategori sistem elektronik untuk mengukur tingkat kesiapan didefinisikan melalui matriks berikut:

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

Gambar 3.5 Matriks Kategori Sistem Elektronik dan Tingkat kesiapan

Sumber: Pengantar Indeks KAMI Versi 3.1 (2015)

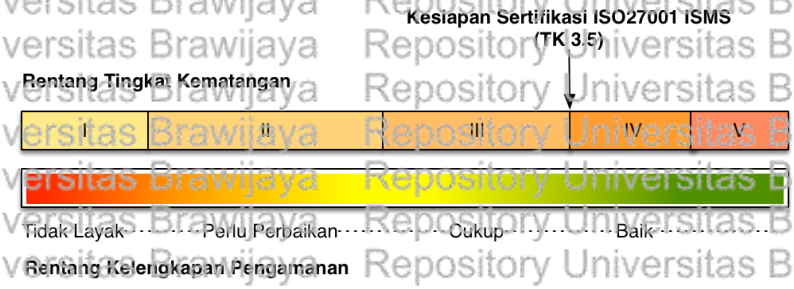
2. *Radar Chart*

Gambar 3.6 *Radar Chart* Hasil Penilaian

Sumber: Indeks KAMI Versi 3.1 (2015)

Hasil yang berbentuk diagram *radar chart* pada Gambar 3.5 ini memiliki lima sumbu sesuai dengan area pengamanan, yakni tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan aset, dan aspek teknologi. Nilai pada masing - masing area keamanan informasi akan digambarkan dengan area berwarna merah. Sedangkan latar belakang hijau tua hingga hijau muda merupakan area perbandingan skor masing – masing area terhadap hubungan kepatuhan pada standar ISO27001, status penerapan, dan kerangka kerja.

Adapun Hasil dari proses evaluasi dengan acuan tingkat kesiapan sertifikasi berdasarkan standar ISO27001, digambarkan dengan garis ukur warna merah gradasi hingga warna hijau seperti pada Gambar 3.6. Dapat dikatakan mencapai kesiapan sertifikasi ISO27001 apabila kategori kematangan mencapai 3,5 atau tingkat kematangan III+ dan garis ukur berada pada warna hijau. Hal tersebut merupakan ambang batas minimum dapat dikatakan baik.



Gambar 3.7 Tingkat Kesiapan Sertifikasi ISO 27001

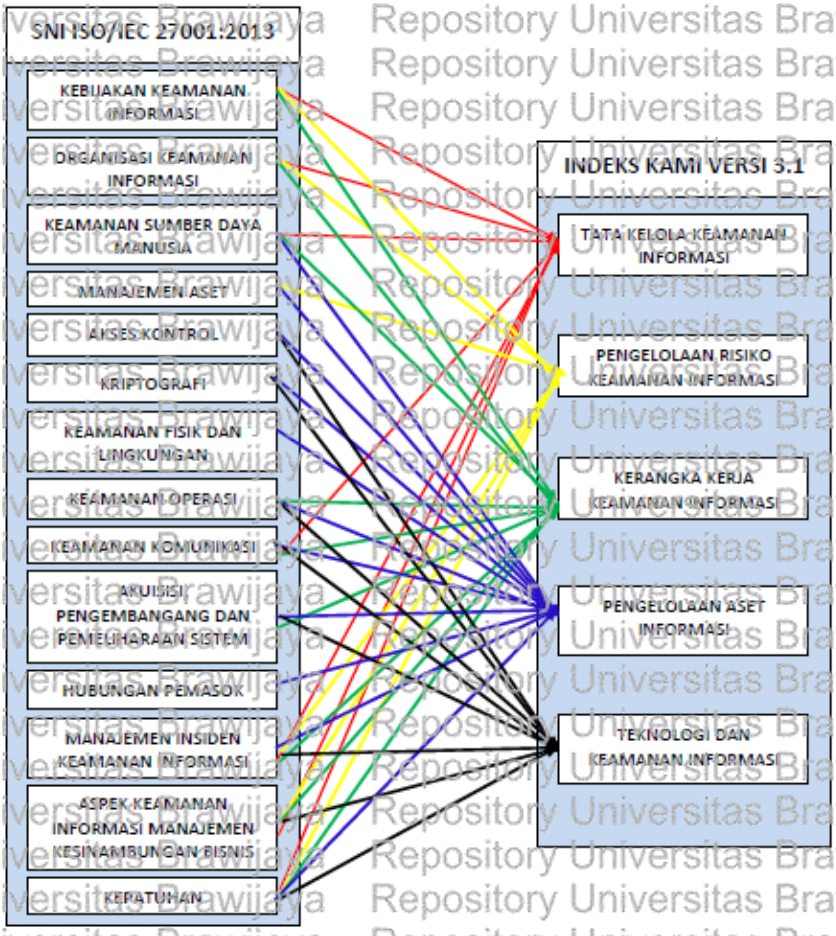
Penilaian rentang tingkat kematangan informasi didefinisikan sebagai berikut:

- Tingkat I : Kondisi Awal atau Reaktif
- Tingkat II : Penerapan Kerangka Kerja Dasar
- Tingkat III : Terdefinisi dan Konsisten atau Proaktif
- Tingkat IV : Terkelola dan Terukur atau Terkendali
- Tingkat V : Optimal

Untuk membantu memberikan uraian yang lebih detail, tingkatan tersebut ditambah empat tingkatan antara, yakni I+, II+, III+, dan IV+. Sehingga total terdapat sembilan tingkat kematangan. Pada awal penilaian, semua responden akan diberikan kategori kematangan tingkat I.

3.8 Rekomendasi

Rekomendasi dibuat dari hasil evaluasi yang disesuaikan dengan kontrol pada standar ISO 27001. Rekomendasi didapatkan dengan cara melakukan perbandingan terhadap persyaratan yang ada pada kontrol ISO 27001. Hubungan antara empat belas kontrol ISO 27001:2013 dengan lima area Indeks KAMI versi 3.1 digambarkan sebagai berikut:



Gambar 3.8 Hubungan antara kontrol ISO 27001:2013 dengan area Indeks KAMI versi 3.1

Sumber: Octaviani, dkk (2019)

Berdasarkan Gambar 3.8 hubungan antara kontrol ISO 27001:2013 dengan area keamanan informasi pada Indeks KAMI dipetakan sebagai berikut pada Tabel 3.2.

Tabel 3.2 Pemetaan Indeks KAMI dengan kontrol ISO 27001:2013

No.	Area Kemanan Informasi Indeks KAMI versi 3.1	Kontrol ISO 27001:2013
1.	Tata Kelola Keamanan Informasi	• Kebijakan keamanan informasi • Organisasi keamanan informasi • Keamanan sumber daya manusia • Keamanan komunikasi • Manajemen insiden keamanan informasi • Aspek keamanan informasi manajeman kesinambungan bisnis • Kepatuhan

Tabel 3.3 Pemetaan Indeks KAMI dengan kontrol ISO 27001:2013 (lanjutan)

No.	Area Kemanan Informasi Indeks KAMI versi 3.1	Kontrol ISO 27001:2013
2.	Pengelolaan Risiko Keamanan Informasi	• Kebijakan keamanan informasi • Organisasi keamanan informasi • Manajemen aset • Manajemen insiden keamanan informasi • Aspek keamanan informasi manajeman kesinambungan bisnis • Kepatuhan
3.	Kerangka Kerja Keamanan Informasi	• Kebijakan keamanan informasi • Organisasi keamanan informasi • Keamanan sumber daya manusia • Keamanan operasi • Keamanan komunikasi • Akuisisi pengembangan dan pemiliharaan • Manajemen insiden keamanan informasi • Aspek keamanan informasi manajeman kesinambungan bisnis • Kepatuhan
4.	Pengelolaan Aset Informasi	• Keamanan sumber daya manusia • Manajemen aset • Akses kontrol • Kriptografi • Keamanan fisik dan lingkungan • Keamanan operasi • Keamanan komunikasi • Akuisisi pengembangan dan pemiliharaan • Hubungan pemasok • Manajemen insiden keamanan informasi • Kepatuhan
5.	Teknologi dan Keamanan Informasi	• Akses kontrol • Kriptografi • Keamanan operasi • Keamanan komunikasi • Akuisisi pengembangan dan pemiliharaan • Manajemen insiden keamanan informasi • Aspek keamanan informasi manajeman kesinambungan bisnis • Kepatuhan

Syarat – syarat yang belum terpenuhi sesuai persyaratan ISO 27001:2013 akan diberikan rekomendasi. Rekomendasi untuk keamanan informasi tersebut dapat digunakan sebagai acuan bagi organisasi untuk mencapai tujuan organisasi dan melakukan perbaikan di masa mendatang, serta dapat melakukan perbaikan tata kelola keamanan informasi sesuai dengan standar ISO 27001:2013.

3.9 Kesimpulan

Tahapan terakhir yakni kesimpulan yang berisi kondisi keamanan informasi yang terjadi saat ini dan saran untuk ke depannya. Kondisi keamanan informasi tersebut merupakan hasil dari evaluasi yang telah dilakukan dan saran ditujukan untuk penelitian selanjutnya.

BAB 4 HASIL DAN ANALISIS

4.1 Responden

Pada penelitian ini menggunakan kuesioner Indeks KAMI untuk mendapatkan nilai atau hasil tingkat keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto. Pengisian kuesioner dilakukan oleh responden atau sampel yang sesuai. Teknik pengambilan sampel yang digunakan pada penelitian ini adalah teknik purposive sampling. Teknik ini digunakan untuk memilih sampel berdasarkan kriteria tertentu.

Pemilihan sampel menggunakan teknik purposive sampling dikarenakan tidak semua populasi memiliki kriteria – kriteria yang sesuai dengan yang ditentukan oleh peneliti. Kriteria sampel pada penelitian ini didapatkan dari tujuan atau topik tertentu yang sesuai dengan tema penelitian. Dengan menetapkankan kriteria yang sesuai dengan tema penelitian, maka responden diharapkan dapat memberikan informasi yang dibutuhkan peneliti.

Berdasarkan Panduan Penerapan Tata Kelola Keamanan Informasi (2011), evaluasi Indeks KAMI dilakukan oleh pejabat yang secara langsung memiliki tanggungjawab dan wewenang dalam pengelolaan keamanan informasi pada lingkup instansi. Responden yang mengisi kuesioner Indeks KAMI versi 3.1 pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto terdapat pada Tabel 4.1.

Tabel 4.1 Responden Kuesioner

No.	Nama	Jabatan	Tugas
1.	Diding Adi Parwoto S. Kom, M. Eng	Kepala Seksi Sistem Informasi	• Menyusun perumusan program kerja Seksi Sistem Informasi dengan meminta masukan dari bawahan agar tercipta program kerja yang relevan dan dapat dilaksanakan. • Melakukan pembagian tugas kepada bawahan dengan memberikan disposisi dan atau perintah agar tercipta pembagian habis tugas di Seksi Sistem informasi. • Melakukan pemberian petunjuk bawahan dengan menilai dan mempertahankan kinerja bawahan agar tercipta kinerja bawahan yang baik sesuai dengan standar kinerja yang telah ditetapkan

Tabel 4.2 Responden Kuesioner (lanjutan)

No.	Nama	Jabatan	Tugas
			• Menyusun rencana program, kegiatan dan pelaksanaan sistem informasi sesuai dengan rencana kerja dinas; • Melakukan pengembangan teknologi informasi dan *e-government*; • Melakukan kerjasama program *e-government* antar lembaga pemerintahan/atau lembaga swasta; • Melakukan pengelolaan sistem informasi Pemerintah Kabupaten Mojokerto; • Melakukan pengelolaan SPSE Pemerintah Kabupaten Mojokerto; • Melakukan evaluasi dan menyusun laporan; dan • Melakukan tugas-tugas kedinasan lain yang diberikan oleh Kepala Bidang Informatika
2.	Ulinnuha Nashirudin S. Kom	Staf Infrastruktur Teknologi Informasi	• Menyusun rencana program infrastruktur teknologi informasi sesuai dengan rencana kerja dinas; • Melakukan pembangunan dan pengembangan infrastruktur teknologi informasi; • Melakukan bimbingan teknis dan peningkatan kapasitas infrastruktur teknologi informasi; • Melakukan pemeliharaan Infrastruktur teknologi informasi; • Melakukan kerjasama dalam rangka pengembangan infrastruktur teknologi informasi; • Melakukan evaluasi dan menyusun laporan; dan • Melakukan tugas kedinasan lain yang diberikan oleh Kepala Bidang Informatika.

Tabel 4.3 Responden Kuesioner (lanjutan)

No.	Nama	Jabatan	Tugas
3.	Akhmad Hadi Iqfanto S. Kom	Staf Sistem Informasi	• Menyusun rencana program, kegiatan dan pelaksanaan sistem informasi sesuai dengan rencana kerja dinas; • Melakukan pengembangan teknologi informasi dan *e-government*; • Melakukan kerjasama program *e-government* antar lembaga pemerintahan/atau lembaga swasta; • Melakukan pengelolaan sistem informasi Pemerintah Kabupaten Mojokerto; • Melakukan pengelolaan SPSE Pemerintah Kabupaten Mojokerto; • Melakukan evaluasi dan menyusun laporan; dan • Melakukan tugas-tugas kedinasan lain yang diberikan oleh Kepala Bidang Informatika.

4.2 Analisis *RACI Chart*

Evaluasi pada penelitian ini menggunakan *RACI chart* dalam pemilihan responden untuk mengisi kuesioner Indeks KAMI. *RACI chart* digunakan untuk memperjelas peran dan fungsi terhadap aktivitas tertentu. Responden yang dipilih adalah responden yang mewakili tabel RACI yang bertanggung jawab dalam keamanan informasi.

RACI merupakan singkatan dari *responsible, accountable, consulted,* dan *informed*. Menurut Michael L Smith dan James Erwin (2005), keterangan peran dari RACI sebagai berikut:

a. *Responsible* : Orang yang melakukan pekerjaan

b. *Accountable* : Orang yang bertanggung jawab terhadap penyelesaian pekerjaan atau menyetujui hasil suatu pekerjaan

c. *Consulted* : Orang yang dimintai pendapat tentang suatu pekerjaan

d. *Informed* : Orang yang selalu mendapatkan informasi tentang kemajuan pekerjaan

Pengklasifikasian responden dalam tabel *RACI chart* dianalisis berdasarkan tugas dan wewenang responden dengan hasil pada Tabel 4.2. Kepala seksi sistem informasi menjadi A*ccountable* (A) dalam memahami area tata kelola keamanan informasi dikarenakan memiliki tugas perumusan program sistem informasi. Dalam pengelolaan risiko juga sebagai peran A karena bertugas dalam pemberian petunjuk pertahanan kinerja bawahannya. Sedangkan bertanggung jawab pada area kerangka kerja sebab memiliki tugas menyusun rencana program, kegiatan, dan pelaksanaan sistem informasi. Adapun dalam pengelolaan aset, bertugas sebagai pengembangan teknologi dan *e-government* dengan peran *Consulted* (C). Dalam tugas pengelolaan sistem informasi, memerlukan informasi pemahaman area teknologi, sehingga disimpulkan memiliki peran *Informed* (I).

Staf Infrastruktur Teknologi Informasi menjadi *Informed* (I) dalam memahami area tata kelola sebab dalam tugasnya menyusun rencana program infrastruktur memerlukan informasi tata kelola keamanan informasi. Pada pengelolaan risiko memiliki peran tanggung jawab atau *Responsible* (R) karena bertugas dalam pemeliharaan infrastruktur teknologi informasi. Sedangkan dalam tugas penyusunan pembangunan infrastruktur diperlukan informasi perencanaan kerangka kerja dengan peran I. Adapun dalam pengelolaan aset, bertanggungjawab (R) atas pemeliharaan infrastruktur teknologi informasi. Dalam pemahaman area teknologi dan keamanan informasi, dapat menjadi peran C sebab memiliki tugas dalam pembangunan dan pengembanan serta peningkatan infrastruktur teknologi informasi.

Staf Sistem Informasi bertanggung jawab pada area tata kelola keamanan informasi dikarenakan memiliki tugas dalam menyusun kegiatan pelaksanaan sistem informasi sesuai rencana kerja dinas. Pada pengelolaan risiko dapat berperan sebagai *Consulted* (C) sebab bertugas melakukan pengembangan teknologi informasi dan *e-government*. Sedangkan pada perencanaan kerangka kerja memiliki tugas melakukan pengelolaan SPSE dengan peran I. Adapun dalam pengelolaan aset dapat dijadikan konsultan (C) karena telah memiliki tugas dalam pengelolaan sistem informasi pemerintahan. Sedangkan dalam memahami area teknologi dan keamanan informasi, bertanggung jawab dalam tugas pengembangan teknologi informasi dan *e-government*.

Tabel 4.4 Tabel *RACI Chart*

Tugas	Kepala Seksi Sistem Informasi	Staf Infrastruktur Teknologi Informasi	Staf Sistem Informasi
Memahami area tata kelola keamanan informasi	A	I	R
Memahami area pengelolaan risiko keamanan informasi	A	R	C
Memahami area kerangka kerja pengelolaan keamanan informasi	R	I	I
Memahami area pengelolaan aset informasi	C	R	C
Memahami area teknologi dan keamanan informasi	I	C	R

Keterangan: R = *Responsible;* A = A*ccountable;* C = *Consulted;* I = *Informed*

Tabel 4.2 menjelaskan bahwa responden berkompeten melaksanakan kebijakan keamanan informasi dalam pengisian kuesioner Indeks KAMI. Kepala seksi sistem informasi, staf infrastruktur teknologi informasi, dan staf sistem informasi dapat mewakili tabel RACI dalam keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto.

4.3 Analisis Hasil

Evaluasi yang dilaksanakan pada penelitian di Diskominfo Kabupaten Mojokerto ini menggunakan evaluasi *criteria based*, pendekatan ini berdasarkan kriteria pada perspektif atau teori tertentu. Indeks KAMI merupakan teori yang digunakan sebagai dasar landasan pada penggunaan kriteria untuk evaluasi penelitian ini. Dari metode Indeks KAMI data yang diambil berupa kuesioner.

Penelitian ini menggunakan Indeks KAMI versi 3.1. Indeks KAMI versi 3.1 terdiri dari bagian kategori sistem informasi dan bagian keamanan informasi. Pada bagian keamanan informasi terdapat lima target area, yakni tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja pengelolaan keamanan informasi, pengelolaan aset informasi, dan teknologi dan keamanan informasi.

4.3.1 Kategori Sistem Elektronik

Kategori sistem elektronik adalah gambaran terkait keadaan sistem elektronik yang digunakan oleh instansi dalam mendukung proses kerja. Total nilai kategori sistem elektronik yang didapatkan oleh Diskominfo Kabupaten Mojokerto adalah 17, hal tersebut memiliki arti bahwa Dinas Komunikasi dan Informatika

Kabupaten Mojokerto terbilang dalam kategori tinggi. Maka proses kerja yang ada pada Diskominfo Kabupaten Mojokerto memiliki ketergantungan tinggi dan membutuhkan penggunaan sistem elektronik.

4.3.2 Tata Kelola Keamanan Informasi

Tata kelola keamanan informasi merupakan bagian yang mengevaluasi kesiapan tata kelola keamanan informasi meliputi fungsi, tugas, dan tanggungjawab pengelolaan keamanan informasi. Area ini merupakan sistem yang memberikan arahan dan mengatur aktivitas keamanan informasi. Hasil area ini meliputi keselarasan strategi keamanan informasi dalam mendukung tujuan organisasi.

Untuk mendukung hasil penelitian dalam bentuk kuesioner, perlu dilakukan konfirmasi dengan menggunakan *checklist*. *Checklist* digunakan untuk mengecek bukti hasil kuesioner yang telah dijawab. Kuesioner yang membutuhkan verifikasi data atau bukti asli adalah pertanyaan yang terjawab dengan status "Dalam Perencanaan/ Diterapkan Sebagian" dan "Diterapkan Menyeluruh", selain itu tidak perlu dilakukan *checklist*.

Kuesioner yang diisi oleh responden menghasilkan *checklist* pada Lampiran C dengan bukti yang ditunjukkan pada Lampiran D. Berdasarkan hasil tersebut, dalam area tata kelola keamanan informasi terdapat 5 (lima) pertanyaan yang perlu dilakukan *checklist*. Pertanyaan tersebut terdiri dari 2 (dua) kuesioner tingkat kematangan II-kategori 2 berstatus "Dalam Perencanaan/ Diterapkan Sebagian" dan 3 (tiga) kuesioner tingkat kematangan III-kategori 2 berstatus "Dalam Perencanaan/ Diterapkan Sebagian". Namun terdapat 2 (dua) pertanyaan yang tidak dapat ditunjukkan buktinya oleh responden seperti pada Tabel 4.5, yakni pada 1 (satu) kuesioner tingkat kematangan II-kategori 2 dan 1 (satu) kuesioner pada tingkat kematangan III-kategori 2.

Tabel 4.5 *Checklist* Area Tata Kelola Keamanan Informasi

Bagian II: Tata Kelola Keamanan Informasi				Status	Bukti	
#	Fungsi/Instansi Keamanan Informasi				Ada	Tidak
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?	Dalam Penerapan / Diterapkan Sebagian		√

Tabel 4.6 *Checklist* Area Tata Kelola Keamanan Informasi (lanjutan)

Bagian II: Tata Kelola Keamanan Informasi				Status	Bukti	
#	Fungsi/Instansi Keamanan Informasi				Ada	Tidak
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	Dalam Penerapan / Diterapkan Sebagian		√

Tabel 4.5 ini menunjukkan bahwa terdapat 2 (dua) pertanyaan yang tidak dapat ditunjukkan buktinya oleh responden, yakni pada kuesioner nomor 2.12 tentang pengelolaan keamanan dengan pihak internal dan eksternal maupun pihak lain dan 2.16 tentang permasalahan keamanan menjadi bagian proses pengambilan keputusan.

4.3.3 Pengelolaan Risiko Keamanan Informasi

Pengelolaan risiko merupakan bagian yang mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Area ini melalui tahapan identifikasi risiko, penilaian risiko, dan pemecahan masalah. Hasil evaluasi risiko digunakan untuk membandingan mitigasi risiko supaya sesuai dengan kebijakan instansi.

Untuk mendukung hasil penelitian dalam bentuk kuesioner, perlu dilakukan konfirmasi dengan menggunakan *checklist*. *Checklist* digunakan untuk mengecek hasil kuesioner yang telah dijawab. Kuesioner yang membutuhkan verifikasi data atau bukti asli adalah pertanyaan yang terjawab dengan status "Dalam Perencanaan/ Diterapkan Sebagian" dan "Diterapkan Menyeluruh", selain itu tidak perlu dilakukan *checklist*.

Kuesioner yang diisi oleh responden menghasilkan *checklist* pada Lampiran C dengan bukti yang ditunjukkan pada Lampiran D. Berdasarkan hasil tersebut, dalam area pengelolaan risiko keamanan informasi terdapat 5 (lima) pertanyaan yang perlu dilakukan *checklist*. Pertanyaan tersebut terdiri dari 4 (empat) kuesioner tingkat kematangan II-kategori 1 buktinya "Dalam Perencanaan/ Diterapkan Sebagian" dan 1 (satu) kuesioner tingkat kematangan V-kategori 3 buktinya "Dalam Perencanaan/ Diterapkan Sebagian". Namun terdapat 1 (satu) pertanyaan yang buktinya tidak dapat ditunjukkan oleh responden seperti pada Tabel 4.7, yakni pada 1 (satu) kuesioner tingkat kematangan II-kategori 1.

Tabel 4.7 *Checklist* Area Pengelolaan Risiko Keamanan Informasi

Bagian III: Pengelolaan Risiko Keamanan Informasi				Status	Bukti	
#			Kajian Risiko Keamanan Informasi		Ada	Tidak
3,7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Dalam Penerapan / Diterapkan Sebagian		V

Tabel 4.7 ini menunjukkan bahwa terdapat 1 (satu) pertanyaan yang buktinya tidak dapat ditunjukkan oleh responden, yaitu pada kuesioner nomor 3,7 tentang pengidentifikasian ancaman dan kelemahan aset informasi.

4.3.4 Kerangka Kerja Pengelolaan Keamanan Informasi

Kerangka kerja pengelolaan keamanan informasi merupakan bagian yang mengevaluasi kelengkapan maupun kesiapan kebijakan dan prosedur pengelolaan keamanan informasi serta strategi yang diterapkan. Area ini juga mengevaluasi penerapan kerangka kerja meliputi *Disaster Recovery Plan* (DRP) dan *Business Continuity Plan* (BCP).

Untuk mendukung hasil penelitian dalam bentuk kuesioner, perlu dilakukan konfirmasi dengan menggunakan *checklist*. *Checklist* digunakan untuk mengecek bukti hasil kuesioner yang telah dijawab. Kuesioner yang membutuhkan verifikasi data atau bukti asli adalah pertanyaan yang terjawab dengan status "Dalam Perencanaan/ Diterapkan Sebagian" dan "Diterapkan Menyeluruh", selain itu tidak perlu dilakukan *checklist*.

Kuesioner yang diisi oleh responden menghasilkan *checklist* pada Lampiran C dengan bukti yang ditunjukkan pada Lampiran D. Berdasarkan hasil tersebut, dalam area kerangka kerja pengelolaan keamanan informasi terdapat 12 (dua belas) pertanyaan yang perlu dilakukan *checklist*. Pertanyaan tersebut terdiri dari 5 (lima) kuesioner tingkat kematangan II-kategori 1 berstatus "Dalam Perencanaan/ Diterapkan Sebagian", 1 (satu) kuesioner tingkat kematangan III-kategori 1 berstatus "Dalam Perencanaan/ Diterapkan Sebagian", 2 (dua) kuesioner tingkat kematangan III-kategori 2 berstatus "Dalam Perencanaan/ Diterapkan Sebagian", 1 (satu) kuesioner tingkat kematangan III-kategori 3 berstatus "Dalam Perencanaan/ Diterapkan Sebagian", 2 (dua) kuesioner tingkat kematangan IV-kategori 3 berstatus "Dalam Perencanaan/ Diterapkan Sebagian", dan 1 (satu) kuesioner tingkat kematangan V-kategori 3 berstatus "Dalam Perencanaan/ Diterapkan Sebagian". Namun terdapat 3 (tiga) pertanyaan yang buktinya tidak dapat ditunjukkan oleh responden seperti pada Tabel 4.8, yakni pada 1 (satu) kuesioner tingkat kematangan II-kategori 1 dan 1 (satu) kuesioner tingkat kematangan III-kategori 2.

Tabel 4.8 *Checklist* Area Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi				Status	Bukti	
#			Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi		Ada	Tidak
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		√
4,12	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Dalam Penerapan / Diterapkan Sebagian		√
#			Pengelolaan Strategi dan Program 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?	Dalam Penerapan / Diterapkan Sebagian		√

Tabel 4.8 ini menunjukkan bahwa terdapat 2 (dua) pertanyaan yang tidak dapat ditunjukkan buktinya oleh responden, yakni pada kuesioner nomor 4,6 tentang pengidentifikasian kondisi yang membahayakan dan menindaklanjuti, pada nomor 4,12 tentang proses evaluasi risiko terkait rencana pembelian dan penanggulangan masalah yang muncul, serta pada nomor 4,27 tentang analisa aspek finansial pada kebijakan dan prosedur.

4.3.5 Pengelolaan Aset Informasi

Pengelolaan aset informasi merupakan bagian yang mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Perlindungan aset meliputi aspek *security management, logical access control, network security controls, environmental controls,* dan *physical security controls*.

Untuk mendukung hasil penelitian dalam bentuk kuesioner, perlu dilakukan konfirmasi dengan menggunakan *checklist*. *Checklist* digunakan untuk mengecek

bukti terhadap hasil kuesioner yang telah dijawab. Kuesioner yang membutuhkan verifikasi data atau bukti asli adalah pertanyaan yang terjawab dengan status "Dalam Perencanaan/ Diterapkan Sebagian" dan "Diterapkan Menyeluruh", selain itu tidak perlu dilakukan *chechklist*.

Kuesioner yang diisi oleh responden menghasilkan *checklist* pada Lampiran C dengan bukti yang ditunjukkan pada Lampiran D. Berdasarkan hasil tersebut, dalam area pengelolaan aset informasi terdapat 14 (empat belas) pertanyaan yang perlu dilakukan *checklist*. Pertanyaan tersebut terdiri dari 4 (empat) kuesioner tingkat kematangan II-kategori 1 berstatus "Diterapkan Menyeluruh", 6 (enam) kuesioner tingkat kematangan II-kategori 1 berstatus "Dalam Perencanaan/ Diterapkan Sebagian", 2 (dua) kuesioner tingkat kematangan II-kategori 2 berstatus "Dalam Perencanaan/ Diterapkan Sebagian", dan 2 (dua) kuesioner tingkat kematangan III-kategori 3 berstatus "Dalam Perencanaan/ Diterapkan Sebagian". Namun terdapat 4 (empat) pertanyaan yang buktinya tidak dapat ditunjukkan oleh responden seperti pada Tabel 4.9, yakni pada 2 (dua) kuesioner tingkat kematangan II-kategori 1, 1 (satu) kuesioner tingkat kematangan II-kategori 2 dan satu kuesioner tingkat kematangan III-kategori 3.

Tabel 4.9 *Checklist* Area Pengelolaan Aset Informasi

Bagian V: Pengelolaan Aset Informasi				Status	Bukti	
#			Pengelolaan Aset Informasi		Ada	Tidak
5.14	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Dalam Penerapan / Diterapkan Sebagian		√
5.17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dalam Penerapan / Diterapkan Sebagian		√
5.19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Dalam Penerapan / Diterapkan Sebagian		√
5.25	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Dalam Penerapan / Diterapkan Sebagian		√

Tabel 4.9 ini menunjukkan bahwa terdapat 4 (empat) pertanyaan yang tidak dapat ditunjukkan buktinya oleh responden, yaitu pada kuesioner nomor 5,14 tentang persyaratan dan prosedur akses aset informasi, nomor 5,17 tentang penyidikan penyelesaian insiden kegagalan keamanan informasi, nomor 5,19

tentang pengamanan fisik sesuai zona, serta nomor 5,25 tentang *backup* dan laporan analisisnya.

4.3.6 Teknologi dan Keamanan Informasi

Teknologi dan keamanan informasi adalah bagian yang mengevaluasi kelengkapan, konsistensi, dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. Keamanan informasi meliputi proteksi peralatan komputer dan non komputer.

Untuk mendukung hasil penelitian dalam bentuk kuesioner, perlu dilakukan konfirmasi dengan menggunakan *checklist*. *Checklist* digunakan untuk mengecek bukti terhadap hasil kuesioner yang telah diisi. Kuesioner yang membutuhkan verifikasi data atau bukti asli adalah pertanyaan yang terjawab dengan status "Dalam Perencanaan/ Diterapkan Sebagian" dan "Diterapkan Menyeluruh", selain itu tidak perlu dilakukan *chechklist*.

Kuesioner yang diisi oleh responden menghasilkan *checklist* pada Lampiran C dengan bukti yang ditunjukkan pada Lampiran D. Berdasarkan hasil tersebut, dalam area teknologi dan keamanan informasi terdapat 9 (sembilan) pertanyaan yang perlu dilakukan *checklist*. Pertanyaan tersebut terdiri dari 8 (delapan) kuesioner tingkat kematangan II-kategori 1 berstatus "Dalam Perencanaan/ Diterapkan Sebagian" dan 1 (satu) kuesioner tingkat kematangan III-kategori 2 berstatus "Dalam Perencanaan/ Diterapkan Sebagian". Seluruh pertanyaan yang ada pada area teknologi dan keamanan informasi dapat ditampilkan buktinya.

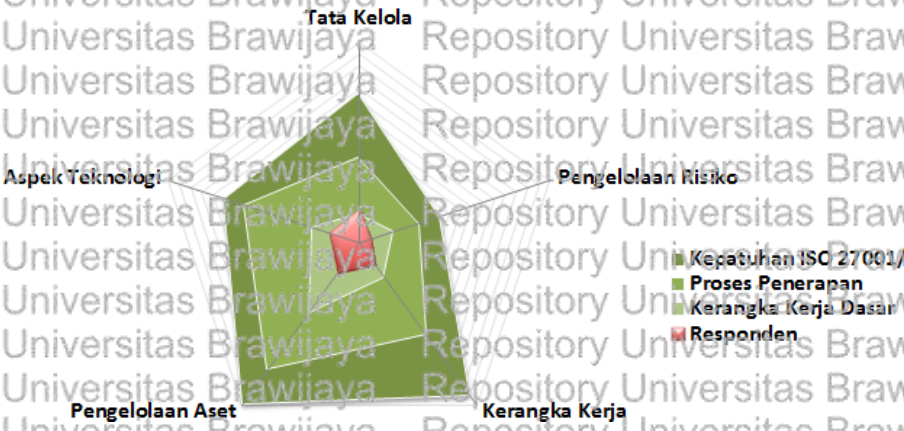
4.4 Perhitungan Data Kuesioner

Hasil kuesioner Indeks KAMI yang diolah dengan format excel menunjukkan terdapat dua hasil penilaian, yaitu tingkat kelengkapan penerapan keamanan informasi dan tingkat kematangan keamanan informasi. Berdasarkan pengumpulan data dihasilkan tingkat kelengkapan penerapan keamanan informasi Dinas Komunikasi dan Informatika Kabupaten Mojokerto dalam bentuk *bar chart* pada Gambar 4.1. Adapun tingkat kelengkapan penerapan keamanan informasi berupa bentuk diagram radar seperti pada Gambar 4.2.

Gambar 4.1 *Bar Chart* Tingkat Kelengkapan Penerapan Keamanan Informasi

Hasil dari Gambar 4.1 dapat disimpulkan sebagai berikut:

a. Pada kategori sistem elektronik, Dinas Komunikasi dan Informasi Kabupaten Mojokerto mendapatkan nilai 17, termasuk dalam kategori **Tinggi**.
b. Kelengkapan penerapan pada standar ISO 27001 melihat dari skor kategori sistem elektronik mendapatkan nilai 121, termasuk dalam kategori **Tidak Layak**, dan berada pada area berwarna **Merah**.



Gambar 4.2 *Radar Chart* Tingkat Kelengkapan Penerapan Keamanan Informasi

Pada Gambar 4.2 terdapat warna merah sebagai kondisi keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto berdasarkan hasil pengisian kuesioner oleh responden. Hasil dari Gambar 4.2 dapat disimpulkan sebagai berikut:

a. Area yang paling baik evaluasinya dari kelima bidang keamanan informasi adalah tata kelola, karena paling mendekati standar kepatuhan ISO27001/SNI
b. Dari kelima area keamanan informasi belum ada yang memenuhi kerangka kerja dasar kecuali bagian tata kelola.

Adapun hasil kuesioner Indeks KAMI pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto yang menunjukkan tingkat kematangan keamanan informasi dapat dilihat pada Gambar 4.3 dengan bentuk tabel skor dengan tingkat keamanannya, serta Tabel 4.10. sebagai persentase tingkat kematangannya.

Tata Kelola	: 29	Tk Kematangan:	I+	
Pengelolaan Risiko	: 10	Tk Kematangan:	I	I
Kerangka Kerja Keamanan Informasi	: 23	Tk Kematangan:	I	s/d
Pengelolaan Aset	: 32	Tk Kematangan:	I+	I+
Teknologi dan Keamanan Informasi	: 27	Tk Kematangan:	I+	

Gambar 4.3 Tingkat Kematangan Keamanan Informasi

Tabel 4.10 Persentase Tingkat Kematangan Keamanan Informasi

Keterangan	Tata kelola	Pengelolaan Risiko	Kerangka kerja	Pengelolaan Aset	Teknologi
Skor Maksimal	126	72	159	168	120
Skor Responden	29	10	23	32	27
Persentase	23%	13,8%	14,4%	19%	22,5%

Berdasarkan hasil Gambar 4.3 dan Tabel 4.7, tingkat kematangan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto pada setiap area adalah sebagai berikut:

a) Tata Kelola Keamanan Informasi

Tingkat kematangan pada bagian tata kelola keamanan informasi yakni berada pada **Level I+**. Skor yang dihasilkan bernilai 29 dengan persentase 23% dari skor maksimal sebesar 126 dengan uraian sebagai berikut:

- Tingkat kematangan II bernilai 17
- Tingkat kematangan III bernilai 12
- Tingkat kematangan IV bernilai 0

Berdasarkan konfirmasi data dengan menggunakan *checklist*, terdapat 2 (dua) pertanyaan berstatus "Dalam Perencanaan/ Diterapkan Sebagian" yang tidak ditemukan bukti yang mendukung, maka status diturunkan menjadi "Dalam Perencanaan". Oleh karena itu, hasil akhir skor rata – rata pada bagian tata kelola keamanan informasi bernilai 25 dengan persentase 19,8%.

b) Pengelolaan Risiko Keamanan Informasi

Tingkat kematangan pada bagian pengelolaan risiko keamanan informasi yakni berada pada **Level I**. Skor yang dihasilkan bernilai 10 dengan persentase 13,8% dari skor maksimal sebesar 72 dengan uraian sebagai berikut:

- Tingkat kematangan II bernilai 10
- Tingkat kematangan III bernilai 0
- Tingkat kematangan IV bernilai 0
- Tingkat kematangan V bernilai 0

Berdasarkan konfirmasi data dengan menggunakan *checklist*, terdapat 1 (satu) pertanyaan berstatus "Dalam Perencanaan/ Diterapkan Sebagian" yang tidak ditemukan bukti yang mendukung, maka status diturunkan menjadi "Dalam Perencanaan". Oleh karena itu, hasil akhir skor rata – rata pada

bagian pengelolaan risiko keamanan informasi bernilai 9 dengan persentase 12,5%.

c) Kerangka Kerja Pengelolaan Keamanan Informasi

Tingkat kematangan pada bagian kerangka kerja pengelolaan keamanan informasi yakni berada pada **Level I**. Skor yang dihasilkan bernilai 23 dengan persentase 14,4% dari skor maksimal sebesar 159 dengan uraian sebagai berikut:

- Tingkat kematangan II bernilai 11
- Tingkat kematangan III bernila 12
- Tingkat kematangan IV bernilai 0
- Tingkat kematangan V bernilai 0

konfirmasi data dengan menggunakan *checklist*, terdapat 3 (tiga) pertanyaan berstatus "Dalam Perencanaan/ Diterapkan Sebagian" yang tidak ditemukan bukti yang mendukung, maka status diturunkan menjadi "Dalam Perencanaan". Oleh karena itu, hasil akhir skor rata – rata pada bagian kerangka kerja pengelolaan keamanan informasi bernilai 20 dengan persentase 12,5%.

d) Pengelolaan Aset Informasi

Tingkat kematangan pada bagian pengelolaan aset informasi yakni berada pada **Level I+**. Skor yang dihasilkan bernilai 32 dengan persentase 19% dari skor maksimal sebesar 168 dengan uraian sebagai berikut:

- Tingkat kematangan II bernilai 32
- Tingkat kematangan III bernila 0

Berdasarkan konfirmasi data dengan menggunakan *checklist*, terdapat 4 (empat) pertanyaan berstatus "Dalam Perencanaan/ Diterapkan Sebagian" yang tidak ditemukan bukti yang mendukung, maka status diturunkan menjadi "Dalam Perencanaan". Oleh karena itu, hasil akhir skor rata – rata pada bagian pengelolaan aset keamanan informasi bernilai 28 dengan persentase 16,6%.

e) Teknologi Dan Keamanan Informasi

Tingkat kematangan pada bagian teknologi dan keamanan informasi yakni berada pada **Level I+**. Skor yang dihasilkan bernilai 27 dengan persentase 22,5% dari skor maksimal sebesar 120 dengan uraian sebagai berikut:

- Tingkat kematangan II bernilai 20
- Tingkat kematangan III bernilai 7
- Tingkat kematangan IV bernilai 0

Berdasarkan konfirmasi data dengan menggunakan *checklist*, seluruh pertanyaan yang ada pada area teknologi dan keamanan informasi terdapat buktinya. Oleh karena itu, hasil akhir skor rata – rata pada bagian teknologi dan keamanan informasi tetap bernilai 27 dengan persentase 22,5%.

4.5 Hasil Akhir Perhitungan Data Kuesioner

Berdasarkan hasil kuesioner yang telah diolah dan dilakukan verifikasi data, maka didapatkan hasil akhir Indeks KAMI pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto adalah sebagai berikut:

Gambar 4.4 Hasil Akhir *Radar Chart* Tingkat Kelengkapan Penerapan Keamanan Informasi

Gambar 4.4 menggambarkan hasil perubahan diagram radar setelah dilakukan verifikasi data. Terdapat penurunan pada setiap area kecuali pada bagian teknologi. Bagian tata kelola tetap menjadi yang paling mendekati diterapkannya kepatuhan ISO27001/SNI dan telah memenuhi kerangka kerja dasar.

Gambar 4.5 Hasil Akhir Tingkat Kelengkapan dan Kematangan Penerapan Keamanan Informasi

Hasil dari Gambar 4.5 dapat disimpulkan tingkat kelengkapan dan kematangan pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto adalah sebagai berikut:

a. Skor kategori sistem elektronik bernilai 17 yang artinya Dinas Komunikasi dan Informasi Kabupaten Mojokerto termasuk dalam kategori **Tinggi**.
b. Tingkat kelengkapan penerapan standar ISO27001 melihat dari skor sistem elektronik mendapatkan nilai 109, termasuk dalam kategori **Tidak Layak**, dan berada pada area berwarna **Merah**.
c. Area pengelolaan risiko dan kerangka kerja keamanan informasi mendapatkan skor di bawah rata – rata pada kondisi merah dan tidak layak. skor pengelolaan risiko bernilai 9 dengan minimum tingkat kematangan II adalah 14. Sedangkan pada kerangka kerja bernilai 10 pada tingkat kematangan II dengan nilai minimum seharusnya 15.
d. Tingkat Kematangan pada masing–masing area tidak terdapat perubahan.
   - Tata kelola mencapai tingkat kematangan **Level I+**;
   - Pengelolaan risiko mencapai tingkat kematangan **Level I**;
   - Kerangka kerja mencapai tingkat kematangan **Level I**;
   - Pengelolaan aset mencapai tingkat kematangan **Level I+**;
   - Aspek teknologi mencapai tingkat kematangan **Level I+**;

Tabel 4.11 Hasil Akhir Persentase Tingkat Kematangan Keamanan Informasi

Keterangan	Tata kelola	Pengelolaan Risiko	Kerangka kerja	Pengelolaan Aset	Teknologi
Nilai Maksimal	126	72	159	168	120
Nilai Responden	25	9	20	28	27
Persentase	19,8%	12,5%	12,5%	16,6%	22,5%

Pada Tabel 4.8, terdapat perbedaan persentase tingkat kematangan pada masing – masing area kecuali pada area teknologi. Tata kelola mengalami penurunan dari nilai responden 29 menjadi 25 dan persentase dari 23% menjadi 19,8%. Pengelolaan risiko mengalami penurunan dari nilai responden 10 menjadi 9 dan persentase dari 13,8% menjadi 12,5%. Kerangka kerja mengalami penurunan dari nilai responden 23 menjadi 20 dan persentase dari 14,4% menjadi 12,5%. Pengelolaan aset mengalami penurunan dari nilai responden 32 menjadi 28 dan persentase dari 19% menjadi 16,6%. Sedangkan teknologi tetap mendapatkan nilai responden 27 dan persentase 22,5%.

BAB 5 PEMBAHASAN

5.1 Analisis dan Rekomendasi Area Tata Kelola Keamanan Informasi

Area tata kelola keamanan informasi memiliki skor rata – rata 25 (19,8%) dari 126 skor maksimal dan berada pada tingkat kematangan Level I+. Hasil penilaian memberikan informasi tentang kondisi tata kelola keamanan informasi pada Dinas Komunikasi dan Informatika (Diskominfo) Kabupaten Mojokerto pada saat ini. Terdapat tiga belas rekomendasi pada setiap kondisi tata kelola keamanan informasi sesuai dengan ISO27001:2013 yang berupa tabel ditampilkan pada Lampiran E.

Berdasarkan hasil penelitian didapatkan bahwa dalam pelaksanaan keamanan informasi, pimpinan Diskominfo Kabupaten Mojokerto belum secara resmi bertanggungjawab terhadap pelaksanaan keamanan informasi. Pimpinan belum membuat rencana strategis bagaimana tujuan TI akan memberikan kontribusi pada tujuan organisasi dengan mengacu pada pembiayaan dan risiko TI terkait. Pada kontrol A.7.2.1 ISO27001 tertera bahwa manajemen sebaiknya mengharuskan semua pelaksana menerapkan keamanan informasi sesuai kebijakan dan prosedur organisasi. Maka dari kontrol tersebut, pimpinan sebaiknya memastikan kebijakan dan tujuan keamanan informasi kompatibel dengan arah strategis organisasi, serta memberikan arahan dan dukungan kepada seluruh anggota untuk ikut andil memberikan kontribusinya dalam menjalankan sistem manajemen keamanan informasi yang efektif.

Tanggung jawab pada setiap pelaksanaan keamanan informasi juga belum didefinisikan dengan spesifik, termasuk tugas dalam pengelolaan keamanan informasi dan pengawasan kepatuhannya. Pada Diskominfo Kabupaten Mojokerto belum ada bagian yang menjaga keamanan informasi secara disiplin sesuai peraturan. Maka rekomendasi yang harus dilakukan yakni membuat penentuan dan pengalokasian pembagian tanggung jawab. Pembagian tugas dilakukan untuk memastikan bahwa tanggungjawab dan wewenang tersebut relevan dengan keamanan informasi dan menyertakan panduan umum dalam pengalokasian peran dan tanggung jawab keamanan di dalam organisasi, seperti yang dijelaskan pada kontrol A.6.1.1 dalam ISO27001.

Pembagian peran pelaksana keamanan informasi juga belum dilakukan secara lengkap dan masih dalam tahap perencanaan, termasuk peran audit yang berfungsi untuk melakukan pemeriksaan seluruh transaksi. Seharusnya dilakukan proses pemisahan tugas dengan otoritas yang relevan seperti kontrol A.6.1.2 ISO27001. Tugas dan tanggungjawab harus dipisahkan untuk mengurangi kemungkinan risiko insiden keamanan, peluang modifikasi yang tidak sah, dan penyalahgunaan sistem dengan sengaja. Maka dari itu tanggung jawab antara ketua, anggota, dan satuan kerja terkait keamanan informasi seharusnya diurai dengan jelas.

Belum ada standar pelaksana pengelolaan keamanan informasi pada Diskominfo Kabupaten Mojokerto. Belum ditetapkannya persyaratan ukuran atau patokan pengetahuan dan keterampilan yang harus dimiliki oleh pelaksana pengelolaan keamanan informasi pada organisasi. Rekomendasi yang harus dilakukan adalah dengan membuat kebijakan standar atau persyaratan kompetensi dan keahlian pengelolaan keamanan sesuai kontrol A.5.1.1 ISO27001.

Pada Diskominfo Kabupaten Mojokerto, pelaksana pengamanan informasi belum sesuai dengan persyaratan/ standar keahlian dan kompetensi pengelolaan pengamanan informasi, sehingga perlu diadakannya proses verifikasi latar belakang terhadap seluruh anggota unit kerja supaya sesuai dengan kontrol A.7.1.1 pada ISO27001. Pemeriksaan verifikasi latar belakang pada pelaksana pengamanan informasi harus dilakukan agar sesuai dengan standar atau persyaratan, sehingga kompetensi dan keahlian sumber daya manusia pada organisasi relevan dan proporsional dengan persyaratan bisnis.

Program pelatihan dan pendidikan juga perlu dilakukan untuk meningkatkan pemahaman keamanan informasi. Pelatihan dapat berupa pendidikan tentang pengetahuan dan keterampilan yang dibutuhkan organisasi, sehingga menjadi kompeten dalam melaksanakan tugas sebagai pengelola sistem keamanan informasi. Dinas Komunikasi dan Informatika Kabupaten Mojokerto sebaiknya mengadakan pelatihan dan penyediaan SDM yang memadai sesuai standar yang relevan dan proporsional sesuai kontrol A.7.2.2 pada ISO27001. Seluruh pihak terkait pengelolaan keamanan informasi perlu mengikuti sosialisasi atau pelatihan keamanan informasi secara mendalam pada aspek teknis ataupun tata kelola TI untuk meningkatkan kompetensi dan keahlian setiap personil. Berbagai program pelatihan yang dapat dilakukan untuk melaksanakan pengamanan informasi antara lain pengenalan ISO27001, manajemen risiko, audit internal, dan jenis-jenis pelatihan bagi programmer.

Identitas atau data pribadi merupakan aset informasi yang sangat berisiko dalam penyalahgunaan akses sehingga dapat mengganggu kelancaran instansi, namun Diskominfo Kabupaten Mojokerto belum melakukan identifikasi data pribadi. Sesuai yang tertera pada kontrol A.18.1.4 dalam ISO27001, maka sebaiknya membuat standar identitas data pribadi dengan menyesuaikan peraturan yang disyaratkan dalam undang-undang. Privasi dan perlindungan informasi identitas pribadi harus dipastikan dengan menerapkan persyaratan dalam mengumpulkan, memproses, dan menyebarkan informasi pribadi, serta membatasi transfer data. Hal tersebut membutuhkan struktur manajemen dan mekanisme kontroi yang sesuai, salah satunya dengan menetapkan petugas pengamanan data yang membuat panduan manajemen tentang peraturan perlindungan data dan prosedur spesifik yang harus diikuti.

Koordinasi yang dilakukan Diskominfo Kabupaten Mojokerto dengan pihak eksternal masih menggunakan cara lisan. Salah satu bentuk koordinasi berupa kerjasama yang memerlukan pertukaran informasi penting bersangkutan dengan

database, maka disarankan adanya prosedur kesepakatan transfer informasi tertulis dengan pihak eksternal supaya hubungan tata kelola berjalan dengan jelas. Berdasarkan kontrol A.13.2.2 pada ISO27001, kesepakatan yang melibatkan pihak ketiga dalam pengelolaan informasi instansi harus didasari dengan suatu kontrak formal yang berisi acuan dan persyaratan keamanan untuk memastikan kesesuaian dengan kebijkan dan standar keamanan instansi.

Dalam pengambilan keputusan, permasalahan keamanan informasi belum digunakan sebagai bagian pengambilan keputusan, seperti halnya masalah belum adanya pemonitoran, pencatatan, atau pendokumentasian berapa banyak akses ilegal yang masuk. Apabila terjadi kebobolan sistem, Dinas Komunikasi dan Informatika baru mulai memperbaikinya. Sebagaimana yang dijelaskan dalam kontrol A.16.1.6 ISO27001, Diskominfo Kabupaten Mojokerto harus mempelajari setiap insiden keamanan yang terjadi dengan melakukan review kajian akar permasalahan. Kebijakan sebaiknya didokumentasi sebagai panduan untuk melindungi informasi dari berbagai ancaman keamanan informasi dan mengurangi dampak terjadinya insiden keamanan.

Proses pengukuran kinerja pengelolaan keamanan informasi belum dilakukan oleh Diskominfo Kabupaten Mojokerto, sehingga belum mengetahui seberapa tepat pegawai telah menjalankan fungsinya. Maka perlu dilakukan peninjauan kebijakan keamanan informasi secara berkala seperti pada kontrol A.5.1.2 pada ISO27001. Kebijakan untuk keamanan informasi perlu ditinjau dalam periode waktu yang ditentukan untuk memastikan kesesuaian, kecukupan, dan efektivitas berkelanjutan.

Dinas Komunikasi dan Informatika Kabupaten Mojokerto belum menerapkan sasaran pengelolaan, evaluasi rutin, dan langkah perbaikan keamanan informasi. Dengan begitu perlu adanya proses kontrol kontinunitas dengan memverifikasi, meninjau, dan mengevaluasi keberlanjutan keamanan informasi seperti kontrol A.17.1.3 dalam ISO27001. Proses evaluasi akan menghasilkan data terkait indeks kesiapan, kelengkapan, dan kematangan kerangka kerja keamanan informasi yang telah dijalankan oleh instansi, serta dapat menjadi pembanding untuk penyusunan ketetapan dan tahap perbaikan selanjutnya.

Pada Diskominfo Kabupaten Mojokerto belum melakukan analisis tingkat kepatuhan keamanan informasi, sehingga perlu dilakukan peninjauan dengan menganalisis dan menilai kepatuhan prosedur keamanan informasi sesuai legislasi atau standar. Manajer sebaiknya melakukan peninjauan secara berkala mengenai kepatuhan pengelolaan informasi terhadap kebijakan keamanan yang sesuai dengan standar dan persyaratan keamanan seperti kontrol A.18.2.2 pada ISO 27001.

Adapun untuk menanggapi insiden keamanan informasi, seperti halnya pembobolan sistem pada Diskominfo Kabupaten Mojokerto. Hal itu perlu diadakan prosedur untuk menentukan kebijakan dan prosedur penanggulangan insiden keamanan seperti dalam kontrol A.16.1.1 ISO27001. Dalam melakukan

pengelolaan kejadian keamanan informasi, harus ditentukan tanggungjawab manajemen dan prosedur – prosedur yang perlu ditentukan untuk memastikan penanganan yang tepat, cepat, serta efektif pada insiden keamanan informasi.

5.2 Analisis dan Rekomendasi Area Pengelolaan Risiko Keamanan Informasi

Area pengelolaan risiko keamanan informasi memiliki skor rata – rata 9 (12,5%) dari skor maksimal yang bernilai 72 dan berada pada tingkat kematangan Level I. Hasil penilaian memberikan informasi tentang kondisi pengelolaan risiko keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto pada saat ini. Terdapat delapan rekomendasi pada setiap kondisi pengelolaan risiko keamanan informasi sesuai dengan ISO27001:2013 yang ditampilkan berupa tabel pada Lampiran E.

Dinas Komunikasi dan Informatika Kabupaten Mojokerto belum memiliki kerangka kerja dan program untuk mengelola risiko keamanan informasi yang didokumentasikan secara resmi. Dalam melakukan pengelolaan kejadian keamanan informasi pada panduan penerapan SMKI tahun 2017, perlu dilakukan penilaian risiko keamanan informasi selama waktu yang ditentukan dan didokumentasikan untuk disimpan sebagai bukti implementasi standar manajemen keamanan informasi. Maka dari itu perlu adanya prosedur terdokumentasi untuk mengelola risiko insiden keamanan informasi sesuai kontrol A.16.1.5 pada ISO 27001.

Seperti yang dijelaskan pada ISO27001:2013, organisasi harus menyimpan informasi terdokumentasi tentang proses penilaian risiko keamanan informasi untuk dievaluasi dengan membandingkan hasil analisis risiko dengan kriteria risiko, serta menganalisis prioritas risiko untuk langkah pemulihan risiko. Namun, pada Diskominfo Kabupaten Mojokerto belum ada penanggung jawab dan pelaporan manajemen risiko, sehingga diperlukan penentuan tanggungjawab dan pelaporan manajemen risiko sesuai kontrol A.6.1.1 ISO27001. Menurut Sarno & Iffano (2009), bahwa pembagian tanggungjawab keamanan informasi harus ditetapkan dengan jelas, kebijakan keamanan informasi harus menyertakan panduan umum dalam pengalokasian peran dan tanggungjawab keamanan di dalam organisasi. Penanggungjawab bertugas untuk mencatat dan melaporkan manajemen risiko.

Kerangka kerja pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto belum termasuk definisi, hubungan aset, kerugian, dan ancaman. Ancaman dapat berupa akses yang yang tidak berwenang mengubah isi *website* dengan pesan yang merugikan. Maka kepemilikan aset yang tertulis pada daftar inventaris perlu didefinisikan sesuai kontrol A.8.1.2 dalam ISO27001. Semua aset yang berhubungan dengan fasilitas pemrosesan informasi harus didefinisikan dengan jelas siapa pemiliknya dan kepemilikan aset – aset harus dikontrol dan dipelihara sesuai dengan kebutuhan dan perkembangan organisasi. Pada

Panduan TIK 2017, sebuah ancaman dapat berpotensi memantik suatu kelemahan aset dan berdampak membahayakan instansi. Organisasi perlu mendefinisikan dengan cara mengidentifikasi jenis-jenis ancaman (*threat*) dan kelemahan (*vulnerability*) dari aset TI yang ada serta dampak (*impact*) jika ancaman yang diidentifikasi terjadi.

Dinas Komunikasi dan Informatika Kabupaten Mojokerto belum pula menetapkan ambang batas risiko. Ambang batas risiko sebagai alat manajemen untuk mengukur ketidakpastian dan dampak yang mungkin terjadi, sehingga dapat mengetahui apakah tingkatan risiko bisa diterima atau tidak. Sehingga diperlukan pencatatan dan pelaporan seluruh kelemahan seperti kontrol A.16.1.3 pada ISO 27001. Informasi terkait batasan – batasan risiko sistem informasi diperoleh dari evaluasi kelemahan dan diukur dengan tepat sehingga dapat mengetahui risiko tersebut. Pengelolaan kelemahan ini bertujuan untuk mengurangi risiko organisasi dari kelemahan – kelemahan yang dimiliki oleh sistem informasi organisasi sehingga dapat menetapkan ambang batas risiko.

Setiap ancaman dan kelemahan mengenai aset belum teridentifikasi. Beberapa jenis aset menurut Panduan Penerapan SMKi (2017) meliputi informasi, layanan, karyawan dengan keterampilan dan pengalamannya, *software*, *hardware*, dan barang yang tidak berwujud (*intangible*), misalnya citra dan reputasi. Sebaiknya Dinas Komunikasi dan Informatika Kabupaten Mojokerto mengidentifikasi inventaris aset – aset dalam bentuk SOP atau prosedur tertulis sesuai A.8.1.1 dalam ISO27001. Pengidentifikasian ancaman dan kelemahan aset dapat dilakukan dengan melakukan penilaian terhadap dampak (*impact*) dan risiko yang mungkin terjadi, mengidentifikasi kriteria penerimaan risiko, serta rencana penanggulangannya.

Belum ada penetapan dampak kerugian aset pada Diskominfo Kabupaten Mojokerto. Salah satu dampak terganggunya aset yakni penyusupan virus komputer menyebabkan data yang terkena virus tidak dapat digunakan kembali. Sehingga diperlukan prosedur penanganan aset seperti kontrol A.8.2.3 pada ISO27001. Klasifikasi informasi harus memperhitungkan kebutuhan bisnis untuk membagi atau membatasi informasi dan dampak bisnis yang berkaitan dengan kebutuhan, seperti kerusakan aset informasi (ISO27001:2009). Pengklasifikasian dampak kerugian aset dapat mempermudah penentuan penanganan dan perlindungannya.

Belum ada juga penyusunan langkah – langkah, pemantauan secara berkala, penyelesaian, dan pengkajian ulang mitigasi risiko. Maka diperlukan pembuatan dokumen mitigasi risiko mengenai aset instansi sesuai kontrol A.15.1.1 dalam ISO27001. Penyusunan dokumen mitigasi risiko disesuaikan dengan tingkatan prioritas, penanggungjawab, target penyelesaian, dan memastikan penggunaan sumber daya secara efektif sehingga dapat menurunkan tingkatan risiko sampai pada ambang batas yang dapat diterima dan mengurangi dampak pada operasional layanan TIK. Pemantauan mitigasi risiko selama periode berkala juga diperlukan untuk memantau kemajuan kerja atau penyelesaiannya, memastikan

konsistensi, dan efektifitasnya. Pengkajian risiko dapat dilakukan dengan mengidentifikasi aset, kelemahan, ancaman, dampak hilangnya kerahasiaan, keutuhan, dan ketersediaan informasi. Menurut penjelasan dalam ISO27001:2009, penilaian risiko (*Risk Assessment)* merupakan tahap awal dalam proses manajemen risiko yang bertujuan mengetahui potensi ancaman dari luar yang dapat mempengaruhi keamanan informasi sebuah instansi dan aspek kelemahan yang ada pada instansi. Hasil dari *risk assessment* berupa besaran risiko, rencana mitigasi atau pengurangan risiko, serta sebuah kontrol keamanan yang dapat diterapkan untuk mencegah risiko terjadi dan menangani risiko apabila terjadi.

Pengelolaan risiko belum menjadi bagian proses penilaian keefektifan pengamanan pada Diskominfo Kabupaten Malang. Pentingnya manajemen risiko menurut Sarno & Iffano (2009) adalah untuk mengetahui seberapa besar risiko atau dampak yang akan diterima oleh instansi apabila keamanan informasi gagal, memahamkan instansi mengenai kelemahan dan ancaman yang dapat menggagalkan keamanan informasi, mengetahui penanganan risiko kegagalan, serta dapat mengetahui kontrol keamanan yang diperlukan oleh instansi. Salah satu pengelolaan risiko yakni meliputi peletakan dan perlindungan peralatan untuk meminimalisir risiko dari ancaman dan bahaya sekitar, sesuai kontrol A.11.2.1 dalam ISO27001.

5.3 Analisis dan Rekomendasi Kerangka Kerja Pengelolaan Keamanan Informasi

Area kerangka kerja pengelolaan keamanan informasi memiliki nilai rata – rata 20 (12,5%) dari nilai maksimal sebesar 159 dan berada pada tingkat kematangan Level I. Hasil penilaian memberikan informasi tentang kondisi kerangka kerja pengelolaan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto pada saat ini. Terdapat lima belas (15) rekomendasi kerangka kerja pengelolaan keamanan informasi sesuai dengan ISO27001:2013 yang ditampilkan berupa tabel pada Lampiran E.

Diskominfo Kabupaten Mojokerto belum mengadakan mekanisme pengelolaan kebijakan dan prosedur yang menggambarkan kebutuhan mitigasi, rekomendasi pertama yakni dengan membuat mekanisme pengelolaan kebijakan dan prosedur keamanan informasi yang mencerminkan kebutuhan mitigasi seperti pada kontrol A.5.1.1 dalam ISO27001:2013. Pada ISO 27001:2009, penetapan kebijakan standar manajemen keamanan informasi sebaiknya disesuaikan dengan karakteristik organisasi, lokasi, aset, serta teknologi yang sesuai kerangka kerja, mencakup pertimbangan persyaratan bisnis dan hukum, selaras dengan manajemen risiko, menetapkan kriteria yang dievaluasi, serta disetujui oleh manajemen, sehingga dapat menghasilkan prinsip, sasaran, dan arahan keseluruhan tindakan untuk kedepannya.

Selain itu Diskominfo Kabupaten Mojokerto belum melakukan identifikasi kondisi yang membahayakan. Menurut Panduan Penerapan SMKI (2017), kondisi yang membahayakan dapat berupa suatu atau serangkaian kejadian terkait keamanan informasi yang dapat menjadi ancaman dan peluang untuk melemahkan keamanan informasi pada operasi bisnis. Ancaman dapat diidentifikasikan berupa ancaman alam, lingkungan, atau manusia. Rekomendasi kedua yakni dengan menilai atau mengidentifikasi kejadian keamanan informasi apakah akan diklasifikasikan sebagai insiden keamanan informasi, seperti kontrol A.6.1.4 pada ISO27001. Salan satu cara pemantauan dan pengkajian SMKI adalah dengan mendeteksi secara cepat kejadian atau kesalahan hasil pengolahan dan menanggapinya, serta mengidentifikasi terhadap upaya pelanggaran (ISO27001:2009).

Pada kontrak dengan pihak ketiga, belum terdapat aspek keamanan informasi. Beberapa hal yang perlu dipertimbangkan untuk membuat kontrak dengan pihak ketiga yakni meliputi kebijakan umum keamanan informasi, pelaporan insiden, tanggungjawab menjaga kerahasiaan aset, hak atas kekayaan intelektual (HAKI), peraturan hak cipta, perlindungan pada setiap perjanjian kerjasama, tata tertib penggunaan dan perlindungan aset, serta perjanjian kontrol akses. Maka perlu membuat kesepakatan atau perjanjian tercantum pada kontrak dengan pihak ketiga sesuai kontrol A.13.2.2 pada ISO27001. Sarno & Iffano (2009) menjelaskan bahwa peraturan yang melibatkan akses pihak ketiga ke fasilitas pemrosesan informasi organisasi harus didasarkan pada kontrak formal yang berisi persyaratan keamanan untuk memastikan kesesuaian dengan kebijakan dan standar keamanan organisasi.

Belum ada konsekuensi terhadap pelanggaran kebijakan keamanan informasi pada Diskominfo Kabupaten Mojokerto. Kebijakan keamanan informasi berperan untuk mengurangi risiko atau pelanggaran meliputi penyalahgunaan sumber daya dan fasilitas yang disediakan instansi untuk memanajemen pengelolaan data dan informasi, pelanggaran hak cipta (HAKI), pelanggaran hak akses pengguna yang memiliki wewenang, insiden yang dapat menyebabkan hilangnya data penting, atau menyebabkan tersebarnya informasi yang rahasia (Indrajit, 2012). Maka perlu menetapkan proses pendisiplinan dengan membuat prosedur resmi untuk menindaklanjuti konsekuensi, seperti pada kontrol A.7.2.3 instansi sebaiknya mengontrol dan dapat mengendaliikan perubahan yang mungkin terjadi serta memberikan tinjauan konsekuensi dalam menghadapi perubahan yang tak diinginkan. Di samping itu pendisiplinan bermanfaat mendidik pegawai untuk mematuhi dan menyenangi peraturan, prosedur, maupun kebijakan yang ada, sehingga dapat menghasilkan kinerja yang baik (Rahmah & Fatmah, 2019).

Diskominfo Kabupaten Mojokerto belum menerapkan prosedur operasional untuk mengelola pemasangan baru. Kontrol yang perlu diperhatikan pada sistem yang baru dipasang meliputi pengelolaan implementasi, tanggungjawab memonitor memastikan pemasangan, dan melaporkannya. Maka dari itu perlu adanya prosedur untuk mengontrol pemasangan baru sebagaimana kontrol

A.12.5.1 pada ISO27001. Dalam pemasangan perangkat lunak pada sistem operasional, menurut Sarno & Iffano (2009) manajer sebaiknya menentukan syarat dan kriteria untuk menerima sistem baru dengan ketentuan yang telah disetujui, jelas, terdokumentasi, serta diuji.

Evaluasi risiko pada sistem baru belum dilakukan, sehingga perlu adanya pengujian pada sistem baru untuk menanggulangi permasalahan yang muncul sesuai kontrol A.14.2.9 pada ISO27001. Evaluasi risiko merupakan proses untuk membandingkan risiko yang telah diperkirakan terhadap ketetapan kriteria risiko sehingga dapat menghasilkan signifikasi risiko (ISO Guide 73:2002). Evaluasi risiko ini diperlukan untuk mengevaluasi dampak bisnis instansi yang mungkin berasal dari kegagalan keamanan, ancaman, kelemahan, dan dampak dari pengendalian aset, maka hal yang dapat dilakukan yakni memperkirakan peringkat risiko dan menetapkan apakah risiko dapat diterima atau diperlukan perlakuan dengan risiko lain.

Berdasarkan hasil penilaian, proses pengembangan sistem yang aman (*secure SDLC*) belum diterapkan. Proses pengembangan sistem akan menjadi aman dengan membuat kebijakan terkait pengembangan perangkat lunak yang aman sesuai standar *platform* teknologi yang digunakan, seperti pada kontrol A.14.2.1 ISO27001:2013 tentang kebijakan pembangunan yang aman. Berpedoman pada panduan umum TKTI tahun 2007, pengembangan *software* aplikasi dilakukan berdasarkan metodologi *System Development Life Cycle* (SDLC) yang dipergunakan secara luas oleh industri *software*, minimal meliputi kebutuhan persyaratan bisnis dalam spesifikasi desain, penyusunan detail *software* aplikasi termasuk pengendaliannya, implementasi desain detail pada kode program, manajemen perubahan persyaratan, pelaksanaan penjaminan mutu, uji coba, serta perlakukan instalasi dan akreditasi.

Penerapan suatu sistem dapat mengakibatkan timbulnya risiko, namun Dinas Komunikasi dan Informatika Kabupaten Mojokerto belum mengadakan proses penanggulangan terhadap penerapan tersebut, maka perlu dilakukan peninjauan dan pengujian untuk memastikan dampak perubahan operasi sistem sesuai kontrol A.14.2.3 pada ISO27001. Saat perubahan atau penerapan suatu sistem terjadi sistem aplikasi harus dikaji ulang dan diuji untuk memastikan tidak ada dampak ekstrim atau mengakibatkan timbulnya risiko baru serta terjadinya ketidakpatuhan terhadap kebijakan. Timbulnya risiko dapat berupa gangguan terhadap jalannya proses bisnis atau dapat menghentikannya.

Belum tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK pada saat situasi yang merugikan. Perencanaan kelangsungan layanan TIK atau *business continuity planning* adalah perencanaan yang menjamin bahwa fungsi – fungsi bisnis kritis organisasi tetap bisa berjalan jika terjadi bencana (Sarno & Iffano, 2009). Perencanaan kelangsungan layanan TIK bisa gagal pula karena asumsi yang salah, melewati batas, dan perubahan terhadap personil atau peralatan. Maka perlu membuat rencana keberlanjutan

keamanan informasi pada kelangsungan layanan TIK sesuai kontrol A.17.1.1 ISO27001.

Diskominfo Kabupaten Mojokerto belum merencanakan uji coba perencanaan pemulihan bencana terhadap layanan TIK dan menganalisis hasilnya sebagai bagian rencana kerja, maka dari itu perlu menyelesaikan dan menganalisa insiden keamanan informasi untuk mengurangi terjadinya lagi di masa depan sesuai kontrol A.16.1.6 ISO27001 Sarno & Iffano (2009) mengemukakan bahwa organisasi harus mempelajari setiap kejadian keamanan yang terjadi, melakukan review dan mempelajarinya termasuk tipe, volume, dan biaya dari kejadian keamanan informasi yang dapat dihitung dan dimonitor. Analisis risiko tersebut dilakukan sebagai bagian dari rencana kerja organisasi.

Belum melakukan evaluasi hasil perencanaan pemulihan bencana untuk menerapkan langkah perbaikan, sehingga Dinas Komunikasi dan Informatika Kabupaten Mojokerto perlu memverifikasi kontrol secara berkala untuk memastikan keefektifan dalam perbaikan sesuai kontrol A.17.1.3 pada ISO27001. Perencanaan pemulihan bencana atau *disaster recovery plan* adalah perencanaan untuk menyiapkan organisasi dalam mengambil atau menentukan langkah apa yang dilakukan jika terjadi bencana serta pemulihannya (Sarno & Iffano, 2009). Perlu dilakukan pengkajian secara berkala dalam perencanaan kelangsungan bisnis untuk memastikan keberlanjutan yang efektif selama situasi yang merugikan.

Proses audit internal belum dilaksanakan oleh Diskominfo Kabupaten Mojokerto, belum ada evaluasi sebagai langkah mengidentifikasi pencegahan dan pembenahan. Sehingga perlu melakukan auditing internal untuk mengevaluasi keamanan informasi seperti kontrol A.12.7.1 ISO27001. Sebaiknya audit dilakukan pada interval waktu yang direncanakan. Hasil pengukuran efektivitas kontrol dan laporan audit internal juga dievaluasi untuk diperiksa mana kontrol yang belum mencapai sasaran, masih lemah (belum efektif) atau yang masih menjadi temuan dalam audit internal (Panduan Penerapan SMKI, 2017).

Audit internal keamanan informasi belum dilaporkan kepada pimpinan. Kontrol audit sistem informasi perlu memperhatikan kebutuhan auditnya harus disetujui dengan persetujuan manajemen, cakupan pemeriksaan harus disetujui dan dikontrol, pemeriksaan harus dibatasi, semua akses harus terpantau dan tercatat, serta semua prosedur, kebutuhan, dan tanggungjawab harus didokumentasi. sebaiknya membuat laporan keamanan informasi melalui saluran manajemen yang tepat secepat mungkin sesuai kontrol A.16.1.2 pada ISO27001. Menurut Sarno & Iffano (2009) seluruh temuan dan dugaan apapun terkait keamanan dalam sistem atau layanan seharusnya disyaratkan untuk dicatat dan dilaporkan. Hasil audit internal tersebut perlu dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi.

Belum ada prosedur untuk menganalisa pengelolaan perubahan. Prosedur kontrol perubahan sistem perlu dilakukan untuk menganalisis aspek finansial termasuk dampak keperluan anggaran terhadap perubahan infrastruktur dan pengelolaannya. Sebaiknya Diskominfo Kabupaten Mojokerto membuat SOP atau prosedur penilaian perubahan untuk menerapkannya, yakni dengan membuat prosedur kontrol perubahan secara formal sesuai A.14.2.2 pada ISO27001. Proses yang dilakukan meliputi pemeliharaan catatan tingkat otorisasi yang disetujui, memastikan perubahan diajukan oleh pengguna yang berhak, memastikan bahwa prosedur yang diubah atau direvisi tidak menjadi rawan, serta memastikan pengguna yang terkait menerima perubahan sebelum implementasi.

Pengujian dan evaluasi kepatuhan keamanan informasi belum dilakukan secara periodik. Melakukan evaluasi secara berkala pada implementasi TIK dilakukan untuk memastikan keselarasan dengan rencana semula. Panduan Penerapan SMKI (2017) menerangkan bahwa status dan perkembangan kegiatan implementasi sistem manajemen keamanan informasi seharusnya dikomunikasikan secara berkala kepada pimpinan agar setiap permasalahan yang membutuhkan pengambilan keputusan pimpinan dapat diselesaikan secara cepat dan tepat, termasuk langkah pembenahan yang diperlukan. Oleh karena itu perlu membuat kebijakan untuk peninjauan pada jangka waktu berkala untuk memastikan keefektifan keamanan informasi seperti kontrol A.5.1.2 ISO2701.

5.4 Analisis dan Rekomendasi Pengelolaan Aset Informasi

Area pengelolaan aset informasi memiliki nilai rata – rata 28 (16,6%) dari nilai maksimal sebesar 168 dan berada pada tingkat kematangan Level I+. Hasil penilaian memberikan Informasi tentang kondisi pengelolaan aset informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto pada saat ini. Terdapat dua puluh empat rekomendasi dalam bidang pengelolaan aset informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto yang ditampilkan berupa tabel pada Lampiran E.

Berdasarkan hasil dari penilaian kuesioner Indeks KAMI ditemukan belum tersedianya definisi klasifikasi aset informasi. Aset terkait sistem informasi yakni aset informasi seperti database dan file, aset piranti lunak seperti piranti lunak aplikasi, aset fisik seperti peralatan komputer, dan layanan seperti perlengkapan umum. Rekomendasi pertama untuk Diskominfo Kabupaten Mojokerto adalah dengan mengidentifikasikan terkait informasi aset sesuai kontrol A.8.1.1 terkait Inventarisasi aset pada ISO 27001. Inventarisasi aset dapat membantu menjamin keefektifan perlindungan aset untuk tujuan bisnis. Setiap aset harus diidentifikasi secara jelas, kepemilikan serta klasifikasi keamanannya harus disepakati dan didokumentasikan sebagai catatan jika terjadi kehilangan atau kerugian aset.

Belum ada proses evaluasi dan pengklasifikasian sesuai tingkat kepentingan aset. Pengklasifikasian dilakukan dengan melabeli informasi sesuai keperluan pengkategorian aset dan keperluan pengamanannya. Hal tersebut dapat

dilakukan dengan melakukan penandaan informasi sesuai klasifikasi informasi seperti kontrol A.8.2.2 pada ISO27001. Penting adanya satu set prosedur yang baik untuk menentukan pemberian tanda dan penanganan informasi sesuai dengan skema klasifikasi yang digunakan oleh organisasi. Kemudian prosedur untuk menangani aset perlu diimplementasikan dan dikembangkan sesuai dengan klasifikasi informasi yang diadopsi oleh organisasi.

Proses pengelolaan perubahan pada proses bisnis, sistem, serta proses teknologi informasi belum tersedia, sehingga perlu pengontrolan perubahan proses bisnis pada organisasi sesuai kontrol A.12.1.2 ISO27001. Perubahan baik yang direncanakan atau muncul sesuai kebutuhan harus dipertimbangkan dan dikaji konsekuensinya terhadap SMKI. Karena perubahan organisasi, proses bisnis, fasilitas pemrosesan informasi dan sistem dapat mempengaruhi keamanan informasi, maka perlu diadakannya pengontrolan. Sarno & Iffano (2009) mengemukakan beberapa yang perlu diperhatikan pada perubahan sistem, yakni perlu mencatat, mengidentifikasi, dan menilai dampak perubahan penting yang terjadi, mensosialisasikan detail perubahan, serta membuat prosedur persetujuan dan prosedur pengidentifikasian tanggungjawab terhadap kegagalan perubahan yang mungkin terjadi.

Diskominfo Kabupaten Mojokerto belum melakukan proses pengelolaan konfigurasi secara konsisten, maka sebaiknya perlu mengontrol pengelolaan sistem operasional sesuai kontrol A.12.5.1 pada ISO27001. Prosedur harus dilaksanakan untuk mengontrol pemasangan perangkat lunak pada sistem operasional. Pengelolaan konfigurasi dapat dilakukan dengan melakukan langkah – langkah dalam membuat, menguji, dan menjalankan sistem. Proses pengelolaan konfigurasi terhadap aset TIK harus dilakukan secara konsisten untuk meminimalisir kerusakan sistem informasi.

Belum tersedia pula proses untuk merilis aset baru pada Diskominfo Kabupaten Mojokerto, rekomendasi selanjutnya yakni dapat membuat standar persyaratan untuk sistem baru atau penyempurnaan seperti kontrol A.14.1.1 ISO27001 terkait analisis dan spesifikasi kebutuhan keamanan informasi. Persyaratan kebutuhan bisnis untuk sistem yang baru harus menjelaskan kebutuhan keamanan sistem informasi (Sarno & Iffano, 2009). Sebelum merilis suatu aset baru, kebutuhan keamanan dan kontrolnya harus mencerminkan nilai bisnis dari aset informasi. Menganalisis kebutuhan keamanan dan mengidentfikasi kontrol agar memenuhi kebutuhan dapat dilakukan dengan penghitungan risiko dan manajemen risiko.

Pendefinisian tanggungjawab pengamanan informasi belum dilakukan pada semua personil di instansi, sehingga Dinas Komunikasi dan Informatika Kabupaten Mojokerto sebaiknya memberikan ketentuan dan pengalokasian peran serta tanggung jawab pada sumber daya seperti yang tertera dalam kontrol A.6.1.1 ISO27001. Tanggung jawab dan wewenang setiap personil perlu didefinisikan untuk peran yang relevan dengan keamanan informasi, hal tersebut harus ditugaskan dan dikomunikasikan pada semua personil di instansi.

Tata tertib penggunaan aset juga belum ada, maka sebaiknya membuat prosedur tata tertib penggunaan aset sesuai kontrol A.8.1.3 pada ISO 27001. Berdasarkan Panduan Penerapan SMKI (2017), terdapat beberapa jenis aset, meliputi informasi, *software*, *hardware*, layanan, orang beserta ketrampilan dan pengalamannya, dan barang tak berwujud (*intangible*). Tata tertib dapat diterapkan dengan memberi panduan tentang tata cara penggunaan komputer, internet dan email yang diijinkan, menjelaskan hal-hal yang dilarang, mencegah agar penggunaan komputer, internet, email dan sumber daya terkait lainnya tidak menimbulkan risiko yang dapat mengganggu operasional proses kerja.

Peraturan terkait instalasi perangkat lunak belum tersedia, maka sebaiknya membuat peraturan pemasangan perangkat lunak seperti pada kontrol A.12.6.2 ISO27001. Sarno & Iffano (2009) menjelaskan hal yang perlu dikontrol dalam penginstalan piranti lunak pada sistem operasi yakni pemutakhiran program hanya dilakukan oleh seorang manajemen yang ditunjuk dengan otorisasi yang memadai. Catatan audit atas semua perubahan terhadap program operasional harus dipelihara dan versi lama dari perangkat lunak harus disimpan sebagai tindakan berjaga – jaga kemungkinan keadaan darurat.

Peraturan atau prosedur penggunaan data pribadi dan akses serta langkah pembenahannya juga belum tersedia, maka Diskominfo Kabupaten Mojokerto perlu menyediakan akses pengguna formal untuk menetapkan / mencabut hak akses dan membuat prosedur penggunaan akses sesuai kontrol A.9.2.2 pada ISO27001. Berdasarkan Panduan Penerapan SMKI (2011), pengguna hak akses perlu dibatasi dengan dasar tugas dan fungsi (tupoksi) yang diberikan pada akses fisik (seperti ruangan) maupun non-fisik. Peraturan akses sebaiknya diberikan secukupnya untuk memenuhi kebutuhan pengguna.

Prosedur pengelolaan akses sudah dijalankan namun belum secara tertulis. Sesuai Panduan Penerapan SMKI (2017), hak akses dibatasi masa berlakunya, dicatat, dimonitor penggunaannya dan direview secara berkala untuk memastikan agar apabila telah berakhir masa tugasnya, hak akses dapat dinonaktifkan. Maka Dinas Komunikasi dan Informatika Kabupaten Mojokerto sebaiknya membuat kebijakan atau prosedur kontrol akses sesuai kontrol A.9.1.1 pada ISO27001. Kebijakan kontrol akses harus ditetapkan dan perlu didokumentasikan.

Ketetapan waktu penyimpanan klasifikasi data dan syarat penghancuran data juga belum dilaksanakan, sehingga perlu dibuat ketetapan atau instruksi waktu penyimpanan dan penghancuran data sesuai kontrol A.9.2.6 pada ISO 27001. Belum ada pula prosedur untuk menghancurkan data yang sudah tidak digunakan lagi, maka perlu membuat prosedur pembuangan data seperti kontrol A.8.3.2 pada ISO27001. Media sistem informasi jika sudah tidak digunakan harus dibuang secara aman dan tidak berbahaya (Sarno & Iffano, 2009). Media atau data yang berisikan informasi penting atau sensitif sebaiknya dirawat dengan cara menyimpan dan membuangnya dengan aman tanpa menimbulkan bahaya, serta tidak melakukan pemotongan, penghancuran, atau pengosongan data.

Data yang membutuhkan pembuangan secara aman meliputi dokumen cetak, rekaman, tape, disket atau kaset, data pengujian, dokumentasi sistem, dan sebagainya.

Ketika terjadi insiden kegagalan, Dinas Komunikasi dan Informatika Kabupaten Mojokerto belum melakukan langkah – langkah penyidikan untuk menanganinya, maka perlu adanya penetapan prosedur untuk mengidentifikasi dan mengumpulkan bukti seperti kontrol A.16.1.7 pada ISO27001. Menurut Sarno & Iffano (2009), Setiap terjadi insiden keamanan, seluruh bukti perlu didata dan dikumpulkan guna untuk melakukan tindakan lanjutan terkait kegagalan keamanan informasi. Setelah menyelesaikan insiden, perlu ada tindakan serta melibatkan pihak legal untuk menanganinya.

Keamanan fisik belum ditentukan berdasarkan zona waktu dan klasifikasi aset. Klasifikasi aset dengan pihak ketiga perlu dibatasi waktunya dan dicatat sesuai keperluan yang telah disetujui bersama atau dapat berupa sebuah kontrak. Sebaiknya merancang perlindungan fisik dan menentukan batasan keamanan seperti pada kontrol A.11.1.1 ISO27001. Perlu diperhatikan untuk vendor, konsultan, mitra, atau pihak ketiga lainnya yang melakukan akses fisik ke dalam aset Dinas Komunikasi dan Informatika Kabupaten Mojokerto harus menandatangani ketentuan/ persyaratan dalam menjaga kerahasiaan informasi.

Proses pengecekan latar belakang sumber daya manusia belum dilakukan oleh Diskominfo Kabupaten Mojokerto. Pemeriksaan tersebut meliputi ketersediaan referensi kelayakan karakter, kelengkapan, dan keakuratan data diri pelamar, serta bukti akademis dan kualifikasi profesi. Rekomendasi selanjutnya yakni memeriksa dan memverifikasi latar belakang SDM sesuai kontrol A.7.1.1 ISO27001. Proses pengecekan latar belakang ini sebaiknya dilakukan pada saat lamaran kerja.

Proses pelaporan insiden pada pihak yang berwajib juga belum dilakukan, maka sebaiknya melakukan proses pelaporan keamanan informasi pada tingkatan manajemen seperti kontrol A.16.1.2 ISO27001. Proses pelaporan dapat dilakukan tindak lanjutnya kepada pihak legal (baik sipil maupun kriminal) sebagai bentuk penanganan apabila terjadi insiden meliputi ketersediaan layanan, perubahan informasi, serta gangguan penyusupan dari pihak yang tidak berwenang. Pada pelaksanaannya harus ditentukan penanggungjawab manajemennya dan prosedur yang mendukung manajemen kejadian untuk memastikan penanganan kejadian keamanan informasi dilakukan secara cepat dan efektif.

Diskominfo Kabupaten Mojokerto belum mengadakan prosedur bagi user yang kontraknya sudah habis atau mutasi, sehingga perlu membuat prosedur hak akses data informasi pada saat pemutusan kontrak atau masa kerja seperti kontrol A.9.2.6 pada ISO27001 terkait penghapusan atau penyesuaian hak akses. Berdasarkan Panduan Penerapan SMKI (2017), jika user menjalani mutasi atau tidak lagi bekerja pada suatu instansi, maka hak aksesnya perlu segera

dinonaktifkan maksimum 2 (dua) hari setelah SK Mutasi atau SK tentang berhenti bekerja ditetapkan. Seluruh hak akses user perlu direview secara berkala sekitar enam bulan sekali untuk memastikan bahwa hak akses user yang sudah berhenti masa kerjanya atau mutasi benar – benar sudah tidak diberlakukan.

Tersedia data yang harus di-*backup* namun tidak tersedia laporannya, sebaiknya harus ada laporan penyalinan cadangan informasi sesuai kontrol A.12.3.1 ISO27001. Seluruh informasi, sistem, dan perangkat lunak yang sudah disalin sebaiknya dicadangkan secara teratur sesuai kebijakan pencadangan yang telah disepakati oleh instansi. Diperlukan adanya laporan untuk menganalisis kepatuhan terhadap prosedur, seperti analisa keteraturan pencadangan.

Belum melakukan perekaman kegiatan keamanan informasi dan belum tersedia pengamanan rekaman. Rekaman merupakan dokumen yang berisi bukti aktivitas yang telah terjadi dan pernyataan hasil yang tercapai (Panduan Penerapan SMKI, 2011). Maka perlu membuat peraturan perlindungan rekaman seperti kontrol A.18.1.3 ISO27001 terkait perlindungan rekaman. Bentuk pengamanan dapat dilakukan dengan membuat panduan penyimpanan dan pemusnahan rekaman data dan informasi tersebut, membatasi penyimpanan untuk mengidentifikasi jenis arsip penting yang perlu dijaga, serta mengontrol perlindungan rekaman dari kehilangan, kerusakan, dan pemalsuan.

Belum ada prosedur pengolahan informasi dan pengamanan pengiriman aset milik pihak ketiga. Dalam Panduan Penerapan SMKI (2017), kebijakan keamanan informasi sebaiknya didistribusikan melalui media komunikasi kepada seluruh karyawan dan pihak ketiga agar mudah dipahami dan dipatuhi. Maka perlu membuat kesepakatan transfer atau pengiriman informasi yang aman antara organisasi dan pihak eksternal seperti pada kontrol A.13.2.2 dalam ISO27001. Seluruh koneksi dengan pihak ketiga harus dibatasi sesuai yang kesepakatan.

Belum ada juga peraturan untuk mengamankan perangkat komputasi apabila digunakan di luar lingkungan kantor, maka sebaiknya menerapkan keamanan peralatan dan aset di luar lokasi resmi (kantor) sesuai A.11.2.6 ISO27001 terkait keamanan peralatan dan aset di luar lokasi. Sesuai Panduan Penerapan SMKI (2017), penggunaan perangkat komputasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto harus mendapat sosialisasi tentang risiko penggunaan sumber daya TI dan menjaga keamanan perangkat komputasi saat digunakan di luar kantor.

Dinas Komunikasi dan Informatika Kabupaten Mojokerto belum menetapkan peraturan pemindahan aset TIK dari lokasi yang ditetapkan, aset TIK meliputi piranti lunak, perangkat keras, data, informasi, dan sebagainya. Disarankan menerapkan peraturan pada aset untuk tidak boleh ke luar lokasi tanpa izin sesuai kontrol A.11.2.5 pada ISO27001. Aset TIK tidak boleh digunakan di luar lingkungan resmi tanpa izin sebelumnya. Apabila diperlukan, peralatan harus didaftar kembali pada saat dikembalikan. Pemeriksaan mendadak dapat dilakukan untuk mendeteksi pemindahan barang tanpa izin.

Belum melakukan pemeriksaan dan perawatan perangkat komputasi, fasilitas pendukung, dan standar kelayakan keamanan lingkungan kerja, sebaiknya melakukan proses pemeliharaan peralatan seperti kontrol A.11.2.4 pada ISO27001. Peralatan sebaiknya dijaga dengan baik sebagai bentuk pemeliharaan untuk memastikan ketersediaan barang dan keberlanjutannya. Menurut Sarno & Iffano (2009), yang perlu dilakukan untuk pemeliharaan peralatan yakni dengan melakukan pemeliharaan peralatan sesuai jadwal *service*, hanya personil tertentu yang dapat melakukan perbaikan, dan membuat catatan dari semua dugaan atau kerusakan.

Adapun belum terdefinisikannya peraturan untuk mengamankan lokasi kerja khusus dari risiko yang dapat membahayakan aset informasi, maka perlu melakukan proses penempatan dan perlindungan peralatan sesuai kontrol A.11.2.1 pada ISO27001 terkait penempatan dan perlindungan peralatan. Langkah yang harus dilakukan Diskominfo Kabupaten Mojokerto adalah menempatkan serta melindungi lokasi kerja penting guna mengurangi risiko kerusakan, ancaman dari lingkungan sekitar, serta kemungkinan penyusupan akses yang tidak sah.

5.5 Analisis dan Rekomendasi Teknologi dan Keamanan Informasi

Area teknologi dan keamanan informasi memiliki skor rata – rata 27 (22,5%) dari nilai maksimal sebesar 120 dan berada pada tingkat kematangan Level I+. Hasil penilaian memberikan informasi tentang kondisi teknologi dan keamanan informasi pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto pada saat ini dengan empat belas rekomendasi sesuai kontrol ISO27001:2013 yang ditampilkan berupa tabel pada Lampiran E.

Berdasarkan hasil penelitian, rekomendasi yang perlu diberikan sebab belum tersedia konfigurasi standar keamanan sistem pada Diskominfo Kabupaten Mojokerto adalah dengan menetapkan kebijakan kontrol akses terkait konfigurasi keamanan sistem sesuai pada kontrol A.9.1.1 ISO27001. Berdasarkan Panduan Umum TKTI (2007), setiap institusi pemerintahan harus memiliki perencanaan arsitektur infrastruktur teknologi. Perencanaan tersebut berguna untuk memastikan infrastruktur teknologi yang digunakan organisasi termasuk topologi, konfigurasi, dan spesifikasi infrastruktur teknologi beserta pendekatannya selalu sesuai dengan kebutuhan.

Analisis kepatuhan penerapan konfigurasi terhadap standar yang ada belum dilakukan, maka sebaiknya melakukan proses peninjauan kepatuhan secara berkala seperti pada A.18.2.3 ISO27001. Sistem informasi perlu ditinjau secara berkala untuk memastikan kepatuhan terhadap standar dan kebijakan keamanan informasi yang diterapkan oleh organisasi. Menurut Sarno & Iffano (2009), sistem informasi harus diperiksa secara berkala atas kesesuaiannya dengan standar implementasi keamanan.

Sistem, aplikasi, serta jaringan belum dipindai secara berkala, maka perlu dilakukan proses peninjauan sistem, aplikasi, serta jaringan secara rutin berkaca pada kontrol A.5.1.2 ISO27001. Peninjauan ulang merupakan langkah antisipasi terhadap suatu perubahan yang dapat menimbulkan pengaruh pada analisis risiko. Apabila perubahan terjadi secara signifikan, maka peninjauan tersebut berguna untuk memastikan kecukupan, kesesuaian, serta efektivitas berkelanjutan.

Keseluruhan infrastruktur belum dirancang untuk memastikan ketersediaan sesuai kebutuhan, Diskominfo Kabupaten Mojokerto perlu melakukan pemrosesan informasi dengan redundansi yang cukup untuk memenuhi ketersediaan sesuai kontrol A.17.2.1 pada ISO27001. Pada Panduan Umum TKTI (2007), dijelaskan bahwa perlu adanya mekanisme untuk menghindari kemungkinan terjadinya tumpang tindih (*redundancy*) TI. Melakukan rencana belanja/ investasi sesuai kebutuhan TIK pada organisasi dapat dilakukan untuk memastikan tidak terjadinya redundansi TIK.

Belum melakukan analisis secara berkala pada semua *log activity*, maka perlu dilakukan peninjauan secara berkala pada *log* seperti kontrol A.12.4.1 ISO27001 terkait pencatatan kejadian. Pencatatan data aktivitas pengguna dan kejadian keamanan harus dibuat dan disimpan untuk suatu periode tertentu sesuai perjanjian agar dapat dimanfaatkan untuk penelitian lanjutan, monitoring akses, dan audit. Dalam memanfaatkan pemrosesan informasi perlu adanya prosedur dan pengkajian ulang secara regular terhadap hasil monitoring aktifitas.

Dinas Komunikasi dan Informatika Kabupaten Mojokerto belum mempunyai standar dalam menggunakan enkripsi, sebaiknya membuat standar atau kebijakan penggunaan kontrol enkripsi sesuai kontrol A.10.1.1 pada ISO27001. Kebijakan mengenai penggunaan kontrol kriptografi perlu diterapkan untuk memaksimalkan manfaat dan meminimalisir risiko terhadap implementasi teknik kriptografi (Sarno & Iffano, 2009). Dalam membangun kebijakan, manajemen penggunaan kontrol kriptografi pada organisasi harus dilindungi, dan melakukan pemulihan terhadap informasi yang dienkripsi apabila terjadi kehilangan, penyalahgunaan, atau kerusakan kunci kriptografi.

Pengamanan untuk mengelola kunci enkripsi belum diterapkan, sebaiknya Dinas Komunikasi dan Informatika Kabupaten Mojokerto menerapkan kebijakan pengelolaan kunci enkripsi seperti pada kontrol A.10.1.2 pada ISO27001. Kebijakan mengenai penggunaan, perlindungan, dan waktu pemakaian kunci kriptografi harus dikembangkan dan diterapkan. Penyusunan kebijakan dengan menghasilkan kunci untuk beragam kriptografi dan aplikasi, pendistribusian kunci kepada pengguna dengan memberikan cara pengaktifannya, penyimpanan kunci kepada pihak yang memiliki wewenang untuk mengakses, serta memperbarui kunci dengan membuat peraturan kapan kunci harus diubah.

Sistem belum secara otomatis mendukung dan menerapkan manajemen penggunaan password, maka perlu melakukan manajemen kata sandi seperti

kontrol A.9.4.3 pada ISO27001. Sesuai Panduan Penerapan SMKI (2017), ketika pertama kali mendapatkan hak akses sebaiknya pengguna segera merubah kata sandi *default* yang telah diberikan. Kata sandi perlu diubah dalam waktu berkala dan ketika diduga telah diketahui oleh orang lain.

Belum menggunakan pengamanan khusus berlapis untuk mengelola sistem. Pengamanan dapat dilakukan dengan melakukan pembatasan penggunaan sistem hingga minimum penggunaan yang dipercaya dan diizinkan, proses pencatatan penggunaan fasilitas sistem, serta menetapkan dan mendokumentasikan tingkatan otorisasi. Sebaiknya Dinas Komunikasi dan Informatika Kabupaten Mojokerto melakukan pengamanan khusus dengan membatasi akses dan mengontrol dengan ketat sesuai kontrol A.9.4.4 ISO27001.

Pembatasan waktu akses dan pemantauan keamanan dalam mencegah dan mendeteksi penggunaan akses jaringan secara tidak resmi belum diterapkan, maka sebaiknya melakukan pembatasan akses seperti kontrol A.9.4.1 ISO27001. Fasilitas *timeout* dilakukan dengan menutup layar terminal dan menutup seluruh aplikasi dan *network* setelah periode pemberhentian ditentukan (Sarno & Iffano, 2009). Pembatasan dengan mematikan setelah periode waktu tanpa aktivitas yang ditentukan untuk mencegah akses pihak tanpa otorisasi.

Diskominfo Kabupaten Mojokerto belum melakukan analisis *malware* secara rutin dan langkah untuk tindaklajutnya. Sebaikya dilakukan pengecekan terhadap berkas yang diterima melalui email untuk memastikan bahwa berkas file tersebut aman dan tidak mengandung virus. Bisa jadi sebuah email dengan lampiran yang terinfeksi sebuah virus dikirim oleh penyerang, sehingga ketika membuka lampiran otomatis menyebabkan koneksi ke server eksternal dan menyebabkan kebocoran informasi. Maka disarankan melakukan kontrol malware sesuai kontrol A.12.2.1 pada ISO27001. Berdasarkan Panduan Penerapan SMKI (2017), seluruh komputer harus dipasang *software* antivirus dan diupdate secara berkala. Setiap pembukaan file harus dilakukan dengan *scanning software* antivirus terlebih dahulu.

Pelaksanaan uji coba dan pengembangan pada Diskominfo Kabupaten Mojokerto belum melibatkan fungsi dan spesifikasi keamanan yang terverifikasi, maka perlu membuat persyaratan terkait spesifikasi keamanan sesuai kontrol A.14.1.1 pada ISO27001. Persyaratan kebutuhan bisnis untuk sistem yang baru atau peningkatan sistem harus menjelaskan kebutuhan keamanan sistem informasi agar terverifikasi saat proses pengembangan.

Pengamanan terhadap area pengujian dan pengembangan belum dilakukan sesuai standar oleh Diskominfo Kabupaten Mojokerto, maka perlu melakukan pemisahan lingkungan pengembangan, pengujian, dan lingkungan operasional sesuai kontrol A.12.1.4 pada ISO27001. Pemisahan lingkungan operasional, uji coba, dan pengembangan perlu dilakukan pemisahan untuk mengurangi terjadinya dampak risiko apabila muncul perubahan operasional ataupun hak

akses yang tidak sah. Kegiatan pengembagan dan pengujian harus dipisahkan sejauh mungkin untuk mencegah akses pengembangan yang tidak tepat.

Dinas Komunikasi dan Informatika Kabupaten Mojokerto belum secara rutin mengkaji kehandalan keamanan informasi dengan melibatkan pihak independen, maka sebaiknya dilakukan peninjauan independen secara rutin seperti kontrol A.18.2.1 ISO27001. Mengkaji ulang keamanan informasi dengan cara independen diperlukan untuk memastikan bahwa keamanan informasi tersebut layak, efektif, serta mencerminkan kebijakan yang baik.

BAB 6 PENUTUP

6.1 Simpulan

Berdasarkan hasil penelitian yang dilakukan pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto, dapat disimpulkan bahwa:

1. Tingkat kelengkapan dan kematangan keamanan informasi Dinas Komunikasi dan Informatika Kabupaten Mojokerto masih tergolong rendah, dikarenakan hasil skor sistem elektronik bernilai 17 dan berada pada status kesiapan tidak layak. Tingkat kelengkapan yang digambarkan pada diagram *bar chart* menunjukkan bahwa Diskominfo Kabupaten Mojokerto berada pada warna merah dengan skor 109, hal itu berarti keamanan informasi pada Diskominfo Kabupaten Mojokerto butuh perbaikan. Tingkat kematangan setiap area keamanan informasi berada pada level I hingga level I+.
2. Sesuai dengan analisis dari kuesioner Indeks KAMI, hasil yang didapat menunjukkan beberapa kontrol ISO 27001:2013 yang belum terpenuhi berdasarkan masing – masing area keamanan informasi pada Indeks KAMI. Sehingga perlu dilakukan rekomendasi sesuai kontrol ISO 27001:2013, pada area tata kelola keamanan informasi antara lain kontrol A.5.1, A.6.1, A.7.1, A.7.2, A.13.2, A.16.1, A.17.1, A.18.1 dan A.18.2; area pengelolaan risiko keamanan informasi antara lain kontrol A.6.1, A.8.1, A.8.2, A.11.2, A.15.1, dan A.16.1; area kerangka kerja keamanan informasi antara lain kontrol A.5.1, A.7.2, A.12.5, A.12.7, A.13.2, A.14.2, A.16.1, dan A.17.1; area pengelolaan aset informasi antara lain kontrol A.6.1, A.7.1, A.8.1, A.8.2, A.8.3, A.9.1, A.9.2, A.11.1, A.11.2, A.12.1, A.12.3, A.12.5, A.12.6, A.13.2, A.14.1, dan A.16.1; serta area teknologi dan keamanan informasi antara lain kontrol 5.1, 9.1, 9.4, 10.1, 12.1, 12.2, 12.4, 14.1, 17.2, dan 18.2.

6.2 Saran

Saran dari hasil penelitian ini untuk penelitian selanjutnya yakni sebagai berikut:

1. Hasil rekomendasi dari penelitian ini dapat diimplementasikan dan dilanjutkan dengan membuat kebijakan dan pengendalian pada Dinas Komunikasi dan Informatika Kabupaten Mojokerto sesuai kebutuhan yang diperlukan.
2. Bagi penelitian selanjutnya, disarankan untuk membuat kebijakan dan prosedur organisasi mengenai keamanan sistem menggunakan kerangka kerja ITIL versi 4 model praktik *IT asset management*.

DAFTAR REFERENSI

Bagian Komunikasi Publik, 2016. *Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks KAMI Bagi Pemerintah Daerah Provinsi*. [online] Badan Siber dan Sandi Negara. Tersedia di: <https://bssn.go.id/penerapan-sistem-manajemen-keamanan-informasi-berbasis-indeks-kami-bagi-pemerintah-daerah-provinsi> [Diakses 12 Oktober 2019]

Basyarahil, F. A., Astuti, H. M., & Hidayanto, B. C., 2017. *Evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi (KAMI) berdasarkan ISO/IEC 27001: 2013 pada direktorat pengembangan teknologi dan sistem informasi (DPTSI) ITS Surabaya*. Jurnal Teknik ITS, 6(1), 116-121.

Cronhoim, S., & Goldkunl, G., 2003. *Strategies for information systems evaluation-six generic types*. Electronic Journal of Information Systems Evaluation, 6(2), 65-74.

Fatmah, D., 2020. *Mastery of information technology and organizational learning culture impact on job performance in education institute sabilillah east java*. Sinergi: Jurnal Ilmiah Ilmu Manajemen, 10(1).

Indrajit, R. E., 2012. *Kebijakan keamanan informasi*. [e-journal] Tersedia di: < https://www.academia.edu/14326531/Kebijakan_Keamanan_Informasi > [Diakses 23 Januari 2020]

Kepala Dinas Komunikasi dan Informatika Kabupaten Mojokerto, 2019. *Perubahan renstra dinas komunikasi dan informatika kabupaten mojokerto tahun 2016-2021*. Mojokerto: Dinas Komunikasi dan Informatika Kabupaten Mojokerto.

Lenawati, M., & Winarno, W. W., 2016. *Tata kelola keamanan informasi pada PDAM menggunakan ISO/IEC 27001: 2013 dan Cobit 5*. Speed-Sentra Penelitian Engineering dan Edukasi, 9(1).

Menteri Komunikasi dan Informatika Republik Indonesia, 2007. *Panduan umum tata kelola teknologi informasi dan komunikasi nasional*. Jakarta: Departemen Komunikasi dan Informatika Republik Indonesia.

Michael, L. & Smith, J. E., 2005. *Role & responsibility charting (RACI) Project Management Forum*.

Octaviani, S., Suprapto, S., & Herlambang, A. 2019. *Evaluasi Kesiapan Kerangka Kerja Keamanan Informasi Pada Dinas Komunikasi dan informatika Kota Batu Dengan Menggunakan Indeks KAMI*. Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 3, no. 3, p. 2741-2745.

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Jakarta: Menteri Komunikasi dan Informatika Republik Indonesia.

Purnama, C., 2016. *Sistem informasi manajemen*. Mojokerto: Penerbit Insan Global.

Purnama, C., & Subroto, W. T., 2016. *Competition intensity, uncertainty environmental on the use of information technology ana its impact on business performance small and medium enterprises (SMEs)*. International Review of Management and Marketing, 6(4).

Putra, E. L., Hidayanto, B. C., & Astuti, H. M., 2014. *Evaluasi keamanan informasi pada divisi network of broadband PT. Telekomunikasi Indonesia Tbk. dengan menggunakan indeks keamanan informasi (KAMI)*. Jurnal Teknik ITS, 3(2), A228-A233.

Putri, S. W., 2008. *Pembangunan disaster recovery plan untuk sistem informasimanajemen terintegrasi ITB*. Tugas Akhir.

Rahmah, M., & Fatmah, D., 2019. *Organizational culture and intrapreneurship employee of the impact on work discipline of employees in brangkal offset*. Jurnal Ilmu Manajemen dan Bisnis, 10(1), 1-8.

Sarno, R., & Iffano, I., 2009. *Sistem manajemen keamanan informasi*. Surabaya: ITSPress.

Saputra, A., 2018. *Rancangan tata kelola organisasi sistem manajemen keamanan informasi dinas komunikasi dan informatika kabupaten bekasi (organization governance design of information security management system bekasi communications and information technology agency)*. Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi, 20(1), 17-29.

Siga, M., Susanto, T. D., & Hidayanto, B. C., 2014. *Evaluasi keamanan informasi menggunakan indeks keamanan informasi pada kantor wilayah ditjen perbendaharaan negara jawa timur*. SESINDO 2014, 2014.

Soenardi, I., & Ichsan, M., 2013. *Analisis kematangan sistem manajemen keamanan informasi badan pendidikan dan pelatihan keuangan diukur menggunakan indeks keamanan informasi*. Jakarta: Badan Pendidikan dan Pelatihan Keuangan.

Solehudin, U., 2005. *Business continuity and disaster recovery plan*. Universitas Indonesia. Page 12. Vol . X Nomor 29 Juli 2015 - Jurnal Teknologi Informasi

Stoneburner, G., Goguen, A., & Feringa, A., 2002. *Risk management guide for information technology systems*. Nist special publication, 800(30), 800-30.

Sugiyono, 2017. *Metode penelitian kuantitatif, kualitatif dan R & D*. Bandung: Alfabet

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.

Yuliad, B., & Nugroho, A., 2016. *Rancangan disaster recovery pada instansi pendidikan studi kasus universitas mercu buana*. Jurnal Teknik Informatika, 9(1).

LAMPIRAN A TRANSKRIP WAWANCARA

NAMA OPD	:	Dinas Komunikasi dan Informasi Kabupaten Mojokerto
HARI/TANGGAL WAWANCARA	:	Senin, 16 September 2019
JAM WAWANCARA	:	09.00 – 10.00 WIB
NAMA RESPONDEN	:	Diding Adi Parwoto, S.Kom., M.Eng
JABATAN RESONDEN	:	Kepala Seksi Sistem Informasi Bidang Informatika

1	**Pertanyaan:**
	Apakah kendala yang dihadapi Dinas Komunikasi dan Informatika Kabupaten Mojokerto saat ini dalam melakukan manajemen teknologi informasi?
	Jawaban:
	Kendala terdapat pada infrastruktur yang belum sepenuhnya siap, servernya masih kurang. Jaringan *Fiber Optic* (FO) belum sepenuhnya menjangkau seluruh Organisasi Perangkat Daerah (OPD), masih yang di lingkup kompleks saja, sehingga OPD yang di luar belum. Untuk sistem informasnya, Kepala OPD masih belum terlalu peduli.

2	**Pertanyaan:**
	Apakah Dinas Komunikasi dan Informatika Kabupaten Mojokerto pernah dilakukan evaluasi secara khusus terhadap tata kelola keamanan informasi?
	Jawaban:
	Hanya evaluasi SPBE dengan nilai 1.7, padahal standart minimal nilai maturity adalah 1,8. Jadi nilai untuk Dinas Komunikasi dan Informatika Kabupaten Mojokerto masih terbilang kurang, berada di bawah rata – rata.

3	**Pertanyaan:**
	Sesuai dengan dilakukannya penilaian SPBE, bagian manakah di dalam organisasi yang akan dinilai?
	Jawaban:
	Dinilai keseluruhan.

4	**Pertanyaan:**
	Bagaimana tindakan pencegahan untuk melindungi teknologi dari malware?
	Jawaban:
	Dalam segi infrastruktur, sudah beberapa kali membeli perangkat *firewall* dengan menggunakan standart Diskominfo yakni php, ci, atau larafel. Namun terkadang OPD membuat sistem dari vendor luar. Pembuatan sistem dari vendor luar berbeda dengan yang sudah ada di Diskominfo, saat dilihat ternyata masih ada cacatnya dan tidak sesuai, maka harus disesuaikan dengan standart Diskominfo terlebih dahulu.

5	**Pertanyaan:**
	Apakah Dinas Komunikasi dan Informatika Kabupaten Mojokerto sudah mengelola jaringan dan keamanan konektivitas?
	Jawaban:
	Untuk pengelolaan jaringan sudah mulai bertahap.

6	**Pertanyaan:**
	Apakah Dinas Komunikasi dan Informatika sudah memastikan semua pengguna memiliki hak akses sesuai kebutuhan masing-masing?
	Jawaban:
	Dalam hal ini sudah mulai dibangun, hak akses sistem *Single Sign On* (SSO) dan hirarki kini masih dalam proses pembangunan.

7	**Pertanyaan:**
	Bagaimanan Dinas Komunikasi dan Informatika Kabupaten Mojokerto memonitor infrastruktur teknologi informasi (TI) dari akses yang tidak sah?
	Jawaban:
	Belum ada pemonitoran, belum mencatatat atau mendokumentasikan berapa banyak akses ilegal yang masuk, hanya apabila terjadi kebobolan sistem baru diperbaiki. Salah satunya hak akses ilegal berupa perubahan tampilan pada web Diskominfo Kabupaten Mojokerto.

8	**Pertanyaan:**
	Apakah proses kerja dan hasil dari mengelola keamanan sistem didokumentasikan?
	Jawaban:
	Ya didokumentasikan.

9	**Pertanyaan:**
	Apakah terdapat *Standart Operational Procedure* (SOP) untuk mengatur semua prosedur pengelolaan keamanan sistem?
	Jawaban:
	Belum terdapat *Standart Operational Procedure* (SOP) untuk mengatur semua prosedur pengelolaan keamanan sistem, perkiraan akhir tahun 2019 akan mulai membuat SOP.

LAMPIRAN B KUESIONER

Bagian I: Kategori Sistem Elektronik

Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan

[Kategori Sistem Elektronik] Rendah, Tinggi, Strategis		**Status**
#	**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	C
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar	C
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus	C
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	C
1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	C
1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi	C
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa	C

1.8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang tidak berdampak bagi kepentingan orang banyak	C
1.9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 provinsi atau lebih [C] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 kabupaten/kota atau lebih	C
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan merugikan finansial)	C

Bagian II: Tata Kelola Keamanan Informasi

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

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Fungsi/Instansi Keamanan Informasi**	
2.1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Tidak Dilakukan
2.2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Tidak Dilakukan
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Tidak Dilakukan
2.6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan
2.7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Tidak Dilakukan
2.8	II	1	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	Tidak Dilakukan
2.9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan

2.10	II	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Tidak Dilakukan
2.11	II	2	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan
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?	Tidak Dilakukan
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?	Tidak Dilakukan
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?	Tidak Dilakukan
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	Tidak Dilakukan
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	Tidak Dilakukan
2.17	IV	3	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?	Tidak Dilakukan
2.18	IV	3	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanaanya, pemantauannya dan eskalasi pelaporannya?	Tidak Dilakukan

2.19	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Tidak Dilakukan
2.20	IV	3	Apakah Instansi 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?	Tidak Dilakukan
2.21	IV	3	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Tidak Dilakukan
2.22	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Tidak Dilakukan

Bagian III: Pengelolaan Risiko Keamanan Informasi

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

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh

#			Kajian Risiko Keamanan Informasi	Status
3.1	II	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan
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?	Tidak Dilakukan
3.3	II	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Tidak Dilakukan
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?	Tidak Dilakukan
3.5	II	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	Tidak Dilakukan

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?	Tidak Dilakukan
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Tidak Dilakukan
3.8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	Tidak Dilakukan
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)?	Tidak Dilakukan
3.10	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Tidak Dilakukan
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?	Tidak Dilakukan
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	Tidak Dilakukan
3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?	Tidak Dilakukan
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?	Tidak Dilakukan
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Tidak Dilakukan
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	Tidak Dilakukan

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi

Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.

#			**[Penilaian]** Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh	**Status**
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 tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?	Tidak Dilakukan
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?	Tidak Dilakukan
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?	Tidak Dilakukan
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?	Tidak Dilakukan
4.5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan Instansi?	Tidak Dilakukan
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?	Tidak Dilakukan
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?	Tidak Dilakukan
4.8	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Tidak Dilakukan

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?	Tidak Dilakukan
4.10	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch,* alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?	Tidak Dilakukan
4.11	III	2	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?	Tidak Dilakukan
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?	Tidak Dilakukan
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?	Tidak Dilakukan
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 kontrol*) dan jadwal penyelesaiannya?	Tidak Dilakukan
4.15	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?	Tidak Dilakukan
4.16	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	Tidak Dilakukan
4.17	III	3	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	Tidak Dilakukan

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?	Tidak Dilakukan
4.19	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	Tidak Dilakukan
#	**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?	Tidak Dilakukan
4.21	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	Tidak Dilakukan
4.22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Tidak Dilakukan
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)?	Tidak Dilakukan
4.24	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	Tidak Dilakukan
4.25	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?	Tidak Dilakukan
4.26	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	Tidak Dilakukan
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?	Tidak Dilakukan

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?	Tidak Dilakukan
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?	Tidak Dilakukan

Bagian V: Pengelolaan Aset Informasi

Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#			**Pengelolaan Aset Informasi**	
5.1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terperlinara ? (termasuk kepemilikan aset)	Tidak Dilakukan
5.2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Tidak Dilakukan
5.3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?	Tidak Dilakukan
5.4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix 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?	Tidak Dilakukan
5.6	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Tidak Dilakukan
5.7	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?	Tidak Dilakukan
			Apakah Instansi anda memiliki dan menerapkan perangkat 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 anda	Tidak Dilakukan
5.9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet	Tidak Dilakukan
5.10	II	1	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	Tidak Dilakukan
5.11	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi	Tidak Dilakukan
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	Tidak Dilakukan
5.14	II	1	Persyaratan dan prosedur pengelolaan /pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Tidak Dilakukan
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	Tidak Dilakukan
5.17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Tidak Dilakukan
5.18	II	1	Prosedur *back-up* dan ujicoba pengembalian data (*restore*) secara berkala	Tidak Dilakukan
5.19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Tidak Dilakukan
5.20	III	2	Proses pengecekan latar belakang SDM	Tidak Dilakukan
5.21	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	Tidak Dilakukan
5.22	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan	Tidak Dilakukan
5.23	III	2	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya (*user access rights*) berikut langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku	Tidak Dilakukan
5.24	III	2	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.	Tidak Dilakukan

5.25	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Tidak Dilakukan
5.26	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	Tidak Dilakukan
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?	Tidak Dilakukan
#	**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?	Tidak Dilakukan
5.29	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Tidak Dilakukan
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?	Tidak Dilakukan
5.31	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Tidak Dilakukan
5.32	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?	Tidak Dilakukan
5.33	II	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (dalam daftar inventaris)	Tidak Dilakukan
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?	Tidak Dilakukan
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?	Tidak Dilakukan
5.36	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	Tidak Dilakukan

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)	Tidak Dilakukan
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	Tidak Dilakukan

Bagian VI: Teknologi dan Keamanan informasi

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

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh				**Status**
#	**Pengamanan Teknologi**			
6.1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Tidak Dilakukan
6.2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	Tidak Dilakukan
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?	Tidak Dilakukan
6.4	II	1	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	Tidak Dilakukan
6.5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/ketuhan konfigurasi?	Tidak Dilakukan
6.6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?	Tidak Dilakukan

6.7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Tidak Dilakukan
6.8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Tidak Dilakukan
6.9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	Tidak Dilakukan
6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Tidak Dilakukan
6.11	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Tidak Dilakukan
6.12	III	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?	Tidak Dilakukan
6.13	III	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	Tidak Dilakukan
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?	Tidak Dilakukan
6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	Tidak Dilakukan
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?	Tidak Dilakukan
6.17	III	2	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?	Tidak Dilakukan
6.18	II	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Tidak Dilakukan
6.19	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Tidak Dilakukan
6.20	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Tidak Dilakukan

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?	Tidak Dilakukan
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?	Tidak Dilakukan
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Tidak Dilakukan
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 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?	Tidak Dilakukan
6.26	IV	3	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	Tidak Dilakukan

LAMPIRAN C CHECKLIST

Bagian II: Tata Kelola Keamanan Informasi				Status	Bukti		Keterangan
#	Fungsi/Instansi Keamanan Informasi				Ada	Tidak	
2.10	II	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Dalam Penerapan / Diterapkan Sebagian	√		Dokumen Rencana Strategis (RENSTRA)
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?	Dalam Penerapan / Diterapkan Sebagian		√	Belum ada SOP
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?	Dalam Penerapan / Diterapkan Sebagian	√		Perbup Tupoksi No. 69 Tahun 2016
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi secara rutin dan resmi?	Dalam Penerapan / Diterapkan Sebagian	√		Perbup Tupoksi No. 69 Tahun 2016

2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	Dalam Penerapan / Diterapkan Sebagian		√	Belum ada SOP
Bagian III: Pengelolaan Risiko Keamanan Informasi				**Status**	**Bukti**		**Keterangan**
#			**Kajian Risiko Keamanan**	**Informasi**	**Ada**	**Tidak**	
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	√		Arsip Inventaris Server dan Aplikasi
3.7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	Dalam Penerapan / Diterapkan Sebagian		√	Belum ada SOP
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 Penerapan / Diterapkan Sebagian	√		Dokumen Rencana Strategis (RENSTRA)
3.10	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	Dalam Penerapan / Diterapkan Sebagian	√		Dokumen Rencana Strategis (RENSTRA)

3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	Dalam Penerapan / Diterapkan Sebagian	√		Perbup Tupoksi No. 69 Tahun 2016
Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi				**Status**	**Bukti**		**Keterangan**
#			**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**		**Ada**	**Tidak**	
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		√	-
4,12	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	Dalam Penerapan / Diterapkan Sebagian		√	-
#			**Pengelolaan Strategi dan Program Keamanan Informasi**				
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 Penerapan / Diterapkan Sebagian	√		Peraturan Bupati SPBE No. 80 Tahun 2018
4.22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?	Dalam Penerapan / Diterapkan Sebagian	√		Dokumen Rencana Kerja (RENJA)

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 Penerapan / Diterapkan Sebagian	√	-
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 Penerapan / Diterapkan Sebagian	√	Dokumen Rencana Strategis (RENSTRA)
Bagian V: Pengelolaan Aset Informasi				**Status**	**Bukti**	**Keterangan**
#			**Pengelolaan Aset Informasi**		**Ada**	**Tidak**
5,1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terperlihara ? (termasuk kepemilikan aset)	Diterapkan Secara Menyeluruh	√	Dokumen Inventaris dan Aplikasi
5,4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut	Dalam Penerapan / Diterapkan Sebagian	√	Hak akses berbeda
			Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?			

5.14	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	Dalam Penerapan / Diterapkan Sebagian		√	Rencana pembuatan SOP
5.16	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	Dalam Penerapan / Diterapkan Sebagian	√		Peraturan Bupati SPBE No. 80 Tahun 2018
5.17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	Dalam Penerapan / Diterapkan Sebagian		√	SOP beum ada
5.18	II	1	Prosedur *back-up* dan ujicoba pengembalian data (*restore*) secara berkala	Diterapkan Secara Menyeluruh	√		Dokumen Rencana Strategis (RENSTRA)
5.19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	Dalam Penerapan / Diterapkan Sebagian		√	-
5.25	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	Dalam Penerapan / Diterapkan Sebagian		√	Tersedia infrastrukturnya, tidak ada laporan
#	**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 Penerapan / Diterapkan Sebagian	√		Finger print
5.29	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	Diterapkan Secara Menyeluruh	√		Terdapat finger print dan username password

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?	Diterapkan Secara Menyeluruh	√		Terdapat pengatur temperature dan suhu
5.31	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	Dalam Penerapan / Diterapkan Sebagian	√		Terdapat UPS dan Jenset
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 Penerapan / Diterapkan Sebagian	√		Terdapat semua kecuali asap
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?	Dalam Penerapan / Diterapkan Sebagian	√		Terdapat finger print dan username password
Bagian VI: Teknologi dan Keamanan Informasi				**Status**	**Bukti**		**Keterangan**
#			**Pengamanan Teknologi**		**Ada**	**Tidak**	
6,1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Dalam Penerapan / Diterapkan Sebagian	√		2 firewall
6,2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, dll)?	Dalam Penerapan / Diterapkan Sebagian	√		Topologi Network

6,7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Dalam Penerapan / Diterapkan Sebagian	√		Aplikasi Memonitor Jaringan
6,8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	Dalam Penerapan / Diterapkan Sebagian	√		Terdapat log semua database
6.11	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	Dalam Penerapan / Diterapkan Sebagian	√		Terdapat username dan password
6.18	II	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	Dalam Penerapan / Diterapkan Sebagian	√		Terdapat firewall dan enkripsi
6.19	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	Dalam Penerapan / Diterapkan Sebagian	√		Windows 10
6.20	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	Dalam Penerapan / Diterapkan Sebagian	√		Windows defender dan antivirus
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	Dalam Penerapan / Diterapkan Sebagian	√		Sesuai dengan akses internet

LAMPIRAN D BUKTI CHECKLIST

DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN MOJOKERTO
JL. KH HASYIM ASHARI NOMOR 12 MOJOKERTO Telp. 0321 391268

Dokumen Rencana Strategis (RENSTRA) Dinas Komunikasi dan Informatik Kabupaten Mojokerto

BUPATI MOJOKERTO
PROVINSI JAWA TIMUR

PERATURAN BUPATI MOJOKERTO
NOMOR 69 TAHUN 2016
TENTANG
KEDUDUKAN, SUSUNAN ORGANISASI, TUGAS DAN FUNGSI SERTA TATA KERJA DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN MOJOKERTO

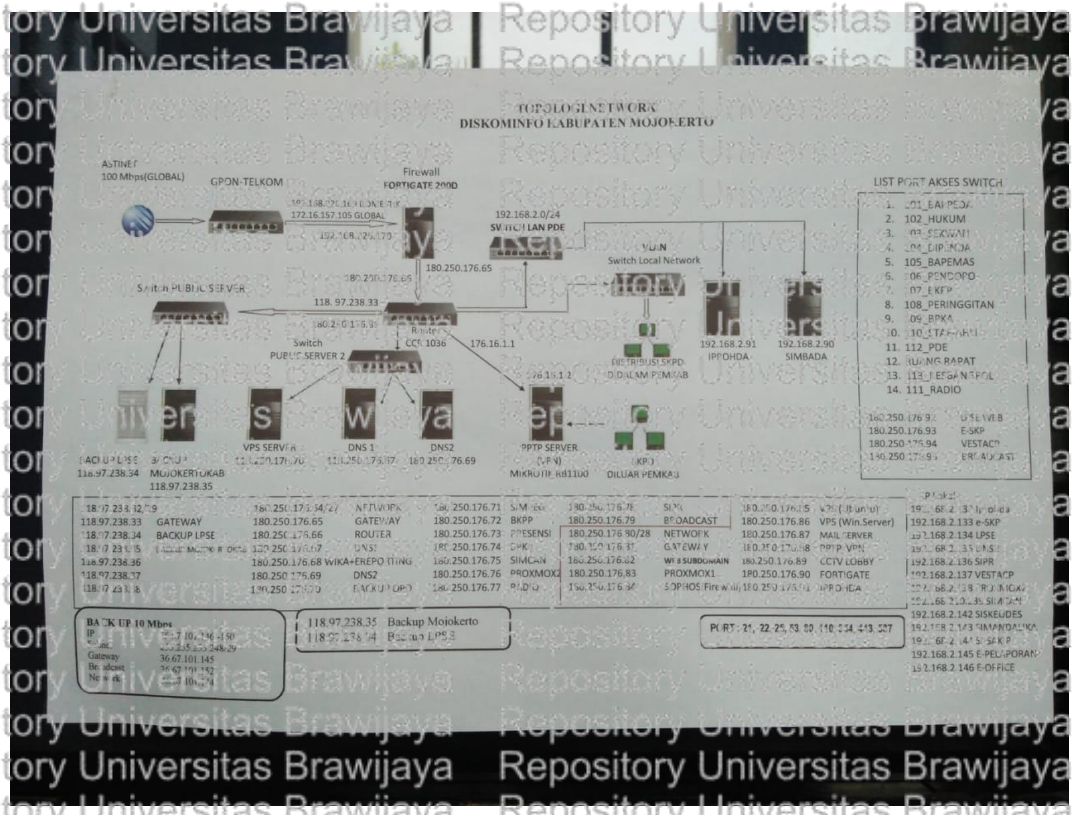
DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MOJOKERTO,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 9 Peraturan Daerah Kabupaten Mojokerto Nomor 9 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Mojokerto, maka perlu menetapkan Peraturan Bupati tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi serta Tata Kerja Dinas Komunikasi dan Informatika Kabupaten Mojokerto;

Mengingat : 1. Undang-Undang Nomor 12 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Jawa Timur juncto Undang-Undang Nomor 2 Tahun 1965 tentang Perubahan Batas Wilayah Kotapraja Surabaya dan Daerah Tingkat II Surabaya (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 19, Tambahan Lembaran Negara Republik Indonesia Nomor 2730);
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);

Peraturan Bupati (Perbup) Mojokerto No 69 2016



Topologi Network Diskominfo Kabupaten Mojokerto

BUPATI MOJOKERTO
PROVINSI JAWA TIMUR

PERATURAN BUPATI MOJOKERTO
NOMOR 80 TAHUN 2018
TENTANG
PENYELENGGARAAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MOJOKERTO,

Menimbang : a. bahwa keterbukaan informasi publik sebagaimana dimaksud dalam Peraturan Presiden Nomor 95 Tahun 2018 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik, merupakan sarana dalam mengoptimalkan pengawasan publik terhadap penyelenggaraan negara dan Badan Publik lainnya serta segala sesuatu yang berakibat pada kepentingan publik;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a perlu menetapkan Peraturan Bupati tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik;

Mengingat : 1. Undang-Undang Nomor 2 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Jawa Timur (Berita Negara Republik Indonesia Tahun 1950 Nomor 41) sebagaimana telah diubah dengan Undang-Undang Nomor 2 Tahun 1965 (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 19, Tambahan Lembaran Negara Republik Indonesia Nomor 2730);

2. Undang-Undang Nomor 28 Tahun 1999 tentang Penyelenggaraan Negara yang Bersih dan Bebas dari Korupsi, Kolusi dan Nepotisme (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 75, Tambahan Lembaran Negara Republik Indonesia Nomor 3851);

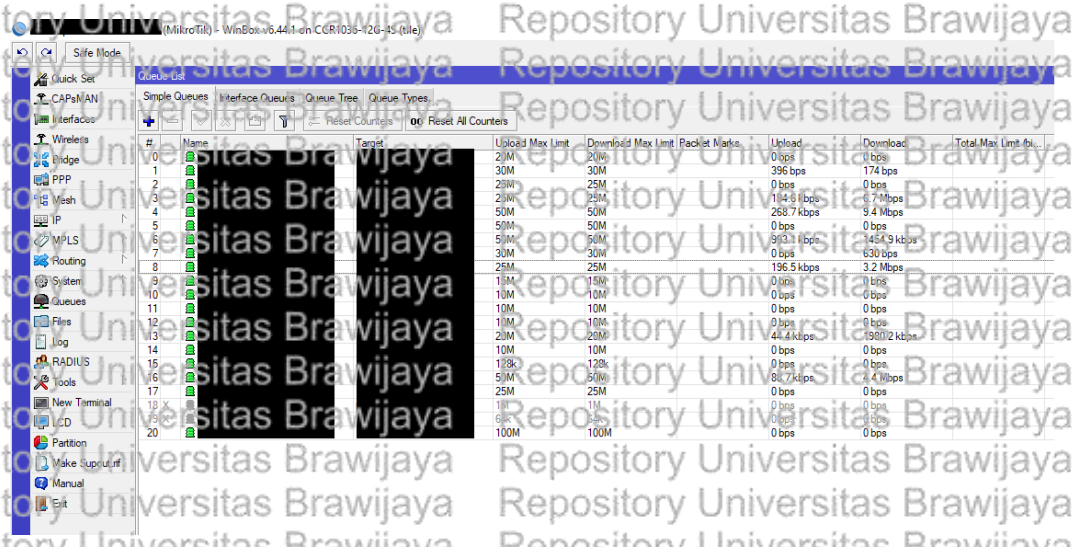
3. Undang-Undang Nomor 17 Tahun 2003 tentang Keuangan Negara (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 47, Tambahan Lembaran Negara Republik Indonesia Nomor 4286);

4. Undang-Undang Nomor 15 Tahun 2004 tentang Pemeriksaan Pengelolaan dan Tanggung Jawab Keuangan Negara (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 66, Tambahan Lembaran Negara Republik Indonesia Nomor 4400);

Peraturan Bupati SPBE No. 80 Tahun 2018

Rencana Kerja (Renja) Dinas Komunikasi dan Informatika Kabupaten Mojokerto

***Finger Print* Pengamanan Fasilitas Fisik**



Aplikasi Memonitor Jaringan

Sistem Operasi menggunakan Windows 10

Anti Virus pada Windows Defender

LAMPIRAN E TABEL REKOMENDASI

Bagian II: Tata Kelola Keamanan Informasi			
No.	**Kondisi *as is***	**Rekomendasi**	**Referensi ISO27001:2013**
1	Pimpinan belum secara resmi bertanggungjawab terhadap pelaksanaan keamanan informasi	Pimpinan mengharuskan semua pelaksana menerapkan kemanan informasi sesuai kebijakan dan prosedur organisasi	A.7.2.1 Tanggung jawab manajemen
2	Belum adanya pembagian tanggung jawab secara spesifik	Menentukan dan mengalokasikan pembagian tanggungjawab	A.6.1.1 Peran dan tanggung jawab keamanan informasi
3	Belum adanya pemetaan peran pelaksana secara lengkap	Melakukan proses pemisahan tugas dengan otoritas yang sesuai	A.6.1.2 Pemisahan tugas
4	Belum ada standar pelaksana pengelolaan keamanan informasi	Membuat Kebijakan standar kompetensi dan keahlian pengelolaan keamanan informasi	A.5.1.1 Kebijakan untuk keamanan informasi
5	Belum sesuainya pelaksana pengamanan informasi dengan persyaratan/ standar kompetensi dan keahlian	Melakukan proses verifikasi latar belakang pada seluruh kandidat sumber daya manusia sesuai standar yang relevan dan proporsional	A.7.1.1 Penyaringan
6	Belum ada program penigkatan dan pemahaman keamanan informasi	Memberikan program pelatihan dan pendidikan tentang keamanan informasi	A.7.2.2 Kesadaran keamanan informasi, pendidikan dan pelatihan
7	Belum melakukan identifikasi data pribadi	Membuat standar identitas data pribadi sesuai peraturan	A.18.1.4 Privasi dan perlindungan informasi identitas pribadi
8	Berkoordinasi dengan pihak eksternal menggunakan cara lisan	Membuat prosedur kesepakatan transfer informasi dengan pihak eksternal	A.13.2.2 Kesepakatan tentang transfer informasi

9	Belum ada prosedur penggunaan permasalahan kemanan informasi sebagai bagian pengambilan keputusan	Membuat prosedur analisis insiden keamanan informasi sebagai pembelajaran	A.16.1.6 Belajar dari insiden keamanan informasi
10	Belum ada proses pengukuran kinerja pengelolaan keamanan informasi	Membuat kebijakan peninjauan keamanan informasi secara berkala	A.5.1.2 Tinjau kebijakan untuk keamanan informasi
11	Belum menerapkan sasaran pengelolaan keamanan informasi, evaluasi secara rutin, dan langkah perbaikan	Melakukan proses kontrol kontiunitas dengan verifikasi, peninjauan dan evaluasi keberlanjutan keamanan informasi	A.17.1.3 Verifikasi, tinjau, dan evaluasi keberlanjutan keamanan informasi
12	Belum melakukan analisa tingkat kepatuhan keamanan informasi	Melakukan peninjauan dengan menganalisis dan menilai kepatuhan prosedur keamanan informasi sesuai standar	A.18.2.2 Kepatuhan dengan kebijakan dan standar keamanan
13	Belum ada kebijakan dan langkah penanggulangan insiden keamanan	Membuat prosedur menanggapi insiden keamanan informasi	A.16.1.1 Tanggung jawab dan prosedur

Bagian III: Pengelolaan Risiko Keamanan Informasi			
No.	**Kondisi *as is***	**Rekomendasi**	**Referensi ISO27001:2013**
1	Belum memiliki program pengelolaan risiko keamanan informasi yang terdokumentasi secara resmi	Membuat prosedur terdokumentasi untuk mengelola risiko insiden keamanan informasi	A.16.1.5 Tanggapan terhadap insiden keamanan informasi
2	Belum ada penanggungjawab dan pelaporan manajemen risiko	Menentukan tanggung jawab dan prosedur pelaporan manajemen risiko	A.6.1.1 Peran dan tanggung jawab keamanan Informasi

3	Kerangka kerja belum mencakup definisi dan hubungan aset, ancaman dan kerugian	Mendefinisikan kepemilikan aset yang terdaftar dalam invetaris	A.8.1.2 Kepemilikan aset
4	Belum menetapkan ambang batas risiko	Mencatat dan melaporkan setiap kelemahan atau batasan2	A.16.1.3 Melaporkan kelemahan keamanan informasi
5	Setiap ancaman dan kelemahan terkait aset belum teridentifkasi	Megidentifikasi inventaris aset2 dalam bentuk sop atau prosedur tertulis	A.8.1.1 Inventarisasi aset
6	Belum adanya penetapan dampak kerugian aset	Membuat prosedur penanganan aset	A.8.2.3 Penanganan aset
7	Belum ada penyusunan langkah - langkah, pemantauan secara berkala, penyelesaian, dan pengkajian ulang mitigasi risiko	Membuat dokumen mitigasi risiko yang terkait dengan aset organisasi	A.15.1.1 Kebijakan keamanan informasi untuk hubungan pemasok
8	Pengelolaan risiko belum menjadi bagian proses penilaian efektifitas pengamanan	Melakukan penempatan dan perlindungan peralatan sebagai bentuk pengamanan untuk mengurangi risiko	A.11.2.1 Penempatan dan perlindungan peralatan

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi			
No.	**Kondisi *as - is***	**Rekomendasi**	**Referensi ISO27001:2013**
1	Belum ada mekanisme pengelolaan kebijakan dan prosedur yang merefleksikan kebutuhan mitigasi	Membuat mekanisme pengelolaan kebijakan dan prosedur keamanan informasi yang merefleksikan kebutuhan mitigasi	A.5.1.1 Kebijakan untuk keamanan informasi
2	Belum melakukan identifikasi kondisi yang membahayakan	Menilai atau mengidentifikasi insiden keamanan informasi	A.16.1.4 Penilaian dan keputusan tentang kejadian keamanan informasi

3	Belum mencantumkan aspek keamanan informasi pada kontrak dengan pihak ketiga	Membuat kesepakatan atau perjanjian tercantum pada kontrak dengan pihak ketiga	A.13.2.2 Kesepakatan tentang transfer informasi
4	Belum ada konsekuensi terhadap pelanggaran kebijakan keamanan informasi	Menetapkan proses pendisiplinan dengan membuat prosedur resmi untuk menindaklanjuti konsekuensi	A.7.2.3 Proses pendisiplinan
5	Belum menerapkan prosedur operasional untuk mengelola pemasangan baru	Membuat prosedur untuk mengontrol pemasangan baru	A.12.5.1 Pemasangan perangkat lunak pada sistem operasional
6	Belum melakukan evaluasi risiko pada sistem baru	Melakukan pengujian pada sistem baru untuk menanggulangi permasalahan yang muncul	A.14.2.9 Pengujian penerimaan sistem
7	Belum menerapkan proses pengembangan sistem yang aman (secure SDLC)	Membuat kebijakan terkait pengembangan perangkat lunak yang aman sesuai standar platform teknologi yang digunakan	A.14.2.1 Kebijakan pembangunan yang aman
8	Belum melakukan proses penanggulangan terhadap penerapan suatu sistem	Peninjauan dan pengujian untuk memastikan damppak perubahan operasi sistem	A.14.2.3 Tinjauan teknis aplikasi setelah perubahan platform operasi
9	Belum tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK	Membuat perencanaan keberlanjutan terkait keamanan informasi pada kelangsungan layanan TIK	A.17.1.1 Merencanakan keberlanjutan keamanan informasi
10	Belum merencanakan uji coba perencanaan pemulihan bencana terhadap layanan TIK dan menganalisis hasilnya sebagai bagian rencana kerja	Menyelesaikan dan menganalisa insiden keamanan informasi untuk mengurangi kemudian terjadi lagi dimasa depan	A.16.1.6 Belajar dari insiden keamanan informasi

11	Belum melakukan evaluasi hasil perencanaan pemulihan bencana untuk menerapkan langkah perbaikan	Memverifikasi kontrol secara berkala untuk memastikan keefektifan dalam perbaikan	A.17.1.3 Verifikasi, tinjau, dan evaluasi keberlanjutan keamanan informasi
12	Belum melaksanakan audit internal	Melakukan auditing internal untuk mengevaluasi keamanan informasi	A.12.7.1 Kontrol audit sistem informasi
13	Audit internal keamanan informasi belum dilaporkan kepada pimpinan	Membuat laporan keamanan informasi melalui saluran manajemen tepat secepat mungkin	A.16.1.2 Pelaporan kejadian keamanan informasi
14	Belum ada prosedur untuk menganalisa pengelolaan perubahan	Membuat SOP atau prosedur penilaian perubahan untuk menerapknannya (prosedur kontrol perubahan secara formal)	A.14.2.2 Prosedur kontrol perubahan sistem
15	Belum melakukan pengujian dan evaluasi kepatuhan keamanan informasi secara periodik	Membuat kebijkan untuk peninjauan pada jangka waktu berkala untuk memastikan keefektifan keamanan informasi	A.5.1.2 Tinjau kebijakan untuk keamanan informasi

Bagian V: Pengelolaan Aset Informasi			
No	**Kondisi *as - is***	**Rekomendasi**	**Referensi ISO27001:2013**
1	Belum tersedia definisi klasifikasi aset informasi	Mengidentifikasikan terkait informasi aset	A.8.1.1 Inventarisasi aset
2	Belum ada proses evaluasi dan pengklasifikasian sesuai tingkat kepentingan	Pelabelan informasi sesuai klasifikasi informasi	A.8.2.2 Pemberian label informasi
3	Belum tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis, dan proses teknologi informasi	Pengontrolan perubahan proses bisnis pada organisasi	A.12.1.2 Manajemen perubahan

4	Belum melakukan proses pengelolaan konfigurasi seacara konsisten	Mengontrol pengelolaan sistem operasional	A.12.5.1 Pemasangan perangkat lunak pada sistem operasional
5	Belum tersedia proses untuk merilis aset baru	Membuat standar persyaratan untuk sistem baru atau penyempurnaan	A.14.1.1 Analisis dan spesifikasi kebutuhan keamanan informasi
6	Belum melakukan pendefinisian tanggungjawab penamanan informasi untuk semua personil di instansi	Menentukan serta mengalokasikan peran dan tanggung jawab sumber daya	A.6.1.1 Peran dan tanggung jawab keamanan Informasi
7	Belum ada tata tertib penggunaan aset	Membuat prosedur tata tertib penggunaan aset	A.8.1.3 Penggunaan aset yang dapat diterima
8	Belum ada peraturan terkait instalasi perangkat lunak	Membuat peraturan pemasangan perangkat lunak	A.12.6.2 Pembatasan pada instalasi perangkat lunak
9	Belum ada peraturan atau prosedur penggunaan data pribadi dan akses serta langkah pembenahannya	Menyediakan akses pengguna formal untuk menetapkan / mencabut hak akses dan membuat prosedur penggunaan akses	A.9.2.2 Provisioning akses pengguna
10	Belum ada prosedur pengelolaan akses tertulis untuk menggunakan aset informasi	Membuat kebijakan atau prosedur kontrol akses	A.9.1.1 Kebijakan kontrol akses
11	Belum ada ketetapan waktu penyimpanan klasifikasi data dan syarat penghancuran data	Membuat ketetapan atau instruksi waktu penyimpanan dan penghancuran data	A.9.2.6 Penghapusan atau penyesuaian hak akses
12	Belum melakukan prosedur penyidikan untuk menyelesaikan insiden kegagalan kemanan informasi	Menetapkan prosedur untuk mendidentifikasi dan pengumpulan bukti	A.16.1.7 Pengumpulan bukti

13	Belum ada ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset	Merancang perlidungan fisik dan menentukan batasan keamanan	A.11.1.1 Perimeter keamanan fisik
14	Belum melakukan proses pengecekan latar belakang SDM	Memeriksa dan memverifikasi latar belakang SDM	A.7.1.1 Penyaringan
15	Belum melakukan proses pelaporan insiden pada pihak yang berwajib	Melakukan proses pelaporan keamanan informasi pada saluran manajemen	A.16.1.2 Pelaporan kejadian keamanan informasi
16	Belum ada prosedur penghancuran data yang sudah tidak diperlukan	Membuat prosedur pembuangan data yang tidak diperlukan	A.8.3.2 Pembuangan media
17	Belum ada prosedur untuk *user* yang mutasi atau habis masa kerjanya	Membuat prosedur hak akses data informasi pada saat pemutusan kontrak	A.9.2.6 Penghapusan atau penyesuaian hak akses
18	Tersedia data yang harus di-*backup* namun tidak tersedia laporannya	Melakukan laporan pensalinan cadangan informasi	A.12.3.1 Pencadangan informasi
19	Belum tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanannya	Membuat peraturan perlindungan rekaman	A.18.1.3 Perlindungan rekaman
20	Belum ada prosedur pengolahan informasi dan pengamanan pengiriman aset milik pihak ketiga	Membuat kesepakatan transfer informasi yang aman antara organisasi dan pihak eksternal	A.13.2.2 Kesepakatan tentang transfer informasi
21	Belum ada peraturan pengamanan perangkat komputasi apabila digunkaan di luar lokasi resmi (kantor)	Menerapkan keamanan peralatan dan aset di luar lokasi (kantor)	A.11.2.6 Keamanan peralatan dan aset di luar lokasi
22	Belum ada proses untuk pemindahan aset dari lokasi yang ditetapkan	Menerapkan peraturan pada aset tidak boleh ke luar lokasi tanpa izin	A.11.2.5 Penghapusan aset

23	Belum melakukan pemeriksaan dan perawatan prangkat komputer, fasilitas pendukung, dan kelayakan keamaan lokasi kerja	Melakukan proses pemeliharaan peralatan	A.11.2.4 Pemeliharaan peralatan
24	Belum ada peraturan untuk mengamakan lokasi kerja penting dari risiko yang dapat membahayakan aset informasi	Melakukan proses penempatan dan perlindungan peralatan	A.11.2.1 Penempatan dan perlindungan peralatan

Bagian VI: Teknologi dan Keamanan Informasi			
No.	**Indeks KAMI**	**Rekomendasi**	**Referensi ISO27001:2013**
1	Belum tersedia konfigurasi standar keamanan sistem	Menetapkan kebijakan kontrol akses mengenai konfigurasi keamanan sistem	A.9.1.1 Kebijakan kontrol akses
2	Belum melakukan analisis kepatuhan penerapan konfigurasi standar yang ada	Melakukan proses peninjauan kepatuhan secara berkala	A.18.2.3 Tinjauan kepatuhan teknis
3	Jaringan, sistem, dan aplikasi belum dipindai secara rutin	Melakukan proses peninjauan jaringan, sistem, dan aplikasi secara rutin	A.5.1.2 Tinjau kebijakan untuk keamanan informasi
4	Keseluruhan infrastruktur belum dirancang untuk memastikan ketersediaan sesuai kebutuhan	Melakukan pemrosesan informasi dengan redundansi yang cukup untuk memenuhi ketersediaan	A.17.2.1 Ketersediaan fasilitas pengolahan informasi
5	Belum melakukan analisis secara berkala pada semua log	Melakukan peninjauan secara berkala pada log	A.12.4.1 Pencatatan kejadian
6	Belum mempunyai standar dalam menggunakan enkripsi	Membuat standar atau kebijakan penggunaan kontrol enkripsi	A.10.1.1 Kebijakan tentang penggunaan kontrol kriptografi

7	Belum menerapkan pengamanan untuk mengelola kunci enkripsi	Menerapkan kebijakan pengelolaan kunci enkripsi	A.10.1.2 Pengelolaan kunci
8	Sistem belum secara otomatis mendukung dan menerapkan manajemen penggunaan *password*	Melakukan manajemen kata sandi	A.9.4.3 Sistem manajemen kata sandi
9	Belum menggunakan pengamanan khusus berlapis untuk mengelola sistem	Melakukan pengamanan khusus dengan membatasi akses dan mengontrok dengan ketat	A.9.4.4 Penggunaan program utilitas istimewa
10	Belum menerapkan pembatasan waktu akses dan pengamanan untuk mendeteksi dan mencegah pengunaan akses jaringan yang tidak resmi	Melakukan pembatasan akses	A.9.4.1 Pembatasan akses informasi
11	Belum ada analisis malware secara rutin dan tindaklajutnya	Melakukan kontrol *malware*	A.12.2.1 Kontrol terhadap Kontrol malware
12	Belum memiliki spesifikasi dan fungsi keamanan yang terverifikasi saat pengembangan dan uji coba	Membuat persyaratan terkait spesifikasi keamanan	A.14.1.1 Analisis dan spesifikasi kebutuhan keamanan informasi
13	Belum melakukan pengamanan lingkungan pengembangan dan uji coba sesuai standar platform teknologi	Melakukan pemisahan lingkungan pengembangan, pengujian, dan lingkungan operasional	A.12.1.4 Pemisahan pengembangan, pengujian dan lingkungan operasional
14	Belum melibatkan pihak independen untuk mengkaji kehandalan kemanan informasi secara rutin	Melakukan peninjauan independen secara rutin	A.18.2.1 Tinjauan independen atas keamanan informasi

LAMPIRAN F KONTROL ISO 27001:2013

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

A.6.1.3	Kontak dengan pihak berwenang	Kontrol: Kontak yang sesuai dengan otoritas yang relevan harus dijaga.
A.6.1.4	Kontak dengan kelompok minat khusus	Kontrol Kontak yang sesuai dengan kelompok minat khusus atau forum keamanan spesialis dan asosiasi profesional lainnya harus dipelihara
A.6.1.5	Keamanan informasi dalam manajemen proyek	Kontrol : Keamanan informasi harus ditangani dalam manajemen proyek, terlepas dari jenis proyeknya
A.6.2 Perangkat seluler dan teleworking		
Tujuan: Untuk memastikan keamanan teleworking dan penggunaan perangkat seluler.		
A.6.2.1	Kontrol kebijakan perangkat seluler	Kebijakan dan langkah-langkah keamanan pendukung harus diadopsi untuk mengelola risiko yang diperkenalkan dengan menggunakan perangkat seluler
A.6.2.2	Teleworking	Kontrol Kebijakan dan langkah-langkah keamanan pendukung harus dilaksanakan untuk melindungi informasi yang diakses, diproses atau disimpan di situs-situs teleworking.
A.7 Keamanan sumber daya manusia		
A.7.1 Sebelum bekerja		
Tujuan: Untuk memastikan bahwa karyawan dan kontraktor memahami tanggung jawab mereka dan cocok untuk peran yang mereka pertimbangkan		
A.7.1.1	Penyaringan	Kontrol Pemeriksaan verifikasi latar belakang pada semua kandidat untuk pekerjaan harus dilakukan sesuai dengan hukum, peraturan dan etika yang relevan dan harus proporsional dengan persyaratan

		bisnis, klasifikasi informasi yang akan diakses dan risiko yang dirasakan
A.7.1.2	Syarat dan ketentuan pekerjaan	Perjanjian kontrak dengan karyawan dan kontraktor harus menyatakan tanggung jawab mereka dan organisasi untuk keamanan informasi
A.7.2 Selama bekerja		
Tujuan: Untuk memastikan bahwa karyawan dan kontraktor sadar dan memenuhi tanggung jawab keamanan informasi mereka.		
A.7.2.1	Tanggung jawab manajemen	Kontrol Manajemen mengharuskan semua karyawan dan kontraktor untuk menerapkan keamanan informasi sesuai dengan kebijakan dan prosedur organisasi yang ditetapkan
A.7.2.2	Kesadaran keamanan informasi, pendidikan dan pelatihan	Kontrol Semua karyawan organisasi dan, di mana ketinggian, kontraktor harus menerima pendidikan dan pelatihan kesadaran yang sesuai dan pembaruan rutin dalam kebijakan dan prosedur organisasi, yang relevan untuk fungsi pekerjaan mereka
A.7.2.3	Proses pendisiplinan	Kontrol Akan ada proses disipliner formal dan dikomunikasikan untuk mengambil tindakan terhadap karyawan yang telah melakukan pelanggaran keamanan informasi.
A.7.3 Pengakhiran dan perubahan pekerjaan		
Tujuan: Untuk melindungi kepentingan organisasi sebagai bagian dari proses mengubah atau mengakhiri pekerjaan		
A.7.3.1	Penghentian atau perubahan tanggung jawab pekerjaan	Kontrol Tanggung jawab keamanan informasi dan tugas yang tetap berlaku setelah pengakhiran atau

		perubahan pekerjaan harus ditetapkan, dikomunikasikan kepada karyawan atau kontraktor dan diberlakukan.
A.8 Manajemen aset		
A.8.1 Tanggung jawab untuk aset		
Tujuan: Untuk mengidentifikasi aset organisasi dan menentukan tanggung jawab perlindungan yang sesuai.		
A.8.1.1	Inventarisasi aset	Kontrol Aset yang terkait dengan informasi dan fasilitas pemrosesan informasi harus diidentifikasi dan inventarisasi aset-aset ini harus dibuat dan dipelihara
A.8.1.2	Kepemilikan aset	Kontrol Aset yang dipelihara dalam inventaris harus dimiliki.
A.8.1.3	Penggunaan aset yang dapat diterima Kontrol	Kontrol Aturan untuk penggunaan informasi yang dapat diterima dan aset yang terkait dengan informasi dan fasilitas pemrosesan informasi harus diidentifikasi, didokumentasikan dan diimplementasikan.
A.8.1.4	Pengembalian aset	Kontrol Semua karyawan dan pengguna pihak eksternal harus mengembalikan semua aset organisasi yang mereka miliki saat pengakhiran kontrak kerja, kontrak, atau perjanjian mereka.
A.8.2 Klasifikasi informasi		
Tujuan: Untuk memastikan bahwa informasi menerima tingkat perlindungan yang tepat sesuai dengan kepentingannya bagi organisasi		
A.8.2.1	Klasifikasi informasi	Kontrol Informasi harus diklasifikasikan dalam persyaratan hukum, nilai, kekritisan dan kepekaan terhadap

		pengungkapan atau modifikasi yang tidak sah
A.8.2.2	Pemberian label informasi	Kontrol Prosedur untuk menangani aset harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi olen organisasi.
A.8.2.3	Penanganan aset	Kontrol Prosedur untuk menangani aset harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi olen organisasi
A.8.3 Penanganan media		
Tujuan: Untuk mencegah pengungkapan yang tidak sah, modifikasi, penghapusan atau penghancuran informasi yang tersimpan di media		
A.8.3.1	Pengelolaan media yang dapat dilepas	Kontrol Prosedur harus diterapkan untuk manajemen media yang dapat dipindahkan sesuai dengan skema klasifikasi yang diadopsi oleh organisasi
A.8.3.2	Pembuangan media	Kontrol Media harus dibuang dengan aman ketika tidak lagi diperlukan, menggunakan prosedur formal
A.8.3.3	Transfer media fisik	Kontrol Informasi yang mengandung media harus dilindungi terhadap akses tidak sah, penyalahgunaan atau korupsi selama transportasi
A.9 Kontrol akses		
A.9.1 Persyaratan bisnis untuk kontrol akses		
Tujuan: Untuk membatasi akses ke fasilitas informasi dan pengolahan informasi.		
A.9.1.1	Kebijakan kontrol akses	Kontrol Kebijakan kontrol akses harus

		ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan bisnis dan informasi
A.9.1.2	Akses ke jaringan dan layanan jaringan	Kontrol Pengguna hanya akan diberikan akses ke jaringan dan layanan jaringan yang telah secara khusus diizinkan untuk digunakan
A.9.2 Manajemen akses pengguna		
Tujuan: Untuk memastikan akses pengguna yang sah dan untuk mencegah akses tidak sah ke sistem dan layanan		
A.9.2.1	Registrasi dan registrasi pengguna	Kontrol Proses pendaftaran dan de-registrasi pengguna formal harus dilaksanakan untuk memungkinkan penugasan hak akses.
A.9.2.2	Provisioning akses pengguna	Kontrol Proses penyediaan akses pengguna formal harus diterapkan untuk menetapkan atau mencabut nak akses untuk semua jenis pengguna ke semua sistem dan layanan.
A.9.2.3	Manajemen hak akses istimewa	Kontrol Alokasi dan penggunaan hak akses istimewa harus dibatasi dan dikendalikan.
A.9.2.4	Pengelolaan informasi otentikasi rahasia pengguna	Kontrol Alokasi informasi otentikasi rahasia harus dikontrol melalui proses manajemen formal
A.9.2.5	Tinjauan hak akses pengguna	Kontrol Pemilik aset harus meninjau nak akses pengguna secara berkala.
A.9.2.6	Penghapusan atau penyesuaian hak akses	Kontrol Hak akses semua karyawan dan pengguna pihak eksternal ke fasilitas pemrosesan informasi dan informasi

		harus dihapus pada saat pemutusan hubungan kerja, kontrak atau perjanjian, atau disesuaikan dengan perubahan.
A.9.3 Tanggung jawab pengguna		
Tujuan: Untuk membuat pengguna bertanggung jawab untuk menjaga informasi otentikasi mereka		
A.9 3.1	Penggunaan informasi otentikasi rahasia	Kontrol Pengguna harus mengikuti praktik organisasi dalam penggunaan informasi otentikasi rahasia.
A.9.4 Sistem dan kontrol akses aplikasi		
Tujuan: Untuk mencegah akses tidak sah ke sistem dan aplikasi		
A.9.4.1	Pembatasan akses informasi	Kontrol Akses ke informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan kontrol akses
A.9.4.2	Prosedur log-on yang aman	Kontrol Jika diperlukan oleh kebijakan kontrol akses, akses ke sistem dan aplikasi harus dikontrol oleh prosedur log-on yang aman
A.9.4.3	Sistem manajemen kata sandi	Kontrol Sistem manajemen kata sandi harus interaktif dan harus memastikan kata sandi berkualitas.
A.9.4.4	Penggunaan program utilitas istimewa	Kontrol Penggunaan program utilitas yang mungkin mampu mengesampingkan sistem dan kontrol aplikasi harus dibatasi dan dikontrol ketat
A.9.4.5	Kontrol akses ke kode sumber program	Kontrol Akses ke kode sumber program harus dibatasi

A.10 Kriptografi		
A.10.1 Kontrol kriptografi		
Tujuan: Untuk memastikan penggunaan kriptografi yang tepat dan efektif untuk melindungi kerahasiaan, keaslian dan / atau integritas informasi		
A.10.1.1	Kebijakan tentang penggunaan kontrol kriptografi	Kontrol Kebijakan tentang penggunaan kontrol kriptografi untuk perlindungan informasi harus dikembangkan dan diimplementasikan
A.10.1.2	Pengelolaan kunci	Kontrol Kebijakan tentang penggunaan, perlindungan, dan masa pakai kunci kriptografi harus dikembangkan dan diterapkan melalui seluruh siklus hidupnya
A.11 Keamanan fisik dan lingkungan		
A.11.1 Area aman		
Tujuan: Untuk mencegah akses fisik yang tidak sah, kerusakan, dan gangguan pada fasilitas informasi dan pemrosesan informasi organisasi		
A.11.1.1	Perimeter keamanan fisik	Kontrol Batas keamanan harus ditentukan dan digunakan untuk melindungi area yang mengandung informasi sensitif atau penting dan fasilitas pemrosesan informasi.
A.11.1.2	Kontrol entri fisik	Kontrol Area aman harus dilindungi oleh kontrol entri yang tepat untuk memastikan bahwa hanya personel yang berwenang yang diperbolehkan mengakses
A.11.1.3	Mengamankan kantor, ruangan dan fasilitas	Kontrol Keamanan fisik untuk kantor, kamar dan fasilitas harus dirancang dan diterapkan

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

A.11.2.4	Pemeliharaan peralatan	Kontrol Peralatan harus dipelihara dengan benar untuk memastikan ketersediaan dan integritasnya yang berkelanjutan
A.11.2.5	Penghapusan aset	Kontrol Peralatan, informasi atau perangkat lunak tidak boleh diambil di luar lokasi tanpa izin sebelumnya
A.11.2.6	Keamanan peralatan dan aset di luar lokasi	Kontrol Keamanan harus diterapkan pada aset di luar lokasi dengan mempertimbangkan risiko berbeda bekerja di luar tempat organisasi
A.11.2.7	Pembuangan atau penggunaan kembali peralatan secara aman	Kontrol Semua peralatan yang mengandung media penyimpanan harus diverifikasi untuk memastikan bahwa data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa secara aman sebelum dibuang atau digunakan kembali
A.11.2.8	Peralatan pengguna yang tidak diawasi	Kontrol Pengguna harus memastikan bahwa peralatan yang tidak dijaga memiliki perlindungan yang tepat
A.11.2.9	Meja yang jelas dan kebijakan layar yang jelas	Kontrol Kebijakan meja yang jelas untuk kertas dan media penyimpanan yang dapat dilepas dan kebijakan layar yang jelas untuk fasilitas pemrosesan informasi harus diadopsi.
A.12 Keamanan operasi		
A.12.1 Prosedur dan tanggung jawab operasional		
Tujuan: Untuk memastikan operasi yang benar dan aman dari fasilitas pemrosesan informasi		

A.12.1.1	Prosedur operasi terdokumentasi	Kontrol Prosedur operasi harus didokumentasikan dan tersedia bagi semua pengguna yang membutuhkannya.
A.12.1.2	Manajemen perubahan	Kontrol Perubahan pada organisasi, proses bisnis, fasilitas pemrosesan informasi dan sistem yang mempengaruhi keamanan informasi harus dikontrol
A.12.1.3	Manajemen kapasitas	Kontrol Penggunaan sumber daya harus dipantau, disesuaikan, dan proyeksi yang dibuat dari kebutuhan kapasitas masa depan untuk memastikan kinerja sistem yang diperlukan
A.12.1.4	Pemisahan pengembangan, pengujian dan lingkungan operasional	Kontrol : Pemisahan lingkungan pengembangan, pengujian dan operasional Pengendalian Pengembangan, pengujian, dan lingkungan operasional harus dipisahkan untuk mengurangi risiko akses tidak sah atau perubahan pada lingkungan operasional
A.12.2 Perlindungan dari malware		
Tujuan: Untuk memastikan bahwa fasilitas pemrosesan informasi dan informasi dilindungi terhadap malware.		
A.12.2.1	Kontrol terhadap 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	Kontrol Salinan cadangan informasi, perangkat lunak dan gambar sistem harus diambil dan diuji secara teratur sesuai dengan kebijakan cadangan yang disepakati
A.12.4 Penebangan dan pemantauan		
Tujuan: Untuk merekam peristiwa dan menghasilkan bukti		
A.12.4.1	Pencatatan kejadian	Kontrol Log peristiwa yang merekam aktivitas pengguna, pengecualian, kesalahan dan kejadian keamanan informasi harus dibuat, dijaga dan ditinjau secara berkala
A.12.4.2	Perlindungan informasi log	Kontrol Fasilitas logging dan informasi log harus dilindungi terhadap gangguan dan akses yang tidak sah.
A.12.4.3	Log administrator dan operator	Kontrol Administrator sistem dan kegiatan operator sistem harus dicatat dan log dilindungi dan ditinjau secara berkala
A.12.4.4	Sinkronisasi jam	Kontrol Administrator sistem dan kegiatan operator sistem harus dicatat dan log dilindungi dan ditinjau secara berkala.
A.12.5 Kontrol perangkat lunak operasional		
Tujuan: Untuk memastikan integritas sistem operasional		
A.12.5.1	Pemasangan perangkat lunak pada sistem operasional	Kontrol Prosedur harus dilaksanakan untuk mengontrol pemasangan perangkat lunak pada sistem operasional
A.12.6 Pengelolaan kerentanan teknis		
Tujuan: Untuk mencegah eksploitasi kerentanan teknis		

A.12.6.1	Pengelolaan kerentanan teknis	Kontrol Informasi tentang kerentanan teknis dari sistem informasi yang digunakan harus diperoleh secara tepat waktu, paparan organisasi terhadap kerentanan tersebut dievaluasi dan tindakan yang tepat diambil untuk mengatasi risiko terkait.
A.12.6.2	Pembatasan pada instalasi perangkat lunak	Kontrol Aturan yang mengatur pemasangan perangkat lunak oleh pengguna harus ditetapkan dan diimplementasikan
A.12.7 Pertimbangan audit sistem informasi		
Tujuan: Untuk meminimalkan dampak kegiatan audit pada sistem operasional		
A.12.7.1	Kontrol audit sistem informasi	Kontrol Persyaratan dan kegiatan audit yang melibatkan verifikasi sistem operasional harus direncanakan secara hati-hati dan disetujui untuk meminimalkan gangguan terhadap proses bisnis
A.13 Keamanan komunikasi		
A.13.1 Manajemen keamanan jaringan		
Tujuan: Untuk memastikan perlindungan informasi dalam jaringan dan fasilitas pemrosesan informasi pendukungnya		
A.13.1.1	Kontrol jaringan	Kontrol Jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi
A.13.1.2	Keamanan layanan jaringan	Kontrol Mekanisme keamanan, tingkat layanan, dan persyaratan manajemen semua layanan jaringan harus diidentifikasi dan dimasukkan dalam perjanjian layanan jaringan,

		apakah layanan ini disediakan di rumah atau dialihdayakan
A.13.1.3	Segregasi dalam jaringan	Kontrol Kelompok layanan informasi, pengguna, dan sistem informasi harus dipisahkan pada jaringan.
A.13.2 Transfer informasi		
Tujuan: Untuk menjaga keamanan informasi yang ditransfer dalam suatu organisasi dan dengan entitas eksternal apa pun		
A.13.2.1	Kebijakan dan prosedur pengalihan informasi	Kontrol Kebijakan, prosedur, dan kendali transfer formal harus diberlakukan untuk melindungi transfer informasi melalui penggunaan semua jenis fasilitas komunikasi
A.13.2.2	Kesepakatan tentang transfer informasi	Kontrol Perjanjian harus menangani transfer aman informasi bisnis antara organisasi dan pihak eksternal.
A.13.2.3	Pesan elektronik	Kontrol Informasi yang terlibat dalam pesan elektronik harus dilindungi dengan tepat
A.13.2.4	Perjanjian kerahasiaan atau nondisclosure	Kontrol Persyaratan untuk kerahasiaan atau perjanjian kerahasiaan non-mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, secara teratur ditinjau dan didokumentasikan
A.14 Akuisisi, pengembangan, dan pemeliharaan sistem		
A.14.1 Persyaratan keamanan sistem informasi		
Tujuan: Untuk memastikan bahwa keamanan informasi merupakan bagian integral dari sistem informasi di seluruh siklus hidup. Ini juga termasuk persyaratan untuk sistem informasi yang menyediakan layanan melalui jaringan publik.		

A.14.1.1	Analisis dan spesifikasi kebutuhan keamanan informasi	Kontrol Persyaratan terkait keamanan informasi harus dimasukkan dalam persyaratan untuk sistem informasi baru atau penyempurnaan sistem informasi yang ada
A.14.1.2	Mengamankan layanan aplikasi di jaringan publik	Kontrol Informasi yang terlibat dalam layanan aplikasi yang melewati jaringan publik harus dilindungi dari kegiatan penipuan, perselisihan kontrak dan pengungkapan tidak sah dan modifikasi
A.14.1.3	Melindungi transaksi layanan aplikasi	Kontrol Informasi yang terlibat dalam transaksi layanan aplikasi harus dilindungi untuk mencegah transmisi yang tidak lengkap, mis-routing, perubahan pesan yang tidak sah, pengungkapan yang tidak sah, duplikasi pesan tidak sah atau replay.
A.14.2 Keamanan dalam proses pengembangan dan dukungan		
Tujuan: Untuk memastikan keamanan informasi dirancang dan diimplementasikan dalam siklus pengembangan sistem informasi		
A.14.2.1	Kebijakan pembangunan yang aman	Kontrol Aturan untuk pengembangan perangkat lunak dan sistem harus ditetapkan dan diterapkan untuk perkembangan dalam organisasi.
A.14.2.2	Prosedur kontrol perubahan sistem	Kontrol Perubahan sistem dalam siklus hidup pengembangan harus dikendalikan oleh penggunaan prosedur kontrol perubahan formal
A.14.2.3	Tinjauan teknis aplikasi setelah perubahan platform operasi	Kontrol Ketika platform operasi berubah, aplikasi bisnis penting harus ditinjau dan diuji untuk memastikan tidak

		ada dampak negatif pada operasi atau keamanan organisasi
A.14.2.4	Batasan pada perubahan paket perangkat lunak	Kontrol Modifikasi paket perangkat lunak harus dihalangi, terbatas pada perubahan yang diperlukan dan semua perubahan harus dikontrol secara ketat
A.14.2.5	Prinsip rekayasa sistem yang aman	Kontrol Prinsip-prinsip untuk rekayasa sistem keamanan harus ditetapkan, didokumentasikan, dipelihara dan diterapkan pada setiap upaya implementasi sistem informasi.
A.14.2.6	Lingkungan pengembangan yang aman	Kontrol Organisasi harus menetapkan dan secara tepat melindungi lingkungan pengembangan yang aman untuk pengembangan sistem dan upaya integrasi yang mencakup seluruh siklus hidup pengembangan sistem.
A.14.2.7	Pengembangan yang dialih dayakan	Kontrol Organisasi harus mengawasi dan memantau aktivitas pengembangan sistem yang dialihdayakan
A.14.2.8	Pengujian keamanan sistem	Kontrol Pengujian fungsi keamanan harus dilakukan selama pengembangan.
A.14.2.9	Pengujian penerimaan sistem	Kontrol Program pengujian penerimaan dan kriteria terkait harus ditetapkan untuk sistem informasi baru, peningkatan versi dan versi baru
A.14.3 Data uji		
Tujuan: Untuk memastikan perlindungan data yang digunakan untuk pengujian		

A.14.3.1	Perlindungan data uji	Kontrol Data uji harus dipilih dengan hati-hati, terlindungi dan terkontrol
A.15 Hubungan pemasok		
A.15.1 Keamanan informasi dalam hubungan pemasok		
Tujuan: Untuk memastikan perlindungan aset organisasi yang dapat diakses oleh pemasok		
A.15.1.1	Kebijakan keamanan informasi untuk hubungan pemasok	Kontrol Persyaratan keamanan informasi untuk memitigasi risiko yang terkait dengan akses pemasok ke aset organisasi harus disetujui oleh pemasok dan didokumentasikan
A.15.1.2	Mengatasi keamanan dalam perjanjian pemasok	Kontrol Semua persyaratan keamanan informasi yang relevan harus ditetapkan dan disepakati dengan masing-masing pemasok yang dapat mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur TI untuk, informasi organisasi
A.15.1.3	Rantai pasokan teknologi informasi dan komunikasi	Kontrol Perjanjian dengan pemasok harus mencakup persyaratan untuk mengatasi risiko keamanan informasi yang terkait dengan layanan teknologi informasi dan komunikasi dan rantai pasokan produk.
A.15.2 Manajemen pengiriman layanan pemasok		
Tujuan: Untuk menjaga tingkat keamanan informasi dan penyediaan layanan yang disepakati sesuai dengan perjanjian pemasok.		
A.15.2.1	Pemantauan dan peninjauan layanan pemasok	Kontrol Organisasi harus secara teratur memantau, meninjau, dan mengaudit layanan pemasok

A.15.2.2	Mengelola perubahan pada layanan pemasok	Kontrol Perubahan pada penyediaan layanan oleh pemasok, termasuk mempertahankan dan meningkatkan kebijakan keamanan informasi yang ada, prosedur dan kontrol, harus dikelola, dengan mempertimbangkan kekritisan informasi bisnis, sistem dan proses yang terlibat dan penilaian ulang risiko.
A.16 Manajemen insiden keamanan informasi		
A.16.1 Manajemen insiden keamanan informasi dan perbaikan		
Tujuan: Untuk memastikan pendekatan yang konsisten dan efektif terhadap manajemen insiden keamanan informasi, termasuk komunikasi tentang peristiwa keamanan dan kelemahan		
A.16.1.1	Tanggung jawab dan prosedur	Kontrol Tanggung jawab manajemen dan prosedur harus ditetapkan untuk memastikan tanggapan yang cepat, efektif dan teratur terhadap insiden keamanan informasi
A.16.1.2	Pelaporan kejadian keamanan informasi	Kontrol Kejadian keamanan informasi harus dilaporkan melalui saluran manajemen yang tepat secepat mungkin
A.16.1.3	Melaporkan kelemahan keamanan informasi	Kontrol Karyawan dan kontraktor menggunakan informasi organisasi sistem dan layanan harus diminta untuk mencatat dan melaporkan setiap kelemahan keamanan informasi yang diamati atau dicurigai dalam sistem atau layanan
A.16.1.4	Penilaian dan keputusan tentang kejadian keamanan informasi	Kontrol Kejadian keamanan informasi harus dinilai dan diputuskan apakah akan

		diklasifikasikan sebagai insiden keamanan informasi
A.16.1.5	Tanggapan terhadap insiden keamanan informasi	Kontrol Insiden keamanan informasi harus direspons sesuai dengan prosedur terdokumentasi
A.16.1.6	Belajar dari insiden keamanan informasi	Kontrol Pengetahuan yang diperoleh dari menganalisa dan menyelesaikan insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan atau dampak dari insiden masa depan
A.16.1.7	Pengumpulan bukti	Kontrol Organisasi harus menetapkan dan menerapkan prosedur untuk identifikasi, pengumpulan, perolehan, dan pelestarian informasi, yang dapat berfungsi sebagai bukti
A.17 Aspek keamanan informasi manajemen kesinambungan bisnis		
A.17.1 Ketahanan keamanan informasi		
Sasaran: Keberlanjutan keamanan informasi harus disematkan dalam sistem manajemen kesinambungan bisnis organisasi.		
A.17.1.1	Merencanakan keberlanjutan keamanan informasi	Kontrol Organisasi harus menentukan persyaratannya untuk keamanan informasi dan kelangsungan manajemen keamanan informasi dalam situasi yang merugikan, misalnya selama krisis atau bencana
A.17.1.2	Menerapkan kontinuitas keamanan informasi	Kontrol Organisasi harus menetapkan, mendokumentasikan, menerapkan dan memelihara proses, prosedur dan kontrol untuk memastikan tingkat keberlanjutan yang

		diperlukan untuk keamanan informasi selama situasi yang merugikan.
A.17.1.3	Verifikasi, tinjau, dan evaluasi keberlanjutan keamanan informasi	Kontrol Organisasi harus memverifikasi kontrol kontinuitas keamanan informasi yang ditetapkan dan diimplementasikan secara berkala untuk memastikan bahwa mereka valid dan efektif selama situasi yang merugikan
A.17.2 Redudansi		
Tujuan: Untuk memastikan ketersediaan fasilitas pemrosesan informasi.		
A.17.2.1	Ketersediaan fasilitas pengolahan informasi	Kontrol Fasilitas pemrosesan informasi harus dilaksanakan dengan redundansi yang cukup untuk memenuhi persyaratan ketersediaan
A.18 Kepatuhan		
A.18.1 Kepatuhan dengan persyaratan hukum dan kontrak		
Tujuan: Untuk menghindari pelanggaran kewajiban hukum, undang-undang, peraturan atau kontrak yang terkait dengan keamanan informasi dan persyaratan keamanan apa pun		
A.18.1.1	Identifikasi peraturan perundangan yang berlaku dan persyaratan kontrak	Kontrol Semua peraturan perundang-undangan yang relevan, peraturan, persyaratan kontrak dan pendekatan organisasi untuk memenuhi persyaratan ini harus secara eksplisit diidentifikasi, didokumentasikan dan diperbarui untuk setiap sistem informasi dan organisasi
A.18.1.2	Hak kekayaan intelektual	Kontrol Prosedur yang sesuai harus dilaksanakan untuk memastikan kepatuhan dengan persyaratan legislatif, peraturan dan kontrak

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

		dengan kebijakan keamanan yang sesuai, standar dan persyaratan keamanan lainnya.
A.18.2.3	Tinjauan kepatuhan teknis	Kontrol Sistem informasi harus ditinjau secara berkala untuk kepatuhan terhadap kebijakan dan standar keamanan informasi organisasi.