TUGAS AKHIR – KS141501

EVALUASI KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE INDEKS KEAMANAN INFORMASI (KAMI VERSI 3.1) (STUDI KASUS: DINAS KOMUNIKASI DAN INFORMATIKA PEMERINTAH DAERAH XYZ)

EVALUATION OF INFORMATION SECURITY USING INDEKS KEAMANAN INFORMASI (KAMI VERSION 3.1) (CASE STUDY: DEPARTMENT OF INFORMATICS AND COMMUNICATION OF XYZ REGION GOVERNMENT)

ISNAINI NUR ROHMAWATI
NRP 052 1144 000 7004

Dosen Pembimbing:
Ir. Khakim Gozali, M.MT

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember
Surabaya 2018

"Halaman ini sengaja dikosongkan"

TUGAS AKHIR – KS141501

EVALUASI KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE INDEKS KEAMANAN INFORMASI (KAMI VERSI 3.1) (STUDI KASUS: DINAS KOMUNIKASI DAN INFORMATIKA PEMERINTAH DAERAH XYZ)

ISNAINI NUR ROHMAWATI
NRP 0521144 000 7004

Dosen Pembimbing:
Ir. Khakim Gozali, M.MT

DEPARTEMEN SISTEM INFORMASI
Fakultas Teknologi Informasi dan Komuniasi
Institut Teknologi Sepuluh Nopember
Surabaya 2018

"*Halaman ini sengaja dikosongkan"*

FINAL PROJECT – KS 141501

EVALUATION OF INFORMATION SECURITY USING INDEKS KEAMANAN INFORMASI (KAMI VERSION 3.1) (CASE STUDY: DEPARTMENT OF INFORMATICS AND COMMUNICATION OF XYZ REGION GOVERNMENT)

ISNAINI NUR ROHMAWATI
NRP 0521144 000 7004

Dosen Pembimbing:
Ir. Khakim Gozali, M.MT

DEPARTMENT OF INFORMATION SYSTEMS
Faculty of Information Technology and Communication
Institut Teknologi Sepuluh Nopember
Surabaya 2018

"Halaman ini sengaja dikosongkan"

LEMBAR PENGESAHAN

EVALUASI KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE INDEKS KEAMANAN INFORMASI (KAMI VERSI 3.1) (STUDI KASUS: DINAS KOMUNIKASI DAN INFORMATIKA PEMERINTAH DAERAH XYZ)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember

Oleh:

ISNAINI NUR ROHMAWATI
05211440007004

Surabaya, 28 Juni 2018

KEPALA
DEPARTEMEN SISTEM INFORMASI

Dr. Ir. Aris Tjahyanto, M.Kom.
NIP 19650310 199102 1 001

"Halaman ini sengaja dikosongkan"

LEMBAR PERSETUJUAN

EVALUASI KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE INDEKS KEAMANAN INFORMASI (KAMI VERSI 3.1) (STUDI KASUS: DINAS KOMUNIKASI DAN INFORMATIKA PEMERINTAH DAERAH XYZ)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Departemen Sistem Informasi
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember

Oleh:

ISNAINI NUR ROHMAWATI
05211440007004

Disetujui Tim Penguji: Tanggal: Ujian : Juli 2018
Periode Wisuda : September 2018

Ir. Khakim Ghozali, M.MT **(Pembimbing I)**

Ir. Achmad Holil Noor Ali, M.Kom **(Penguji I)**

Sholiq, S.T, M.Kom, M.SA **(Penguji II)**

"Halaman ini sengaja dikosongkan"

EVALUASI KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE INDEKS KEAMANAN INFORMASI (KAMI VERSI 3.1) (STUDI KASUS: DINAS KOMUNIKASI DAN INFORMATIKA PEMERINTAH DAERAH XYZ)

Nama Mahasiswa : Isnaini Nur Rohmawati
NRP : 05211440007004
Jurusan : Sistem Informasi FTIK-ITS
Dosen Pembimbing 1: Ir. Khakim Ghozali, M.MT

ABSTRAK

Pemerintah Daerah XYZ merupakan salah satu pemerintah daerah yang menerapkan smart city yang diprakarsai oleh Kementerian Komunikasi dan Informatika. sebagai salah satu daerah yang terpilih dalam pengembangan 100 smar city di Indoensia, Pemerintah Daerah XYZ mempunyai tanggung jawab besar terhadap kemajuan Negara. Penggunaan teknologi informasi sangat penting dan sangat berperan untuk mewujudkan program e-government dan merealisasikan instansi pemerintah dengan tata kelola pemerintahan yang baik (Good Corporate Governance). Keberadaan dinas Komunikasi dan Informatika mempunyai peran strategis dalam pembangunan kabupaten menuju smart city. Tetapi, banyak halangan dan masalah dalam penerapan teknologi infomasi, yaitu kejahatan teknologi infomasi. Sehingga keamanan informasi diperlukan untuk mempertahankan dan mengembangkan kelangsungan pemerintahan. Kementerian Komunikasi dan Informatika telah membuat suatu alat bantu untuk mengukur tingkat kelengkapan dan kematangan keamanan informasi yang dapat digunakan untuk instansi pemerintah dari berbagai tingkatan, ukuran maupun tingkat kepentingan penggunaan TIK. Alat bantu tersebut dinamakan dengan Indeks Keamanan Informasi (Indeks KAMI). Indeks KAMI mempunyai ruang lingkup yang memenuhi semua aspek keamanan dalam standar

internasional mengenai keamanan informasi yaitu berdasar ISO 27001. Penelitian ini menggunakan Indeks KAMI versi 3.1 yang diambil dari ISO/IEC 27001:2013, dengan alur penelitian mulai dari tahap penggalian data, penyusunan dan penerapan evaluasi menggunakan Indeks KAMI sampai dengan pembahasan dan kesimpulan. Penelitian berfokus pada penilaian evaluasi pada lingkup tata kelola keamanan informasi. Hasil penelitian adalah mengetahui nilai status Area Indeks KAMI. Pembuatan saran perbaikan dan rekomendasi dilakukan setelah mendapatkan nilai skor pada penilaian Indeks KAMI. Rekomendasi dari penelitian dapat dijadikan sebagai bahan pertimbangan dan bahan perbaikan untuk meningkatkan keamanan informasi dan mengembangkan proses bisnis dalam dinas Komunikasi dan Informatika Daerah XYZ.

***Kata Kunci**: **evaluasi, keamanan informasi, self-assessment, Indeks KAMI, dinas Komunikasi dan Informatika Daerah XYZ**.*

EVALUATION OF INFORMATION SECURITY USING INDEKS KEAMANAN INFORMASI (KAMI VERSION 3.1) (CASE STUDY: DEPARTMENT OF INFORMATICS AND COMMUNICATION OF XYZ REGION GOVERNMENT)

Name	**: Isnaini Nur Rohmawati**
NRP	**: 05211440007004**
Department	**: Information Systems FTIK -ITS**
Supervisor 1	**: Ir. Khakim Ghozali, M.MT**

ABSTRACT

XYZ Regional Government is one of the local governments that implement smart city initiated by the Ministry of Communications and Informatics. as one of the areas selected in the development of 100 smart cities in Indonesia, the XYZ Regional Government has a great responsibility to the progress of the State. The use of information technology is very important and very instrumental to realize e-government programs and realize government agencies with good governance (Good Corporate Governance). The existence of the Office of Communication and Informatics has a strategic role in the development of the district towards the smart city. However, many obstacles and problems in the application of information technology. So information security is needed to maintain and develop the continuity of government. The Ministry of Communication and Informatics has developed a tool for measuring the level of completeness and maturity of information security that can be used for government agencies of various levels, sizes and importance of ICT use. The tool is called the Indeks Keamanan Informasi (Indeks KAMI). Indeks KAMI has a scope that meets all aspects of security in international standards on information security that is based on ISO 27001. This study uses Indeks KAMI version 3.1 taken from ISO / IEC 27001: 2013, with the research flow from the stage of data mining, preparation and application evaluation

using OUR Index up to the discussion and conclusion. The result of this research is to know the total value Total status in Indeks KAMI. Making recommendations and improvements recommendations made after obtaining scores on the assessment of the previous Indeks KAMI. Recommendations from the research can be used as material considerations and improvement materials to improve information security and develop business processes in XYZ Regional Communications and Informatics office.

Keyword: : evaluation, information security, self-assessment, Indeks KAMI, Ministry of Communication and Informatics XYZ

KATA PENGANTAR

Syukur Alhamdulillah dipanjatkan oleh peneliti atas segala petunjuk, pertolongan, kasih sayang, dan kekuatan yang diberikan oleh Allah SWT. Hanya karena ridho-Nya, peneliti dapat menyelesaikan laporan Tugas Akhir, dengan judul **EVALUASI KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE INDEKS KEAMANAN INFORMASI (KAMI VERSI 3.1) (STUDI KASUS: DINAS KOMUNIKASI DAN INFORMATIKA PEMERINTAH DAERAH XYZ)**

Pada kesempatan ini, saya ingin menyampaikan banyak terima kasih kepada semua pihak yang telah memberikan dukungan, bimbingan, arahan, bantuan, dan semangat dalam menyelesaikan tugas akhir ini, yaitu kepada:

- Orang tua penulis yang senantiasa mendoakan dan mendukung, serta kakak-kakak tercinta yang selalu mendorong penulis untuk segera menyelesaikan tugas akhir ini.
- Pihak Kominfo yaitu Ibu Fatma, Bapak Mamat, Ibu Indah, dan Ibu Reza yang bersedia meluangkan waktunya untuk melakukan wawancara dan mencarikan data-data yang diperlukan untuk tugas akhir ini.
- Bapak Ir. Khakim Ghozali, M.MT, selaku dosen pembimbing yang yang telah meluangkan waktu untuk membimbing dan mendukung dalam penyelesaian tugas akhir ini.
- Bapak Tony Dwi Susanto, ST, MT, Ph.D, ITIL, COBIT, TOGAF, selaku dosen wali yang senantiasa memberikan pengarahan selama penulis menempuh masa perkuliahan dan pengerjaan tugas akhir ini.
- Bapak Agus Zainal Arifin, S.Kom, M.Kom., dan Bapak Darmaji, S.T., M.Kom., selaku Pembina CSSMoRA ITS yang telah membantu penulis selama masa perkuliahan baik lahir maupun batin.

- Bapak Hermono, selaku admin laboratoriun MSI yang membantu penulis dalam hal administrasi penyelesaian tugas akhir ini.
- Teman – teman Lab MSI dan OSIRIS yang telah memberikan semangat dalam menyelesaikan tugas akhir
- Teman-teman Depag 2014, "Teman Masa Gitu" dan teman-teman Pramuka ITS, yang selalu memberikan semangat dalam pengerjaan tugas akhir ini.
- Serta pihak lain yang telah mendukung dan membantu dalam kelancaran penyelesaian tugas akhir ini.

Penyusunan laporan ini masih jauh dari sempurna, untuk itu peneliti menerima kritik dan saran yang membangun untuk perbaikan di masa mendatang. Penelitian ini diharapkan dapat menjadi salah satu acuan bagi penelitian – penelitian yang serupa dan bermanfaat bagi pembaca.

Surabaya, Juni 2018
Penulis,

Isnaini Nur Rohmawati

DAFTAR ISI

"Halaman ini sengaja dikosongkan"

DAFTAR GAMBAR

"Halaman ini sengaja dikosongkan"

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab Pendahuluan merupakan penjelasan awal mengenai penelitian yang dianalisa. Di dalam bab ini akan diuraikan mengenai identifikasi masalah yang meliputi latar belakang masalah, rumusan masalah, batasan masalah, tujuan tugas akhir, manfaat dari kegiatan tugas akhir, dan relevansi terhadap pengerjaan tugas akhir, serta target luaran yang ingin dicapai setelah pengerjaan tugas akhir.

1.1 Latar Belakang Masalah

Kementerian Komunikasi dan Informatika (Kominfo) menyatakan bahwa tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik sebagai upaya peningkatan kualitas layanan dan realisasi tata kelola pemerintahan yang baik (*Good Corporate Governance*)[1]. Tahun 2017, Instansi Pemerintah XYZ terpilih menjadi bagian dari program pengembangan 100 *smart city* di Indonesia oleh Kemenkominfo. Dengan adanya program tersebut, membuktikan bahwa instansi tersebut telah mengupayakan peningkatan kualitas pada pemerintahan Indonesia. Selain *smart city*, Ia juga menyelenggarakan pemerintahan bersifat *e-government*, seperti membuat layanan publik dengan mengimplementasikan layanan sistem elektronik untuk keperluan *goverment to goverment* (G2G) ataupun *goverment to citizen* (G2C). Contoh layanan berbasis sistem elektronik lainnnya adalah *e-planning, e-budgetting, e-Kontrolling, e-asset* dan aplikasi elektronik lainnya. Sistem aplikasi tersebut saling terintegrasi dan disebut sebagai *Goverment Resource Management System* (GRMS). Selain dari beberapa aplikasi diatas, juga terdapat sistem aplikasi yang dapat dilakukan secara daring seperti perizinan online, cek NIK/KK, akta kelahiran online, dan lain sebagainya.

Pembuatan sistem aplikasi terintegrasi mempunyai banyak manfaat, salah satunya adalah aliran informasi yang real-

time. Tetapi, selain dari manfaat yang diberikan juga terdapat ancaman yang bisa merusak suatu organisasi. Ancaman terbesar pemanfaatan teknologi informasi adalah kejahatan teknologi informasi. Dari kejahatan TI tersebut, diperlukan adanya keamanan informasi. Melalui siaran pers yang diadakan oleh Kementerian Komunikasi dan Informatika pada 2013 lalu, mereka memaparkan bahwa tindak pidana yang paling sering dilaporkan ialah mengenai akses ilegal, perubahan data, berita bohong yang merugikan konsumen, dan konten yang melanggar kesusilaan[2]. Dari dua hal tindak pidana teratas, yaitu akses ilegal dan perubahan data adalah tindak pidana yang dapat menyebabkan kerugian besar terhadap suatu instansi pemerintahan/non pemerintahan. Karena dalam instansi tersebut banyak menyimpan data sensitif dan bersifat rahasia.

Menteri Komunikasi dan Informatika, Rudiantara, mengatakan bahwa mulai Maret 2018 seluruh perizinan melalui kementerian & lembaga harus melalui online dan setiap aplikasi dalam keseluruhan instansi harus terintegrasi dan saling terkoordinasi[3]. Sedangkan Sekretaris Ditjen Aplikasi Informatika, Mariam F memaparkan bahwa pada tahun 2017 terdapat serangan yang mencapai 205,5 juta serangan, dengan peningkatan sebesar 66%. Kemudian terjadi situasi kritis seperti Wannacry dan ransomware. Hal tersebut mutlak bahwa keamanan informasi dibutuhkan untuk melindungi informasi dan memperahankan serta peningkatan ekonomi masyarakat[4].

Untuk menangani beberapa masalah diatas, Kementerian Komunikasi dan Informatika mengeluarkan alat bantu untuk mengevaluasi Tingkat kematangan penerapan keamanan informasi di sebuah organisasi. Alat tersebut telah disesuaikan dengan kritteria SNI ISO/IEC 27001 dan dinamakan sebagai aplikasi Indeks Keamanan Informasi (Indek KAMI). Indeks KAMI digunakan sebagai indikator penerapan informasi secara nasional[5].

Sejak tahun 2008, Kementerian Kominfo yaitu pada Direktorat Keamanan Informasi Dirjen Aptika telah melakukan pembinaan kepada Penyelenggara Sistem Elektronik Layanan Publik untuk mengimplementasikan aplikasi Indeks KAMI. Hal tersebut dilakukan sebagai upaya peningkatan kualitas dan penjaminan penyediaan layanan publik sesuai dengan tata kelola pemerintahan dan korporasi yang baik[5]. Selain itu penerapan keamanan informasi yang sesuai dengan kelayakan Indeks KAMI merupakan bentuk tanggung jawab yang sesuai dengan Pasal 15 Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik[6].

1.2 Perumusan Masalah

Berdasarkan latar belakang tersebut, permasalahan yang akan diangkat pada penelitian tugas akhir ini adalah sebagai berikut:

1. Berapakah total skor dari penilaian Indeks KAMI di Instansi Pemerintah XYZ?
2. Bagaimana hasil rekomendasi untuk peningkatan keamanan informasi pada Instansi Pemerintah XYZ?

1.3 Batasan Masalah

Berdasarkan deskripsi permasalahan diatas, adapun batasan masalah dari penelitian tugas akhir ini adalah sebagai berikut:

1. Penerapan evaluasi Indeks KAMI dilakukan pada satu Area Indeks KAMI, yaitu pada Area Tata Kelola Keamanan Informasi.
2. Penilaian dilakukan dalam satu unit bagian milik Dinas Komunikasi dan Informatika XYZ.
3. Lingkup evaluasi keamanan informasi meliputi kesiapan/kelengkapan penerapan pengamanan dan kematangan penerapan pengamanan sesuai Indeks KAMI.

1.4 Tujuan Penelitian

Berdasarkan hasil perumusan masalah dan batasan masalah yang telah disebutkan sebelumnya, maka tujuan yang dicapai dari tugas akhir ini adalah sebagai berikut:

1. Mengetahui nilai skor kematangan keamanan informasi berdasarkan penilaian Area Indeks KAMI pada Instansi Pemerintah XYZ.
2. Memberikan rekomendasi kepada Instansi Pemerintah XYZ untuk meningkatkan keamanan informasi di instansi tersebut.

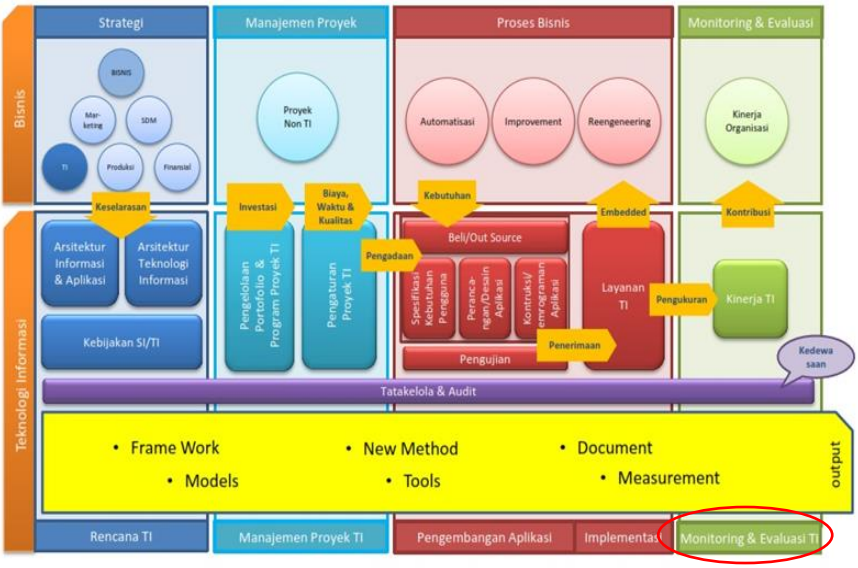
1.5 Manfaat Penelitian

Manfaat yang dapat diperoleh dari pengerjaan tugas akhir ini adalah sebagai berikut:

1. Manfaat Teoritis
   Penelitian ini diharapkan dapat mendapatkan khasanah keilmuan dalam bidang sistem informasi khususnya mengenai penerapan evaluasi keamanan informasi di bidang instansi pemerintahan.
2. Manfaat Praktis
   a. Bagi pihak Instansi Pemerintah XYZ, memperoleh kondisi kekinian mengenai keamanan informasi area sehingga dapat dilakukan perbaikan dan dapat mempertahankan serta meningkatkan kualitas keamanan informasi di Pemerintah Kabupaten XYZ.
   b. Bagi penulis, mendapatkan wawasan dan pengalaman dalam penerapan ilmu SI/TI
   c. Bagi penelitian berikutnya, dapat dijadikan referensi bidang penelitian untuk evaluasi keamanan informasi di instansi pemerintahan dan melakukan pengembangan terhadap studi selanjutnya.

1.6 Relevansi

Penelitian ini memiliki relevansi terhadap beberapa mata kuliah di Departemen Sistem Informasi, salah satunya adalah Audit Sistem Informasi dan Keamanan Aset Informasi. Karena penelitian berupa evaluasi yang berhubungan dengan audit dan berada dalam bidang keamanan informasi.



Gambar 1.1.1 Relevansi Usulan Tugas Akhir dengan Roadmap Lab. MSI

Sumber:[7]

Berdasarkan gambar diatas, usulan tugas akhir yang diajukan dan relevansi terhadap mata kuliah diatas sesuai dengan ranah penelitian pada Laboratorium Manajemen Sistem Informasi (MSI) yang ada pada Departemen Sistem Informasi ITS. Oleh karena itu, topik tugas akhir yang diajukan penulis merupakan topik untuk Laboratorium MSI.

1.7 Sistematika Penulisan

Sistematika penulisan tugas akhir ini dibagi menjadi tujuh bab, yakni:

BAB I PENDAHULUAN

Bab ini berisi pendahuluan yang menjelaskan latar belakang, rumusan masalah, batasan masalah, tujuan tugas akhir, manfaat, relevansi dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Definisi dan penjelasan pustaka yang dijadikan referensi dalam pembuatan tugas akhir ini akan dijelaskan pada bab dua. Teori yang dipaparkan di antaranya mengenai Indeks Keamanan Informasi (KAMI) versi 3.1, ISO/IEC 27001, Tata Kelola, Tata Kelola Teknologi Informasi, Manajemen Risiko Teknologi Informasi, dan Perbedaan Indeks KAMI versi 2.3 & Indeks KAMI versi 3.1.

BAB III METODOLOGI

Bab ini menggambarkan uraian dan urutan pekerjaan yang akan dilakukan dalam penyusunan tugas akhir ini.

BAB IV PERANCANGAN

Bab ini menjelaskan perancangan studi kasus yang diangkat, objek penelitian, perangkat yang dilakukan oleh penulis untuk mengumpulkan data kondisi kekinian, serta metode pengolahan data.

BAB V IMPLEMENTASI

Bab ini menjelaskan hasil yang didapatkan dari proses pengumpulan data, yakni meliputi kondisi kekinian, kondisi yang diharapkan dari pihak organisasi, dan apa saja hambatan yang dihadapi ketika mengumpulkan data.

BAB VI HASIL DAN PEMBAHASAN

Bab ini berisi tentang bagaimana kesenjangan yang terjadi antara kondisi kekinian dan kondisi ideal, kemudian menjelaskan bagaimana proses penilaian perangkat keamanan

informasi, hasil skor akhir dari penilaian perangkat keamanan informasi, dan rekomendasi yang diberikan untuk area yang nilainya kurang baik.

BAB VII KESIMPULAN DAN SARAN

Bab ini berisi tentang simpulan dari keseluruhan tugas akhir dan saran maupun rekomendasi terhadap penelitian tugas akhir ini untuk perbaikan ataupun penelitian lanjutan yang memiliki kesamaan dengan topik yang diangkat.

“*Halaman ini sengaja dikosongkan”*

BAB II
TINJAUAN PUSTAKA

Tinjauan Pustaka berisi Penelitian Sebelumnya dan Dasar Teori dimana bab ini menjelaskan mengenai penelitian-penelitian terkait yang mendukung seperti Pengertian Keamanan Informasi, Sistem Manajemen Keamanan Informasi(SMKI), SNI ISO/IEC 27001:2013, Indeks KAMI dan sebagai acuan atau landasan dalam pengerjaan tugas akhir ini. Landasan teori akan memberikan gambaran secara umum terhadap penjabaran tugas akhir.

2.1 Studi Sebelumnya

Dalam penelitian ini, digunakan beberapa penelitian terdahulu sebagai pedoman dan referensi dalam melaksanakan proses-proses dalam penelitian, seperti yang terdapat pada Tabel 2.1 dibawah ini. Informasi yang disampaikan dalam Tabel 1 berisi tentang informasi penelitian sebelumnya, hasil penelitian, dan hubungan penelitian terhadap penelitian sebelumnya dalam rangka tugas akhir ini.

Tabel 2.1 Peneilian Sebelumnya

Judul	Evaluasi Keamanan Informasi Menggunakan Indeks Kemanan Informasi (KAMI) Berdasarkan SNI ISO/IEC 27001:2009 Studi Kasus: Bidang Aplikasi dan Telematika Dinas Komunikasi dan Informatika Surabaya[8]
Penulis, tahun	Moch. Rashid Ridho, 2012
Metode	• Penelitian menggunakan metode Indeks KAMI versi 2.3 dan mengacu pada SNI ISO/IEC 27001:2009. • Peneliti terlebih dahulu menetapkan Peran dan Tingkat

	Kepentingan TIK dalam Instansi, dilanjutkan dengan menilai Kelengkapan Pengamanan 5 Area. • Peneliti meneliti dan menilai peran TIK dan lima area Indeks KAMI dengan dilakukan peneliti sendiri. • Peneliti melakukan wawancara dan obervasi untuk mengumpulkan bukti dan memperkuat penelitian.
Hasil Penelitian	Setelah melakukan Studi Literatur, Wawancara dan Survey, hasil yang didapat pada penelitian adalah : • Nilai yang didapat untuk Peran dan Tingkat Kepentingan TIK berada pada Kategori Kritis. • sedangkan tingkat kematangan lima area mendapatkan total skor 498 dimana tergolong baik dalam implementasi SNI ISO/IEC 27001:2009.
Relevansi	• Penelitian dilakukan dalam instansi pemerintahan. • Menggunakan metode evaluasi Indeks KAMI. • Mempunyai tujuan yang sama, yaitu mengetahui kepentingan serta peran TIK didalamnya dan melakukan evaluasi terhadap suatu instansi serta memberikan rekomendasi untuk perbaikan lebih baik.
Kelebihan	Peneliti menggunakan framework Indeks KAMI yang telah disarankan dan diwajibkan untuk

	instansi pemerintah oleh Menteri Komunikasi dan Informatika.
Kekurangan	Kekurangan dari penelitian ini adalah tidak terdapat gap analysis yang menjelaskan mengenai keadaan terkini dengan perbaikan yang untuk kedepannya.
Judul	Evaluasi Pengelolaan Keamanan Jaringan di ITS dengan Menggunakan Standar Indeks Keamanan Informasi (KAMI) Kemenkominfo RI[9]
Penulis, tahun	Luthfiya Ulinnuha, 2013
Metode	• Penelitian dilakukan melalui tahap observasi, wawancara dan studi literatur. • Penelitian dilakukan pada DPTSI ITS dengan menggunakan Indeks KAMI versi 2.3 dengan acuan ISO 27001:2009. • Penilaian dibuat berdasarkan hasil dari survey dan informasi yang berasal dari narasumber.
Hasil Penelitian	Hasil penelitian yang didapat berdasarkan pada informasi narasumber adalah sebagai berikut: • Penilaian yang dilakukan oleh peneliti pada instansi terkait menunjukkan nilai 29 yang berarti mempunyai status tinggi dan sangat diperhitungkan dalam instansi tersebut. • Nilai Keseluruhan Skor pada peran penggunaan TIK menghasilkan angka 286 yang

	masuk dalam kondisi Tinggi dengan status kesiapan perlu perbaikan.
Relevansi	Penelitian mempunyai tujuan yang sama yaitu menggunakan evaluasi Indeks KAMI untuk mengetahui peran dan kepentingan TIK dalam sebuah instansi sehingga dapat memberikan perbaikan lebih baik.
Kelebihan	Penelitian terkait menjelaskan secara rinci dan detail mengenai langkah-langkah dalam penyusunan kerangka audit.
Kekurangan	• Pada penelitian terkait, peneliti tidak melakukan perbandingan terhadap satu kerangka kerja dengan kerangka kerja lainnya. • Peneliti tidak melakukan *gap analysis* yang dapat menunjukkan kondisi eksisting dengan kondisi perbaikan yang diharapkan.
Judul	Penilaian *Service Desk* Layanan Teknologi Informasi Menggunakan OGC Self-Assessment Berbasis ITIL (Studi Kasus : Unit Sistem Informasi PT.KAI (Persero) Daerah Operasi 8 Surabaya)[10]
Penulis, tahun	Erina Umiyati, 2015
Metode	• Peneliti menggunakan metode OGC *self assessment* pada layanan *service desk* • Penulis menggunakan metode ITIL sebagai acuan untuk melakukan penilaian evaluasi dengan *self assessment*
Hasil Penelitian	Setiap tahapan dari penelitian ini

	menghasilkan sebagai berikut: • Peneliti mengumpulkan data dengan menjabarkan poin utama setiap pertanyaan dan dijabarkan ke dalam sub-sub pertanyaan. • Setiap sub-sub pertanyaan mengacu pada pemenuhan poin utama dan dijadikan sebagai bahan pengumpulan data. • Peneliti melakukan evaluasi capability level dengan pencapaian level 1,5 yang mengindikasikan bahwa adanya kesungguhan manajemen dalam mendukung pelaksanaan peran dan fungsi Unit sistem informasi sebagai *service desk*. • Terdapat 17 usulan rekomendasi dari hasil penelitian yang dilakukan.
Relevansi	• Penelitian dilakukan dalam perusahaan pemerintah. • Memiliki tujuan sama yaitu melakukan penilaian evaluasi terhadap instansi terkait dengan menggunakan metode *self assessment.*
Kelebihan	Penelitian dilakukan tidak hanya dalam satu divisi, melainkan dengan cakupan yang lebih luas yaitu terhadap keseluruhan instansi yang bersangkutan.
Kekurangan	Metode yang digunakan untuk evaluasi berbeda dengan metode

	penilaian pada Indeks KAMI.
Judul	Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya[11]
Penulis, tahun	Firzah Abdullah Basyarahil, 2017
Metode	• Peneliti menggunakan metode Indeks KAMI versi 3.1, yaitu kerangka kerja evaluasi berdasarkan SNI ISO/IEC 27001:2013 dan merupakan versi terbaru yang dikeluarkan oleh kementerian Komunikasi dan Informatika. • Menggunakan *self assessment* untuk menilai evaluasi dan *gap analysis* untuk membandingkan kondisi pada penelitian terkait.
Hasil Penelitian	Penelitian mengggunakan Indeks KAMI versi 3.1 yang berarti mempunyai hasil sedikit berbeda, yaitu: • Pada penilaian tingkat penggunaan Sistem Elektronik di DPTSI ITS, didapatkan nilai skor sebesar 26, dimana nilai menunjukkan kateori **Tinggi**. • Penilaian pada Lima Area Indeks KAMI menunjukkan nilai sebesar 249, yaitu mencapai tingkat II yang menunjukkan golongan Tidak Layak. Hal tersebut

	mempengaruhi instansi yang belum dapat melakukan sertifikasi ISO.
Relevansi	Peneliti mempunyai tujuan yang sama yaitu melakukan evaluasi terhadap instansi tertentu dan menggunakan metode Indeks KAMI versi 3.1 yang akan digunakan pada penelitian ini.
Kelebihan	Penelitian ini menyediakan langkah-langkah secara rinci dalam melakukan evaluasi terhadap instansi terkait.
Kekurangan	Penelitian menggunaka *self assessment* dan *gap analysis* tetapi tidak menilai secara *object assessment.*

Sumber:[8];[9];[10];[11]

Berdasarkan tabel diatas, telah didapatkan penjelasan mengenai studi sebelumnya yang dijadikan acuan dalam penelitian ini. Penelitian tersebut membahas terkait evaluasi keamanan informasi pada instansi pemerintahan dan instansi pendidikan. Dari beberapa analisa diatas, dapat diambil inti atau kesimpulan mengenai penelitian sebelumnya yang akan dijadikan sebagai acuan utama dan acuan pendukung sebagaimana tertulis dalam tabel berikut.

Tabel 2.2 kesimpulan penelitian sebelumnya

Penelitian 1	Penelitian 2	Penelitian 3	Penelitian 4
merupakan penelitian yang akan dijadikan sebagai **acuan pendukung**, karena	Merupakan penlitian yang akan dijadikan sebagai **acuan pendukung**,	merupakan penelitttian yang akan dijadikan sebagai **acuan utama**,	Merupakan penelitian yang akan dijadikan sebagai **acuan utama**,

mengguunakan metode Indeks KAMI versi berbeda.	karena menggunakan metode Indeks KAMI versi berbeda dengan instansi berbeda	karena menggunakan metode *self assessment*.	karena menggunakan metode Indeks KAMI versi yang sama.

Sumber: [peneliti, 2018]

2.2 Dasar Teori

Dasar teori merupakan bagian yang akan dijadikan sebagai pengumpulan informasi terkait melalui berbagai pustaka. Pada bagian ini akan dibahas teori dan penelitian lain sebagai pendukung pengerjaan Tugas Akhir.

2.2.1 Definisi Evaluasi

Ketika melakukan usaha atau pekerjaan, maka seseorang akan mendapatkan hasil. Tetapi, sebelum mendapatkan hasil tersebut, seseorang harus melalui tahap penilaian. Penilaian biasa disebut sebagai evaluasi. Tahap evaluasi dilakukan untuk dapat mengukur seberapa besar usaha yang telah dilakukan dan untuk dapat menjadi bahan perbaikan pada usaha selanjutnya. Menurut KBBI, evaluasi adalah penilaian atau memberikan penilaian[12]. Dalam kamus Oxford, evalusi berarti pembuatan keputusan tentang jumlah, angka/bilangan, atau nilai sesuatu[13]. Selain itu evaluasi berarti studi sistematis individual yang dilakukan secara berkala atau secara ad-hoc untuk menilai seberapa baik sebuah program berjalan[14]. Pendapat lain mengatakan bahwa evaluasi adalah pengumpulan informasi secara sistematis mengenai aktivitas, karakteristik dan keluaran program untuk digunakan oleh sebagian orang agar mengurangi ketidakpastian, meningktkan efektivitas, dan membuat keputuan dengan menanggap pada apa yang program tersebut lakukan[15]. Dari berbagai pengertian diatas, maka evaluasi dapat didefinisikan

menjadi suatu proses untuk menyediakan informasi tentang sejauh mana suatu kegiatan telah tercapai, bagaimana perbedaan pencapaian itu dengan suatu standar tertentu untuk mengetahui apakah ada selisih diantara keduanya, serta bagaimana manfaat yang telah dikerjakan dibandingkan dengan harapan-harapan yang ingin diperoleh[16].

Terdapat tahapan-tahapan yang harus dilalui ketika menjalankan proses evaluasi. Walaupun setiap proses evaluasi kemungkinan mempunyai tahapan yang berbeda, tetapi masih terdapat tahapan-tahapan penting dan bersifat umum yang sering digunakan dalam melakukan proses evaluasi[16].

- **Menentukan apa yang akan dievaluasi**, dalam hal ini sering kali mengacu pada program kerja instansi/perusahaan.
- **Merancang kegiatan evaluasi**, sebelum melakukan evaluasi dilakukan rancangan (desain) evaluasi. Yaitu merancang data apa saja yang dibutuhkan, tahapan kerja yang dilalui, siapa yang dilibatkan, apa yang akan dihasilkan agar menjadi jelas.
- **Mengumpulkan data**, pengumplan data dapat dilakukan sesuai dengan kaidah-kaidah ilmiah yang berlaku dan sesuai dengan kebutuhan & kemampuan.
- **Mengolah dan menganalisis data**, data yang terkumpul diolah dan dikelomokkan lalu dianalisis dan menghasilkan fakta terpecaya. Fakta kemudian akan dibandingkan dengan harapan untuk menghasilkan gap.
- **Pelaporan hasil evaluasi**, pemanfaatan evaluasi bagi pihak-pihak berkepentingan.

2.2.2 Teknologi Informasi

Isilah Teknologi Informasi sudah tidak asing didengar oleh telinga. Awal mula kepopuleran istilah tersebut dimulai pada akhir dekade 70-an, dimana sebelumnya dikenal dengan teknologi kompuputer atau pengolahan data elektronis atau EDP (Electronic Data Processing)[17].

Terdapat beberapa definisi mengenai Teknologi Informasi. Turban mengulas bahwa istilah teknologi informasi adalah

untuk menjabarkan sekumpulan sistem informasi, pemakai, dan manajemen. Pendapat tersebut masih menjelaskan pengertian dalam arti luas[18]. Menurut Kamus Oxford, teknologi Informasi adalah studi atau penggunaan peralatan elektronika, terutama kompter, untuk menyimpan, menganalisa, dan mendistibusikan informasi apa saja, termasuk kata-kata, bilangan, dan gambar[19]. Sedangkan Martin mendefinisikan teknologi informasi tidak hanya sebatas pada teknologi komputer (perangkat keras dan perangkat lunak) untuk memproses dan menyimpan informasi[20].

Dalam kamus KBBI, teknologi informasi terdiri dari 2 gabungan kata. Yaitu dari kata teknologi dan informasi. Teknologi mempunyai arti sebagai metode ilmiah untuk mencapai tujuan praktis[21], sedangkan Informasi berarti pemberitahuan, kabar atau berita tentang sesuatu[22]. Jadi, dua kata tersebut jika digabungkan akan mempunyai pengertian segala bentuk alat yang diterapkan dan digunakan untuk menyimpan, memproses dan mengirimkan informasi dalam bentuk elektronis[23].

Teknologi informasi telah mempunyai perkembangan pesat. Ia telah berperan dalam berbagai aspek, mulai dari memudahkan pekerjaan yang mudah sampai dengan fasilitator utama untuk kelangsungan bisnis perusahaan. Secara garis besar, dapat dikatakan bahwa[17]:

- Teknologi Informasi menggantikan peran manusia. Yaitu teknologi informasi melakukan otomasi terhadap suatu tugas atau proses;
- Teknologi memperkuat peran manusia, yakni dengan menyajikan informasi terhadap suatu tugas atau proses;

Teknologi Informasi berperan dalam restrukturisasi terhadap peran manusia. Dalam hal ini, teknologi berperan dalam melakukan perubahan-perubahan terhadap sekumpulan tugas atau proses.

2.2.3 Sistem Informasi

Sistem Informasi merupakan suatu hal yang telah disebut berkali-kali. Walaupun begitu, sering kali orang-orang tidak mengetahui pengertian dari sistem informasi. Sistem informasi mempunyai beberapa definisi atau pengertian. Secara umum ia adalah bentuk penggabungan kata, terdiri dari dua kata yaitu sistem dan informasi. Sistem mempunyai arti perangkat unsur yang secara teratur saling berkaitan sehingga membentuk suatu loyalitas. Secara sederhana, sistem dapat diartikan sebagai suatu kumpulan atau himpunan dari unsur atau variabel-variabel yang saling terorganisisasi, saling berinteraksi, saling bergantung sama lain[24]. Sedangkan informasi mempunyai arti sebagai pemberitahuan, kabar atau berita tentang sesuatu, hal tersebut mempunyai maksud bahwa informasi merupakan data yang telah diolah menjadi sebuah bentuk berarti bagi penerimanya dan bermanfaat dalam pengambilan keputusan[24]. Jika dua kata tersebut dikaitkan dan dihubungkan, maka sistem informasi berarti sekumpulan elemen yang terorganisasi untuk mencapai tujuan dalam organisasi[25].

Menurut Alter (1992), sistem informasi adalah kombinasi antara prosedur kerja, informasi, orang dan teknologi informasi yang diorganisasikan untuk mencapai tujuan dalam sebuah organisasi[17]. Turban, McLean, dan Wetherbe (1999) menjelaskan bahwa sebuah sistem informasi mengumpulkan, memproses, menyimpan, menganalisis, dan menyebarkan informasi untuk tujuan yang spesifik[18]. Dan Hall (2001), menyebutkan bahwa sistem informasi adalah sebuah rangkaian prosedur formal di mana data dikelompokkan, diproses menjadi informasi dan didistribusikan kepada pemakai[17].

Sistem informasi yang berhubungan dengan komputer disebut dengan sistem informasi berbasis komputer (Computer-Based Information System/CBIS), dimana sistem informasi tersebut mempunyai beberapa komponen. Komponen-komponen sistem informasi adalah sebagai berikut[24]:

- **Perangkat Keras (*hardware*)**, adalah alat yang mencakup peranti-peranti fisik seperti komputer dan printer.

- **Perangkat Lunak (*software*)**, merupakan instruksi yang memungkinkan perangkat keras untuk dapat memproses data.
- **Manusia (*people*)**, adalah pihak yang bertanggung jawab dalam pengembangan sistem informasi, pemrosesan dan penggunaan sistem informasi.
- **Basis data (*database*)**, merupakan sekumpulan tabel, hubungan, dan lain-lain yang berkaitan dengan penyimpanan data.
- **Telekomunikasi (*telecommunication*)**, yaitu sistem penghubung yang memungkinkan sumber daya dapat dipakai secara bersama atau diakses oleh sejumlah pemakai.
- **Prosedur (*procedure*),** merupakan sekumpulan aturan yang dipakai untuk mewujudkan pemrosesan data dan pembangkitan keluaran yang dikehendaki.

2.2.4 Keamanan Informasi

Keamanan informasi merupakan salah satu istilah yang sering didengar saat ini. Pada awal kemunculan komputer, istilah yang digunakan pada saat itu adalah keamanan komputer, menggambarkan tentang spesifikasi kebutuhan untuk melindungi lokasi fisik teknologi komputer dari ancaman luar. Seiring berjalannya waktu, istilah tersebut mempresentasikan keseluruhan aksi untuk mempertahankan sistem komputer dari kerugian. Sehingga, hal tersebut berevolusi menjadi konsep yang sekarang dikenal yaitu keamanan informasi, melindungi seluruh informasi dalam suatu organisasi[26].

Terdapat beberapa definisi yang menggambarkan apa itu keamanan informasi. Keamanan informasi menggambarkan usaha untuk melindungi komputer dan non peralatan komputer, fasilitas, data dan informasi dari penyalahgunaan oleh orang yang tidak bertanggung jawab[27]. Keamanan informasi berarti penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (*business continuity*), meminimasi risiko bisnis (*reduce business risk*) dan

memaksimalkan atau mempercepat pengembalian investasi dan peluang bisnis[28].

Informasi merupakan salah satu asset organisasi yang sangat berharga dan penting sehingga perlu dilindungi, tetapi terkadang perusahaan mengabaikan hal tersebut sampai terjadi ancaman yang menyerang. Keamanan informasi harus dilakukan karena dapat mencegah tindakan dari serangan penggunaan komputer atau akses yang tidak bertanggung jawab serta dapat mempertahankan asset penting perusahaan[29]. Berdasarkan lubang keamanan yang ada, terdapat 4 klasifikasi keamanan yaitu[30]:

a. **Keamanan yang bersifat fisik (*physical security*)**, hal yang mencakup kelemahan yang berasal dari peralatan dan media yang digunakan. Seperti karyawan yang menaruh akun dan password pada note kertas yang bisa terlihat oleh semua orang, atau orang yang kehilangan komputer jinjing (laptop) dimana data tersebut memiliki sifat confidential.
b. **Keamanan yang berhubungan dengan orang (*personal security*)**, yaitu hal-hal yang mencakup kelemahan berasal dari profil pihak/karyawan yang mempunyai akses. Contoh lain adalah penggunaan Teknik *social engineering.*
c. **Keamanan dari data dan media serta Teknik komunikasi (*communications security*)**, yaitu kelemahan dalam perangkat lunak untuk pengolahan data. Seperti pelaku kejahatan memasukkan virus ke dalam komputer dan mendapatkan informasi yang bukan hak akses pelaku tersebut.
d. **Keamanan dalam operasional atau manajemen teknologi informasi (*management security*)**, yaitu hal-hal yang mencakup kelemahan dalam kebijakan dan prosedur. Sering kali perusahaan tidak memiliki kebijakan dan prosedur sehingga penggunaan teknologi informasi tidak terkontrol dan terkondisikan.

Selain itu, kemanan informasi mempunyai banyak tujuan. Dua tujuan diantaranya adalah sebagai berikut[29]:

- Melindungi data/informasi yang tersimpan dalam/luar komputer dari kerusakan atau kehancuran yang dilakukan secara sengaja atau tidak sengaja;
- Mencegah dan mendeteksi perubahan terhadap informasi yang dilakukan oleh tidak berkewenangan serta menjaga agar informasi tidak tersebar luas kepada yang tidak berkewenang.

Dari tujuan-tujuan diatas, maka perlindungan terhadap informasi juga mempunyai beberapa aspek. Aspek-aspek yang terdapat dalam keamanan informasi terbagi menjadi 3, yaitu[28]:

- ***Confidentiality*** **(Kerahasiaan)**
  Confidentiality merupakan perlindungan terhadap informasi dari akses tidak berwenang atau akses tanpa otorisasi[29]. Aspek ini menjamin kerahasiaan data dan informasi, memastikan informasi hanya diakses oleh orang-orang yang berwenang dan menjamin kerahasiaan terhadap pengiriman, penerimaan dan penyimpanan data[28].
- ***Integrity*** **(Integritas)**
  Integrity adalah penyajian informasi yang akurat, benar dan lengkap[29]. Aspek ini berarti menjamin bahwa data tidak diubah tanpa terdapat izin pihak yang berwenang, menjaga keakuratan dan keutuhan informasi serta metode prosesnya menjamin aspek integritas itu sendiri[28].
- ***Availability*** **(Ketersediaan)**
  Availability adalah menyediakan sistem informasi untuk menunjang proses bisnis[29]. Aspek tersebut menjamin bahwa data akan tersedia saat akan dibutuhkan, memastikan pengguna berhak menggunakan informasi dan perangkat terkait (asset yang berhubungan bilamana diperlukan)[28].

Ketiga aspek diatas tidak dapat dipisahkan dan saling berkaitan, sehingga keamanan informasi dapat terjaga. Tiga aspek tersebut juga mempunyai singkatan yang sering disebut sebagai CIA (Confidentiality, Integrity, dan Avaliability).

Berikut adalah gambar keterkaitan antara tiga aspek keamanan informasi:

Gambar 2.2.1 diagram CIA

Sumber:[27]

2.2.5 Sistem Manajemen Keamanan Informasi (SMKI)

Keamanan informasi telah disebutkan bahwa dapat mencegah tindakan dari serangan penggunaan komputer dan akses secara tidak bertanggung jawab serta sebagai bentuk suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Hal tersebut terkadang membuat seseorang akan bertindak secara berlebihan. Sesuatu jika terlalu disikapi secara berlebihan, dalam konteks ini berarti over protective tidak akan pernah merasa aman. Karena setiap waktu ia merasa hal-hal buruk akan terjadi. Maka dari itu, perlu adanya sistem pengelolaan keamanan informasi. Karena dengan adanya pengelolaan tersebut, suatu instansi atau perusahaan tetap dapat fokus terhadap bisnis dan menngembangkan usaha atau layanan yang menjadi prioritasnya[30].

Sistem Manajemen Keamanan Informasi (SMKI) atau dalam bahasa inggris sering disebut sebagai *Information Security Management System* (ISMS) merupakan suatu proses yang disusun berdasarkan pendekatan risiko bisnis untuk merencanakan (*Plan*), mengimplementasikan dan mengoperasikan (*Do*), memonitor dan meninjau ulang (*Check*), serta memelihara dan meningkatkan atau mengembangkan (*Act*) terhadap Keamanan Informasi perusahaan[30]. pendapat lain mengatakan bahwa ISMS adalah sebuah sistem proses, dokumen, teknologi dan orang-

orang yang membantu mengelola, memantau, mengevaluasi dan memperbaiki keamanan informasi organisasi[31]. Ia juga dapat berarti sebagai sebuah pendekatan terstruktur dan sistematis untuk mengelola informasi sehingga tetap aman. Singat kata SMKI adalah suatu pendekatan proses 'Plan-Do-Check-Act'dengan dukungan manajemen[30].

Implementasi SMKI tidak hanya sekedar implementasi tanpa bantuan apa-apa. Ia harus didukung dengan beberapa hal berikut untuk dapat diimplementasikan. Yaitu dengan dukungan perencanaan (*Planning*), kebijakan keamanan (*security policy*), program (prosedur dan proses), penilaian risiko (*risk assessment*) dan sumber daya manusia (*people*)[30].

Standar SMKI merupakan standar yang dimiliki Sistem Manajemen Keamanan Informasi, karena di dalamnya menyangkut suatu cara pengelolaan yang mana sangat diperlukan suatu standar pengelolaan. Terdapat berbagai model standar SMKI dan penerapannya. Masing-masing memfokuskan diri pada area yang berbeda dalam praktek SMKI. Salah satu standar SMKI sebagai rujukan adalah ISO/IE 27001[30].

2.2.5.1 SMKI berdasarkan ISO/IEC 27001

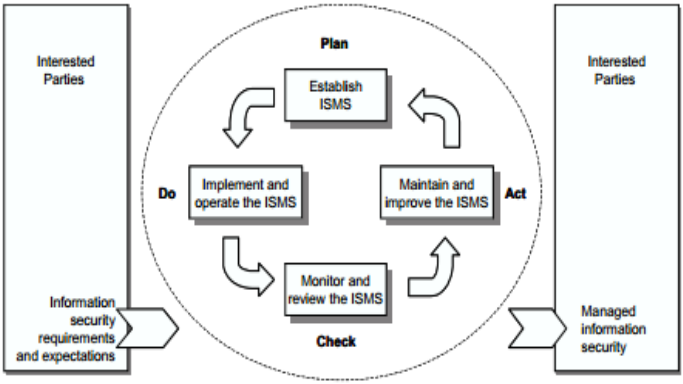
ISO/IEC 27001 adalah standar Keamanan Informasi (*information security*) yang diterbitkan oleh ISO (*The International Organization for Standardization*) dan IEC (*The International Electrotechnical Commission*) pada bulan Oktober 2005 yang menggantikan standar BS-77992:2002. ISO 27001 berisi mengenai persyaratan standar yang harus dipenuhi untuk membangun SMKI, ia juga mendefinisikan keperluan-keperluan untuk Sistem Manajemen Keamanan Informasi (SMKI) dan memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah organisasi dalam implementasi konsep keamanan informasi di organisasi[30].

ISO 27001 patut dijadikan pertimbangan dalam implementasi SMKI adalah karena beberapa hal berikut[30]:

a. ISO/IEC 27001 menyediakan model lengkap terkait SMKI, seperti[30]:
   - Membangun SMKI (*establishing*);
   - Implementasi SMKI (*implementation*);
   - Operasional SMKI (*operational*);
   - Memonitor SMKI (*monitoring*);
   - Mengkaji ulang SMKI (*reviewing*);
   - Memelihara SMKI (*maintaining*);
   - Mengembangkan SMKI (*improving*).

b. ISO/IEC 27001 mempunyai desain agar implementasi SMKI menjadi fleksibel dikembangkan karena bergantung pada[30]:
   - Kebutuhan organisasi (*needs*);
   - Tujuan organisasi yang akan dicapai (*objectives*);
   - Persyaratan keamanan yang diperlukan (*security requirement*);
   - Proses bisnis yang ada (*the processes*);
   - Jumlah pegawai dan ukuran struktur organisasi (*employe and the size structure of organization*).

Pendekatan proses yang didefinisikan dalam ISO/IEC 27001 adalah siklus PDCA (Plan-Do-Check-Act) yang terlihat pada gambar berikut:



Gambar 2.2.2 Model PDCA dalam aplikasi proses SMKI

Sumber:[32]

Dari gambar diatas, dapat dijelaskan mengenai proses "Plan-Do-Check-Act" sebagai berikut[30]:

1. **Plan**
   Tahapan yang merupakan perencanaan dan perancangan SMKI. Seperti membangun komitmen, kebijakan, Kontrol, prosedur, instruksi kerja dan lain-lain sehingga tercipta SMKI sesuai dengan keinginan.
2. **Do**
   Tahapan pengimplemetasian dan operasi dari kebijakan, Kontrol, proses dan prosedur SMKI yang telah dibangun/direncanakan pada tahapan plan.
3. **Check**
   Tahapan yang membahas kegaitan monitoring pelaksanaan SMKI, termasuk melakukan evaluasi dan audit terhadap SMKI.
4. **Act**
   Adalah tahapan kegiatan pengembangan (improvement) dimana di dalamnya merupakan kegiatan perbaikan dan pengembangan SMKI.

2.2.6 (KAMI versi 3.1) sebagai *Tools* SMKI

Indeks Keamanan Informasi merupakan sebuah alat evaluasi yang digunakan untuk menganalisa tingkat kesiapan pengamanan informasi pada instansi pemerintahan[33]. Ditujukan untuk menganalisa dan memberi gambaran mengenai kondisi kelengkapan dan kematangan pada keamanan informasi. Indeks KAMI dibuat berdasarkan pada penerapan ISO/IEC 27001 dan memiliki versi terbaru yaitu versi 3.1 yang setara dengan ISO/IEC 27001:2013. Dibuat oleh Kementerian Komunikasi dan Informatika (Kominfo). Bentuk evaluasi yang diterapkan dalam Indeks KAMI dirancang untuk dapat digunakan oleh instansi pemerintah dari berbagai tingkatan, ukuran maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya Tugas Pokok dan Fungsi. Evaluasi Indeks Keamanan Informasi mencakup penilaian sistem elektroik dan 5 area, yaitu[33]:

1. **Kategori Sistem Elektronik**

2. **Area Tata Kelola Keamanan Informasi**
3. **Area Pengelolaan Risiko Keamanan Informasi**
4. **Area Kerangka Kerja Keamanan Informasi**
5. **Area Pengelolaan Aset Informasi**
6. **Area Teknologi dan Keamanan Informasi**

2.2.6.1 Perhitungan skor penilaian Indeks KAMI versi 3.1

Pertanyaan setiap Area pada Indeks KAMI mempunyai 2 keperluan, yaitu[33]:

1. Pengelompokan kategori tingkat kesiapan penerapan pengamanan sesuai dengan **Kelengkapan** Kontrol standar ISO/IEC 27001:2013

Pengelompokan ini responden diminta memberikan tanggapan mulai dari area yang terkait dengan bentuk:

- kerangka kerja dasar keamanan informasi (pertanyaan dengan label kategori pengamanan ‘1’);
- efektivitas dan konsistensi penerapan (pertanyaan label kategori pengamanan‘2’);
- dan kemampuan untuk selalu meningkatkan kinerja keamanan informasi (pertanyaan label kategori pengamanan ‘3’).

Terdapat empat jawaban untuk setiap pertanyaan yang ada pada Indeks KAMI. Berikut adalah gambar tabel status pengamanan dalam Indeks KAMI sesuai dengan kesiapan minimum yang diprasyaratkan oleh proses sertifikasi standar ISO/IEC 27001:2013:

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

Gambar 2.2.3 Matriks Skor Pengamanan

Sumber:[33]

Pertanyaan dengan label kategori pengamanan ‘3’ pada keseluruhan area pertanyaan Indeks KAMI hanya dapat memberikan skor nilai/hasil apabila semua pertanyaan terkait label kategori pengamanan ‘1’ dan ‘2’ terisi dengan status pengamanan “Diterapkan Sebagian”.

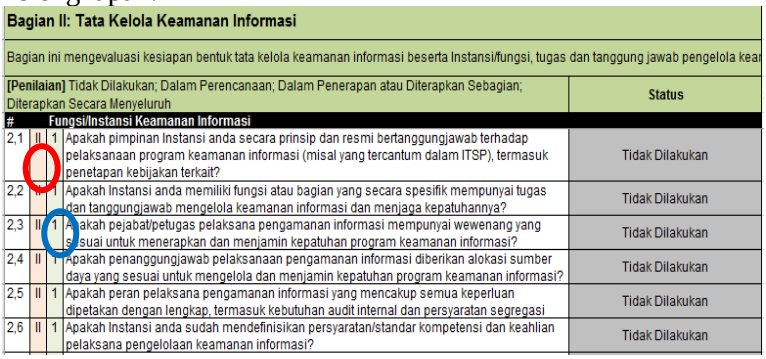
2. Pengelompokan berdasarkan tingkat **Kematangan** penerapan pengamanan yang mengacu pada tingkatan keamanan oleh kerangka kerja COBIT atau CMMI

Pada pengelompokan ini, tingkat kematangan akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di Kementerian/Lembaga. Definisi tingkat kematangan adalah sebagai berikut:

- Tingkat I – Kondisi Awal
- Tingkat II – Penerapan Kerangka Kerja Dasar
- Tingkat III – Terdefinisi dan Konsisten
- Tingakt IV – Terkelola dan Terukur
- Tingkat V – Optimal

Terdapat penambahan tingkatan sebagai uraian yang lebih detail, yaitu terdapat tingkatan -I+, II+, III+, dan IV+ yang menjadikan total 9 tingkatan kematangan. Tingkat kematangan yang setara dengan ISO/IEC 27001:2013 memiliki ambang batas minimum kesiapan dengan tingkat III+.

Ilustrasi dibawah menunjukkan label kematangan dan kelengkapan:



Bagian II: Tata Kelola Keamanan Informasi

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

[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	Tidak Dilakukan
2,6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan

Gambar 2.4 pengelompokan label kematangan dan kelengkapan

Sumber:[33]

Keterangan :

- Lingkar merah pada label menunjukkan label pengelompokan kematangan (kolom disebelah kanan nomor urut)
- Lingkar biru menunjukkan label kelengkapan/kategori pengamanan (kolom sebelah kiri pertanyaan).

2.2.6.2 Area Penilaian dan Pemetann Indeks Keamanan Informasi versi 3.1 dengan Kontrol ISO/IEC 27001:2013

Area yang akan dilakukan evaluasi penilaian keamanan informasi adalah bagian Tata Kelola Keamanan Informasi. Area Tata Kelola Keamanan Informasi dipilih karena tata kelola secara umum dapat didefinisikan sebagai struktur hubungan dan proses yang mengarahkan dan mengontrol organisasi agar tujuan organisasi dapat tercapai dan memastikan bahwa proses yang memberikan dukungan optimal terhadap pemenuhan tujuan organisasi telah dipenuhi oleh sumber daya TI[34].

Hal tersebut, menyimpulkan bahwa tata kelola TI menyeleraskan bisnis dan TI dan mengarahkan pada pemenuhan nilai bisnis organisasi. Dalam konteks keamanan informasi, tata kelola dapat melindungi aset informasi berdasarkan keselarasan bisnis dan TI sehingga dapat meminimalkan risiko, memastikan keberlanjutan bisnis dan memaksimalkan keuntungan yang didapat dari kesempatan bisnis dan investasi[34].

Tabel 2.3 pemetaan Indeks KAMI area tata kelola keamanan informasi dengan kontrol ISO/IEC 27001:2013

Pertanyaan Area Indeks KAMI	Klausul Kontrol ISO/IEC 27001:2013
Tata Kelola Keamanan Informasi	
# Fungsi/Instansi Keamanan Informasi	

Pertanyaan Area Indeks KAMI				Klausul Kontrol ISO/IEC 27001:2013
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?	A.5.1.1 *Policies for information security*
2,2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	A.6.1.1 *Information security roles and responsibilities*
2,3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	A.6.1.2 *segregation of duties*
2,4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	A.12.1.3 *Capacity management* A.8.1.3 *Acceptable use of Assets*
2,5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit	A.6.1.2 *Segregation of duties* A.8.2.3 *Handling of*

Pertanyaan Area Indeks KAMI				Klausul Kontrol ISO/IEC 27001:2013
			internal dan persyaratan segregasi kewenangan?	*assets*
2,6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	A.7.1.2 *Terms and conditions of employment*
2,7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	A.7.1.1 *Screening* A.7.2.2 *Information security awareness, education and training*
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?	A.7.2.2 *Information security awareness, education and training* A.7.2.3 *Disciplinary process*
2,9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	A.7.2.2 *Information security awareness, education and training*

Pertanyaan Area Indeks KAMI				Klausul Kontrol ISO/IEC 27001:2013
2.10	II	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	A.7.2.1 *Management responsibilities*
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?	A.7.2.1 *Management responsibilities*
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?	A.6.1.4 *Contact with special interest group* A.13.2.1 *Information transfer policies and procedures* A.13.2.2 *Agreements on information transfer*
2.13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan	A.6.1.3 *Contact with authorities* A.13.2.4 *Confidentiality or non*

Pertanyaan Area Indeks KAMI				Klausul Kontrol ISO/IEC 27001:2013
			pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?	*disclosure agreements*
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?	A.17.1.1 *Planning information security continuity* A.17.1.2 *Implementing information security continuity*
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?	A.16.1.2 *Reporting information security events*
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?	A.5.1.2 *Review of the policies for information security* A.8.2.1 *Classification of information*

Pertanyaan Area Indeks KAMI				Klausul Kontrol ISO/IEC 27001:2013
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?	A.6.1.5 *Information security in project management* A.8.2.3 *Handling of assets*
2.18	IV	3	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	A.5.1.2 *Reviews of the policies for information security* A.6.1.5 *Information security in project management* A.18.2.1 *Independent review of information security*
2.19	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	A.7.2.3 *Disciplinary process*
2.20	IV	3	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi	A.17.1.3 *Verify, review and evaluate information security*

Pertanyaan Area Indeks KAMI				Klausul Kontrol ISO/IEC 27001:2013
			pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi?	*continuity* A.18.2.1 *Independent review of information security*
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?	A.18.1.1 *Identification of applicable legislation and contractual requirements*
2.22	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	A.16.1.1 *Responsibilities and procedures* A.18.1.3 *Protection of records*

Sumber: [penulis, 2018]

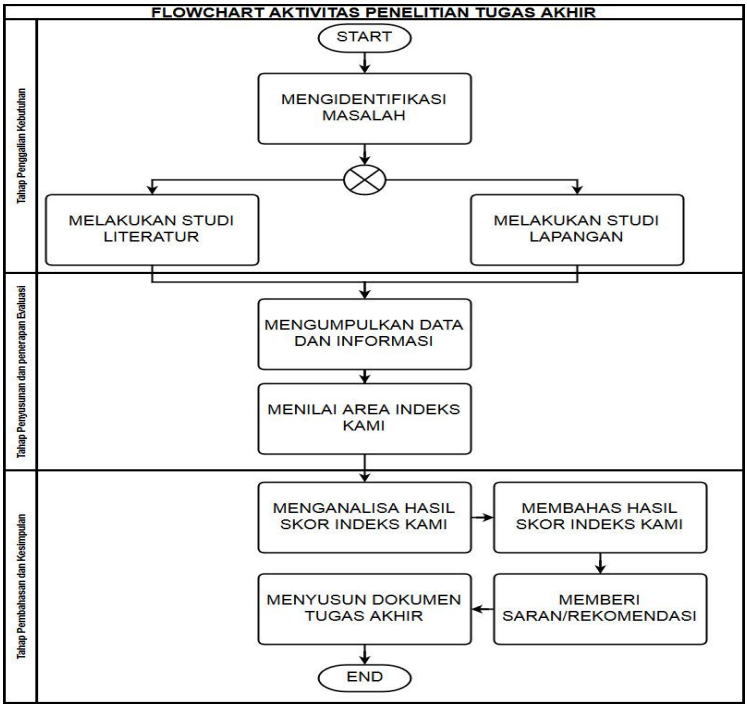
“Halaman ini sengaja dikosongkan”

BAB III
METODOLOGI

Metodologi penelitian merupakan bab yang menjelaskan mengenai langkah-langkah penelitian dalam pengerjaan tugas akhir agar penelitian dapat terselesaikan secara sistematis, terorganisir, jelas, dan terarah.

3.1 Tahapan Pelaksanaan Tugas Akhir

Alur tahapan pelaksanaan yang dilakukan dalam mengerjakan tugas akhir ini sesuai dengan alur pada gambar 3.1.



Gambar 3.1 Alur Metodologi Pengerjaan Tugas Akhir

Sumber:[penulis, 2018]

3.1.1 Tahap Penggalian Kebutuhan

Tahapan penggalian kebutuhan merupakan tahapan awal dari pengerjaan penelitian tugas akhir ini. Tahap ini menggali masalah dan latar belakang mengenai kebutuhan untuk menerapkan evaluasi pada dinas Komunikasi dan Informatika Pemerintah Daerah XYZ. Kemudian pencarian studi literatur dan studi lapangan instansi yang berkaitan dengan penerapan evaluasi keamanan informasi dengan Indeks KAMI. Hasil tahapan ini adalah berupa kondisi saat ini pada instansi, seperti jumlah aset informasi, proses bisnis yang menggunakan digital online dan struktur organisasi serta tugas pokok dan fungsi organisasi. Data tersebut didapatkan melalui aktivitas berikut dan selanjutnya menjadi input untuk tahapan penyusunan evaluasi keamanan informasi.

3.1.1.1 Mengidentifikasi Masalah

Proses ini merupakan aktivitas awal sebelum dapat melakukan penerapan evaluasi. Aktivitas yang dilakukan adalah menggali data/informasi melalui berbagai media dan sumber. Melakukan observasi terhadap tempat penelitian terkait dengan melakukan teknik wawancara terhadap pihak yang berkaitan.. Hasil luaran berupa rumusan masalah, tujuan dan data-data pendukung yang dapat membantu merumuskan permasalahan serta menjwab permasalahan yang digunakan sebagai masukan untuk aktivitas dan tahap selanjutnya.

Tabel 3.1 Input, proses, output Identifikasi Masalah

INPUT	PROSES	OUTPUT
• Media mengenai pentingnya keamanan informasi • Peraturan yang mendukung keamanan informasi	• Mengidentifikasi masalah keamanan informasi pada instansi • Menghubungkan masalah dengan pentingnya keamanan informasi	Dapat merumuskan masalah penelitian, membuat tujuan dan batasan penelitian

INPUT	PROSES	OUTPUT
dan evaluasi indeks KAMI.		

Sumber: [penulis, 2018]

3.1.1.2 Melakukan Studi Literatur

Pada aktivitas ini, akan dilakukan penggalian data melalui berbagai pustaka. Pustaka yang diambil berdasarkan penelitian sabelumnya yang berbentuk jurnal, penelitian tugas akhir atau artikel dan informasi-informasi lainnya yang berhubungan dengan penelitian ini. Tujuan dari aktivitas ini adalah untuk membantu pengerjaan penelitian tugas akhir yang dikerjakan saat ini.

Tabel 3.2 *input,* proses, output studi literatur

INPUT	PROSES	OUTPUT
Latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian.	• Mempelajari setiap literatur yang berhubungan dengan topik penelitian tugas akhir ini. • Menghubungkan setiap pustaka dengan topik penelitian tugas akhir ini.	Konsep penelitian yang menerapkan evaluasi indeks KAMI

Sumber: [penulis, 2018]

3.1.1.3 Melakukan Studi Lapangan

Merupakan aktivitas yang dilakukan dengan melakukan wawancara dengan pihak instansi terkait. Wawancara dilakukan dengan tujuan mengetahui Indeks KAMI mana yang cocok digunakan dalam instansi, karena pada batasan masalah dijelaskan bahwa hanya menggunakan 1 Area penilaian Indeks KAMI.

Tabel 3.3 *input*, proses, *output* studi lapangan

INPUT	PROSES	OUTPUT
Konsep penelitian yang berhubungan dengan keamanan informasi dan Indeks KAMI	Menggali kebutuhan terhadap penyelesaian keamanan informasi yang sesuai dengan area indeks KAMI	Perangkat Indeks KAMI yang sesuai dengan kebutuhan penyelesaian masalah di intansi

Sumber: [penulis, 2018]

3.1.2 Tahap Penyusunan dan Penerapan Evaluasi

Tahapan selanjutnya adalah penyusunan evaluasi dengan membuat beberapa pertanyaan yang telah tertulis dalam kerangka kerja Indeks KAMI dan akan diberikan kepada pihak yang bersangkutan. Selain mempermudah dalam melakukan evaluasi, pertanyaan tersebut juga sebagai bentuk agar dapat dijawab dalam berbagai tingkatan dan ukuran.

3.1.2.1 Mengumpulkan data dan informasi

Pada aktivitas ini, akan dilakukan pengumpulan data dan informasi terkait yang berhubungan dengan penerapan evaluasi. Sebelum melakukan pengumpulan data, dilakukan anlisis untuk membuat pertanyaan pengumpulan data. Pertanyaan tersebut dijadikan sebagai salah satu acuan fakta dan bukti dalam memberi nilai justifikasi Indeks KAMI. Data dan informasi dapat berupa dokumen-dokumen pendukung yang memudahkan mendapatkan informasi yang belum terdapat dalam hasil wawancara. Dokumen-dokumen pendukung yang berhubungaan dengan kelengkapan evaluasi Indeks KAMI. Hasil dari aktivitas ini adalah mengetahui kondisi terkini instansi terkait.

Tabel 3.4 *Input,* proses, *output,* pengumpulan data dan informasi

INPUT	PROSES	OUTPUT
• Membuat identifikasi poin pertanyaan; • Melakukan pemetaan poin pertanyaan dengan kontrol ISO 27001; • Membuat pertanyaan untuk pengumpulan data;	Mengumpulkan data dan informasi mengenai instansi yang sesuai dengan data keperlua evaluasi Indeks KAMI	• Kondisi terkini instansi dan dokumen yang berhubungan dengan Indeks KAMI; • Perangkat evaluasi Indeks KAMI yang siap digunakan.

Sumber: [penulis, 2018]

3.1.2.2 Menilai Area Tata Kelola Keamanan Informasi Indeks KAMI

Aktivitas ini dilakukan setelah diketahui status akhir pada Kategori Sistem Elektronik. Penilaian Area dilakukan dengan tujuan dapat mengetahui dan menentukan nilai kematangan penerapan keamanan informasi pada instansi terkait. Penilaian dilakukan dengan melakukan wawancara dan observasi pada pihak penanggung jawab. Bentuk pertanyaan disesuaikan dengan kerangka kerja Area Tata Kelola Keamanan Informasi Indeks KAMI dengan mengikutsertakan beberapa review dokumen dan data pendukung lainnya. Review dokumen dan data pendukung akan dijadikan sebagai bukti dalam penilaian Area Tata Kelola Keamanan Informasi Indeks KAMI.

Tabel 3.5 *input, proses, ouput* menilai area tata kelola keamanan informasi

INPUT	PROSES	OUTPUT
Dokumen pendukung evaluasi penilaian Area Tata Kelola Kemanan Informasi Indeks KAMI	Menilai Area Tata Kelola Kemanan Informasi berdasarkan pertanyaan Indeks KAMI	Hasil nilai skor penilaian Area Tata Kelola Keamanan Informasi

Sumber: [penulis, 2018]

3.1.3 Tahap pembahasan dan kesimpulan

Tahapan pembahasan dan Kesimpulan merupakan tahapan terakhir dalam penelitian tugas akhir. Dalam tahapan ini akan dijelaskan mengenai hasil perhitungan pada Area Indeks KAMI. Selain itu, pada tahap ini juga terdapat kesimpulan penilaian Area Indeks KAMI dan saran perbaikan serta pembuatan tugas akhir sebagai bentuk dokumen tertulis penelitian.

3.1.3.1 Menganalisa hasil skor Area Indeks KAMI

Setelah dilakukan penilaian pada setiap pertanyaan Area Tata Kelola Keamanan Informasi, maka dilakukan penjumlahan dari setiap jawaban. Total nilai menunjukkan kematangan pada area tersebut. Berikut adalah penjelasan perhitungan kematangan pada Area Tata Kelola Keamanan Informasi:

Jumlah pertanyaan Tahap 1	8
Jumlah pertanyaan Tahap 2	8
Jumlah pertanyaan Tahap 3	6
Batas Skor Min untuk Skor Tahap Penerapan 3	48
Total Skor Tahap Penerapan 1 & 2	0
Status Peniliaian Tahap Penerapan 3	Tidak Valid

Gambar 3.2 informasi penilaian tahap 1,2,3

Sumber: [33]

Informasi pertama yaitu terdapat informasi mengenai jumlah pertanyaan tahap 1, tahap 2 dan tahap 3. Untuk dapat menjawab pertanyaan tahap 3 perlu skor minimal 1 & 2. Total

keseluruhan skor jawaban tahap 1 dan tahap 2 adalah harus minimal 48. Maka penilaian terhadap tahap 3 dapat dihitung sebagai valid.

Skor Tingkat Kematangan II	0
Skor Minimum Tingkat Kematangan II	*12*
Skor Pencapaian Tingkat Kematangan II	*36*
Status	No
Skor Tingkat Kematangan III	0
Validitas Tingkat Kematangan III	No
Skor Minimum Tingkat Kematangan III	8
Skor Pencapaian Tingkat Kematangan III	14
Status	No
Skor Tingkat Kematangan IV	0
Validitas Tingkat Kematangan IV	No
Skor Minimum Tingkat Kematangan IV	24
Skor Pencapaian Tingkat Kematangan IV	54
Status	No

Gambar 3.3 Informasi penilaian tingkat kematangan

Sumber: [33]

Kemudian informasi selanjutnya adalah skor tingkat kematangan. Berikut adalah skor minimum dan maksimum setiap tingkat kematangan

- **Skor Tingkat Kematangan II**, total penjumlahan jawaban dengan label tingkat kematangan II harus mendapatkan skor nilai minimal 12 dan pencapaian 36.
- **Skor Tingkat Kematangan III**, mempunyai nilai skor (label tingkat III) minimal 8 dan nilai pencapaian 14. Pada tingkat ini terdapat validitas yang harus dipenuhi di tingkat kematangan II. Instansi tidak akan mendapatkan skor tingkat kematangan III yang valid jika nilai tingkat kematangan II kurang dari 48.
- **Skor Tingkat Kematangan IV**, mempunyai nilai skor minimal pada jawaban pertanyaan (label tingkat IV) minimal 24 dan pencapaian 54. Pada tingkat ini juga diperlukan validitas, yaitu dengan persyaratan bahwa pada tingkat kematangan III telah valid dan skor pada label kematangan III adalah minimal 10.

Setiap pertanyaan dengan tingkat label kelengkapan dan kematangan mempengaruhi penentuan Tingkat akhir Kelengkapan dan Kematangan setiap Area. Hasil tersebut telah disamakan/dipadankan dengan ISO 27001:2013 jika mendapatkan skor Tingkat Kematangan III+. Banyaknya total nilai evaluasi tidak berpengaruh terhadap tingkat Kematangan, tetapi berdasar validitas setiap tingkat Kematangan.

Tabel 3.6 input, proses, output analisa penilaian area Indeks KAMI

INPUT	PROSES	OUTPUT
Hasil nilai skor penilaian Area Tata Kelola Keamanan Informasi	Megnanalisa skor yang didapat dari total penjumlahan nilai pada seluruh pertanyaan Indeks KAMI	Hasil Tingkat Kematangan Area Tata Kelola Keamanan Informasi

Sumber:[penulis, 2018]

3.1.3.2 Membahas hasil skor penilaian Area Indeks KAMI

Pada proses ini, yaitu kesimpulan terhadap analisa yang dilakukan. Setelah melakukan analisa, maka kesimpulan yang dibuat adalah kelayakan instansi dengan kesesuain terhadap standar ISO 27001. Kalyakan didapat jika telah mengetahui tingkat kematangan pada Area Indeks KAMI. Kelayakan terhadap ISO 27001 didapat jika memenuhi tingkat Kematangan III+.

Tabel 3.7 input, proses, output pembahasan penilaian area Indeks KAMI

INPUT	PROSES	OUTPUT
Hasil Tingkat Kematangan pada penilaian Area Tata Kelola Keamanan	Membahas hasil analisa dan menyimpulkan analisa yang dilakukan	Hasil Tingkat Kematangan berdasar pada kelayakan pada ISO 27001

INPUT	PROSES	OUTPUT
Informasi		

Sumber:[penulis, 2018]

3.1.3.3 Membuat saran/rekomendasi

Saran/rekomendasi merupakan maasukan untuk peningkatan efektivitas kemanan informasi dalam instansi. Pada bagian ini, pemberian saran/rekomendasi dibuat berdasarkan jawaban setiap pertanyaan. Rekomendasi dibuat satu tingkatan lebih tinggi dari jawaban yang didapat. Tujuan dari pembuatan rekomendasi tersebut adalah karena peningkatan Kematangan didasarkan pada peningkatan keamanan informasi pada instansi.

Tabel 3.8 *input,* proses, *output* saran/rekomendasi

INPUT	PROSES	OUTPUT
Hasil tingkat kematangan berdasar kelayakan standar ISO 27001	Membuat rekomendasi sesuai dengan kelayakan pada standar Indeks KAMI dan mengacu pada ISO 27001	Hasil rekomendasi yang sesuai dengan efektivitas peningkatan pengelolaan tata Kelola keamanan informasi

Sumber:[penulis, 2018]

3.1.3.4 Menyusun dokumen Tugas Akhir

Setelah melakukan serangkaian tahapan dan aktivitas diatas, maka dilakukan aktivitas terakhir untuk melengkapi penelitian ini. Yaitu dengan menyusun laporan tugas akhir sebagai dokumentasi semua yang telah dilakukan selama proses pengerjaan penelitian. Format penyusunan dokumen tugas akhir menyesuaikan ketentuan dari Departemen Sistem Informasi dan laboratorium Manajemen Sistem Informasi. Berikut adalah sistematika penulisan Tugas Akhir:

a. BAB I Pendahuluan

Pada bab ini akan dijelaskan mengenai latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat tugas akhir, serta relevansi tugas akhir.

b. BAB II Tinjauan Pustaka

Pada bab ini akan dijelaskan mengenai penelitian-penelitian sebelumnya yang telah dilakukan dan dasar teori yang berasal dari pustaka dan teori-teori yang mendukung dan berkaitan dengan permasalahan yang akan dibahas dalam penelitian tugas akhir.

c. BAB III Metodologi

Pada bab ini akan dijelaskan alur proses dari pengerjaan tugas akhir mulai dari identifikasi permasalahan sampai dengan penyusunan dokumen tugas akhir.

d. BAB IV Perancangan

Pada bab ini akan dijelaskan proses pengumpulan data dan informasi yang digunakan dalam pembahasan tugas akhir.

e. BAB V Implementasi

Bab ini berisi tentang implementasi dan penjelasan setiap alur proses yang dijelaskan secara singkat pada metodologi pada penelitian tugas akhir.

f. BAB VI Hasil dan pembahasan

Pada bab ini menyajikan analisis dan pembahasan dalam penyelesaian penelitian tugas akhir.

g. BAB VII Kesimpulan dan Saran

Pada bab ini berisi kesimpulan dan saran yang ditujukan untuk kelengkapan penyempurnaan tugas akhir.

Tabel 3.9 *input,* proses, *output* penyusunan dokumen tugas akhir

INPUT	PROSES	OUTPUT
• Latar belakang masalah • Tinjauan pustaka • Hasil penilaian Kategori Sistem	Menyusun dokumen penelitian Tugas Akhir	Dokumen Tugas Akhir

Elektronik dan analisanya • Hasil penilaian Area Indeks KAMI dan analisanya • Hasil saran/rekomendasi		

Sumber:[penulis, 2018]

“Halaman ini sengaja dikosongkan”

BAB IV
PERANCANGAN

Bab ini akan menjelaskan mengenai proses perancangan penelitian Tugas Akhir. Perancangan dilakukan untuk mempersiapkan perangkat yang digunakan untuk pengumpulan data dan penilaiannya. Selain itu, perancangan dibuat sebagai panduan pengerjaan Tugas Akhir yang dapat membantu melihat gambaran secara umum mengenai Tata Kelola keamanan informasi pada instansi terkait.

4.1 Perancangan Studi Kasus

Studi kasus merupakan aspek penting dalam penelitian. Terdapat berbagai macam pengertian studi kasus. studi kasus adalah suatu proses mengeksplorasi dan deskriptif dari suatu kasus maupun beragam kasus dari waktu ke waktu melalui pengumpulan data yang mendalam serta melibatkan berbagai macam sumber informasi dalam sebuah konteks[11]. Pendapat lain mengemukakan bahwa studi kasus akan memunculkan kesempatan untuk melihat keseluruhan proses, mempelajari berbagai aspek, menguji hubungan dengan aspek lain dan menggunakan kapasitas pemahaman peneliti[10]. Menurut Yin, studi kasus merupakan penyelidikan empiris yang mengamati fenomena alam dengan menggunakan cara sistematis pada pengumpulan data seperti wawancara dan observasi. Dari hal tersebut, dapat dilihat bahwa studi kasus perlu dirancang dalam penelitian karena ia proses yang melibatkan pengumpulan data.

Terdapat beberapa metode/pemodelan dalam pembuatan studi kasus. Yin mengkategorikan studi kasus menjadi tiga kategori, yaitu:

- Eksplorasi : menggali fenomena dalam yang berfungsi sebagai tempat tujuan untuk peneliti.
- Deskriptif : menggambarkan fenomena ilmiah yang terjadi dalam dengan tujuan untuk

menggambarkan data yang terjadi dalam bentuk narasi.

- *Explanatory* : menjelaskan fenomena dalam data secara jelas dan detail mulai dari dasar sampai mendalam

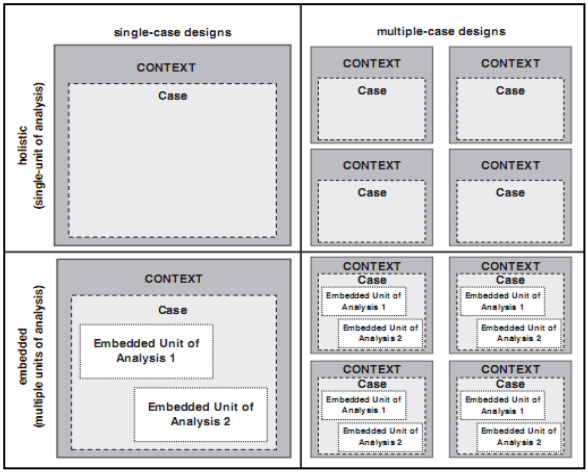
Menurut pengertian diatas, tujuan utama studi kasus ini adalah untuk dapat mengetahui nilai kematangan dan kelayakan keamanan informasi pada instansi terkait dan dapat memberikan rekomendasi sehingga dapat membantu meningkatkan keamanan informasi pada instansi.

Kategori diatas, jika dihubungkan dengan studi kasus penelitian yang akan diambil, maka termasuk ke dalam kategori eksplorasi, karena penelitian menunjukkan adanya penggalian data saat melakukan evaluasi dengan tujuan untuk mengetahui nilai kematangan dan kelayakan keamanan informasi pada studi kasus yang diambil.

Perancangan pertama diatas adalah mengetahui kategori studi kasus yang akan diambil. Kemudian untuk pemodelan kedua adalah mengetahui studi kasus termasuk dalam kasus model (*case design*) mana. Terdapat dua *case design*, yaitu *single case design* dan *multiple case design*. *Single case design* adalah penggunaan satu kasus untuk pengujian dan *multiple case design* adalah penggunaan lebih dari satu kasus untuk pengujian. *Case design* yang diambil pada studi kasus penelitian ini adalah termasuk ke dalam *single case*, karena hanya terdapat satu kasus yaitu sistem manajemen keamanan informasi.

Setelah menentukan case design, perancangan selanjutnya adalah mengetahui *unit of anlysis* dari sebuah *case design*. *Unit of analysis* adalah alat konseptual untuk membimbing investigator terlibat dalam pengamatan bermakna serta observasi dan analisis yang sistematis. *Unit of analysis* dapat berupa individu, group, artifact, interaksi antar individu, atau dibatasi dengan sistem yang didefinisikan oleh investigator. Pada penelitian yang diambil, *unit of analysis* yang digunakan adalah *multiple unit of analysis*, karena studi kasus akan dilakukan pada keseluruhan instansi beserta sub dalam instansi

yang menggunakan sistem manajemen keamanan informasi. Penggambaran case design dan unit of analysis dapat dilihat pada gambar di bawah ini:



Gambar 4.1 *unit of analysis*

Sumber : [11]

4.2 Perancangan Pengumpulan Data Kondisi Kekinian

Pengumpulan kondisi kekinian merupakan pengumpulan data awal yang dilakukan untuk mengetahui gambaran secara umum pelaksanaan sistem manajemen keamanan informasi pada instansi terkait. Pengumpulan data kondisi kekinian dilakukan dengan cara membuat poin-poin informasi yang dibutuhkan untuk dapat menggambarkan kondisi kekinian terkait sistem manajemen keamanan informasi.

4.2.1 Data yang diperlukan

Dalam melakukan penelitian, dibutuhkan data yang dapat mendukung tahapan penggalian data dan informasi sesuai studi kasus penelitian. Data tersebut dapat digali dengan membuat poin-poin yang dapat menggambarkan keseluruhan kondisi instansi tersebut. Gambaran umum yang ingin didapat

adalah terkait dengan tata kelola keamanan informasi seperti tugas pokok dan fungsi instansi, peran pengelola keamanan informasi, pihak-pihak yang bertanggung jawab pengelola keamanan informasi, prosedur dan kebijakan keamanan informasi dan aset informasi instansi.

Penggalian data diambil dengan cara menggunakan beberapa metode, yaitu menggunakan wawancara, melakukan observasi dan melihat/*review* dokumen.

1. Instrumen Wawancara
   Instrumen wawancara merupakan daftar pertanyaan yang akan diajukan pada saat wawancara dengan narasumber. Pembuatan instrumen wawancara pada penelitian ini dibuat berdasarkan saat perancangan perangkat pengumpulan data yang akan dijelaskan pada sub bab berikutnya.
2. Observasi dan/atau *Review* Dokumen
   Selain wawancara, terdapat observasi yang dilakukan untuk mengamati atau mengetahui kondisi sebenarnya pada instansi terkait. Kemudian terdapat review dokumen yang digunakan untuk mendukung informasi yang berkaitan dengan hasil wawancara dan belum didapatkan saat melakukan wawancara.

Untuk memudahkan dalam mendapatkan data yang diperlukan, terdapat tabel berisi poin-poin dari data yang diinginkan. Tabel tersebut terbagi ke dalam tiga penjabaran, yaitu Tujuan, Sasaran dan Sumber dari masing-masing metode diatas. Berikut adalah tabel yang berisikan tujuan, sasaran dan sumber dari setiap metode:

Tabel 4.1 tujuan, sasaran dan sumber pengumpulan data metode wawancara dan observasi/review dokumen

Tujuan	Sasaran	Sumber
Metode wawancara		
Mengetahui pembagian tanggung jawab, alokasi SDM,	- Tupoksi dan struktur organisasi - Jumlah SDM pengelola dan	Indeks KAMI 3.1 ISO 27001:2013

Tujuan	Sasaran	Sumber
kompetensi SDM, standar, perangkat hukum, serta kebijakan yang diterapkan terkait tata kelola keamanan informasi.	pelaksana keamanan informasi - Kompetensi dan keahlian SDM pengelola dan pelaksana keamanan informasi - Program sosialisai dan peningkatan pemahaman keamanan informasi - Koordinasi dengan pihak tertentu - Alokasi keberlangsungan bisnis - Pelaporan kondisi & kepatuhan program keamanan informasi - Pengukuran kinerja dan penilaian kinerja pengelolaan keamanan informasi - Perangkat hukum dan kebijakan terkait keamanan informasi	
Observasi/*review* dokumen		
mengetahui bukti dari dokumen terkait tata kelola keamanan informasi, standar, perangkat hukum, dan data SDM yang ada.	- Dokumen tupoksi dan struktur organisasi bagian keamanan informasi - Dokumen standar kompetensi bagi SDM pengelola dan pelaksana keamanan informasi	Indeks KAMI 3.1 ISO 27001:2013

Tujuan	Sasaran	Sumber
	- Dokumen undang-undang tentang identifikasi data pribadi - Dokumen keberlanjutan bisnis mengenai layanan TIK - Dokumen hasil laporan kondisi keamanan informasi - Dokumen standar dan perangkat hukum terkait mengenai keamanan informasi	

Sumber: [penulis, 2018]

4.3 Perancangan Perangkat *Assessment*

Perangkat *Assessment* merupakan perangkat yang akan digunakan dalam menilai pelaksanaan Sistem Manajemen Keamanan Informasi yang dilakukan di instansi terkait. Ide pembuatan perangkat ini bersumber dari salah satu penelitian sebelumnya, yaitu Tugas Akhir Erina Umiyati mengenai penilaian *service desk* dengan menggunakan *self assessment*[10].

4.3.1 Perancangan Perangkat Pengumpulan Data

Perangkat Pengumpulan Data merupakan perangkat yang dibuat untuk mengetahui poin-poin dari setiap pertanyaan pada Indeks KAMI. Poin-poin tersebut, dapat dibuat sebagai daftar pertanyaan dan kegiatan observasi yang membantu dalam menjawab pertanyaan Indeks KAMI. Pembuatan perangkat tersebut dimulai dalam beberapa tahapan, yaitu:

1. **Membuat poin setiap pertanyaan Indeks KAMI**
   Indeks KAMI memiliki satu pertanyaan dengan bebrapa nilai jawaban. Untuk mendapatkan nilai yang pasti,

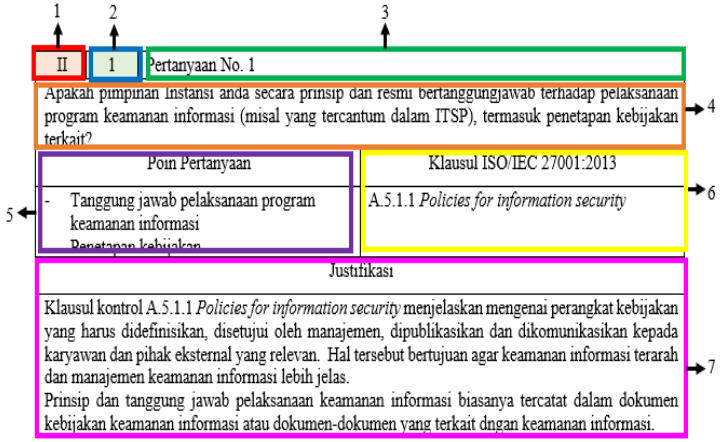
dibutuhkan beberapa sub pertanyaan atau pengumpulan data. Hal tersebut dilakukan juga agar dapat mengetahui tujuan dari pertanyaan Indeks KAMI. Pembuatan poin atau dapat disebut sebagai pencarian keyword dari setiap pertanyaan dilakukan karena dapat mempermudah dan memahami maksud pertanyaan Indeks KAMI. Setiap pertanyaan Indeks KAMI diidentifikasi, kemudian dicari setiap keyword pada pertanyaan tersebut dan ditulis pada tabel poin pertanyaan. Setiap poin pertanyaan yang dijelaskan, dapat dibuat sebagai tujuan pertanyaan yang akan dijadikan sebagai bahan dan arah pertanyaan wawancara dan observasi.

2. **Mencocokkan setiap poin dengan klausul kontrol ISO 27001:2013**

   setelah membuat poin pertanyaan pada setiap pertanyaan Indeks KAMI, langkah selanjutnya adalah melakukan pemetaan terhadap klausul kontrol ISO 27001:2013. Pemetaan dilakukan untuk mengetahui rujukan atau sumber setiap poin pertanyaan sehingga mempermudah memahami poin tersebut, membantu dalam membuat pertanyaan dan observasi, sehingga dapat menilai bagaimana kondisi instansi terkait. Selain itu, pemetaan dilakukan agar dapat mengetahui bagaimana rujukan atau sumber dari sebuah rekomendasi pada setiap pertanyaan Indeks KAMI.

   Hasil pemetaan tersebut, kemudian dilanjutkan dengan justifikasi yang menjelaskan hubungan antara poin pertanyaan dengan klausul kontrol ISO 27001:2013. Berikut adalah gambar identifikasi poin pertanyaan, pemetaan dengan klausul kontrol ISO 27001:2013 dan justifikasinya yang dijelaskan dalam gambar berikut.

   Selain itu, detail perangkat dapat dilihat dalam **Lampiran A.**



Gambar 4.2 identifikasi poin pertanyaan dan pemetaan kontrol ISO/IEC 27001:2013

Sumber: [penulis, 2018]

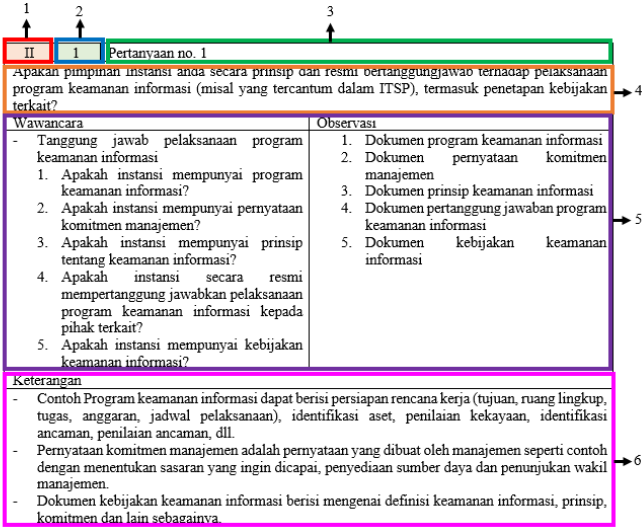
Keterangan:

1. Label pertanyaan berdasarkan tingkat kematangan penerapan pengamanan
2. Label pertanyaan berdasarkan kategori tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol oleh standar ISO 27001:2013
3. Nomor Pertanyaan berdasarkan Indeks KAMI
4. Pertanyaan Indeks KAMI
5. Identifikasi Poin pertanyaan berdasarkan pertanyaan pada Indeks KAMI
6. Klausul Kontrol ISO/IEC 27001:2013 yang dipetakan dengan poin pertanyaan
7. Justifikasi atau detail Klausul Kontrol ISO 27001:2013 dan hubungan dengan poin pertanyaan

3. Penyusunan pertanyaan dan kegiatan observasi berdasarkan poin pertanyaan

Tahap setelah melakukan identifikasi poin pertanyaan dan pemetaan, selanjutnya adalah pembuatan pertanyaan wawancara dan observasi. Arah pertanyaan dibuat

berdasarkan identifikasi poin pertanyaan yang dilakukan pada tahap sebelumnya. Penyusunan pertanyaan yang terarah dilakukan agar dapat mempermudah mendapatkan pengumpulan fakta dan bukti, hal tersebut dapat membantu dalam penilaian evaluasi Indeks KAMI. Berikut adalah gambar daftar pertanyaan dan observasi sebagai perangkat pengumpulan data:



Gambar 4.3 perangkat wawancara dan observasi

Sumber: [penulis, 2018]

Keterangan:

1. Label pertanyaan berdasarkan tingkat kematangan penerapan pengamanan
2. Label pertanyaan berdasarkan kategori tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol oleh standar ISO 27001:2013
3. Nomor Pertanyaan berdasarkan Indeks KAMI
4. Pertanyaan Indeks KAMI
5. Daftar pertanyaan dan observasi berdasarkan poin pertanyaan yang telah dibuat
6. Keterangan atau penjelasan mengenai pertanyaan agar memudahkan menjawab

Selain itu, detail perangkat dapat dilihat dalam **Lampiran B.**

4.3.2 Perancangan Perangkat Audit

Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan dan pengamanan informasi pada instansi pemerintah. Alat tersebut dapat digunakan dalam berbagai tingkatan dan ukuran instansi pemerintah. Pertanyaan-pertanyaan dalam Indeks KAMI belum tentu dapat dijawab semuanya, tetapi yang harus diperhatikan adalah jawaban yang merefleksikan kondisi penerapan keamanan informasi sesungguhnya dalam instansi. Untuk membantu hal tersebut, maka dibuat beberapa pertanyaan seperti perancangan perangkat diatas. Kemudian, untuk menilai dari hasil pertanyaan tersebut, alat evaluasi Indeks KAMI akan memberikan nilai atau skor akhir setelah melakukan evaluasi. Alat evaluasi Indeks KAMI dapat dikembangkan yang juga bisa disebut dengan *assessment sheet*. *Assessment sheet* merupakan alat/perangkat yang digunakan untuk membantu proses penilaian evaluasi. Pada *assessment sheet* Indeks KAMI, penilaian dilakukan menggunakan aplikasi *Ms. Excel*. Di dalam *assessment sheet*, terdapat beberapa bagian, yaitu:

1. Pengantar

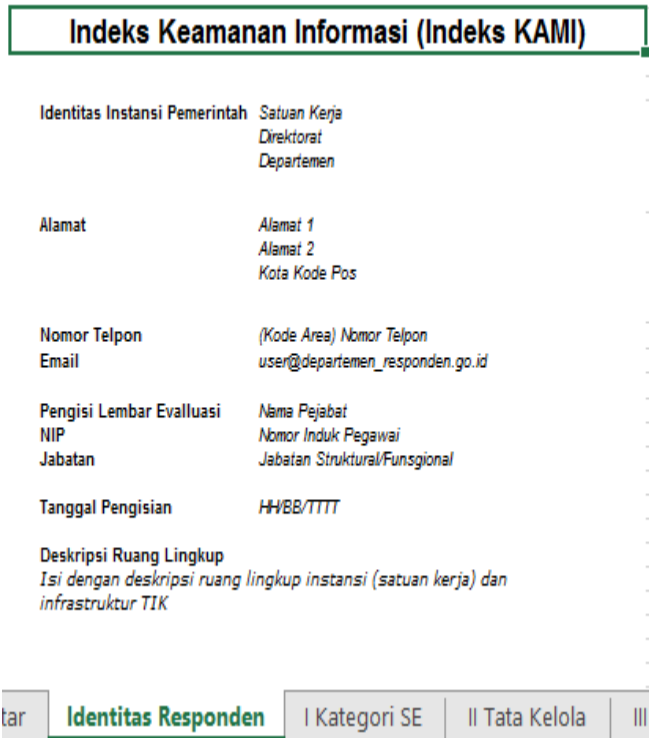
Bagian ini merupakan pendahuluan alat evaluasi Indeks KAMI. Dalam bagian ini, dijelaskan mengenai pengertian dan kegunaan alat evaluasi, penilaian Indeks KAMI dan bagaimana pengisian dalam Indeks KAMI. Alat evaluasi Indeks KAMI menjadi dasar acuan dalam membuat perancangan audit ini. Berikut adalah gambar pengantar Indeks KAMI:

Gambar 4.4 pengantar Indeks KAMI

Sumber:[33]

2. Identitas Responden

Pada bagian ini, terdapat data identitas pengisi atau responden Indeks KAMI. Di dalam Identitas responden, terdapat isian seperti Identitas Intansi, Alamat, No. Telepon, dsb. Berikut adalah contoh gambar identitas responden pada Indeks KAMI:

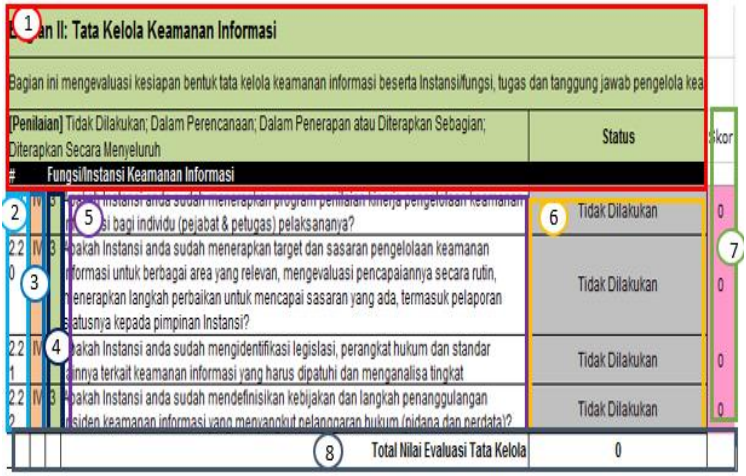


Gambar 4.5 identitas responden

Sumber: [33]

3. Penilaian Area Indeks KAMI

Merupakan penilaian yang terdiri atas pertanyaan-pertanyaan dan skor penilaian berdasarkan evaluasi yang ada. Dalam *assessment sheet*, mencakup tabel yang berisi kelengkapan dan kematangan pertanyaan, pertanyaan Indeks KAMI, status penilaian dan skor nilai. Setelah mengetahui beberapa pertanyaan tersebut, terdapat kesimpulan untuk menentukan penilaian apakah evaluasi Tidak dilakukan, Dalam Perencanaan, Diterapkan sebagian atau Diterapkan secara menyeluruh. Berikut adalah gambaran assessment sheet tabel penilaian Indeks KAMI:



Gambar 4.6 perangkat Indeks KAMI

Sumber: [33]

Keterangan :

1. Deskripsi Area Keamanan Informasi pada Indeks KAMI
2. Nomor pertanyaan Area Indeks KAMI
3. Label pertanyaan berdasarkan tingkat kematangan penerapan pengamanan.
4. Label pertanyaan berdasarkan kategori tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol oleh standar ISO 27001:2013.
5. Daftar pertanyaan pada Indeks KAMI
6. Status penilaian Indeks KAMI.
7. Skor nilai berdasarkan status penilaian yang didapat.
8. Total nilai evaluasi pada Area Indeks KAMI

Selain itu, detail perangkat dapat dilihat dalam **Lampiran C.**

"*Halaman ini sengaja dikosongkan*"

BAB V
IMPLEMENTASI

Pada bab ini menjelaskan hasil dari proses penentuan studi kasus dan perancangan perangkat penggalian data yang didapatkan melalui wawancara, observasi, dan review dokumen.

5.1 Pemilihan Area Penilaian Indeks KAMI

Bagian ini merupakan bagian yang membahas kondisi awal organisasi . pada bagian ini akan menjelaskan sedikit mengenai pemilihan bidang untuk dilakukan evaluasi berdasarkan penilaian Area Indek KAMI.

5.1.1 Diskusi Pemilihan Penilaian Area Indeks KAMI

Sebelum melakuan pengumpulan data pada unit yang dipilih, dilakukan diskusi antara peneliti dengan pihak diskominfo. Diskusi mengenai Area apa pada Indeks KAMI yang harus dilakukan penilaian evaluasi. Berdasarkan batasan masalah yang diambil di bab sebelumnya, peneliti menawarkan hanya satu penilaian area Indeks KAMI dan disetujui oleh pihak diskominfo. Diskusi tersebut menghasilkan kesepakatan area evaluasi Indeks KAMI yang akan dibuat sebagai penilaian. Area yang diambil sebagai *assessment* pada penelitian ini adalah Tata Kelola Keamanan Informasi.

5.1.2 Diskusi Pemilihan Bidang untuk Evaluasi

Diskusi selanjutnya membahas mengenai bidang-bidang pada diskominfo yang akan dijadikan sebagai bahan evaluasi dengan menggunakan penilaian Indeks KAMI. Peneliti menawarkan evaluasi dilakukan pada seluruh bidang/instansi pada Dinas Komunikasi dan Informatika XYZ. Pihak Diskominfo tidak merasa keberatan dengan penawaran tersebut, tetapi saat akan dilakukan pengambilan data berupa wawancara dan observasi, pihak Diskominfo menyatakan bahwa penilaian hanya akan dilakukan pada satu unit. Yaitu unit LPSE. Hal tersebut disebabkan karena diskominfo belum

menerapkan tata kelola keamanan informasi dan masih melakukan pembuatan dokumen keamanan informasi. Kemudian, pihak UPT LPSE telah melakukan 17 standarisasi berdasarkan standar yang sesuai dengan LKPP. Maka dari itu, diskominfo mengarahkan evaluasi hanya dilakukan pada satu unit saja.

5.2 Pengumpulan Data dan Informasi

Pada bagian ini, akan dilakukan pengumpulan data dan informasi sesuai dengan pertanyaan evaluasi pada Indeks KAMI. Sebelum melakukan pengumpulan data dan informasi, peneliti terlebih dahulu melakukan penjabaran setiap pertanyaan indeks KAMI ke dalam beberapa sub pertanyaan. Hal tersebut dilakukan untuk mempermudah dalam memberikan penilaian dan justifikasi status dan skor Indeks KAMI.
Pengumpulan data dan informasi dilakukan dalam dua metode, yaitu melakukan wawancara dan melakukan kegiatan observasi/review dokumen.

5.2.1 Pengumpulan Data dan Informasi Berdasarkan Wawancara

Sebelum melakukan wawancara, peneliti terelebih dahulu melakukan proses pengelompokan poin setiap pertanyaan. Hal tersebut dilakukan dengan tujuan agar mendapatkan pertanyaan-pertanyaan lebih banyak yang dapat mempermudah dalam pengumpulan data dan penilaian Indeks KAMI.

Wawancara dilakukan dengan salah narasumber di UPT LPSE. Narasumber merupakan ketua unit LPSE. Wawancara dengan ketua LPSE dilakukan hanya sekali dan bertempat di dalam ruang kantor UPT LPSE.

Selain dari keua LPSE, peneliti juga melakukan sedikit wawancara dengan bagian administrasi sistem elektronik.

Karena bagian tersebut bertugas sebagai teknis pelaksanaan teknologi informasi dan pengamanan terhadapnya.
Hasil dari wawancara merupakan fakta yang terdapat dalam unit tersebut dan sebagai gambaran umum kondisi keamanan informasi unit LPSE. Hasil dari wawancara dapat dilihat dalam **Lampiran D**.

5.2.2 Pengumpulan Data dan Informasi Berdasarkan Observasi/Review Dokumen

Selain dari pengumpulan data dan informasi berdasarkan wawancara, peneliti juga menggunakan metode observasi/review dokumen. Hal ini digunakan untuk menambah temuan dalam setiap penilaian evaluasi sekaligus sebagai bukti pendukung.

Sebelum dilakukan observasi/review dokumen, peneliti melakukan pengelompokan poin seperti saat akan melakukan wawancara. Kemudian poin tersebut dijabarkan dalam kegiatan observasi/review dokumen.

Observasi/review dokumen dilaksanakan saat telah melakukan kegiatan wawancara. Dokumen dilihat dan disesuaikan dengan pemenuhan poin pertanyaan pada setiap pertanyaan Indeks KAMI.
Hasil dari pengumpulan data dan Informasi berdasarkan observasi/review dokumen adalah dokumen-dokumen pendukung dalam menilai gambaran umum keamanan informasi unit LPSE. Hasil observasi/review dokumen dapat dilhat pada **Lampiran E**.

5.2.3 Profil Organisasi

Dinas Komunikasi dan Informatika merupakan salah satu instansi perangkat daerah yang membidangi urusan komunikasi dan informatika. Pada Kabupaten XYZ, dinas Komunikasi dan Informatika memiliki struktur organisasi dengan tiga bagian dan satu UPT. UPT tersebut berfokus pada pengadaan barang yang biasa disebut sebagai Layanan

Pengadaan Secara Elektronik dan disingkat menjadi LPSE. Pada penelitian yang diambil, peneliti berfokus pada evaluasi keamanan informasi pada UPT LPSE Kabupaten XYZ.
UPT LPSE ini mempunyai beberapa ranah tugas yang berkaitan dengan layanan pengadaan, selain itu juga mengatur pengadaan secara elektronik agar lebih terarah dan teratur serta dapat lebih mudah dipantau. Teknologi informasi pada UPT ini sangat penting karena data yang dimuat bersifat besar dan sensitif, seperti data pelelangan yang notabene memiliki nilai nominal besar. Maka dari itu, penggunaan teknologi informasi pada UPT sangat penting.

5.2.4 Gambaran Tata Kelola Keamanan Informasi berasarkan kelengkapan Indeks KAMI.

Gambaran tata kelola akan dijelaskan berdasarkan kondisi kekinian yang ada pada instansi setelah dilakukan penggalian data dan informasi. Hal ini dilakukan untuk mengetahui kesenjangan yang terdapat pada kondisi unit LPSE dengan nilai kondisi ideal pada Indeks KAMI.

1. **Gambaran Tata kelola keamanan informasi berdasarkan Kategori Pengamanan ‘1’ pada Indeks KAMI**

   Kategori Pengamanan ‘1’ pada pertanyaan Indeks KAMI merupakan gambaran mengenai kerangka kerja dasar keamanan informasi. Kerangka kerja dasar pada tata kelola keamanan informasi berisi tentang penerapan program keamanan informasi, penetapan fungsi dan tugas, pemberian wewenang, pemberian persyaratan/standar kompetensi dan sosialisasi untuk kepatuhan keamanan informasi

   UPT LPSE memiliki kondisi sedang melakukan standarisasi yang akan dinilai oleh LKPP. UPT memiliki kebijakan keamanan informasi sebagai penerapan program keamanan informasi, telah melakukan pembentukan fungsi dan tugas yang tergambar dalam struktur organisasi. Instansi juga memberika wewenang seperti wewenang dalam hak akses sistem. Selain tu, UPT memberikan

defisni syarat standar kompetensi untuk setiap keahlian yang dibutuhkan dalam UPT LPSE.

Kondisi tersebut, secara umum tergambar sebagai kondisi yang telah menerapkan kerangka kerja dasar tata kelola keamanan informasi.

Kekurangan dari penilaian kondisi pada kerangka kerja dasar adalah kurangnya dokumen pendukung yang menyebabkan penilaian skor tidak maksimal.

2. **Gambaran Tata Kelola Keamanan Informasi berdasarkan Kategori Pengamanan '2' pada Indeks KAMI**

   Kategori Pengamanan '2' pada pertanyaan Indeks KAMI adalah mengenai efektivitas dan penerapan keamanan informasi. Di dalam label ini, berisi mengenai penerapan peningkatan kompetensi, integrasi proses kerja dengan persyaratan keamanan informasi, penggunaan data pribadi, pengelolaan keamanan informasi dan koordinasinya dengan pihak terkait serta tanggung jawab untuk pembuatan kelangsungan layanan TIK dan DRP.

   Unit LPSE telah melakukan peningkatan kompetensi seperti melakukan pelatihan untuk karyawan LPSE dan ikut serta dalam bimbingan teknis standarisasi LPSE. Melakukan koordinasi dengan pihak terkait seperti bidang lain dalam diskominfo dan LPSE pusat, LKPP maupun pelanggan pemakai sistem LPSE.

   Hal tersebut menunjukkan bahwa kondisi dengan Kategori Pengamanan '2' telah dirancang dan bahkan sebagian telah dilakukan oleh unit LPSE.

   Kekurangan dari penilaian kondisi efektivitas dan penerapan keamanan informasi adalah dokumen yang ada belum lengkap sehingga membuat penilaian skor tidak maksimal dan kurang.

3. **Gambaran Tata Kelola Keamanan Informasi berdasarkan Kategori Pengamanan '3' pada Indeks KAMI**

   Kategori Pengamanan '3' pada pertanyaan Indeks KAMI menunjukkan peningkatan kinerja keamanan informasi. Berisi tentang program khusus untuk memenuhi tujuan

dan sasaran kepatuhan keamanan informasi, program penilaian kinerja, penerapan pengelolaan keamanan informasi sampai dengan evaluasinya, kepatuhan terhadap legislasi dan perangkat hukum dan langkah penanggulangan insiden.
Pada UPT LPSE, belum dilakukan penerapan terhadap kinerja keamanan informasi. Kondisi tersebut menunjukkan bahwa penerpan peningkatan kinerja belum dilakukan bahkan belum dirancang, sehingga hasil dari penilaian **label** ‘3’ adalah sangat kurang.

5.3 Hambatan

Dalam melakukan wawancara dan observasi penulis terbantu dengan tanggapan pihak Kominfo dan UPT LPSE yang bersedia melakukan wawancara dan pengambilan data langsung pada kantor UPT LPSE apabila diperlukan komunikasi secara langsung. Namun terdapat hambatan yang dilalui oleh penulis, yaitu dalam mengambil data, narasumber sedikit kebingungan menjawab pertanyaan karena baru melakukan standarisasi yang dikeluarkan oleh LKPP dengan 17 bagian di dalamnya. Narasumber agak kebingungan mencari mana data untuk standar keamanan informasi dengan standar lainnya.

BAB VI
HASIL DAN PEMBAHASAN

Bab ini akan menjelaskan hasil yang didapatkan dari penelitian ini, dan pembahasan secara keseluruhan yang didapatkan dari penelitian.

6.1 Hasil Analisis Kesenjangan Pengelolaan Keamanan Informasi

Berikut ini adalah analisis kesenjangan yang didapatkan antara kondisi kekinian yang ada di UPT LPSE Diskominfo Kab. XYZ dengan kondisi ideal yang tertera dalam Indeks KAMI yang mengacu pada standar ISO 27001:2013. Analisis kesenjangan ini akan dilakukan untuk area tata kelola keamanan informasi yang ada pada tabel berikut:

Tabel 6.1 Hasil Analisa kesenjangan kategori tata kelola keamanan informasi

No.	Kondisi Kekinian	Kondisi Ideal	Kesenjangan
1	UPT LPSE telah memiliki kebijakan layanan dan menetapkan kebijakan keamanan informasi, tetapi belum memiliki program pelaksanaan keamanan informasi karena belum memiliki	UPT LPSE harus memiliki dokumen perencanaan strategi TI, membuat strategi program keamanan informasi dan menerapkan program di dalamnya serta memiliki kebijakan untuk keamanan informasi	LPSE belum menentukan pembuatan strategi dan bagaimana menerapkan program keamanan informasi, tetapi telah menentukan dokumen keamanan informasi pada LPSE. Sehingga penerapan program keamanan

No.	Kondisi Kekinian	Kondisi Ideal	Kesenjangan
	dokumen strategi perencanaan teknologi informasi.		informasi belum dapat diukur sampai mana penerapan dan pelaksanaannya.hal tersebut membuat LPSE masih dalam tahap perkembangan dan penerapan serta perbaikan dokumen.
2	UPT LPSE memiliki satu bagian fungsi yang mengatur segala teknisi untuk layanan dan sistem pada LPSE, begitu pula dengan keamanan informasi di dalamnya. Seperti kewenangan dalam pemberian hak akses untuk memasuki sistem dan	Instansi terkait membuat tugas dan tanggung jawab secara secara detail mengenai pengelolaan keamanan informasi.	LPSE telah membuat bagian yang mempunyai tugas dan fungsi keamanan informasi.

No.	Kondisi Kekinian	Kondisi Ideal	Kesenjangan
	mengelolanya.		
3	LPSE belum meiliki dokumen wewenang setiap bagian, tetapi terdapat prosedur seperti pemberian hak akses dan penggunaan fasilitas oleh koordinator keamanan informasi.	Instansi membuat dokumen kewenangan pada setiap bagian dan menerapkan kewenangan tersebut untuk menjaga kepatuhan keamanan informasi.	LPSE harus membuat dokumen kewenangan sebelum membuat prosedur kewenangan seperti pemberian hak akses server dan penggunaan fasilitas pada LPSE. Hal tersebut diakibatkan oleh satu staff yang mempunyai tugas dan wewenang yang bercampur, sehingga wewenang tidak tertulis dengan baik. LPSE masih dalam tahap belum dilakukan dan baru akan melakukan perancangan pada dokumen wewenang keamann informasi.
4	LPSE memiliki	Instansi harus memiliki dokumen	LPSE telah memenuhi dan

No.	Kondisi Kekinian	Kondisi Ideal	Kesenjangan
	dokumen kebutuhan kapasitas dan pencatatan serta laporan evaluasinya.	alokasi sumber daya dengan rincian jelas untuk menjamin kepatuhan dan pengelolaan program keamanan informasi.	memiliki dokumen penggunaan sumber daya, melakukan pencatatan dan melakukan evaluasi penggunaan sumber daya yang diberikan.
5	LPSE belum memiliki dokumen keperluan untuk peran pengelola keamanan informasi, menentukan kebutuhan untuk audit internal dan belum membuat persyaratan untuk pemisahan kewenangan.	Instansi memiliki dokumen keperluan dan memetakan dokumen tersebut hingga keperluan untuk audit internal dan persyaratan untuk pemisahan kewenangan.	LPSE harus membuat dokumen keperluan peran pelaksana pengamanan informasi, kemudian melakukan pemetaan setiap keperluan sehingga dapat memunculkan kebutuhan untuk audit internal dan membuat persyaratan yang harus dipenuhi sebagai bentuk pemisahan wewenang. Hal tersebut membuat pengelola tidak dapat menentukan

No.	Kondisi Kekinian	Kondisi Ideal	Kesenjangan
			pengelolaan apa yang baik dan pengelolaan apa yang masih dalam perbaikan dan siapa yang berhak dalam mengelola dan bagaimana mengelola. LPSE dalam bagian ini masih dalam tahap belum dilakukan dan harus membuat perencanaan keperluan setiap peran pelaksana pengamanan informasi.
6	LPSE memiliki dokumen matriks kompetensi sebagai bentuk definisi persyaratan keahlian LPSE dan dokumen berisikan satu staff memiliki lebih dari	Instansi mempunyai dokumen persyaratan/standar kompetensi khusus untuk pengelola keamanan informasi dan mendefinisikan persyaratan atau standar tersebut.	Matrik kompetensi berisi keahlian yang saat ini dimiliki oleh LPSE dan rencana keahlian yang harus dicapai pada waktu yang ditentukan, tetapi belum dipisah antara pengelola keamanan informasi dengan keahlian layanan. Hal tersebut dikarenakan

No.	Kondisi Kekinian	Kondisi Ideal	Kesenjangan
	satu keahlian (antara layanan dan keamanan informasi tergabung menjadi satu).		anggota LPSE sedikit dan setiap staff memiliki tugas dan tanggung jawab masih bercampur jadi satu.
7	LPSE memiliki dokumen matriks kompetensi berisikan keahlian yang sedang dimiliki oleh LPSE dan keahlian yang dibutuhkan LPSE.	Instansi memiliki pengelola yang memiliki standar yang telah memadai standar dan sesuai dengan kebutuhan LPSE.	LPSE masih belum mencapai standar keahlian yang memadai sesuai dengan standar LKPP dan belum mencapai kebutuhan oleh LPSE. LPSE harus melakukan banyak hal seperti bagaimana cara agar mencapai keahlian yang sesuai dan sepadan dengan standar yang dipakai.
8	LPSE memiliki dokumen tata cara pembuatan password dan menjaga integritas LPSE. Selain	Instansi harus memiliki dokumentasi sosialisasi untuk pemahaman keamanan informasi, kepentingan informasi dan	LPSE harus membuat dokumentasi sosialisasi atas kepatuhan keamanan informasi dan pemahaman informasi.

No.	Kondisi Kekinian	Kondisi Ideal	Kesenjangan
	itu, pelatihan yang dilakukan masih berfokus pada pelatihan pengelolaan layanan.	menjaga kepatuhannya.	
9	LPSE memiliki dokumen target peningkatan kompetensi dan keahlian.	Instansi telah menerapkan program peningkatan kompetensi dan keahlian pengelolaan keamanan informasi.	LPSE sedang merencanakan program peningkatan kompetensi tetapi belum menerapkan program peningkatan kompetensi dan keahlian keamanan informasi.
10	LPSE telah melakukan integrasi persyaratan keamanan informasi pada proses kerja, tetapi belum memiliki dokumentasi integrasi persyaratan	Instansi memiliki dokumen integrasi persyaratan keamanan informasi pada proses kerja.	LPSE baru merancang dokumen integrasi keamanan informasi pada proses kerja yang ada, yang berarti integrasi sudah dilakukan tetapi tidak memiliki bukti dokumen.

No.	Kondisi Kekinian	Kondisi Ideal	Kesenjangan
	tersebut.		
11	Instansi belum melakukan dentifikasi tetapi melakukan pengamanan data.	Data pribadi telah diidentifikasi dan dilindungi sesuai dengan undang-undang yang berlaku.	LPSE sedang merencanakan pengamanan data yang disesuaikan dengan standar dan undang-undang yang berlaku.
12	LPSE melakukan koordinasi secara langsung pada pihak terkait seperti penanganan permasalahan, pengamanan transaksi informasi pada sistem LPSE	Instansi melakukan koordinasi dengan berbagai pihak, memiliki dokumentasi dan dapat menyelesaikan permasalahan yang terjadi.	LPSE memiliki dokumen permasalahan yang terjadi dan penanganan permasalahan yang ada.
13	LPSE melakukan koordinasi dengan pihak satuan terkait secara lisan.	Instansi melakukan koordinasi dengan satuan terkait dan mendokumentasikan koordinasi tersebut.	LPSE belum melakukan dokumentasi terkait koordinasi dengan satuan terkait.
14	LPSE mempunyai dokumen tugas dan tanggung jawab	Instansi memiliki dokumen tugas dan tanggung jawab untuk keputusan sampai dengan pengelolaan	LPSE belum mengalokasikan tanggung jawab untuk merancang, melaksanakan dan mengelola

No.	Kondisi Kekinian	Kondisi Ideal	Kesenjangan
	pengelola kelangsungan layanan dan dokumen pengelolaan risiko.	dokumen kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*)	langkah kelangsungan layanan TIK.
15	LPSE memiliki dokumen pelaporan permasalahan layanan untuk pimpinan instansi yang dilakukan rutin sebulan sekali.	Instansi melakukan pelaporan kondisi, kinerja/efektivitas dan kepatuhan keamanan informasi kepada pimpinan instansi secara rutin dan resmi.	LPSE belum memiliki dokumen laporan kondisi dan kinerja/efektivitas keamanan informasi dan belum pernah melakukan pelaporan.
16	LPSE belum memiliki dokumen keamanan informasi sebagai konsideran atau sebagai proses pengambilan keputusan.	Instansi memiliki dokumen kondisi dan permasalahan dan dibuat dalam dokumentasi dengan konsideran atau bagian proses pengambilan keputusan.	Instansi belum memutuskan kondisi dan permasalahan keamanan informasi menjadi sebuah bagian konsiderana tau bagian proses pengembilan keputusan.
17	LPSE belum memiliki program khusus untuk memenuhi	Instansi memiliki program khusus untuk memenuhi target dan sasaran serta sebagai	Instansi masih harus membangun dan merancang program untuk memenuhi target

No.	Kondisi Kekinian	Kondisi Ideal	Kesenjangan
	target dan mematuhi tujuan dan kepatuhan keamanan informasi.	bentuk kepatuhan terhadap tujuan kepatuhan pengamanan informasi.	kepatuhan target kepatuhan keamanan informasi sebelum dapat menerapkan program. Hal tersebut merupakan langkah paling awal dalam menerapkan program pemenuhan target dan sasaran kepatuhan keamanan informasi.
18	LPSE belum memiliki dokumen proses pengukuran kinerja, metrik dan parameternya , serta belum memiliki cakupan isi mekanisme, waktu pengukuran, pelaksana, pemantauan dan eskalasi laporan.	Instansi telah memiliki dokumen proses pengukuran kinerja, metriks dan parameternya, mendefinisikan dokumen tersebut dan memiliki cakupan mekanisme, waktu pengukuran, pelaksana, pemantauan dan eskalasi pelaporan.	Tidak terdapat dokumen proses pengukuran kinerja dan harus membuat dokumen pengukuran kinerja.

No.	Kondisi Kekinian	Kondisi Ideal	Kesenjangan
19	LPSE tidak memiliki program penilaian kinerja	Instansi memiliki dokumentasi penerapan penilaian kinerja bagi individu.	LPSE belum memiliki program penilaian kinerja, karena langkah awal sebelum menerapkan program penilaian kinerja adalah membuat dokumen penilaian kinerja dan langkah awal tersebut belum dilaksanakan oleh pihak LPSE.
20	LPSE tidak memiliki penerapan target dan sasaran pengelolaan keamanan informasi, tidak melakukan evaluasi, tidak melakukan perbaikan dan	Instansi telah menerapkan target dan sasaran pengelolaan keamanan informasi, mengevalusi pencapaian tersebut secara rutin, membuat langkah perbaikan dan melakukan laporan status kepada pimpinan instansi.	LPSE masih dalam tahap awal belum dilakukan dan harus melakukan perancangan terhadap penerapan target dan sasaran pengelolaan keamanan informasi, merancang evaluasi, merancang bagaimana perbaikan dilakukan dan bagaimana melaporkan status

No.	Kondisi Kekinian	Kondisi Ideal	Kesenjangan
			kepada pimpinan instansi.
21	LPSE tidak melakukan identifikasi legislasi yang harus dipatuhi terkait keamanan informasi.	Instansi telah melakukan identifikasi legislasi dan perangkat hukum yang terkait keamanan informasi dan menganalisa tingkat kepatuhannya.	Instansi belum melakukan identifikasi dan belum melakukan tindakan yang berhubungan dengan kepatuhan keamanan informasi dengan legislasi dan perangkat hukum terkait. Tahap tersebut membuat LPSE tidak melakukan tindakan dan harus membuat perencanaan terhadap legislasi yang bersangkutan dengan keamanan informasi dan legislasi mana yang harus dipatuhi.
22	LPSE belum membuat dokumen pengelolaan insiden dan dokumen kebijakan	Intansi telah memiliki dokumen pengelolaan insiden dan kebijakan pengelolaan insiden.	LPSE belum memiliki dokumen pengelolaan insiden dan harus membuat dokumen

No.	Kondisi Kekinian	Kondisi Ideal	Kesenjangan
	mengenai pengelolaan insiden.		pengelolaan insiden dan kebijakannnya.

Sumber:[penulis, 2018]

6.2 Penilaian Kesiapan Area Tata Kelola Keamanan Informasi

Penilaian area bertujuan untuk menilai kondisi kemaatangan keamanan informasi sesuai dengan standar ISO 27001:2013.

Dalam penilaian area tersebut akan terdapat beberapa warna yang berbeda dalam tabel penilaian. Warna tersebut menunjukkan tingkatan yang berbeda. Berikut akan berisikan keterangan dari tingkatan warna yang terdapat dalam penilaian lima area Indeks KAMI:

Tabel 6.2 keterangan tingkat keamanan, kategori pengamanan dan status penilaian

Tingkat Keamanan		Tingkat Kematangan Keamanan II
		Tingkat Kematangan Keamanan III
		Tingkat Kematangan Keamanan IV
		Tingkat Kematangan Keamanan V
Kategori Pengamanan		Kategori Kematangan Pengamanan I
		Kategori Kematangan Pengamanan II
		Kategori Kematangan Pengamanan III
Status		Tidak Dilakukan

Pengamanan		Dalam Perenanaan
		Dalam Penerapan/ Diterapkan Sebagian
		Diterapkan Secara Menyeluruh

Sumber: [33]

Setiap kategori pertanyaan memiliki nilai skor yang berbeda. Gambar 6. berikut adalah pemetaan skor Indeks KAMI berdasarkan masing-masing kategori:

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

Gambar 6.1 matriks kategori pengamanan dan status pengamanan

sumber: [33]

6.2.1 Hasil Penilaian Tata Kelola Keamanan Informasi

Tabel dibawah ini merupakan hasil penilaian yang berkaitan penilaian Tata Kelola Keamanan Informasi yang ada pada UPT LPSE Diskominfo XYZ yang mana didapatkan total nilai untuk evaluasi tata kelola sebesar 23. Berikut adalah hasil penilaian Indeks KAMI:

Tabel 6.3 hasil penilaian tata kelola keamanan informasi

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**	Skor
#	**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?	Dalam Penerapan / Diterapkan Sebagian	2
2,2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Diterapkan Secara Menyeluruh	3
2,3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Dalam Perencanaan	1
2,4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	3

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	0
2,6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Dalam Penerapan / Diterapkan Sebagian	2
2,7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Dalam Perencanaan	1
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?	Dalam Perencanaan	1
2,9	II	2	Apakah Instansi anda menerapkan program	Dalam Perencanaan	2

			peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?		
2.10	II	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	Tidak Dilakukan	0
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?	Dalam Perencanaan	2
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	Dalam Perencanaan	2

			menyelesaikan permasalahan yang ada?		
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?	Dalam Perencanaan	2
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 Perencanaan	2
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan	Tidak Dilakukan	0

			kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?		
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	0
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	0
2.18	IV	3	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan	Tidak Dilakukan	0

			eskalasi pelaporannya?		
2.19	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Tidak Dilakukan	0
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	0
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	0
2.22	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah	Tidak Dilakukan	0

			penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?		
Total Nilai Evaluasi Tata Kelola				**23**	

Sumber:[penulis, 2018]; [33]

6.3 Pembahasan

Berikut adalah penjelasan dari hasil penilaian skor Indeks KAMI pada Area Tata Kelola Keamanan Informasi.

6.3.1 Pemberian Status penilaian Indeks KAMI

Ketika mendapatkan hasil status penilaian setiap pertanyaan, harus dilakukan terlebih dahulu pemberian justifikasi. Pemberian justifikasi dibuat untuk mengetahui makssud dari setiap status penilaian yang didapat dan alasan mendapatkan skor nilai tersebut. Hasil justifikasi dan penjelasan penilaian Indeks KAMI dapat dilihat berdasrkan pada **lampiran E**.

Pada Tabel di bawah ini akan dijelaskan bahwa kategori kontrol 1 dengan pertanyaan yang berjumlah 8 bernilai 13. Sedangkan untuk pertanyaan tahap 2 dengan jumlah 8 bernilai 10. Dari hasil yang didapat maka jumlah nilai untuk Tahap Penerapan 1 dan 2 berjumlah 23.

Untuk mengetahui status kelengkapan pada bagian ini adalah dengan membandingkan jumlah tahap penerapan 1 dan 2 dengan skor minimal Tahap Penerapan 3 yang sudah ditentukan pada aplikasi indeks KAMI pada bagian Tata Kelola yaitu 48. Didapat bahwa jumlah skor pada tahap penerapan 1 dan 2 adalah 23 sehingga dapat disimpulkan skor tidak melebihi Tahapan Penerapan 3. Maka dari itu bagian Tata Kelola disimpulkan masih menduduki Tingkat Kematangan I+.

Tabel 6.4 tingkat kelengkapan tata kelola keamanan informasi

Kategori Pengamanan (Tahapan)	Pertanyaan Tata Kelola	Nilai
1	8	13
2	8	10
3	6	0
Total	22	23

Sumber:[penulis, 2018]

Nilai tingkat kelengkapan pada masing-masing kategori pengamanan terkait dengan tata kelola keamanan informasi akan menentukan tingkat kematangan pada bagian ini. Semakin tinggi nilai tingkat kelengkapan maka semakin tinggi pula tingkat kematangan keseluruhan pada tiap bagian. Berikut merupakan hasil tingkat kematangan pada bagian Tata Kelola Keamanan Informasi:

Tabel 6.5 tingkat kematangan tata kelola keamanan informasi

Kategori Tingkat Kematangan	Pertanyaan Tata Kelola	Nilai	Tingkat Validitas Kematangan
II	13	21	I+
III	3	2	No
IV	6	0	No
Total	22	23	

Sumber:[penulis, 2018]

Area Tata Kelola Keamanan Informasi hanya valid ditingkat kematangan I+ yang artinya dalam Penerapan Kerangka Kerja Dasar:

- Sudah adanya pemahaman mengenai perlunya pengelolaan keamanan informasi
- Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluruhan risiko

yang ada, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan
- Kelemahan teknis dan non-teknis tidak teridentifikasi dengan baik
- Pihak yang terlibat belum semuanya menyadari tanggung jawab mereka

Area Tata Kelola Keamanan Informasi ini medapat poin 23 dari 126 dimana poin ini terbilang sangat rendah karena pihak LPSE hanya menerapkan:
- pembagian tanggung jawab terkait program keamanan informasi
- menerapkan fungsi terkait tugas dan tanggung jawan dalam pengelolaan keamanan informasi
- membuat dokumen peningkatan kompetensi sesuai standar yang berlaku
- dilakukan koordinasi dengan pihak terkait (internal dan eksternal) untuk menerapkan dan menjamin kepatuhan pengamanan informasi

6.3.2 Hasil Temuan Positif dan Negatif

Berdasarkan penilaian yang dilakukan sebelumnya, maka ditemukan Temuan Positif dan Temuan Negatif. Temuan positif merupakan temuan yang sudah dilaksanakan sesuai dengan ISO 27001:2013. Sedangkan Temuan Negatif adalah temuan yang belum melakukan standarisasi sesuai ISO 27001:2013. Pada temuan negatif, selanjutnya akan dijadikan sebagai bahan masukan untuk saran perbaikan. Berikut adalah temuan positif dan negatif setelah penilaian Indeks KAMI :

Tabel 6.6 hasil temuan positif dan temuan negatif

No.	Temuan Positif	Temuan Negatif
1	UPT LPSE telah memiliki kebijakan keamanan informasi dan kebijakan layanan sebagai bentuk prinsisp dan tanggung jawab	Pembuatan dokumen kebijakan keamanan informasi hanya sebagian dari pelaksanaan program keamanan informasi, dimana

No.	Temuan Positif	Temuan Negatif
	pelaksanaan program keamanan informasi.	
2	LPSE telah membentuk satu bagian yang mempunyai tugas dan tanggung jawab terhadap pengelolaan keamanan informasi maupun teknologi informasi.	Tidak ditemukan temuan negatif.
3	UPT memiliki prosedur pemberian akses ruang server dan fasilitas UPT sebagai bentuk kewenangan koordinator keamanan informasi	UPT LPSE belum memiliki dokumen kewenangan setiap bagian dan belum memiliki bukti penerapan kewenangan setiap bagian.
4	UPT telah memiliki dokumen penggunaan sumber daya, melakukan pencatatan dan melakukan evaluasi.	Tidak ditemukan temuan negatif.
5	Tidak ditemukan temuan positif.	UPT LPSE belum mendefinisikan keperluan dan pemetaan peran pelaksana pengelola keamanan informasi, jadi UPT harus mendidentifikasi kebutuhan apa saja yang diperlukan oleh bagian pengelola dan pengamanan informasi, mengidentifikasi kebutuhan audit internal dan membuat persyaratan-persyaratan tertentu sebagai bentuk

No.	Temuan Positif	Temuan Negatif
		pemisahan kewenangan.
6	LPSE memiliki dokumen matriks kompetensi yang berisikan keahlian apa saja yang dimiliki oleh setiap staff dan keahlian seperti apa yang diperlukan oleh LPSE. Serta bagaimana pemenuhan	UPT LPSE belum memiliki dokumen standar kompetensi dan keahlian khusus untuk keamanan informasi.
7	Untuk saat ini, kompetensi dan keahlian yang dimiliki oleh pengelola keamanan informasi masih *basic*. Sedangkan kebutuhan berdasarkan standar LKPP adalah mempunyai level *advanced*.	Instansi belum memiliki keahlian yang memadai dengan persyaratan/standar yang berlaku.
8	LPSE telah melakukan sosialisasi mengenai layanan dan kepentingan keamanan informasi dalam menggunakan sistem LPSE.	LPSE belum memiliki bukti sosialisasi pemahaman dan kepentingan keamanan informasi.
9	LPSE memiliki dokumen untuk peningkatan kompetensi dan keahlian.	LPSE belum memiliki dokumentasi penerapan program peningkatan keahlian untuk pelaksana pengelolaan keamanan informasi.
10	LPSE telah melakukan integrasi sistem LPSE	LPSE tidak melakukan dokumentasi terhadap

No.	Temuan Positif	Temuan Negatif
	dan memiliki pengamanan di dalamnya.	intergrasi proses kerja yang memerlukan keperluan/persyaratan keamana informasi di dalamnya.
11	LPSE mempunyai pengaman untuk pengamanan data pribadi ataupun data-data lainnya yang bersifat rahasia.	LPSE belum melakukan pemilihan dan identifikasi data pribadi dan belum disesuaikan dengan undang-undang yang berlaku.
12	LPSE telah melakukan koordinasi dengan pihak tertentu seperti penanganan permasalahan dalam mengakses sistem LPSE.	LPSE belum memiliki dokumentasi koordinasi yang mencakup identifikasi persyaratan/kebutuhan pengamanan.
13	Secara lisan, LPSE telah melakukan koordinasi dengan pihak satuan terkait.	LPSE tidak memiliki dokumentasi koordinasi dengan pihak satuan terkait.
14	LPSE memiliki dokumen tugas dan tanggung jawab pengelolaan kelangsungan layanan TIK.	LPSE belum mengalokasikan keputusan, perancangan, pelaksanaan dan pengelolaan langkah kelangsungan layanan TIK.
15	LPSE memiliki pelaporan permasalahan kepada pimpinan instansi secara rutin sebulan sekali.	Dokumen pelaporan kondisi dan permasalahan belum dibuat untuk keamanan informasi. Hanya dijalankan untuk laporan layanan.
16	Tidak ditemukan temuan positif.	LPSE belum memutuskan kondisi dan permasalahan

No.	Temuan Positif	Temuan Negatif
		menjadi bagian konsideran atau bagian dari proses pengambilan keputusan strategis.
17	Tidak ditemukan temuan positif.	LPSE belum memiliki program untuk memenuhi target dan sasaran kepatuhan pengamanan informasi.
18	Tidak ditemukan temuan positif.	LPSE belum membuat dokumen pengukuran kinerja yang mencakup definisi metrik, parameter dan berisi mekanisme, waktu pengukuran, pelaksana, pemantauan dan eskalasi pelaporannya.s
19	Tidak ditemukan temuan positif.	LPSE belum merancang program penilaian kinerja bagi pelaksana pengelolaan kemanan informasi.
20	Tidak ditemukan temuan positif.	LPSE belum membuat dokumen untuk penerapan target dan sasaran pengelolaan keamanan informasi, dokumen evaluasi, dokumen perbaikan dan dokumen pelaporan kepada pimpinan instansi.
21	Tidak ditemukan temuan positif.	LPSE belum membuat dokumen legislasi dan perangkat hukum terkait keamanan informasi yang harus dipatuhi dan belum melakukan identifikasi terhadapnya.
22	Tidak ditemukan	LPSE harus mulai merancang

No.	Temuan Positif	Temuan Negatif
	temuan positif.	dokumen pengelolaan insiden keamanan informasi dan kebijakannya.

Sumber:[penulis, 2018]

6.3.3 Saran Perbaikan Area Tata Kelola Keamanan Informasi

Setelah melakukan penilaian dengan indeks KAMI versi 3.1 dan mengetahui hasil dari setiap area yang terdapat dalam indeks KAMI versi 3.1, maka tahap selanjutnya adalah membuat saran perbaikan pada setiap bagian yang masih kurang baik.

Saran perbaikan untuk area Tata Kelola Keamanan Informasi ini berisikan saran perbaikan untuk pertanyaan yang mendapat nilai kurang/ tidak dilakukan pada instansi terkait. Saran perbaikan ini mengacu pada ISO/IEC 27002:2013.

Tabel 6.7 saran dan perbaikan area tata kelola keamanan informasi

No	Pertanyaan	Status	Nilai
2,1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	Dalam Penerapan / Diterapkan Sebagian	2
Saran Perbaikan **Kontrol A.5.1.1 Policies for information security** Hal pertama yang harus dilakukan ketika melaksanakan manajemen keamanan informasi adalah menetapkan tujuan yang jelas dan mendapatkan dukungan, sedangkan pada UPT sendiri belum menetapkan tujuan dan arah yang jelas			

<table>
<tr><th>No</th><th>Pertanyaan</th><th>Status</th><th>Nilai</th></tr>
<tr><td colspan="4">mengenai keamanan informasi dan telah menetapkan kebijakan tanpa membentuk arah dan tujuan yang jelas.
LPSE harus melengkapi dokumen kebijakan sesuai standar ISO 27001 maksimal dalam kurun waktu 3 bulan atau sesuai kesepakatan. Dokumen kebijakan keamanan informasi yang dimiliki oleh instansi, harus mencakup hal-hal berikut:
- Definisi keamanan informasi, sasaran umum dan cakupan, serta pentingnya keamanan sebagai mekanisme untuk berbagi informasi;
- Penyataan komitmen manajemen, dukungan terhadap tujuan, dan prinsip keamanan informasi;
- Penjelasan singkat mengenai kebijakan keamanan, prinsip, persyaratan standar dan kesesuaian sebagai bagian penting untuk organisasi
- Selain itu, untuk mendukung pertanggung jawaban pelaksanaan program, LPSE dapat melakukan sosialisasi kebijakan kepada pengguna dan tataran organisasi.</td></tr>
<tr><td>2,3</td><td>Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?</td><td>Dalam Perencanaan</td><td>1</td></tr>
<tr><td colspan="4">Saran Perbaikan
Kontrol A.6.1.2 Segregation of duties
Dalam kurun waktu 1 bulan atau waktu yang disepakati, LPSE harus telah memiliki dokumen kewenangan dan telah disetujui oleh pihak Kominfo dan LPSE pusat. Dokumen tersebut harus didukung dengan hal-hal berikut:
- Memiliki Bagian/fungsi untuk pelaksana pengamanan dan pengelolaan keamanan informasi.</td></tr>
</table>

No	Pertanyaan	Status	Nilai
	- Mendefinisikan tugas dan tanggung jawab pengelolaan keamanan informasi setiap bagian/fungsi dalam organisasi. - Mengidentifikasi dan menetapkan aset dan proses keamanan yang berkaitan dengan sistem. - Mendokumentasikan setiap aset atau proses keamanan yang telah disetujui. Instansi membuat wewenang dengan menetapkan tingkat otorisasi dengan jelas.		
2,5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	Tidak Dilakukan	0
Saran Perbaikan **Kontrol A.6.1.2 *Segregation of duties*** **Kontrol A.8.2.3 *Handling of assets*** Untuk segregasi kewenangan harus diurus agar tidak ada satu orang yang dapat mengakses, memodifikasi, atau menggunakan aset tanpa adanya otorisasi. Jika sulit untuk memisahkan kewenangan, maka dapat menerapkan kontrol lain seperti melakukan monitoring kegiatan, melakukan audit dan pengawasan manajemen. Segregasi kewenangan ini merupakan sebuah cara untuk mengurangi risiko penyalahgunaan terhadap aset organisasi. Instansi harus membuat dokumen yang berisikan peran dari para pelaksana pengamanan informasi dan persyaratan terkait kewenangan masing-masing pihak dalam waktu 2 bulan atau sesuai dengan kesepakatan instansi.			
2,6	Apakah Instansi anda sudah mendefinisikan	Dalam Penerapan /	2

No	Pertanyaan	Status	Nilai
	persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	Diterapkan Sebagian	
Saran Perbaikan **Kontrol A.7.1.2 *Terms and conditions of employment*** Instansi harus membuat dokumen yang lebih detail mengenai persyaratan/standar kompetensi dengan maksimal waktu 3 bulan atau sesuai kesepakatan kesanggupan pihak LPSE. Dokumen yang berisikan standar kompetensi dan keahlian yang harus dimiliki oleh para pelaksana pengelolaan keamanan informasi dengan spesifikasi sebagai berikut: - Minimal 2 minggu telah Memiliki keterampilan dan kualifikasi yang sesuai dan dididik secara teratur - Karyawan menerima pendidikan dan pelatihan kesadaran yang tepat dan terupdate setelah dokumen selesai dibuat dijalankan sesuai dengan kebijakan dan prosedur keamanan informasi yang ada - Menerapkan tingkat kesadaran keamanan informasi yang relevan dengan peran dan tanggung jawab dalam organisasi tepat setelah dokumen selesai dibuat.			
2,7	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	Dalam Perencanaan	1
Saran Perbaikan **Kontrol A.7.1.1 *Screening*** **Kontrol A.7.2.2 *Information security awareness, education and training*** Sebelum dilakukan penilaian terhadap kompetensi untuk pelaksana pengamanan informasi, maka harus dilakukan penelusuran kelayakan kredit untuk pelaksana pengamanan			

<table>
<tr><th>No</th><th>Pertanyaan</th><th>Status</th><th>Nilai</th></tr>
<tr><td colspan="4">informasi. Kelayakan kredit dilakukan sebagai langkah verifikasi bahwa informasi yang dibuat telah benar adanya. Kelayakan kredit dapat dilangsungkan selama 2 minggu atau sesuai kesepakatan instansi.
Penilaian terhadap kompetensi dan keahlian karyawan dapat dilakukan dengan menilai:
- Pernyataan komitmen manajemen untuk keamanan informasi
- Tanggung jawab masing-masing individu terkait aktivitas yang dilakukan dalam mengamankan dan melindungi informasi milik instansi
- Pendidikan keamanan informasi dan materi pelatihan lebih lanjut</td></tr>
<tr><td>2,8</td><td>Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?</td><td>Dalam Perencanaan</td><td>1</td></tr>
<tr><td colspan="4">Saran Perbaikan
Kontrol A.7.2.2 Information security awareness, education and training
Kontrol A.7.2.3 Disciplinary process
Semua stakeholder instansi harus menerima pendidikan terkait kewaspadaan terhadap informasi dan pelatihan terhadap pemahaman prosedur dan kebijakan terkait keamanan informasi. Penerapan program sosialisasi harus dilaksanakan maksimal dalam kurun waktu 1 bulan setelah dokumen kebijakan keamanan informasi selesai dibuat, pendidikan dan pelatihan keamanan informasi harus mencakup aspek-aspek sebagai berikut:
- Komitmen manajemen untuk keamanan informasi di seluruh organisasi</td></tr>
</table>

No	Pertanyaan	Status	Nilai
- Tanggung jawab masing-masing individu atas tindakan terhadap pengamanan dan perlindungan informasi milik organisasi dan milik eksternal - Prosedur dasar keamanan informasi, seperti pelaporan insiden keamanan informasi			
2,9	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Dalam Perencanaan	2
Saran Perbaikan **Kontrol A.7.2.2 *Information security awareness, education and training*** Instansi harus memiliki program peningkatan kompetensi. Program pelaksanaan peningkatan kompetensi harus dirancang maksimal dalam kurun waktu 1 bulan setelah dokumn kompetensi selesai dibuat. Semua stakeholder instansi harus menerima pendidikan terkait kewaspadaan terhadap informasi dan pelatihan terhadap pemahaman prosedur dan kebijakan terkait keamanan informasi, dimana pendidikan dan pelatihan keamanan informasi mencakup aspek-aspek sebagai berikut: - Komitmen manajemen untuk keamanan informasi di seluruh organisasi - Tanggung jawab masing-masing individu atas tindakan terhadap pengamanan dan perlindungan informasi milik organisasi dan milik eksternal - Prosedur dasar keamanan informasi, seperti pelaporan insiden keamanan informasi			
2,10	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	dalam proses kerja yang ada?		
Saran Perbaikan **Kontrol A.7.2.1 *Management responsibilities*** - Instansi terlebih dahulu harus mengetahui persyaratan keamanan informasi. Persyaratan keamanan informasi didefinisikan atau diidentifikasi paling lambat dalam waktu kurang dari 1 bulan setelah melakukan program sosialisasi atau setelah membuat dokumen kewenangan. - Setelah itu, instansi harus melakukan pemetaan dan dicocokkan antara proses kerja yang terintegrasi dengan persyaratan keamanan informasi maksimal 1 bulan setelah mengidentifikasi persyaratan keamanan informasi. Apakah persyaratan keamanan informasi perlu pada proses kerja tersebut atau tidak, maka harus diberikan alasan kenapa proses kerja tersebut dibuat menjadi salah satu proses kerja terintegrasi dengan persyaratan keamanan informasi.			
2,11	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Dalam Perencanaan	2
Saran Perbaikan **Kontrol 18.1.4 *Privacy and protection of personally identifiable information*** Privasi dan perlindungan informasi terkait data pribadi harus dipastikan sebagaimana disyaratkan dalam undang-undang dan peraturan yang berlaku dengan relevan. Instansi terkait juga harus membuat kebijakan terkait perlindungan			

No	Pertanyaan	Status	Nilai
data pribadi serta mengkomunikasikannya dengan semua orang yang terlibat dalam pengelolaan data pribadi. Selain penerapan undang-undang, peraturan, dan kebijakan juga dapat diperlukan struktur manajemen yang tepat beserta kontrol-kontrolnya seperti menunjuk orang-orang yang bertanggung jawab (petugas privasi yang memberi bimbingan pada manajer, pengguna dan penyedia layanan yang bertanggung jawab pada masing-masing prosedur)			
2,12	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	Dalam Perencanaan	2
Saran Perbaikan **Kontrol A.6.1.4 *Contact with special authorities*** **Kontrol A.13.2.1 *Information transfer policies and procedures*** **Kontrol A.13.2.2 *Agreements on information transfer*** Instansi harus saling mendukung dan mempunyai hubungan baik dengan para pengguna aset informasi. Karena dapat menunjang pelaksanaan keamanan informasi dalam organisasi. Selain itu, instansi harus tetap menjaga informasi dalam organisasi. Beberapa dokumen yang dibutuhkan untuk menjaga hubungan dengan pihak terkait: - Melakukan pembatasan informasi dan mendefinisikan kategori informasi mana yang boleh diberikan dan tidak. Mengaktegorikan informasi mana yang bersifat rahasia atau terbuka. - Membuat perjanjian secara tertulis dengan pihak satuan terkait. - Mengidentifikasi akses yang akan digunakan oleh pihak terkait.			

No	Pertanyaan	Status	Nilai
Hal yang harus dipertimbangkan dalam membuat kontrak adalah sebagai berikut: - Kebijakan keamanan informasi; - Perlindungan aset (prosedur dan kontrol); - Deskripsi jenis layanan yang disediakan; - Tingkatan layanan yang dapat diterima; Kewajiban masing-masing pihak dalam perjanjian;			
2,13	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?	Dalam Perencanaan	2
Saran Perbaikan **Kontrol A.6.1.4** ***Contact with special interest group*** **Kontrol A.13.2.1** ***Confidentiality or non disclosure agreements*** Instansi harus saling mendukung dan mempunyai hubungan baik dengan para pengguna aset informasi. Karena dapat menunjang pelaksanaan keamanan informasi dalam organisasi. Selain itu, instansi harus tetap menjaga informasi dalam organisasi. Beberapa dokumen yang dibutuhkan untuk menjaga hubungan dengan pihak terkait: - Melakukan pembatasan informasi dan mendefinisikan kategori informasi mana yang			

No	Pertanyaan	Status	Nilai
	boleh diberikan dan tidak. Mengaktegorikan informasi mana yang bersifat rahasia atau terbuka. - Membuat perjanjian secara tertulis dengan pihak satuan terkait. - Mengidentifikasi akses yang akan digunakan oleh pihak terkait. Hal yang harus dipertimbangkan dalam membuat kontrak adalah sebagai berikut: - Kebijakan keamanan informasi; - Perlindungan aset (prosedur dan kontrol); - Deskripsi jenis layanan yang disediakan; - Tingkatan layanan yang dapat diterima; - Kewajiban masing-masing pihak dalam perjanjian.		
2,14	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	Dalam Perencanaan	2
Saran Perbaikan **Kontrol A.17.1.1 *Planning information security continuity*** **Kontrol A.17.1.2 *Implementing information security continuity*** Instansi harus menentukan bahwa keberlangsungan keamanan informasi menjadi bagian dari proses manajemen keberlangsungan bisnis dan pemulihan bencana. Syarat keamanan informasi harus ditentukan ketika merencanakan keberlangsungan bisnis dan pemulihan bencana. Instansi juga harus melakukan analisis dampak bisnis terkait aspek keamanan informasi untuk menentukan syarat keamanan informasi yang berlaku pada situasi yang merugikan.			

No	Pertanyaan	Status	Nilai
Informasi lebih detail mengenai manajemen keberlangsungan bisnis dapat ditemukan pada ISO/IEC 27031, ISO/IEC 22313, dan ISO/IEC 22301 LPSE juga harus memastikan: - Adanya struktur manajemen yang berwenang, berpengalaman, dan berkompetensi untuk mempersiapkan, memitigasi, dan menanggapi suatu peristiwa yang mengganggu - Pihak terkait harus memiliki kewenangan, tanggung jawab, dan kompetensi dalam mengelola insiden dan menjaga keamanan informasi - Mengembangkan dan menyetujui dokumentasi rencana, respon, dan pemulihan prosedur secara rinci sebagaimana organisasi akan mengelola suatu peristiwa yang mengganggu dan akan menjaga keamanan informasi untuk tingkat yang telah ditentukan, berdasarkan pada tujuan kelangsungan keamanan informasi manajemen yang disetujui			
2,15	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	Tidak Dilakukan	0
Saran Perbaikan **Kontrol A.16.1.2 *Reporting information security events*** Penanggungjawab pengelola keamanan informasi harus terlebih dahulu membuat buku laporan kondisi keamanan informasi. Laporan tersebut, dapat berisi kondisi saat ini, permasalahan yang berhubungan dengan keamanan informasi (*confidentiality*, *integrity*, *availability*) ataupun pelaporan lain yang masih berkesinambungan dengan keamanan informasi instansi. Maka dari itu, perlu adanya : - Kebijakan keamanan informasi yang menjelaskan			

No	Pertanyaan	Status	Nilai
	laporan kepada pimpinan instansi; - Prosedur melaporkan kondisi keamanan informasi; - Form laporan keamanan informasi.		
2,16	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	Tidak Dilakukan	0
Saran Perbaikan **Kontrol A.5.1.2** ***Review of the policies for information security*** **Kontrol A.8.2.1** ***Classification of information*** Kondisi dan permasalahan dalam instansi harus diidentifikasi terlebih dahulu. Informasi harus terlebih dahulu diklasifikasi, dengan tujuan agar kebutuhan, prioritas dan tingkat perlindungan informasi memiliki perbedaan tingkat derajat kerahasiaan dan kepentingan. Untuk mengetahui apakah kondisi dan permasalahan menjadi bagian dari konsideran atau proses pengambilan strategi, maka instansi perlu mengklasifikasikan: - berdasarkan nilainya (value); - persyaratan-persyaratan legalnya; - dan berdasarkan tingkat kepentingannya (sensitive and critically) terhadap organisasi.			
2,17	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	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	tanggungjawabnya?		
Saran Perbaikan **Kontrol A.6.1.5 *Information security in project management*** **Kontrol A.8.2.3 *Handling of assets*** Penerapan program untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi dapat diterapkan dalam bentuk dan bagian manajemen proyek agar dapat memastikan bahwa keamanan informasi telah diidentifikasi dan ditangani sebagai bagian dari proyek. Metode manajemen proyek ini harus berisi: - Tujuan keamanan informasi termasuk dalam tujuan proyek - penilaian risiko keamanan informasi dilakukan pada tahap awal dari proyek untuk mengidentifikasi kendali yang diperlukan - keamanan informasi adalah bagian dari semua tahapan metodologi proyek yang diterapkan Keamanan informasi harus ditangani dan ditinjau secara teratur dalam semua proyek. Tanggung jawabnya juga harus dialokasikan secara spesifik dalam manajemen proyek.			
2,18	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	Tidak Dilakukan	0
Saran Perbaikan **Kontrol A.5.1.2 *Review of the policies for information security***			

No	Pertanyaan	Status	Nilai
Kontrol A.6.1.5 ***Information security in project management*** **Kontrol A.18.2.1** ***independent review of information security*** Keamanan informasi yang telah dibuat dalam program-program harus dilakukan peengkuran pada interval tertentu. Pengukuran kinerja dapat dilakukan selama kurun waktu tertentu, disesuaikan dengan kebutuhan organisasi. Organisasi jika ingin mengetahui kinerja pengelolaan keamanan informasi dapat dibuat dengan mengukur : - penanggung jawab pengukuran kinerja keamanan informasi. - Bagaimana mekanisme pelaksanaan pengukuran kinerja. - Kapan dilaksanakan pengukuran kinerja. - Bagaimana memantau pengukuran kinerja yang akan dilakukan. - Bagaiman membuat laporan pengukuran kinerja. Berarti LPSE juga dapat membuat prosedur untuk pengukuran kinerja sebagai tambahan dalam proses pengukuran kinerja. Penerapan proses pengukuran kinerja untuk memenuhi tujuan dan sasaran kepatuhan pengamanan informasi dapat diterapkan/ diintegrasikan pada manajemen proyek agar dapat memastikan bahwa risiko terkait keamanan informasi telah diidentifikasi dan ditangani sebagai bagian dari proyek. Metode manajemen proyek ini harus mensyaratkan: - Tujuan keamanan informasi termasuk dalam tujuan proyek - penilaian risiko keamanan informasi dilakukan pada tahap awal dari proyek untuk mengidentifikasi kendali yang diperlukan - keamanan informasi adalah bagian dari semua tahapan metodologi proyek yang diterapkan Keamanan informasi harus ditangani dan ditinjau secara teratur dalam semua proyek. Tanggung jawabnya juga			

No	Pertanyaan	Status	Nilai
harus dialokasikan secara spesifik dalam manajemen proyek.			
2,19	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Tidak Dilakukan	0
Saran Perbaikan **Kontrol A.7.2.3 *Disciplinary process*** Diterapkan program penilaian kinerja pengelolaan keamanan informasi bagi masing-masing individu terkait. Penilaian kinerja terhadap masing-masing individu dapat dilihat dari beberapa hal antara lain: - Kedisiplinan dalam menjalankan keamanan informasi sesuai dengan prosedur dimana instansi harus terlebih dahulu menerapkan proses kedisiplinan secara formal - Pelanggaran yang pernah dilakukan terkait keamanan informasi organisasi - Motivasi dalam memenuhi kebijakan keamanan informasi yang ada - Kepatuhan terhadap syarat dan kondisi kerja, termasuk kebijakan keamanan informasi organisasi - Memiliki keterampilan dan kualifikasi yang sesuai dengan persyaratan yang telah ditentukan sebelumnya			
2,20	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah	Tidak Dilakukan	0

No	Pertanyaan	Status	Nilai
	perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi?		
Saran Perbaikan **Kontrol A.17.1.3** ***Verify, review and evaluate information security continuity*** **Kontrol A.18.2.1** ***Independent review of information security*** Target dan sasaran keamanan informasi terdapat dalam kebijakan keamanan informasi yang mana harus dilakukan peninjauan secara rutin untuk memastikan kesesuaian, kecukupan, dan efektivitasnya secara terus menerus. Selain dari kebijakan keamanan informasi, dokumen kelangsungan layanan juga menjadi salah satu target yang harus dievaluasi. Karena di dalam dokumen kelangsungan layanan terdapat sasaran dan target keamanan informasi dan tata cara pelaksanaan keamanan informasi. Tinjauan tersebut harus mencakup penilaian peluang perbaikan kebijakan organisasi dan pendekatan untuk mengelola keamanan informasi dalam menanggapi perubahan lingkungan organisasi, situasi bisnis, kondisi hukum atau lingkungan teknis. Jika terjadi revisi saat melakukan review kebijakan ini maka harus mendapatkan persetujuan dari manajemen terkait.			
2,21	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Tidak Dilakukan	0
Saran Perbaikan **Kontrol A.18.1.1 Identification of applicable legislation**			

No	Pertanyaan	Status	Nilai
and contractual requirements Semua aturan legislatif yang relevan, peraturan, dan syarat kontrak untuk memenuhi persyaratan ini harus secara diidentifikasi secara eksplisit, didokumentasikan dan terus diperbarui. Terkait kontrol spesifik dan tanggung jawab masing-masing individu juga harus diidentifikasikan dan didokumentasikan. LPSE harus mengidentifikasi semua undang-undang yang berlaku untuk instansi dalam rangka memenuhi persyaratan untuk jenis bisnis yang dijalankan. Beberapa contoh undang-undang yang menyangkut keamanan informasi ada: - Undang-undang no.11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. - Peraturan Menteri Komunikasi dan Informatika no.4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi.			
2,22	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	Tidak Dilakukan	0
Saran Perbaikan **Kontrol A.16.1.1 *Responsibilities and Procedures*** **Kontrol A.18.1.3 *Protection of records*** LPSE harus membuat dokumen penanggulangan insiden keamanan informasi dan mendefinisikan kebijkannya. Dokumen penanggulangan insiden harus selesai dibuat maksimal 2 bulan atau sesuai kesepakatan setelah dokumen program target dan sasaran pengelolaan keamanan informasi diterapkan minimal 1 bulan. Berikut ini adalah pedoman untuk tanggung jawab dan prosedur yang berkaitan dengan manajemen insiden keamanan informasi:			

No	Pertanyaan	Status	Nilai
	- Mempersiapkan prosedur untuk persiapan dan perencanaan respon terhadap insiden - Prosedur terkait pemantauan, pendeteksian, analisis, dan pelaporan insiden keamanan informasi - Prosedur terkait insiden *logging* - Prosedur penanganan bukti forensik - Prosedur respon termasuk untuk eskalasi, pemulihan kendali dari insiden, dan komunikasi untuk pihak internal dan eksternal instansi Dalam prosedur juga harus memastikan bahwa pelaksana harus berkompeten dalam menangani masalah terkait insiden keamanan informasi. Tujuan dari pengelolaan insiden keamanan informasi harus disepakati dengan manajemen, dan harus dipastikan bahwa mereka yang bertanggung jawab untuk manajemen insiden keamanan informasi memahami prioritas organisasi untuk menangani insiden keamanan informasi. Detail panduan tentang pengelolaan insiden keamanan informasi disediakan dalam ISO/IEC 27035.		

Sumber:[penulis, 2018]

“Halaman ini sengaja dikosongkan”

BAB VII
KESIMPULAN DAN SARAN

Bab ini akan menjelaskan kesimpulan dari penelitian, beserta saran yang dapat bermanfaat untuk perbaikan di penelitian selanjutnya.

7.1 Kesimpulan

Kesimpulan yang didapat berdasarkan penelitian yang dilakukan adalah sebagai berikut:

1. Jumlah skor yang didapat pada UPT LPSE adalah 23. Skor tersebut didapatkan dari penjumlahan nilai pertanyaan label '1' sebanyak 13 dan skor label '2' sebanyak 10.
2. Hasil tersebut menunjukkan kematangan pada Area Tata Kelola keamanan informasi dalam UPT LPSE menunjukkan level **I+**
3. Hasil tersebut bermakna **Penerapan Kerangka Kerja Dasar**, dimana alur komunikasi belum jelas dan tanpa pengawasan dan manajemen non-teknis belum teridentifikasi.
4. Evaluasi Keamanan Informasi ini bersifat evaluasi sumatif, karena membuat penilaian yang mengacu pada suatu standar. Berikut adalah rekomendasi untuk penilaian Area Tata Kelola Keamanan Informasi:
    - Membuat komitmen manajemen dan dilakukan secara formal dan tertulis.
    - Membuat dokumen kewenangan dan dikomunikasikan kepada seluruh staff LPSE.
    - Pihak LPSE harus mendokumentasikan setiap kegiatan yang berhubungan dengan peningkatan kompetensi/keahlian staff LPSE.

- Pihak LPSE harus mendokumentasikan setiap perjanjian dengan pihak terkait.
- Pihak LPSE harus merencanakan pengukuran kinerja dan memulai membuat dokumen pengukuran kinerja.

5. Pada penelitian yang diangkat, masih terdapat beberapa kekurangan, yaitu:
   - Pada proses pengerjaan evaluasi yang berbeda dengan metodologi yang ditulis. Seperti penambahan proses analisa kontrol Indeks KAMI, yang belum terdapat pada alur metodologi.
   - Dasar analisa/justifikasi kontrol Indeks KAMI yang belum memiliki dasar kuat sehingga hasil yang didapatkan belum maksimal.

7.2 Saran dan Penelitian Selanjutnya

Saran yang dapat diberikan dari hasil pengerjaan tugas akhir dengan studi kasus Evaluasi Keamanan Informasi adalah sebagai berikut:

1. Untuk penelitian selanjutnya
   - Melakukan penelitian lebih lanjut mengenai *self-asessment* pada Indeks KAMI.
2. Untuk Unit LPSE Kominfo
   - Alangkah lebih baikya jika mengikuti petunjuk teknis secara detail dengan megikuti acara Bimbingan Teknis yang diadakan oleh pihak Kominfo mengenai proses penilaian pada Indeks KAMI guna memahami perolehan skor yang didapat maupun untuk perbaikan serta pengembangan proses penilaian untuk kedepannya
   - Perhatikan cara pengujian pada pertanyaan yang membutuhkan jenis penilaian lebih dari satu, maka lakukan pengujian terhadap kualitas dan juga kuantitas pada item yang dinilai agar nilai yang diberikan pada pertanyaan tersebut benar-benar valid

DAFTAR PUSTAKA

[1] T. Direktorat Keamanan Informasi, *PANDUAN PENERAPAN TATA KELOLA KEAMANAN INFORMASI BAGI PENYELENGGARA PELAYANAN PUBLIK*. Kominfo RI, 2011.

[2] Kementerian Komunikasi dan Informatika, "Ancaman Cyber Attack dan Urgensi Keamanan Informasi Nasional," *Siaran Pers*, 2013. [Online]. Available: https://kominfo.go.id/index.php/content/detail/3479/Siaran+Pers+No.+83-PIH-KOMINFO-11-2013+tentang+Ancaman+Cyber+Attack+dan+Urgensi+Keamanan+Informasi+Nasional/0/siaran_pers. [Accessed: 01-Mar-2018].

[3] W. Ferrissa and Kementerian Komunikasi dan Informatika, "Menkominfo: E-Government Mulai Maret 2018, Semua Perizinan Harus Online," *Sorotan Media*, 2017. [Online]. Available: https://kominfo.go.id/content/detail/12004/menkominfo-e-government-mulai-maret-2018-semua-perizinan-harus-online/0/sorotan_media. [Accessed: 01-Mar-2018].

[4] Viska and Kementerian Komunikasi dan Informatika, "Sesditjen Aptika Tegaskan Keamanan Siber Jadi Isu Penting," *Berita Kementerian*, 2018. [Online]. Available: https://kominfo.go.id/content/detail/12503/sesditjen-aptika-tegaskan-keamanan-siber-jadi-isu-penting/0/berita_satker. [Accessed: 01-Mar-2018].

[5] I. Rahayu and Kasubdit Budaya Keamanan Informasi, "Sosialisasi Aplikasi," Bandung, 2015.

[6] Presiden Republik Indonesia, *UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 11 TAHUN 2008 tentang Informasi dan Transaksi Elektronik*. Indonesia, 2008.

[7] Departemen Sistem Informasi, *Roadmap Laboratorium*

2017, 1st ed. Surabaya: Institut Teknologi Sepuluh Nopember, 2017.

[8] M. R. Ridho, *Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan SNI ISO/IEC 27001:2009 Studi Kasus: Bidang Aplikasi dan Telematika Dinas Komunikasi dan Informatika Surabaya*. Surabaya: Institut Teknologi Sepuluh Nopember, 2012.

[9] L. Ulinnuha, *Evaluasi Pengelolaan Keamanan Jaringan di ITS dengan Menggunakan Standar Indeks Keamanan Informasi (KAMI) Kemenkominfo RI*. Surabaya: Institut Teknologi Sepuluh Nopember, 2013.

[10] E. Umiyati, *Penilaian Service Desk Layanan Teknologi Informasi Menggunakan OGC Self-Assessment Berbasis ITIL (Studi Kasus : Unit Sistem Informasi PT.KAI (Persero) Daerah Operasi 8 Surabaya)*. Surabaya: Institut Teknologi Sepuluh Nopember, 2015.

[11] F. A. Basyarahil, *INDEKS KEAMANAN INFORMASI (KAMI) BERDASARKAN ISO / IEC 27001 : 2013 PADA DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) ITS SURABAYA EVALUATING INFORMATION SECURITY MANAGEMENT USING INDEKS KEAMANAN INFORMASI (KAMI) BASED ON ISO / IEC*. Institut Teknologi Sepuluh Nopember, 2016.

[12] "Kamus Besar Bahasa Indonesia (KBBI)." [Online]. Available: https://kbbi.web.id/evaluasi. [Accessed: 01-Mar-2018].

[13] "English Oxford Living Dictionary." [Online]. Available: https://en.oxforddictionaries.com/definition/evaluation. [Accessed: 01-Mar-2018].

[14] GAO, "Performance Measurement and Program Evaluation," *Glossary*. United State General Accounting Office, 2005.

[15] R. L. Schalock, *Outcome-Based Evaluation*, Berilustra. Springer Science & Business Media, 2013.

[16] H. Umar, *Evaluasi Kinerja Perusahaan*. Jakarta:

Gramedia Pustaka Utama, 2005.

[17] A. Kadir, *Pengenalan Sistem Informasi*, 1st ed. Yogyakarta: ANDI, 2003.

[18] E. Turban, M. Ephraim, and J. Wethere, *Information Technology for Management Making Connections for Strategis Advantage*, 2nd ed. John Wiley & Sons, Inc, 1999.

[19] "English Oxford Living Dictionaries." [Online]. Available: https://en.oxforddictionaries.com/definition/information_technology. [Accessed: 26-Feb-2018].

[20] M. Eppler, *Managing Information Technology What Managers Need to Know*, 3rd ed. New Jersey: Pearson Educational International, 1999.

[21] "Kamus Besar bahasa Indonesia (KBBI)." [Online]. Available: https://kbbi.web.id/teknologi. [Accessed: 27-Feb-2018].

[22] "Kamus Besar Bahasa Indonesia (KBBI)." [Online]. Available: https://kbbi.web.id/informasi. [Accessed: 27-Feb-2018].

[23] H. J. Lucas, *Information Technology for Management*. Irwin/McGraw-Hill, 2000.

[24] H. Al Fatta, *Analisis dan Perancangan Sistem Informasi untuk Keunggulan Bersaing Perusahaan dan Organisasi Modern*, 1st ed. Yogyakarta: ANDI, 2007.

[25] V. S. Bagad, *Management Information Systems*, 3rd ed. Technical Publications Pune, 2008.

[26] M. E. Whitman and H. J. Mattord, *Principles of Information Security*, 6th ed. Boston: Cengage Learning, 2018.

[27] B. Metivier, "Fundamental Objectives of Information Security:," 2017. .

[28] C. Chazar, "Standar Manajemen Keamanan Informasi Berbasis ISO/IEC 27001: 2005," *J. Inf.*, vol. VII, no. 2, pp. 48–57, 2015.

[29] I. Isa, *Evaluasi Pengontrolan Sistem Informasi*, 1st ed. Yogyakarta: Graha Ilmu, 2012.

[30] R. Sarno and I. Iffano, *Sistem Manaemen Keamanan*

Informasi, 1st ed. Surabaya: ITS Press, 2009.

[31] Cnni, "Information Security Management system (ISMS)." [Online]. Available: http://cnii.cybersecurity.my/main/resources/ISMS.pdf. [Accessed: 28-Feb-2018].

[32] Altha, "Menghadapi Tantangan Keamanan Teknologi Informasi dengan Implementasi Sistem Manajemen Keamanan Informasi berbasis ISO 27001 di Sektor Publik," 2017. [Online]. Available: http://www.altha.co.id/news/menghadapi-tantangan-keamanan-teknologi-informasi-dengan-implementasi-sistem-manajemen-keamanan-informasi-berbasis-iso-27001-di-sektor-publik. [Accessed: 02-Mar-2018].

[33] Kementerian Komunikasi dan Informatika, "Indeks KAMI Versi 3.1." Kementerian Komunikasi dan Informatika, Jakarta, 2013.

[34] M. Utomo, A. H. N. Ali, and I. Affandi, "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO / IEC 27001 : 2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I," *J. Tek. Its*, vol. 1, no. 1, pp. 288–293, 2012.

BIODATA PENULIS

ISNAINI NUR ROHMAWATI, lahir 18 Mei 1996 di kota Pasuruan. Penulis merupakan anak terakhir dari dua bersaudara. Penulis pernah menempuh pendidikan formal di SDN Nogosari Pandaan Pasuruan, MTs Wali Songo Ponorogo, MA Wali Songo Ponorogo, dan akhirnya masuk menjadi mahasiswa program sarjana S1 Departemen Sistem Informasi Institut Teknologi Sepuluh Nopember (ITS) angkatan 2014. Akhir masa perkuliahan di jurusan Sistem Informasi ITS, penulis memilih untuk mengerjakan tugas akhir di Laboratorium Manajemen Sistem Informasi (MSI). Penulis mengambil topik mengenai evaluasi manajemen keamanan informasi dibawah bimbingan Bapak Ir. Khakim Ghozali, M.MT. Selama menjadi mahasiswa di jurusan Sistem Informasi, penulis aktif dalam unit kegiatan mahasiswa(UKM) pramuka dan di tahun keempat menjabat sebagai Pemangku Adat. Tidak hanya itu, penulis juga aktif menjadi pengurus CSSMoRA PT di tahun ketiga. Untuk kepentingan penelitian penulis dapat dihubungi melalui e-mail: isnaini.nurrahma1448@gmail.com.com

“*Halaman ini sengaja dikosongkan”*

LAMPIRAN A
Daftar Tabel Identifikasi Poin Pertanyaan pada Area Tata Kelola Keamanan Informasi dan Pemetaan dengan Klausul Kontrol ISO/IEC 27001:2013

Tabel A.1 identifikasi poin pertanyaan pada Area Tata Kelola Keamanan Informasi dengan pemetaan kontrol ISO 27001:2013

II	1	Pertanyaan No. 1
Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
- Tanggung jawab pelaksanaan program keamanan informasi dan Penetapan kebijakan		A.5.1.1 *Policies for information security*
Justifikasi		
Klausul kontrol A.5.1.1 *Policies for information security* menjelaskan mengenai perangkat kebijakan yang harus didefinisikan, disetujui oleh manajemen, dipublikasikan dan dikomunikasikan kepada karyawan dan pihak eksternal yang relevan. Hal tersebut bertujuan agar keamanan informasi terarah dan manajemen keamanan informasi lebih jelas. Prinsip dan tanggung jawab pelaksanaan keamanan informasi biasanya tercatat dalam dokumen kebijakan keamanan informasi atau dokumen-dokumen yang terkait dngan keamanan informasi.		

II	1	Pertanyaan No. 2
Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Pembagian peran dan		A.6.1.1 *Information security*

penanggung jawab	*roles and responsibilities*
Justifikasi	
Klasul kontrol A.6.1.1 *Information security roles and responsibilities* menjelaskan tentang tanggung jawab seluruh keamanan informasi yang didefinisikan dan dialokasikan. Hal tersebut merupakan salah satu penjelasan dalam tanggung jawab mengelola keamanan informasi yang dialokasikan dan dibagi ke dalam bagian-bagian atau fungsi tertentu.	

II	1	Pertanyaan No. 3
Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Pembagian tugas dan wewenang		A.6.1.2 *Segregation of duties*
Justifikasi		
Klausul kontrol A.6.1.2 *Segregation of duties* menjelaskan mengenai pertentangan dalam tugas dan tanggung jawab harus dipisahkan untuk mengurangi peluang pada modifikasi tidak sah atau tidak disengaja dan pada penyalahgunaan aset informasi.		

II	1	Pertanyaan No. 4
Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Alokasi sumber daya		A.12.1.3 *Capacity management* A.8.1.3 *Acceptable use of Assets*
Justifikasi		
Klausul A.12.1.3 *Capacity management* menjelaskan		

mengenai penggunaan sumber daya yang harus dipantau, disesuaikan dan proyeksi yang terbuat dari kebutuhan kapasitas mendatang untuk memastikan kinerja sistem yang diperlukan. Hal tersebut berhubungan dengan kapasitas sumber daya dan alokasi penggunaannya Klausul A.8.1.3 *Acceptable use of Assets* menjelaskan mengenai aturan penggunaan informasi yang dapat diterima dan aset yang terkait dengan informasi dan fasilitas pemrosesan informasi harus diidentifikasi, didokumentasikan dan diimplementasikan. Kontrol tersebut berhubungan dengan pengelolaan dan penggunaan sumber daya, termasuk penggunaan informasi beserta seluruh aset di dalamnya.

II	1	Pertanyaan No. 5
Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Pemetaan peran pelaksana pengamanan informasi		A.6.1.2 *Segregation of duties* A.8.2.3 *Handling of assets*
Justifikasi		
Klausul A.6.1.2 *Segregation of duties* menjelaskan mengenai pertentangan dalam tugas dan tanggung jawab harus dipisahkan untuk mengurangi peluang pada modifikasi tidak sah atau tidak disengaja dan pada penyalahgunaan aset informasi. Klausul A.8.2.3 *Handling of assets* menjelaskan prosedur untuk menangani aset yang harus dikembangkan dan diimplementasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi.		

II	1	Pertanyaan No. 6
Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana		

pengelolaan keamanan informasi?	
Poin Pertanyaan	Klausul ISO/IEC 27001:2013
Definisi syarat/standar kompetensi dan keahlian	A.7.1.2 *Terms and conditions of employment*
Justifikasi	
Kalusul kontrol A.7.1.2 menjelaskan perjanjian kontrak dengan karyawan maupaun kontraktor harus menyatakan tanggung jawab mereka dana organisasi sebagai keamanan informasi.	

II	1	Pertanyaan No. 7
Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Kompetensi dan keahlian pelaksana pengamanan informasi		A.7.1.1 *Screening*
Justifikasi		
Klasul kontrol A.7.1.1 merupakan kontrol mengenai pemeriksaan verifikasi latar belakang pada semua kandidat yang harus dilakukan sesuai hukum yang relevan, aturan dan etika harus proposional dengan kebutuhan bisnis, klasifikasi informasi yang akan diakses dan persepsi risiko.		

II	1	Pertanyaan No. 8
Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
- Sosialisasi pemahaman keamanan informasi - Sosialisasi kepentingan		A.7.2.2 *Information security awareness, education and training*

kepatuhan keamanan informasi	A.7.2.3 *Disciplinary process*
Justifikasi	
Klausul kontrol A.7.2.2 *Information security awareness, education and training* merupakan kontrol mengenai semua karyawan oraganisasi yang relevan dan kontraktor harus menerima edukasi dan pelatihan kesadaran yang relevan dan pembaruan rutin kebijakan serta prosedur sesuai dengan fungsi pekerjaan mereka. Hal tersebut mendukung poin mengenai pemahaman keamanan informasi dan kepatuhan keamanan informasi sebagai salah satu edukasi dalam peningkatan kesadaran keamanan informasi. Klausul Kontrol A.7.2.3 *Disciplinary process* berbicara mengenai proses disiplin formal yang harus dikomunikasikan untuk mengambil tindakan terhadap karyawan yang melakukan pelanggaran keamanan informasi. Hal tersebut berhubungan dengan bagaimana meningkatkan kepatuhan terhadap keamanan informasi yang ada.	

II	2	Pertanyaan No. 9
Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Penerapan program peningkatan kompetensi dan keahlian pelaksana pengelolaan keamanan informasi		A.7.2.2 *Information security awareness, education and training*
Justifikasi		
Klausul Kontrol A.7.2.2 *Information security awareness, education and training* menjelaskan mengenai bagaimana setiap pihak yang relevan, seperti karyawan, kontraktor harus menerima edukasi dan pelatihan relevan terhadap kesadaran dan pembaruan kebijakan dan prosedur sesuai dengan		

pekerjaan mereka. Penjelasan tersebut berhubungan dengan poin pertanyaan mengenai program peningkatan kompetensi dan keahlian karyawan, karena kontrol tersebut berbicara mengenai edukasi dan pelatihan setiap karyawan yang relevan.

II	2	Pertanyaan No. 10
Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Integrasi keperluan/persyaratan keamanan informasi pada proses kerja		A.7.2.1 *Management responsibilities*
Justifikasi		
Klausul Kontrol A.7.2.1 *Management responsibilities* berbicara mengenai manajemen yang mengharuskan semua pihak yang terlibat (karyawan dan kontraktor) menerapkan keamanan informasi yang sesuai dengan kebijakan dan prosedur organisasi yang ditetapkan. Hal tersebut menjelaskan mengenai bagaimana manajemen menerapkan persyaratan keamanan informasi yang tepat dalam setiap kegiatan atau proses kerja yang ada.		

II	2	Pertanyaan No. 11
Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
- Informasi data pribadi - pengamanan data pribadi		A.18.1.4 *Privacy and protection of personally identificable information*
Justifikasi		
Klausul Kontrol A.18.1.4 *Privacy and protection of personally*		

identificable information menjelaskan bahwa privasi dan informasi identitas pribadi harus dilindungi dan dipastikan sebagaimana disyaratkan dalam undang-undang dan peraturan relevan yang masih berlaku. Penjelasan tersebut berhubungan dengan bagaimana data pribadi dilindungi dan informasi pribadi apa saja yang boleh diambil.

II	2	Pertanyaan No. 12
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?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Tanggung jawab koordinasi pihak pengelola/pengguna aset informasi		A.6.1.4 *Contact with special interest group* A.13.2.1 *Information transfer policies and procedures* A.13.2.2 *Agreements on information transfer*
Justifikasi		
Klausul Kontrol A.6.1.4 *Contact with special interest group* menjelaskan mengenai bagaimana menjaga hubungan yang sesuai dengan kelompok minat khusus atau forum keamanan spesialis dan asosiasi profesional lainnya. Klausul Kontrol A.13.2.1 *Information transfer policies and procedures* berbicara tentang pemberlakuan kebijakan, prosedur dan kendali transfer formal sebagai perlindungan transfer informasi melalui berbagai penggunaan semua jenis fasilitas komunikasi. Klausul Kontrol A.13.2.2 *Agreements on information transfer* menjelaskan mengenai bagaimana perjanjian harus menjadikan transfer informasi bisnis antara organisasi dan		

pihak eksternal menjadi aman. Ketiga hal tersebut berhubungan dengan bagaimana berbagai belak pihak yang berkepentingan dengan aset informasi harus membuat peraturan atau persyaratan keamanan agar masalah dapat terselesaikan dan hubungan antara belah pihak tetap terjaga.

II	2	Pertanyaan No. 13
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?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Koordinasi untuk penerapan dan jaminan kepatuhan pengamanan informasi dengan berbagai pihak		A.6.1.3 *Contact with authorities* A.13.2.4 *Confidentiality or non disclosure agreements*
Justifikasi		
Klausul Kontrol A.6.1.3 *Contact with authorities* merupakan kontrol mengenai hubungan yang sesuai dengan wewenang yang bersangkutan harus dijaga. Klausul Kontrol A.13.2.4 *Confidentiality or non disclosure agreements* menjelaskan mengenai persyaratan atau kebutuhan konfidensial atau perjanjian terbuka yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, ditinjau dan didokumentasikan secara teratur. Hubungan kontrol tersebut adalah bahwa koordinasi dengan satuan terkait perlu dijaga dan dilakukan perjanjian agar menjamin keamanan informasi yang ada.		

III	2	Pertanyaan No. 14
Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah		

didefinisikan dan dialokasikan?	
Poin Pertanyaan	Klausul ISO/IEC 27001:2013
Definisi dan alokasi tanggung jawab keberlangsungan layanan TIK	A.17.1.1 *Planning information security continuity* A.17.1.2 *Implementing information security continuity*
Justifikasi	
Klausul Kontrol A.17.1.1 *Planning information security continuity* berbicara tentang organisasi yang harus menentukan persyaratan untuk keamanan informasinya dan kelangsungan manajemen keamanan informasi dalam berbagai situasi sampai dengan situasi yang merugikan, seperti saat kritis atau bencana. Klausul Kontrol A.17.1.2 *Implementing information security continuity* merupkan kontrol mengenai organisasi yang harus menetapkan, mendokumentasikan, menerapkan dan memelihara proses, prosedur, dan kontrol untuk memastikan tingkat kesinambungan yang diperlukan untuk keamanan informasi selama situasi yang merugikan. Hal tersebut merupakan	

III	2	Pertanyaan No. 15
Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Pelaporan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi		A.16.1.2 *Reporting information security events*
Justifikasi		

Klausul Kontrol A.16.1.2 *Reporting information security events* berbicara mengenai kejadian keamanan informasi yang harus dilaporkan secepat mungkin melalui saluran manajemen yang tepat. Hal tersebut bersangkutan dengan pelaporan yang dilakukan secara rutin agar mengetahui kinerja/efektivitas dan bagaimana kepatuhan terhadap keamanan informasi.

III	2	Pertanyaan No. 16
Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Proses pengambilan keputusan untuk kondisi dan permasalahan keamanan informasi		A.5.1.2 *Review of the policies for information security* A.8.2.1 *Classification of information*
Justifikasi		
Klausul Kontrol A.5.1.2 *Review of the policies for information security* berbicara mengenai peninjauan kebijakan untuk keamanan informasi pada interval yang telah direncanakan atau saat terjadi perubahan yang signifikan, untuk memastikan kesesuaian, kecukupan dan efektivitas keberlanjutannya. Klausul Kontrol A.8.2.1 *Classification of information* menjelaskan mengenai informasi yang harus diklasifikasi dalam persyaratan hukum, nilai, kekritisan dan kepekaan terhadap penyingkapan atau modifikasi yang tidak sah. Kontrol tersebut berhubungan dengan poin pertanyaan yang mengungkapkan bahwa setiap permasalahan keamanan informasi juga melakukan peninjauan kebijakan untuk dapat mengetahui efketivitas keamanan informasi dan bagaimana informasi dibahas dan dibuat dalam pengambilan keputusan agar tidak terjadi suatu kejadian yang buruk.		

IV	3	Pertanyaan No. 17

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?	
Poin Pertanyaan	Klausul ISO/IEC 27001:2013
Program kepatuhan pengamanan informasi pada aset informasi	A.6.1.5 *Information security in project management* A.8.2.3 *Handling of assets*
Justifikasi	
Klausul Kontrol A.6.1.5 *Information security in project management* berbicara mengenai keamanan informasi yang harus ditangani walaupun dalam manajemen proyek dan terlepas dari segala jenis proyek yang ada. Klausul Kontrol A.8.2.3 *Handling of assets* menjelaskan mengenai prosedur untuk menangani aset yang harus dikembangkan dan diimplmentasikan sesuai dengan skema klasifikasi informasi yang diadopsi oleh organisasi. Hal tersebut berhubungan dengan penanganan aset atau kegiatan yang harus sesuai dengan skema yang ada dan memenuhi tujuan dan sasaran keamanan informasi. Selain itu, keamanan informasi dalam manajemen proyek juga membantu dalam pembuatan program untuk mematuhi tujuan dan sasaran kepatuhan keamanan informasi.	

IV	3	Pertanyaan No. 18
Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Pengukuran kinerja pengelolaan keamanan informasi: - metrik pengukuran - parameter pengukuran		A.5.1.2 *Reviews of the policies for information security* A.6.1.5 *Information security in project management*

kinerja - mekanisme pelaksanaan - waktu pengukuran - pelaksana pengukuran kinerja - pemantauan - eskalasi pelaporan	A.18.2.1 *Independent review of information security*
Justifikasi	
Klausul Kontrol A.5.1.2 *Review of the policies for information security* berbicara mengenai peninjauan kebijakan untuk keamanan informasi pada interval yang telah direncanakan atau saat terjadi perubahan yang signifikan, untuk memastikan kesesuaian, kecukupan dan efektivitas keberlanjutannya. Klausul Kontrol A.6.1.5 *Information security in project management* berbicara mengenai keamanan informasi yang harus ditangani walaupun dalam manajemen proyek dan terlepas dari segala jenis proyek yang ada. Klausul Kontrol A.18.2.1 *Independent review of information security* berbicara mengenai pendekatan organisasi untuk mengelola keamanan informasi dan implementasinya yang harus ditinjau secara independen pada interval yang telah direncanakan atau ketika perubahan signifikan terjadi. Hal tersebut menjelaskan bagaimana instansi mendefinisikan hal tersebut ke dalam suatu definisi, seperti halnya dengan program pada suatu proyek dan melakukan peninjauan serta melakukan peninjauan terhadapnya.	

IV	3	Pertanyaan No. 19
Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Penilaian kinerja bagi pelaksana keamanan informasi		A.7.2.3 *Disciplinary process*

Justifikasi
Klausul Kontrol A.7.2.3 *Disciplinary process* berbicara mengenai proses disiplin formal yang harus dikomunikasikan untuk mengambil tindakan terhadap karyawan yang melakukan pelanggaran keamanan informasi. Hal tersebut berhubungan dengan penilaian kinerja dari proses disiplin yang dibuat oleh instansi

IV	3	Pertanyaan No. 20
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?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
- pembuatan dan penerapan target pengelolaan keamanan informasi - evaluasi pencapaian - pembuatan dan penerapan perbaikan - pelaporan status		A.17.1.3 *Verify, review and evaluate information security continuity* A.18.2.1 *Independent review of information security*
Justifikasi		
Klausul Kontrol A.17.1.3 *Verify, review and evaluate information security continuity* menjelaskan mengenai organisasi yang harus melakukan verifikasi kontrol kontinuitas keamanan informasi yang telah ditetapkan dan diimplementasikan secara berkala untuk memastikan bahwa ia valid dan efektif selama situasi yang tidak terduga. Klausul Kontrol A.18.2.1 *Independent review of information security* berbicara mengenai pendekatan organisasi untuk mengelola keamanan informasi dan implementasinya yang harus ditinjau secara independen pada interval yang telah direncanakan atau ketika perubahan signifikan terjadi		

IV	3	Pertanyaan No. 21
Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
Identifikasi legislasi, perangkat hukum dan standar		A.18.1.1 *Identification of applicable legislation and contractual requirements*
Justifikasi		
Klausul Kontrol A.18.1.1 *Identification of applicable legislation and contractual requirements* menjelaskan tentang peraturan perundang-undangan yang bersangkutan, peraturan, persyaratan kontrak dan pendekatan organisasi untuk memenuhi persyaratan harus diidentifikasi secara eksplisit, didokumentasikan dan diperbarui untuk setiap sistem informasi dan organisasi. Hal tersebut berhubungan dengan bagaimana instansi melakukan identifikasi terhadap legislasi, perangkat hukum atau standar lainnya yang terkait dengan keamanan nformasi.		

IV	3	Pertanyaan No. 22
Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?		
Poin Pertanyaan		Klausul ISO/IEC 27001:2013
- Kebijakan penanggulangan insiden keamanan informasi - Langkah penanggulangan insisden keamanan informasi		A.16.1.1 *Responsibilities and procedures* A.18.1.3 *Protection of records*
Justifikasi		
Klausul Kontrol A.16.1.1 berbicara mengenai tanggung jawab		

manajemen dan prosedur yang harus ditetapkan untuk memastikan tanggapan yang cepat, efektif dan teratur terhadap insiden keamanan informasi.
Klausul Kontrol A.18.1.3 berbicara mengenai rekaman atau apapun yang bersangkutan dengan kebijakan keamanan informasi harus terlindungi dari kehilangan, kerusakan, kesalahan, akses tidak berhak dan pengeluaran yang tidak benar, sesuai dengan persyaratan legislatif, peraturan, kontrak dan bisnis.
Hal tersebut mendukung poin pertanyaan bagaimana instansi melakukan langkah penanggulangan insiden dan kebijakannya yang menyangkut hokum

“Halaman ini sengaja dikosongkan”

LAMPIRAN B
Daftar Pertanyaan Wawancara dan Observasi/review dokumen Area Tata Kelola Keamanan Informasi

Tabel B.1 daftar pertanyaan wawancara dan observasi/review dokumen

<table>
<tr><td>II</td><td>1</td><td colspan="2">Pertanyaan no. 1</td></tr>
<tr><td colspan="4">Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?</td></tr>
<tr><td colspan="3">Wawancara</td><td>Observasi</td></tr>
<tr><td colspan="3">- Tanggung jawab pelaksanaan program keamanan informasi dan penetapan kebijakan
1. Apakah instansi mempunyai program keamanan informasi?
2. Apakah instansi mempunyai pernyataan komitmen manajemen?
3. Apakah instansi mempunyai prinsip tentang keamanan informasi?
4. Apakah instansi mempunyai strategi teknologi informasi?
5. Apakah instansi mempunyai kebijakan keamanan informasi?</td><td>1. Dokumen program keamanan informasi
2. Dokumen pernyataan komitmen manajemen
3. Dokumen prinsip keamanan informasi
4. Dokumen strategi teknologi informasi
5. Dokumen kebijakan keamanan informasi</td></tr>
</table>

<table>
<tr><td colspan="3">Keterangan</td></tr>
<tr><td colspan="3">- Contoh Program keamanan informasi dapat berisi persiapan rencana kerja (tujuan, ruang lingkup, tugas, anggaran, jadwal pelaksanaan), identifikasi aset, penilaian kekayaan, identifikasi ancaman, penilaian ancaman, dll.</td></tr>
<tr><td>II</td><td>1</td><td>Pertanyaan no. 2</td></tr>
<tr><td colspan="3">Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?</td></tr>
<tr><td colspan="2">Wawancara</td><td>Observasi</td></tr>
<tr><td colspan="2">Pembagian peran dan penanggung jawab
1. Bagaimanan alokasi tugas dan tanggung jawab keamanan informasi?
2. Apakah terdapat fungsi/bagian dari organisasi yang fokus terhadap pengelolaan keamanan informasi?
3. Apakah tugas dan tanggung jawab pengelolaan keamanan informasi dikomunikasikan dan dijelaskan kepada seluruh pihak dalam instansi?
4. Bagaimana cara instansi agar</td><td>1. Dokumen panduan dan alokasi tugas dan tanggung jawab keamanan informasi
2. Dokumen penjelasan dan definisi tanggung jawab dalam aset fisik, aset informasi dan proses pengamanan.
3. Dokumen tupoksi organisasi
4. Rekaman/catatan komunikasi tugas dan tanggung jawab pengelola keamanan informasi</td></tr>
</table>

<table>
<tr><td colspan="2">keamanan informasi tetap terjaga kepatuhannya?
5. Apakah cara tersebut dilaksanakan sampai sekarang?</td><td></td></tr>
<tr><td colspan="3">Keterangan</td></tr>
<tr><td colspan="3">- Pengelolaan keamanan informasi dapat berisi bagaimana mengelola keamanan informasi, penetapan ambang batas keamanan, mekanisme dan prosedur dan pengaturannya.</td></tr>
<tr><td>II</td><td>1</td><td>Pertanyaan no. 3</td></tr>
<tr><td colspan="3">Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?</td></tr>
<tr><td colspan="2">Wawancara</td><td>Observasi</td></tr>
<tr><td colspan="2">Pembagian tugas dan wewenang
1. Apakah instansi mempunyai pejabat/pelaksana pengamanan informasi?
2. Apakah instansi menetapkan setiap kewenangan pelaksana pengamanan informasi keamanan informasi dengan jelas?
3. Apakah terdapat kontrak atau perjanjian dari instansi yang</td><td>1. Tupoksi pelaksana pengamanan informasi
2. Dokumen definisi kewenangan pelaksana keamanan informasi
3. Kontrak/janji instansi untuk mengatur kewenangan pejabat/petugas pelaksana pengamanan informasi</td></tr>
</table>

mengatur kewenangan pejabat/petugas pelaksana pengamanan informasi? 4. Bagaimana cara pelaksana pengamanan informasi menerapkan keamanan informasi? 5. Bagaimana cara pelaksana pengamanan informasi menjamin kepatuhan keamanan informasi?	

Keterangan

- Kewenangan ditetapkan dengan penjelasan yang sesuai dengan keadaan instansi dan dimasukkan ke dalam dokumen kebijakan keamanan informasi atau dokumen SMKI keamanan informasi

II	1	Pertanyaan no. 4

Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?

Wawancara	Observasi
1. Apakah instansi menetapkan aturan untuk penggunaan sumber daya pengelolaan keamanan informasi? 2. Apakah	1. Aturan umum penggunaan sumber daya untuk pengelolaan keamanan informasi 2. Dokumen pembagian akses dan penggunaan akses

penanggung jawab diberikan akses yang sesuai dalam penggunaan sumber daya (seperti penggunaan internet dan komputer)? 3. Apakah terdapat kebijakan yang mengatur penggunaan sumber daya pengelolaan keamanan informasi? 4. Apakah penggunaan sumber daya dapat memastikan kinerja sistem yang efektif?	3. Log atau aktivitas penggunaan sumber daya dalam mengelola keamanan informasi 4. Dokumen kebijakan penggunaan sumber daya keamanan informasi 5. Log/aktivitas efektivitas penggunaan kinerja sistem dengan penggunaan sumber daya
Keterangan	
- Aturan-aturan sumber daya adalah aturan yang mengatur penggunaan sumber daya dan pemberdayaannya yang dibuat organisasi tertulis dalam dokumen keamanan informasi.	
II 1 Pertanyaan no. 5	
Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	
Wawancara	Observasi
1. Apakah setiap kebutuhan pelaksana pengamanan informasi dipetakan dan dijelaskan? 2. Apakah instansi sudah menentukan	1. Pemetaan keperluan pelaksana pengamanan informasi

audit internal? 3. Apakah instansi menjelakan setiap kebutuhan untuk audit internal? 4. Apakah instansi memiliki pemisahan dalam tugas dan tanggung jawab manajemen? 5. Apakah setiap pemisahan kewenangan memiliki definisi atau ketentuan tertentu? 6. Apakah terdapat persyaratan dalam membuat pemisahan kewenangan?	
Keterangan	
Persyaratan segregasi kewenangan dapat berisi persyaratan-persyaratan pada standar tertentu atau sesuai dengan keadaan instansi.	
II | 1 | Pertanyaan no. 6	
Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	
Wawancara	Observasi
1. Apakah instansi mempunyai persyaratan/standar kompetensi untuk pelaksana pengelolaan keamanan	1. Dokumen persyaratan/standar kompetensi pengelola keamanan informasi 2. Dokumen keahlian pengelola keamanan informasi

informasi? 2. Apakah instansi mempunyai keahlian khusus untuk pelaksana pengelolaan keamanan informasi? 3. Apakah keahlian dan persyaratan tersebut dicantumkan dalam definisi tertentu? 4. Apakah terdapat kebijakan/aturan khusus yang mengatur persyaratan/standar kompetensi pelaksana pengelolaan keamanan informasi?	
Keterangan	

II	1	Pertanyaan no. 7

Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?

Wawancara	Observasi
1. Apakah instansi memiliki persyaratan/standar untuk menentukan kompetensi dan keahlian karyawan? 2. Apakah persyaratan	1. Dokumen persyaratan/standar kompetensi dan keahlian

dan standar tersebut didefinisikan dan disesuaikan dengan keadaan yang terdapat pada instansi? 3. Apakah pelaksana memiliki minimal standar kompetensi dan keahlian? 4. Apakah persyaratan kompetensi dan keahlian telah diterapkan dalam kebijakan yang berlaku dalam instansi?	
Keterangan	

II	1	Pertanyaan no. 8

Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?

Wawancara	Observasi
1. Apakah instansi memiliki program khusus atau ajakan kepada karyawan atau pihak yang terlibat untuk peningkatan keamanan informasi? 2. Apakah instansi memiliki program khusus untuk	1. Dokumentasi kegiatan sosialisasi pemahaman keamanan informasi 2. Dokumen Program keamanan informasi

meningkatkan kepatuhan keamanan informasi? 3. Apakah terdapat pelatihan untuk karyawan mengenai pemahaman keamanan informasi? 4. Apakah terdapat pelatihan untuk pihak ketiga mengenai peningkatan pemahaman keamanan informasi?	
Keterangan	

II	2	Pertanyaan no. 9

Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?

Wawancara	Observasi
1. Apakah instansi mempunyai program untuk peningkatan kompetensi dan keahlian? 2. Apakah instansi memiliki penilaian terhadap kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	1. Dokumen program keamanan informasi 2. Dokumen kompetensi dan keahlian

3. Apakah program kompetensi dan keahlian dilaksanakan sesuai dengan kebijakan keamanan informasi instansi?		
Keterangan		
II	2	Pertanyaan no. 10
Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?		
Wawancara		Observasi
1. Apakah instansi memiliki proses kerja yang memerlukan keperluan/persyaratan keamanan informasi? 2. Apakah antara satu proses kerja dengan proses kerja lain telah melakukan integrasi keamanan informasi?		
Keterangan		
II	2	Pertanyaan no. 11
Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?		
Wawancara		Observasi
1. Apakah instansi memiliki data pribadi sesuai dengan peraturan		1. Dokumen identifikasi data pribadi 2. Dokumen pengamanan data

perundang-undangan yang berlaku? 2. Apakah instansi memiliki identifikasi data pribadi untuk proses kerja? 3. Apakah terdapat pengamanan untuk melindungi data pribadi? 4. Apakah pengamanan telah disesuaikan dengan undang-undang atau legislasi yang berlaku?	pribadi
Keterangan	

II	2	Pertanyaan no. 12

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?

Wawancara	Observasi
1. Apakah instansi memiliki pihak-pihak yang mengelola dan menggunakan aset informasi? 2. Apakah terdapat	1. Dokumen kontrak antara pengelola pihak internal dan eksternal

ketentuan/aturan setiap pihak yang terlibat dalam pengelolaan dan penggunaan aset informasi instansi? 3. Apakah terdapat kontrak atau perjanjian antara pihak yang menjamin keamanan informasi yang ada? 4. Apakah jika terdapat permasalahan yang berhubungan dengan pihak pengelola/pengguna informasi selalu dapat terselesaikan?	
Keterangan	

II	2	Pertanyaan no. 13

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?

Wawancara	Observasi
1. Apakah instansi melakukan koordinasi dengan pihak satuan terkait ? 2. Bagaimana menjaga koordinasi dengan satuan terkait mengenai keamanan	1. Dokumen koordinasi dan kontrak antara pihak pengelola keamanan informasi dengan satuan terkait

informasi? 3. Apakah koordinasi dilakukan ketika terjadi permasalahan atau dilakukan secara rutin? 4. Apakah pada koordinasi terdapat pembatasan informasi yang disampaikan kepada pihak terkait?	
Keterangan	

III	2	Pertanyaan no. 14

Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?

Wawancara	Observasi
1. Apakah instansi mempunyai atau sedang merancang keberlangsungan layanan TIK? 2. Apakah instansi merancang dokumen keberlangsungan layanan TIK berdasarkan aset yang ada? 3. Apakah instansi telah membuat tim kelangsungan layanan? 4. Apakah tim tersebut telah didefinisikan dan dibagi dalam	1. Dokumen kelangsungan layanan TIK

bagian-bagian tertentu?	
Keterangan	

III	2	Pertanyaan no. 15

Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?

Wawancara	Observasi
1. Apakah terdapat prosedur untuk melaporkan kondisi keamanan informasi pada instansi? 2. Apakah terdapat kondisi tertentu untuk melakukan pelaporan? 3. Apakah laporan dilakukan secara rutin atau resmi?	1. Prosedur pelaporan kondisi, kinerja/efektivitas dan kepatuhan program keamanan informasi 2. Log atau dokumen laporan kondisi keamanan informasi
Keterangan	

III	2	Pertanyaan no. 16

Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?

Wawancara	Observasi
1. Apakah instansi pernah mempunyai permasalahan	1. Catatan kondisi dan permasalahan keamanan informasi

keamanan informasi? 2. Apakah instansi melakukan klasifikasi terhadap kondisi dan permasalahan keamanan informasi? 3. Apakah permasalahan yang terjadi, dilakukan review dan dilakukan evaluasi?	2. Dokumen Pengambilan keputusan berdasarkan permasalahan keamanan informasi
Keterangan	
- Jika kondisi dan permasalahan keamanan informasi menjadi konsideran, maka ia menjadi bagian pertimbangan yang akan dijadikan sebagai penetapan keputusan dan aturan. - Jika kondisi dan permasalahan keamanan informasi menjadi proses keputusan strategis, maka ia menjadi salah satu hasil evaluasi.	
IV | 3 | Pertanyaan no. 17	
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?	
Wawancara	Observasi
1. Apakah instansi mempunyai sasaran/tujuan terhadap kepatuhan pengamanan informasi?	1. Dokumen program khusus mengenai kepatuhan tujuan dan sasaran pengamanan informasi

2. Apakah instansi memiliki ajakan atau program khusus untuk membantu mematuhi tujuan/sasaran kepatuhan pengamanan informasi?	
Keterangan	

IV	3	Pertanyaan no. 18

Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?

Wawancara	Observasi
1. Apakah instansi mempunyai pengukuran kinerja pengelolaan keamanan informasi? 2. Apakah pengukuran kinerja dibuat dengan mendefinisikan metriks dan parameter? 3. Apakah instansi menetapkan mekanisme pengukuran kinerja? 4. Apakah instansi mendefinisikan waktu pengukuran dan pelaksananya?	1. Dokumen pengukuran kinerja

Keterangan		
IV	3	Pertanyaan no. 19
Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?		
Wawancara		Observasi
1. Apakah instansi memiliki program penilaian kinerja pengelolaan keamanan informasi? 2. Apakah program tersebut pernah dilaksanakan?		1. Dokumen program penilaian kinerja
Keterangan		
IV	3	Pertanyaan no. 20
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?		
Wawancara		Observasi
1. Apakah instansi mempunyai sasaran/target yang ingin dicapai di setiap area? 2. Apakah sasaran tersebut mempunyai kriteria penilaian? 3. Apakah instansi sudah melaksanakan		1. Sasaran/target pengelolaan keamanan informasi 2. Log aktivitas yang mendukung sasaran/target pengelolaan keamanan informasi 3. Penilaian sasaran/target

kegiatan yang mendukung tercapainya sasaran? 4. Apakah instansi melakukan evaluasi dari penerapan kegiatan bersserta sasaran yang dibuat? 5. Apakah instansi melakukan perbaikan pada sasaran yang telah dilakukan evaluasi? 6. Apakah instansi pernah melakukan pelaporan status setelah melakukan perbaikan?	pengelolaan keamanan informasi
Keterangan	
- Area pada bagian ini adalah lingkungan yang memiliki aset fisik/informasi dan/atau proses informasi di dalamnya.	
IV | 3 | Pertanyaan no. 21	
Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	
Wawancara	Observasi
1. Apakah instansi mempunyai perangkat hukum atau standar yang mengatur keamanan informasi di dalamnya? 2. Apakah instansi pernah melakukan	1. Dokumen kepatuhan terhadap standar dan perangkat hukum.

identifikasi pada legislasi yang dipatuhi oleh instansi? 3. Apakah instansi memperbarui seluruh legislasi yang dipatuhi secara rutin?	
Keterangan	

IV	3	Pertanyaan no. 22

Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?

Wawancara	Observasi
- Langkah penanggulangan insiden 1. Apakah instansi mempunyai dokumen penanggulangan insiden? 2. Apakah di dalam dokumen terdapat isitilah atau definisi-definisi tertentu? 3. Apakah instansi memiliki prosedur mengenai penanggulangan insiden? - Kebijakan penanggulangan insiden 1. Apakah instansi memiliki kebijakan yang menyangkut	1. Dokumen penanggulangan insiden 2. Prosedur penanggulangan insiden 3. Kebijakan penanggulangan insiden

insiden dan penangannya? 2. Apakah penanganan insiden didefinisikan dan terhubung dengan aturan hukum (misal: UU ITE)?	
Keterangan	

LAMPIRAN C
Perangkat Evaluasi Area Tata Keamanan Informasi pada Indeks KAMI

Tabel C.1 dafar pertanyaan Indeks KAMI area Tata Kelola Keamanan Informasi

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**	Skor
#	**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	0
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	0

2,3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Tidak Dilakukan	0
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	0
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	0
2,6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan	Tidak Dilakukan	0

			keahlian pelaksana pengelolaan keamanan informasi?		
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	0
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	0
2,9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan	0
2.10	II	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja	Tidak Dilakukan	0

			yang ada?		
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	0
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	0
2.13	II	2	Apakah pengelola keamanan informasi secara proaktif	Tidak Dilakukan	0

			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?		
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	0
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi	Tidak Dilakukan	0

			kepada pimpinan Instansi secara rutin dan resmi?		
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	0
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	0
2.18	IV	3	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi	Tidak Dilakukan	0

			pelaporannya?		
2.19	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	Tidak Dilakukan	0
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	0
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	0

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	0
			Total Nilai Evaluasi Tata Kelola	**0**	

LAMPIRAN D
Hasil pengumpulan data berdasarkan wawancara

Lampiran berisikan hasil wawancara terkait kondisi kekinian pada Unit LPSE. Berikut adalah hasilnya:

Nama :	Indah Isti'anah
Jabatan :	Kepala LPSE
Waktu :	09.00 – selesai
Tanggal :	28 Mei 2018
Tempat :	Kantor LPSE

Tabel D.1 hasil wawancara

II	1	Pertanyaan No. 1
Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?		
Poin Pertanyaan : komitmen manajemen		
1.	**Pertanyaan :** Apakah instansi mempunyai pernyataan komitmen manajemen?	
Jawaban : UPT memiliki pernyataan komitmen agar keamanan informasi dan penyediaan layanan tetap terjaga. Pernyataan komitmen manajemen dibuat sesuai dengan pernyataan LKPP dan diskominfo, karena LPSE dibawah pengawasan LKPP dan berada pada bagian diskominfo. Dalam UPT LPSE, pernyataan komitmen juga bisa disebut sebagai kebijakan layanan dan kebijakan keamanan informasi		
2.	**Pertanyaan :** Apakah instansi secara prinsip melaksanakan keamanan informasi?	
Jawaban : secara prinsip, UPT melaksanakan keamanan informasi berdasarkan tiga aspek keamanan informasi, yaitu sesuai dengan CIA (*confidentiality, integrity, availability*).		

3.	**Pertanyaan :** Apakah instansi mempunyai strategi teknologi informasi?
Jawaban : Diskominfo sedang membangun dokumen strategi teknologi informasi dan di dalamnya juga terdapat strategi milik UPT LPSE. Jadi untuk sekarang, UPT belum memiliki dokumen strategi teknologi informasi yang digunakan.	
Poin Pertanyaan : Tanggung jawab pelaksanaan keamanan informasi	
4.	**Pertanyaan :** Apakah instansi mempunyai program keamanan informasi?
Jawaban : untuk program, UPT telah melakukan identifikasi pada aset dan risiko, serta pembagian tugas dan tanggung jawab untuk mencegah jika terjadi sesuatu. Jadi UPT baru melakukan tugas dan tanggung jawab yang diberikan kepada kami.	
5.	**Pertanyaan :** Apakah instansi mempunyai kebijakan keamanan informasi?
Jawaban : Instansi memiliki kebijakan keamanan informasi, yang dibuat memang khusus untuk keamanan informasi pada LPSE	
II	1	Pertanyaan No. 2
Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?		
Poin Pertanyaan : tugas dan tanggung jawab pengelola keamanan informasi		
1.	**Pertanyaan :** Bagaimanan alokasi tugas dan tanggung jawab keamanan informasi?
Jawaban : alokasi tugas dan tanggung jawab dibuat berdasarkan standar pada LPSE pusat dan secara umum berdasarkan pada peraturan bupati mengenai UPT daerah. Sedangkan untuk	

keamanan informasi, mengikuti seperti layaknya tugas dan tanggung jawab layanan. Yang membedakan adalah pada proses layanan diganti dengan keamanan informasi.	
2.	**Pertanyaan :** Apakah terdapat fungsi/bagian dari organisasi yang fokus terhadap pengelolaan keamanan informasi?
Jawaban : di dalam UPT LPSE sendiri, memiliki satu fungsi/bagian yang mengurus seluruh teknis teknologi informasi. Termasuk mengelola keamanan informasi yang ada pada LPSE sendiri. Bagian tersebut bernama Administrasi Sistem Elektronik. Selain dari masalah teknis, bagian tersebut yang berhak memberikan hak akses seperti pada server atau sistem lainnya serta menjaga/memelihara sistem pada UPT LPSE.	
3.	**Pertanyaan :** Apakah tugas dan tanggung jawab pengelolaan keamanan informasi dikomunikasikan dan dijelaskan kepada seluruh pihak dalam instansi?
Jawaban : tugas dan tanggung jawab harus dikomunikasikan dan dijelaskan kepada seluruh instansi karena berhubungan dengan peraturan bupati yang mengatur Unit Pelaksana Teknis Daerah.	
4.	**Pertanyaan :** Bagaimana cara instansi agar keamanan informasi tetap terjaga kepatuhannya?
Jawaban : Setiap kali mengakses server, harus ada bagian dari administrasi sistem elektronik sebagai pemberi hak akses menemani orang tersebut. Kemudian adanya perjanjian pada setiap staff bahwa akan menjaga kerahasiaan segala informasi pada LPSE. Selain itu juga terdapat aturan mengenai penggunaan password.	
5.	**Pertanyaan :** Apakah cara tersebut dilaksanakan sampai sekarang?
Jawaban : Ya, tentu daja. Kontrak perjanjian masih berlaku. Begitu pula	

dengan prosedur akses ruang server dan penggunaan fasilitas pada LPSE. Dan sampai sekarang, permasalahan mengenai keamanan informasi		
II	1	Pertanyaan No. 3
Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?		
Poin Pertanyaan : Pembagian tugas dan tanggung jawab		
1.	**Pertanyaan :** Apakah instansi mempunyai pejabat/pelaksana pengamanan informasi?	
Jawaban : Punya, tetapi pejabat/pelaksana pengamanan ini adalah bagian dari administrasi sistem elektronik. Jadi bagian administrasi sistem elektronik juga menjabat sebagai pelaksana pengamanan informasi.		
2.	**Pertanyaan :** Apakah instansi menetapkan setiap kewenangan pelaksana pengamanan informasi keamanan informasi dengan jelas?	
Jawaban : Penetapan kewenangan pelaksana pengamanan informasi ditulis sesuai dengan tugas dan fungsi dari bagian tersebut. Jadi untuk lebih detail mengenai kewenangan yang dimiliki oleh pengaman informasi belum ditulis secara detail. Hanya masih beberapa bagian saja. Seperti kewenangan terhadap akses kontrol.		
3.	**Pertanyaan :** Apakah terdapat kontrak atau perjanjian dari instansi yang mengatur kewenangan pejabat/petugas pelaksana pengamanan informasi?	
Jawaban : Kalau kontrak mengenai pelaksana pengamanan informasi, saat ini terdapat perjanjian yang menerangkan tentang kewenangan hak akses untuk server LPSE. Sedangkan kewenangan yang lain tidak tertulis seperti kontrak atau perjanjian.		

4.	**Pertanyaan :** Bagaimana cara pelaksana pengamanan informasi menerapkan keamanan informasi?
Jawaban : Pelaksana pengamanan informasi selalu mencatat siapa saja yang menggunakan hak akses pada sistem ataupun ruang server, membuat prosedur penggunaan fasilitas maupun mengawasi dan mencatat seluruh fasilitas seperti membuat log penggunaan fasilitas dan akses sistem/server.	
5.	**Pertanyaan :** Bagaimana cara pelaksana pengamanan informasi menjamin kepatuhan keamanan informasi?
Jawaban : Penanggung jawab melakukan perjanjian agar kewenangan tidak dilakukan semena-mena. Selain itu, si penanggung jawab juga selalu menulis log kondisi LPSE dan mengawasi fasilitas yang mungkin dapat menyebabkan kebocoran data atau adanya aktivitas aneh, seperti hak akses yang tidak diizinkan. Contohnya adalah ia selalu memfoto kondisi ruang server, membuat log kondisi pada sistem.	
II	1 Pertanyaan No. 4
Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	
Poin Pertanyaan : Alokasi sumber daya	
1.	**Pertanyaan :** Apakah instansi menetapkan aturan untuk penggunaan sumber daya pengelolaan keamanan informasi?
Jawaban : Sebenarnya penggunaan sumber daya berdasarkan kebutuhan yang ada pada instansi. Jadi, LPSE melakukan identifikasi terhadap sumber daya terlebih dahulu. Kemudian membuat rancangan utilisasi sumber daya dan perkiraan kebutuhan sumber daya sampai tahun depan. Untuk aturan sendiri, LPSE tidak mempunyai aturan khusus yang menerangkan tentang sumber daya, tetapi LPSE memiliki panduan dari LKPP yang	

memberi arahan mengenai bagaimana membuat dokumen pengelolaan kapasitas dan harus diisi seperti apa saja.	
2.	**Pertanyaan :** Apakah penanggung jawab diberikan akses yang sesuai dalam penggunaan sumber daya?
Jawaban : Tentu saja kami harus memberikan akses atau kebutuhan yang sesuai dengan sumber daya yang diinginkan. Seperti pada sistem, kebutuhan apa saja di dalamnya. Butuh harddisk berapa. Kemudian pada bagian trainer, harus membu	
3.	**Pertanyaan :** Apakah terdapat kebijakan yang mengatur penggunaan sumber daya pengelolaan keamanan informasi?
Jawaban : Kami tidak mempunyai kebijakan khusus yang mengatur penggunaan sumber daya, tapi LPSE hanya mempunyai pedoman dari LKPP dan panduan bagaimana LPSE harus membuat dan bagimana mengelola sumber daya yang ada pada unit kami.	
4.	**Pertanyaan :** Apakah penggunaan sumber daya dapat memastikan kinerja sistem yang efektif?
Jawaban : Penggunaan sumber daya dibuat berdasarkan kebutuhan yang ada pada LPSE. Sedangkan untuk memastikan sistem atau proses pada LPSE telah efektif, perlu adanya evaluasi setelah kapasitas telah berjalan.	
II	1 Pertanyaan No. 5
Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	
Poin Pertanyaan : Pemetaan keperluan peran pelaksana pengamanan informasi	
1.	**Pertanyaan :** Apakah setiap kebutuhan pelaksana pengamanan informasi dipetakan dan dijelaskan?

Jawaban : Belum terdapat pemetaan kebutuhan secara detail untuk setiap bagian		
Poin Pertanyaan : Kebutuhan audit internal		
2.	**Pertanyaan :** Apakah instansi sudah menentukan audit internal?	
Jawaban : Untuk saat ini, LPSE belum menentukan kebutuhan audit internal.		
3.	**Pertanyaan :** Apakah instansi menjelakan setiap kebutuhan untuk audit internal?	
Jawaban : LPSE belum menjelaskan setiap kebutuhan untuk audit internal.		
Poin Pertanyaan : persyaratan segregasi kewenangan		
4.	**Pertanyaan :** Apakah instansi memiliki pemisahan dalam tugas dan tanggung jawab manajemen?	
Jawaban : LPSE tentu saja memisahkan setiap tugas dan tanggung jawab manajemen. Tetapi, jika mengenai kewenangan, LPSE belum memiliki kewenangan yang jelas.		
5.	**Pertanyaan :** Apakah setiap pemisahan kewenangan memiliki definisi atau ketentuan tertentu?	
Jawaban : Tidak ada ketentuan atau definisi khusus dalam membuat kewenangan. Hanya perjanjian yang memang dibuat sendiri oleh LPSE.		
6.	Apakah terdapat persyaratan dalam pemisahan kewenangan?	
Jawaban : Tidak terdapat persyaratan tertentu, hanya dihubungkan dengan tugas dan tanggung jawab yang ada, kemudian dilakukan pembagian kewenangan.		
II	1	Pertanyaan No. 6

Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	
Poin Pertanyaan : definisi syarat/standar kompetensi dan keahlian	
1.	**Pertanyaan :** Apakah instansi mempunyai persyaratan/standar kompetensi untuk pelaksana pengelolaan keamanan informasi?
Jawaban : Iya. LPSE mempunyai persyaratan dan standar kompetensi yang harus dipenuhi. Dalam pengelolaan keamanan informasi, LPSE harus memenuhi standar minimal yang dikeluarkan LKPP.	
2.	Apakah instansi mempunyai keahlian khusus untuk pelaksana pengelolaan keamanan informasi?
Jawaban : Tentu saja setiap bagian dalam LPSE harus memiliki keahlian khusus, agar dapat unit dengan baik dan benar. Tetapi untuk saat ini, LPSE masih fokus pada keahlian khusus layanan.	
3.	Apakah keahlian dan persyaratan tersebut dicantumkan dalam definisi tertentu?
Jawaban : Mungkin adanya definisi sekarang yang ada, seperti dalam dokumen sedang mencapai tingkat apa. Jika dalam layanan sekarang misal ada keahlian IT service management, ditulis IT servicenya masih dalam tingkat apa, kemudian bagaimana mencapai tingkat selanjutnya. Jadi, mungkin tidak ada definisi khusus tertentu. Kan dibilang bahwa keahlian berdasarkan apa yang dibutuhkan di LPSE sekarang.	
4.	Apakah terdapat kebijakan/aturan khusus yang mengatur persyaratan/standar kompetensi pelaksana pengelolaan keamanan informasi?
Jawaban : Tidak ada kebijakan khusus atau aturan khusus yang mengatur persyaratan/standar kompetensi dan dari LKPP hanya memberikan standarisasi berupa, bahwa LPSE harus	

mempunyai keahlian kompetensi berdasarkan kebutuhan dan diidentifikasi.		
II	1	Pertanyaan No. 7
Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?		
Poin Pertanyaan : kompetensi dan keahlian pelaksana pengamanan informasi		
1.	Apakah instansi memiliki persyaratan/standar untuk menentukan kompetensi dan keahlian karyawan?	
Jawaban : LPSE pasti memiliki standar untuk menentukan kompetensi yang harus ditempuh. Karena kami harus menggunakan standar berdasarkan LKPP, maka seluruh panduan mengenai standar kompetensi dibuat berdasarkan LKPP. Tetapi identifikasi tetapi tergantung pada unit yang ada pada LPSE sendiri.		
2.	Apakah persyaratan dan standar tersebut didefinisikan dan disesuaikan dengan keadaan yang terdapat pada instansi?	
Jawaban : Ya, persyaratan memang didefinisikan dan diidentifikasi sesuai dengan kebutuhan yang ada dalam instansi. Misal sekarang setiap bagian memiliki kompetensi *beginner*, mempunyai target menjadi *advanced*, maka yang harus dilakukan adalah bagaimana membuat setiap bagian berkembang, yaitu salah satu contohnya melakukan pelatihan. Kemudian kapan pelatihan dan hasilnya apa. Setiap hal tersebut didefinisikan atau dijelaskan agar tahu perkembangannya.		
3.	Apakah pelaksana memiliki minimal standar kompetensi dan keahlian?	
Jawaban : Ya, setiap bagian dan personal memiliki minimal satu kompetensi. Setiap keahlian atau kompetensi selalu dibuat sasaran agar dapat berkembang dan menjadi lebih mahir.		
4.	Apakah persyaratan kompetensi dan keahlian telah	

	diterapkan dalam kebijakan yang berlaku dalam instansi?
Jawaban : Belum, kompetensi dan keahlian belum memiliki aturan atau kebijakan yang mendukung agar dilaksanakan tepat waktu. Jadi sekarang masih membuat matriks kompetensi yang berisikan penjelasan mengenai keahlian dan kompetensi yang dimiliki oleh setiap bagian dan personal/staff LPSE.	
II	1 Pertanyaan No. 8
Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	
Poin Pertanyaan : sosialisasi pemahaman keamanan informasi	
1.	Apakah instansi memiliki program khusus atau ajakan kepada karyawan atau pihak yang terlibat untuk peningkatan keamanan informasi?
Jawaban : Ada ajakan. Seperti cara pergantian dan pembuatan *password*, ajakan agar selalu menjaga informasi karena peretas dapat mengintai, ajakan bahwa informasi yang ada adalah bersifat rahasia, jadi harus dilindungi dengan benar.	
2.	Apakah terdapat pelatihan untuk karyawan mengenai pemahaman keamanan informasi?
Jawaban : Untuk saat ini, pelatihan khusus untuk keamanan informasi belum ada. Masih berfokus pada pelatihan pengelolaan layanan.	
3.	Apakah terdapat pelatihan untuk pihak ketiga mengenai peningkatan pemahaman keamanan informasi?
Jawaban : Ya, untuk pengguna sistem LPSE, terdapat pelatihan sendiri bagaimana mengakses sistem dengan baik dan benar. Jadi bukan hanya bagaimana melakukan pengadaan, tetapi juga berbicara mengenai informasi harus dijaga, kemudian penggunaan akses sistem LPSE tidak boleh disalahgunakan.	

Poin Pertanyaan : sosialisasi kepentingan kepatuhan keamanan informasi		
4.	Apakah instansi memiliki program khusus untuk meningkatkan kepatuhan keamanan informasi?	
Jawaban : Untuk program khusus belum ada, tetapi saat ini mulai dilakukan pengelolaan pasword agar informasi tetap terjaga. Selain itu, terdapat prosedur khusus untuk akses ke dalam server. Hal tersebut dapat menambah peningkatan kepatuhan terhadap keamanan informasi pada LPSE.		
II	2	Pertanyaan No. 9
Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?		
Poin Pertanyaan : penerapan program peningkatan kompetensi dan keahlian pelaksana pengelolaan keamanan informasi		
1.	Apakah instansi mempunyai program untuk peningkatan kompetensi dan keahlian?	
Jawaban : Iya, tentu saja LPSE ada program untuk meningkatkan kompetensi para staff bidang. Program peningkatan biasanya dilakukan dengan pelatihan.		
2.	Apakah instansi memiliki penilaian terhadap kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	
Jawaban : LPSE belum membuat penilaian terhadap peningkatan kompetensi. Tetapi, jika sudah melakukan pelatihan dapat disimpulkan bahwa staff tersebut telah mengalami peningkatan kompetensi dan keahlian.		
3.	Apakah program kompetensi dan keahlian dilaksanakan sesuai dengan kebijakan keamanan informasi instansi?	
Jawaban : Iya, disesuaikan dengan pemenuhan kebijakan keamanan informasi. Selain itu, juga disesuaikan dengan fungsi dan tugas yang ada pada LPSE.		

II	2	Pertanyaan No. 10
Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?		
Poin Pertanyaan : integrasi keperluan/persyaratan keamanan informasi pada proses kerja		
1.	Apakah instansi memiliki proses kerja yang memerlukan keperluan/persyaratan keamanan informasi?	
Jawaban : Iya, LPSE pasti memerlukan keperluan keamanan informasi. Karena proses kerja pada LPSE adalah melakukan layanan secara elektronik. Jadi,secara umum proses kerja sudah menggambarkan hal yang dilakukan secara digital. Maka dari itu persyaratan keamanan informasi harus ada.		
2.	Proses kerja apa saja yang membutuhkan persyaratan keamanan informasi?	
Jawaban : Mungkin proses kerja seperti pengadaan barang pada sistem LPSE. Transaksi pengadaan dan nilai uang pada sistem LPSE. Kegiatan itu yang paling penting yang harus terdapat pemenuhan persyaratan keamanan informasinya.		
3.	Apakah antara satu proses kerja dengan proses kerja lain telah melakukan integrasi keamanan informasi?	
Jawaban : Untuk sistem LPSE, sudah terintegrasi dengan LPSE pusat. Tetapi untuk proses kerja lain, seperti laporan kepada pimpinan instansi atau hal-hal lain masih menggunakan manual. Jadi integrasi persyaratan keamanan informasinya masih renatan dan tidak selalu terpenuhi.		
II	2	Pertanyaan No. 11
Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?		
Poin Pertanyaan : informasi data pribadi		

1.	Apakah instansi memiliki data pribadi sesuai dengan peraturan perundang-undangan yang berlaku?
Jawaban : Instansi memiliki data pribadi, tetapi data tersebut belum dihubungkan dengan undang-undang yang ada. Karena LPSE tidak terlalu banyak memerlukan data pribadi. Hanya data secara umum. Seperti informasi yang digunakan pada BKN.	
2.	Apakah instansi memiliki identifikasi data pribadi untuk proses kerja?
Jawaban : Untuk keperluan LPSE sendiri, LPSE belum mengidentifikasi data pribadi apa saja yang dibutuhkan untuk mempermudah proses kerja.	
3.	Apakah terdapat pengamanan untuk melindungi data pribadi?
Jawaban : Tentu saja terdapat keamanan yang melindungi data pribadi. Pengamanan dimulai dari login pada sistem LPSE. Jika untuk mengakses server, pertama sebelum memasuki ruangan dilakukan scan finger, lalu jika ingin masuk ruang server, harus ditemani oleh bagian yang berhak atas seluruh akses server, kemudian memasukkan login pada sistem.	
4.	Apakah pengamanan telah disesuaikan dengan undang-undang atau legislasi yang berlaku?
Jawaban : Seharusnya sesuai dengan undang-undang. Karena keamanan dibuat berdasarkan standar pada LKPP. Dimana standar tersebut menganut standar internasional.	
II	2	Pertanyaan No. 12
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?	

Poin Pertanyaan : Tanggung jawab koordinasi dengan pihak pengelola/pengguna aset informasi	
1.	Apakah instansi memiliki pihak-pihak yang mengelola dan menggunakan aset informasi?
Jawaban : LPSE memiliki pihak-pihak pengguna aset informasi pada LPSE sendiri. Seperti pengguna website pada LPSE, para penyedia pengadaan barang/jasa.	
2.	Apakah terdapat ketentuan/aturan setiap pihak yang terlibat dalam pengelolaan dan penggunaan aset informasi instansi?
Jawaban : Ada aturan, tetapi aturan tersebut bukan mengeatur khusus untuk pengelola aset informasi. Tetapi terdapat aturan yang menjelaskan bagaimana melakukan pengadaan barang secara elektronik. Jadi, untuk saat ini, LPSE belum menentukan atuan atau ketentuan tentang pengelolaan aset informasi.	
3.	Apakah terdapat kontrak atau perjanjian antara pihak yang menjamin keamanan informasi yang ada?
Jawaban : Tidak ada aturan khusus maupun perjanjian jika ingin menggunakan aset informasi atau sistem pada LPSE. Hanya sedikit memberikan data diri secukupnya dan dapat langsung masuk dalam sistem LPSE. Jika berhubungan dengan penyediaan barang/jasa baru ada aturan sendiri.	
4.	Apakah jika terdapat permasalahan yang berhubungan dengan pihak pengelola/pengguna informasi selalu dapat terselesaikan?
Jawaban : Untuk saat ini, semua permasalahan masih dapat ditangani. Karena permasalahan yang ditangani sering kali hampir sama, jadi masalah dapat diatasi.	
II	2	Pertanyaan No. 13
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?	
Poin Pertanyaan : Koordinasi untuk penerapan dan jaminan kepatuhan pengamanan informasi dengan berbagai pihak	
1.	Apakah instansi melakukan koordinasi dengan pihak satuan terkait ?
Jawaban : Tentu aja LPSE melakukan koordinasi dengan pihak satuan tertentu. LPSE merupakan satuan unit yang berada pada salah satu bagian dalam dinas Kominfo, selain itu LPSE tetap bertanggung jawab untuk LPSE pusat dan LPSE juga diawasi oleh LKPP karena sebagai lembaga yang mengurusi standarisasi dan kebijakan untuk unit LPSE.	
2.	Bagaimana menjaga koordinasi dengan satuan terkait mengenai keamanan informasi?
Jawaban : LPSE melakukan koordinasi dengan berbagai pihak. Seperti koordinasi dengan LPSE pusat, melakukan pelaporan mengenai pengadaan apa yang ada. Kemudian siapa saja penyedianya, dan melakukan evaluasi. Begitu pula dengan LKPP, seperti pelaporan dan tanggung jawab terhadap terlaksananya kepatuhan standar yang dibuat oleh LKPP.	
3.	Apakah koordinasi dilakukan ketika terjadi permasalahan atau dilakukan secara rutin?
Jawaban : Untuk saat ini, koordinasi sebenarnya dilakukan hampir sering dilakukan. Tetapi juga tidak dilakukan secara rutin. Koordinasi paling sering dilakukan dengan LKPP. Karena agar LPSE terstandarisasi, LPSE sering berkomunikasi dengan LKPP, untuk menentukan apakah LPSE telah memenuhi standar atau belum.	
4.	Apakah pada koordinasi terdapat pembatasan informasi yang disampaikan kepada pihak terkait?
Jawaban : Ada, biasanya informasi yang bersifat pengadaan dilaporkan kepada LPSE pusat. Tetapi laporan yang bersifat internal,	

contohnya server tidak perlu dilaporkan kepada LPSE pusat. Hanya untuk pihak internal saja.		
III	2	Pertanyaan No. 14
Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?		
Poin Pertanyaan : Definisi dan alokasi tanggung jawab keberlangsungan layanan TIK		
1.	Apakah instansi mempunyai atau sedang merancang keberlangsungan layanan TIK?	
Jawaban : Iya, sebenarnya LPSE sudah ada SOP kelangsungan layanan, tapi jika diingat-ingat lagi, sepertinya LPSE belum memiliki dokumen kelangsungan layanan TIK.		
2.	Apakah instansi merancang dokumen keberlangsungan layanan TIK berdasarkan aset yang ada?	
Jawaban : Dokumen TIK belum ada, jadi belum mengerti apakah nanti berdasarkan aset yang ada atau dari risiko keamanan informasi pada LPSE.		
3.	Apakah instansi telah membuat tim kelangsungan layanan?	
Jawaban : Untuk saat ini, LPSE sedang merancang tim yang akan membuat dokumen kelangsungan layanan.		
4.	Apakah tim tersebut telah didefinisikan dan dibagi dalam bagian-bagian tertentu?	
Jawaban : Tentu saja belum ada tim dan pembagian tim yang membuat atau merancang dokumen layanan TIK. Saat ini sudah ada tugas dan tanggung jawab bagi pengelola kelangsungan layanan, tetapi belum dibuat dan dibagi ke dalam tim-tim.		
III	2	Pertanyaan No. 15
Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan		

kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	
Poin Pertanyaan : pelaporan kondisi, kinerja/efektivitas dan kepatuhan program keamanan informasi	
1.	Apakah instansi pernah melakukan pelaporan kondisi terkait keamanan informasi?
Jawaban : Iya, LPSE pasti pernah melakukan pelaporan kondisi. Laporan terkait segala kondisi. Mulai dari layanan maupun sampai dengan keamanan informasi. Contoh pelaporannya seperti, kondisi sistem LPSE, pelaporan ruang server.	
2.	Apakah terdapat prosedur untuk melaporkan kondisi keamanan informasi pada instansi?
Jawaban : Untuk pelaporan sendiri, tidak terdapat prosedur khusus. Hanya langsung dapat melaporkan ke kepala LPSE tanpa ada alur sulit.	
3.	Apakah terdapat kondisi tertentu untuk melakukan pelaporan?
Jawaban : Sebenarnya tidak ada kondisi tertentu. Baik sistem dan server dalam keadaan normal ataupun sedanga dalam masalah harus dilakukan pelaporan. Tapi, biasanya lebih sering membuat laporan jika ada masalah dalam sistem.	
4.	Apakah laporan dilakukan secara rutin atau resmi?
Jawaban : Pelaporan dapat dilakukan secara rutin, biasanya dilakukan dua minggu atau sebulan sekali. Mungkin juga tidak terlalu rutin. Seharusnya dilakukan secara resmi, tetapi jika laporan terhadap kepala LPSE belum dilakukan pembukuan. Hanya laporan bahwa sistem aman, kondisi server aman.	
III	2 Pertanyaan No. 16
Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	
Poin Pertanyaan : Proses pengambilan keputusan untuk kondisi dan permasalahan keamanan informasi	

1.	Apakah instansi pernah mempunyai permasalahan keamanan informasi?
Jawaban : Tentu saja LPSE pernah mengalami permasalahan keamanan informasi. Seperti sistem LPSE yang pernah ke-*hack* atau database tidak dapat diakses.	
2.	Apakah instansi melakukan klasifikasi terhadap kondisi dan permasalahan keamanan informasi?
Jawaban : Ya, LPSE melakukan klasifikasi kondisi dan permasalahan. Kemudian hasil klasifikasi dimasukkan ke dalam daftar risiko dan pengelolaan risiko.	
3.	Apakah permasalahan yang terjadi, dilakukan review dan dilakukan evaluasi?
Jawaban : Biasanya kalau permasalahan megenai layanan, pasti dilakukan review, apa penyebabnya, solusinya bagaimana. Jadi ya, pasti ada review dan evaluasi perbaikan. Apalagi untuk sistem LPSE.	
4.	Apakah instansi membuat keamanan informasi menjadi bagian dari pengambilan strategis atau sebuah konsideran?
Jawaban : Untuk saat ini, keamanan informasi dapat membantu mengambil keputusan dalam LPSE. Seperti dapat membantu efektivitas sistem.	
IV	3	Pertanyaan No. 17
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?		
Poin Pertanyaan : Program kepatuhan pengamanan informasi pada aset informasi		
1.	Apakah instansi mempunyai sasaran/tujuan terhadap kepatuhan pengamanan informasi?
Jawaban :	

LPSE belum memiliki sasaran/tujuan terhadap kepatuhan pengamanan informasi.	
2.	Apakah instansi memiliki ajakan atau program khusus untuk membantu mematuhi tujuan/sasaran kepatuhan pengamanan informasi?
Jawaban : Sebenarnya, ajakan untuk mematuhi kepatuhan pengamanan informasi dilakukan seperti adanya pelatihan, pasti kesadaran akan keamanan informasi meningkat. Untuk saat ini juga diberlakukan bahwa jika ingin mengakses ruang server, harus izin dulu kepada bagian administrasi sistem elektronik.	
IV	3	Pertanyaan No. 18
Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	
Poin Pertanyaan : Pengukuran kinerja pengelolaan keamanan informasi	
1.	Apakah instansi mempunyai pengukuran kinerja pengelolaan keamanan informasi?
Jawaban : LPSE belum mempunyai dokumen pengukuran kinerja untuk pengelolaan keamanan informasi.	
2.	Apakah pengukuran kinerja dibuat dengan mendefinisikan metriks dan parameter?
Jawaban : LPSE belum memiliki pengukuran kinerja, ya.. jadi belum ada definisi metriks dan parameternya juga.	
3.	Apakah instansi menetapkan mekanisme pengukuran kinerja?
Jawaban : LPSE belum pernah menetapkan bagaimana mekanisme pengukuran kinerja.	
4.	Apakah instansi mendefinisikan waktu pengukuran dan pelaksananya?
Jawaban :	

LPSE juga belum pernah pastinya membuat kapan harus diukur tapi sudah mulai membayangkan pelaksanaan pengukuran kinerja. Menurut pemikiran kami, kami akan mulai mengembangkan ke tahap selanjutnya jika dokumen kerangka kerja sudah lengkap dan sudah terverifikasi oleh LKPP.		
IV	3	Pertanyaan No. 19
Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?		
Poin Pertanyaan : Penilaian kinerja bagi pelaksana keamanan informasi		
1.	Apakah instansi memiliki program penilaian kinerja pengelolaan keamanan informasi?	
Jawaban : LPSE belum pernah melakukan penilaian kinerja, jadi sampai saat ini LPSE masih belum memiliki program penilaian kinerja apalagi yang berhubungan dengan keamanan informasi.		
2.	Apakah program tersebut pernah dilaksanakan?	
Jawaban : LPSE belum prenah melakukan program tersebut. Karena memang belum dibuat oleh LPSE.		
IV	3	Pertanyaan No. 20
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?		
Poin Pertanyaan : pembuatan dan penerapan target pengelolaan keamanan informasi		
1.	Apakah instansi mempunyai sasaran/target yang ingin dicapai di setiap area?	
Jawaban : Saat ini, LPSE belum mempunyai target keamanan informasi		

secara pasti. Karena dari LPSE sendiri masih merancang dokumen-dokumen yang harus dipenuhi untuk standarisasi.	
2.	Apakah sasaran tersebut mempunyai kriteria penilaian?
Jawaban : LPSE belum mempunyai kriteria penilaian terhadap target yang ditentukan.	
3.	Apakah instansi sudah melaksanakan kegiatan yang mendukung tercapainya sasaran?
Jawaban : LPSE belum pernah melakukan kegiatan yang mendukung tercapainya target pengelolaan keamanan informasi	
Poin Pertanyaan : evaluasi pencapaian	
4.	Apakah instansi melakukan evaluasi dari penerapan kegiatan berserta sasaran yang dibuat?
Jawaban : Karena LPSE baru diganti dan baru saja bergabung dengan kominfo, maka banyak sekali perubahan dan baru saja membuat dokumen untuk kelengkapan dan standarisasi LPSE. Jadi LPSE belum pernah melakukan evaluasi berdasarkan kegiatan	
Poin Pertanyaan : pembuatan dan penerapan perbaikan	
5.	Apakah instansi melakukan perbaikan pada sasaran yang telah dilakukan evaluasi?
Jawaban : LPSE belum pernah melakukan evaluasi, maka dari itu instansi juga belum pernah melakukan perbaikan terhadap evaluasi yang dibuat.	
Poin Pertanyaan : pelaporan status	
6.	Apakah instansi pernah melakukan pelaporan status setelah melakukan perbaikan?
Jawaban : LPSE sering melaporkan kondisi internal maupun sistem LPSE pada LPSE pusat. Tetapi yang dimaksud jika status pelaporan setelah dilakukan evaluasi dan perbaikan, selama ini LPSE belum pernah melakukan evaluasi ya karena seperti dikatakan sebelumnya bahwa LPSE masih membuat dokumen	

untuk standarisasi LPSE.		
IV	3	Pertanyaan No. 21
Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?		
Poin Pertanyaan : Identifikasi legislasi, perangkat hukum dan standar		
1.	Apakah instansi mempunyai perangkat hukum atau standar yang mengatur keamanan informasi di dalamnya?	
Jawaban : Sebenarnya keamanan informasi pada LPSE belum semua diidentifikasi. Masih beberapa saja. Untuk perangkat hukum atau standar sendiri, LPSE memiliki standar yang diambil dari standarisasi menurut LKPP. Standar tersebut merujuk pada beberapa standar internasional. Salah satunya adalah standar ISO.		
2.	Apakah instansi pernah melakukan identifikasi pada legislasi yang dipatuhi oleh instansi?	
Jawaban : Tentu saja LPSE pernah melakukan identifikasi pada pematuhan legislasi, seperti kepatuhan terhadap peraturan bupati. Tetapi, jika berhubungan dengan keamanan informasi, LPSE belum melakukan identifikasi terhadap legislasi yang keamanan informasi.		
3.	Apakah instansi memperbarui seluruh legislasi yang dipatuhi secara rutin?	
Jawaban : LPSE belum pernah melakukan pembaharuan terhadap legislasi, karena selama ini ketika didirikan unit ini, peraturan belum berubah. Tetapi justru ada penambahan peraturan baru yang membuat pekerjaan/tugas unit semakin banyak.		
IV	3	Pertanyaan No. 22
Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan		

informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	
Poin Pertanyaan : Kebijakan penanggulangan insiden keamanan informasi	
1.	Apakah instansi mempunyai dokumen penanggulangan insiden?
Jawaban : Untuk saat ini, dokumen penanggulangan insiden hanya berbentuk SOP dan form. jadi terdapat prosedur jika terdapat permasalahan yang menyangkut sistem atau layanan pada LPSE.	
2.	Apakah di dalam dokumen terdapat isitilah atau definisi-definisi tertentu?
Jawaban : Ada, seperti istilah gangguan ada pengertiannya. Permasalahan juga mempunyai definisi. Jadi istilahnya ya seperti itu dan istilah tersebut dimasukkan dalam dokumen prosedur penanggulangan permasalahan.	
Poin Pertanyaan : Langkah penanggulangan insisden keamanan informasi	
3.	Apakah instansi memiliki prosedur mengenai penanggulangan insiden?
Jawaban : Iya, instansi memiliki prosedur atau SOP mengenai penanggulangan insiden, tetapi jika spesifik untuk keamanan informasi, LPSE belum punya SOP penanggulangan insiden yang berhubungan dengan keamanan informasi. Mungkin secara umum, hampir sama dengan SOP penanggulangan permasalahan layanan. Hanya istilah saja yang mungkin berbeda.	

“Halaman ini sengaja dikosongkan”

LAMPIRAN E
Hasil observasi/review dokumen berdasarkan perangakat pengumpulan data

Tabel E.1 hasil observasi/review dokumen

II	1	Pertanyaan no. 1	
Dokumen program keamanan informasi			Tidak Tersedia
Dokumen pernyataan komitmen manajemen			Tidak Tersedia
Dokumen prinsip keamanan informasi			Tidak Tersedia
Dokumen strategi teknologi informasi			Tidak Tersedia
Dokumen kebijakan keamanan informasi			Tersedia
II	1	Pertanyaan no. 2	
Dokumen tupoksi organisasi			Tersedia
Tugas dan tanggung jawab pengelola keamanan informasi			Tersedia
Surat Keterangan Pembentukan Tim LPSE			Tersedia
II	1	Pertanyaan no. 3	
Tupoksi pelaksana pengamanan informasi			Tersedia
Dokumen definisi kewenangan pelaksana keamanan informasi			Tidak Tersedia
Kontrak/janji instansi untuk mengatur kewenangan pejabat/petugas pelaksana pengamanan informasi			Tersedia
II	1	Pertanyaan no. 4	
Log atau aktivitas penggunaan sumber daya dalam mengelola keamanan informasi			Tersedia
SOP pengelolaan kapasitas			Tersedia
Dokumen pencatatan kapasitas			Tersedia
Dokumen evaluasi kapasitas			Tersedia
II	1	Pertanyaan no. 5	
Pemetaan keperluan pelaksana pengamanan informasi			Tidak Tersedia
II	1	Pertanyaan no. 6	
Dokumen persyaratan/standar kompetensi pengelola keamanan informasi			Tersedia

Dokumen keahlian pengelola keamanan informasi			Tersedia
II	1	Pertanyaan no. 7	
Dokumen persyaratan/standar kompetensi dan keahlian			Tersedia
II	1	Pertanyaan no. 8	
Dokumentasi kegiatan sosialisasi pemahaman keamanan informasi			Tidak Tersedia
Dokumen Program keamanan informasi			Tidak Tersedia
II	2	Pertanyaan no. 9	
Dokumen program keamanan informasi			Tidak Tersedia
Dokumen kompetensi dan keahlian			Tersedia
II	2	Pertanyaan no. 11	
Dokumen identifikasi data pribadi			Tidak Tersedia
Dokumen pengamanan data pribadi			Tersedia
II	2	Pertanyaan no. 12	
Dokumen kontrak antara pengelola pihak internal dan eksternal			Tidak Tersedia
SOP gangguan permasalahan dengan pihak terkait			Tersedia
Form Pencatatan Permasalahan			Tersedia
Form Penangan Permasalahan			Tersedia
II	2	Pertanyaan no. 13	
Dokumen koordinasi dan kontrak antara pihak pengelola keamanan informasi dengan satuan terkait			Tersedia
III	2	Pertanyaan no. 14	
Dokumen kelangsungan layanan TIK			Tidak Tersedia
SOP kelangsungan layanan			Tersedia
III	2	Pertanyaan no. 15	
Prosedur pelaporan kondisi, kinerja/efektivitas dan kepatuhan program keamanan informasi			Tidak Tersedia
Log atau dokumen laporan kondisi keamanan informasi			Tidak Tersedia
III	2	Pertanyaan no. 16	

Catatan kondisi dan permasalahan keamanan informasi			Tidak Tersedia
Dokumen Pengambilan keputusan berdasarkan permasalahan keamanan informasi			Tidak Tersedia
IV	3	Pertanyaan no. 17	
Dokumen program khusus mengenai kepatuhan tujuan dan sasaran pengamanan informasi			Tidak Tersedia
IV	3	Pertanyaan no. 18	
Dokumen pengukuran kinerja pengelolaan keamanan informasi			Tidak Tersedia
IV	3	Pertanyaan no. 19	
Dokumen program penilaian kinerja			Tidak Tersedia
IV	3	Pertanyaan no. 20	
Sasaran/target pengelolaan keamanan informasi			Tidak Tersedia
Log aktivitas yang mendukung sasaran/target pengelolaan keamanan informasi			Tidak Tersedia
Penilaian sasaran/target pengelolaan keamanan informasi			Tidak Tersedia
IV	3	Pertanyaan no. 21	
Dokumen kepatuhan terhadap standar dan perangkat hukum			Tidak Tersedia
IV	3	Pertanyaan no. 22	
Dokumen penanggulangan insiden			Tidak Tersedia
Prosedur penanggulangan insiden			Tidak Tersedia
Kebijakan penanggulangan insiden			Tidak Tersedia

“Halaman ini sengaja dikosongkan”

LAMPIRAN F

Fakta, Bukti dan Kesesuaian

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?	
			Temuan/ Fakta	UPT LPSE hanya memiliki dokumen kebijakan layanan yang berisi : - Kebijakan umum; - Kebijakan Layanan; - Kebijakan Keamanan Informasi. Kemudian, dari kebijakan keamanan informasi, telah terdapat dokumen pendukung kebijakan, seperti adanya dokumen backup sistem dan dokumen kompetensi.
			Bukti	- Perbup No. 72 mengenai UPT (**FOTO 4**); - Dokumen Kebijakan umum, Layanan dan Keamanan Informasi pada UPT LPSE (**FOTO 1, FOTO 2, FOTO 3**)
			Kesesuaian (Ya/Tidak)	Ya
2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga	

			kepatuhannya?	
			Temuan/ Fakta	LPSE memiliki tugas dan tanggung jawab untuk keamanan informasi, lebih tepatnya pada koordinator keamanan informasi. Dokumen tersebut menjelaskan tentang tugas dan tanggung jawab yang diberikan kepada setiap personil. Selain dari dokumen tersebut, Kepala Diskominfo juga telah menyetujui dan mengeluarkan SK sebagai bukti peresmian LPSE dan anggota staff pada LPSE.
			Bukti	- Perbup No. 72 mengenai UPT (**FOTO 4**); - SK pelaksana dan operasional layanan UPT LPSE (**FOTO 6**) - Tugas Pokok dan Fungsi UPT LPSE (**FOTO 7**)
			Kesesuaian (Ya/Tidak)	Ya
3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	
			Temuan/ Fakta	LPSE telah memiliki SK pembentukan tim anggota LPSE, kemudian LPSE juga telah memiliki dokumen tugas dan tanggung jawab dalam unit LPSE. Setiap anggota LPSE

				memiliki lebih dari satu kewenangan yang dipegang.
			Bukti	- SK pelaksana dan operasional layanan UPT LPSE (**FOTO 6**) - Tugas Pokok dan Fungsi UPT LPSE (**FOTO 7**)
			Kesesuaian (Ya/Tidak)	Ya
4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?	
			Temuan/ Fakta	LPSE memiliki form pencatatan kapasitas yang dirancang untuk seluruh bagian dan fungsi pada LPSE. Selain dari form pencatatan kapasitas tersebut, LPSE juga membuat SOP pengelolaan kapasitas agar kapasitas yang sudah dialokasikan digunakan secara optimal. Kemudian LPSE juga melakukan evaluasi penggunaan kapasitas yang dijadikan sebagai bahan masukan untuk efektivitas pengelolaan kapasitas LPSE.
			Bukti	- Formulir pencatatan kapasitas (**FOTO 8**) - SOP pengelolaan Kapasitas (**FOTO 9**) - Dokumen laporan evaluasi dan tindak lanjut pengelolaan kapasitas

				(**FOTO 10**)
			Kesesuaian (Ya/Tidak)	Ya
5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	
			Temuan/ Fakta	LPSE belum pernah memetakan keperluan setiap bagian dan dilakukan pemisahan kewenangan. LPSE juga belum pernah menentukan kebutuhan audit internal.
			Bukti	
			Kesesuaian (Ya/Tidak)	Ya
6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	
			Temuan/ Fakta	LPSE telah membuat dokumen kompetensi diman dokumen tersebut berisi : - Perbandingan kebutuhan kompetensi LPSE dengan kompetensi yang dimiliki oleh anggota staff; - Jenis kompetensi yang harus diambil setiap staff sesuai dengan kebutuhan pada setiap bagian/fungsi;

				- Perencanaan pelaksanaan peningkatan kompetensi oleh setiap staff bidang/fungsi.
			Bukti	- Dokumen Matriks Kompetensi (**FOTO 11**)
			Kesesuaian (Ya/Tidak)	Ya
7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	
			Temuan/ Fakta	Matriks kompetensi dibuat berdasarkan panduan standarisasi LKPP. LPSE telah memiliki kompetensi dan keahlian sesuai dengan persyaratan yang berlaku.
			Bukti	- Dokumen Matriks Kompetensi (**FOTO 11**)
			Kesesuaian (Ya/Tidak)	Ya
8	II	1	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	
			Temuan/ Fakta	LPSE pernah melakukan bimbingan standarisasi LPSE kepada staff LPSE. Hal tersebut dilakukan dengan tujuan agar staff dapat lebih memahami

				LPSE dan meningkatkan standar pada LPSE. LPSE mengadakan bimbingan secara menyeluruh untuk pmahaman sstnadarisasi LPSE. Tetapi untuk secara fokus terhadap bimbingan atau sosialisasi keamanan informasi, LPSE masih merancang dokumen terkait.
			Bukti	- Berita Acara pembinaan Layanan UPT LPSE (**FOTO 12**)
			Kesesuaian (Ya/Tidak)	Ya
9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?	
			Temuan/ Fakta	Matriks Kompetensi yang dimiliki oleh LPSE juga berisikan target pelaksanaan peningkatan kompetensi, dimana dalam dokumen tersebutt berisi jenis keahlian apa yang akan ditingkatkan dan kapan waktu batas akhir proses peningkatan. LPSE telah menentukan kapan harus meningkatkan keahlian dan kompetensi.
			Bukti	- Dokumen Matriks Kompetensi (**FOTO 11**)
			Kesesuaian (Ya/Tidak)	Ya

10	II	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?	
			Temuan/ Fakta	LPSE belum mengidentifikasi dan mendefinisikan proses kerja apa yang harus terintegrasi dengan keperluan/persyaratan keamanan informasi.
			Bukti	
			Kesesuaian (Ya/Tidak)	Ya
11	II	2	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?	
			Temuan/ Fakta	Data pribadi yang digunakan pada LPSE disesuaikan dengan form data pribadi miliki LPSE pusat. Pengamanan data pribadi telah dijabarkan pada dokumen kebijakan keamanan informasi. Bahwa untuk melindungi seluruh data, maka instansi harus membuat password dengan ketentuan tertentu, menjaga akun dan pengelolaan lainnya. Kebijakan tersebut dibuat agar data pribadi dan data lainnya tetap terjaga.
			Bukti	- Dokumen Kebijakan Keamanan Informasi (**FOTO 3**)

			Kesesuaian (Ya/Tidak)	Ya
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?	
			Temuan/ Fakta	LPSE turut aktif dalam melakukan koordinasi dengan pengguna aset informasi pada LPSE. Pengguna tersebut merupakan pengguna sistem LPSE. Biasanya, komunikasi yang dilakukan jika terdapat permasalahan pada LPSE. Permasalahan tersebut masuk ke dalam bagian helpdesk dan akan diselesaikan bagian administrasi sistem elektronik jika menyangkut teknis sistem. Data pengguna yang diberikan kepada LPSE valid karena dilakukan tahap verifikasi dan vailidasi data. Tahap validasi tersebut telah disetujui oleh LPSE pusat terlebih dahulu.
			Bukti	- Formulir penanganan masalah dengan pihak pengguna sistem (**FOTO 13**) - Dokumen perjanjian

				kerahasiaan (**FOTO 14**)
			Kesesuaian (Ya/Tidak)	Ya
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?	
			Temuan/ Fakta	Menurut narasumber, LPSE selalu berkodinasi dengan LKPP terkait standarisasi LKPP, tetapi belum terdapat hasil koordinasi tersebut. LPSE hanya memiliki surat keterangan mengenai himbauan kepada LPSE untuk melakukan standarisasi. LPSE pernah melakukan perjanjian kerahasiaan dengan salah saru anggota Diskominfo untuk melakukan pertukaran informasi.
			Bukti	- Surat Keterangan Stndarisasi LKPP (**FOTO 15**) - Dokumen perjanjian kerahasiaan (**FOTO 14**)
			Kesesuaian (Ya/Tidak)	Ya
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?	
			Temuan/ Fakta	LPSE memiliki dokumen layanan yang berisikan tugas dan tanggung jawab koordinator kelangsungan layanan.
			Bukti	- Dokumen organisasi Layanan pada bagian kordinator kelangsungan layanan (**FOTO 16**)
			Kesesuaian (Ya/Tidak)	Ya
15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	
			Temuan/ Fakta	LPSE hanya melaporkan keadaan keamanan informasi jika ditanya oleh pimpinan instansi. LPSE belum pernah melaporkan kondisi keamanan informasi kepada pimpinan instansi secara resmi dan rutin.
			Bukti	
			Kesesuaian (Ya/Tidak)	Ya
16	III	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?	

			Temuan/ Fakta	LPSE belum melaporkan kondisi permasalahan keamanan informasi dengan hubungan bagian konsideran dan proses pengambilan keputusan strategis.
			Bukti	
			Kesesuaian (Ya/Tidak)	Ya
17	IV	2	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?	
			Temuan/ Fakta	LPSE tidak memiliki program khusus untuk mematuhi tujuan kepatuhan pengamanan informasi.
			Bukti	
			Kesesuaian (Ya/Tidak)	Ya
18	IV	3	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?	
			Temuan/ Fakta	LPSE tidak memiliki proses pengukuran kinerja, metriks besserta parameternya.
			Bukti	
			Kesesuai	Ya

			an (Ya/Tidak)	
19	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	
			Temuan/ Fakta	LPSE tidak menerapkan program penilaian kinerja
			Bukti	
			Kesesuaian (Ya/Tidak)	Ya
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?	
			Temuan/ Fakta	LPSE belum menetpkan target dan sasaran pengelolaan keamanan informasi.
			Bukti	
			Kesesuaian (Ya/Tidak)	Ya
21	IV	3	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	
			Temuan/ Fakta	LPSE belum mengidentifikasi legilasi dengan keamanan

				informasi yang harus dipatuhi
			Bukti	
			Kesesuaian (Ya/Tidak)	Ya
22	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	
			Temuan/ Fakta	LPSE belum mendefinisikan kebijakan dan langkah penanggulangan insiden
			Bukti	
			Kesesuaian (Ya/Tidak)	Ya

“*Halaman ini sengaja dikosongkan”*

LAMPIRAN G
Bukti Pendukung

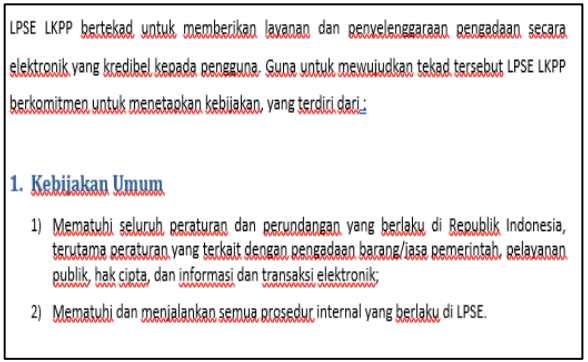
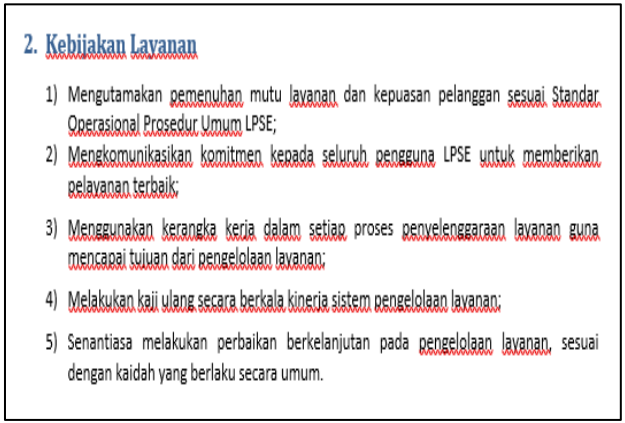
FOTO 1	FOTO 2
	
Sreenshot dokumen kebijakan Umum UPT LPSE	*Screenshot* dokumen kebijakan Layanan UPT LPSE

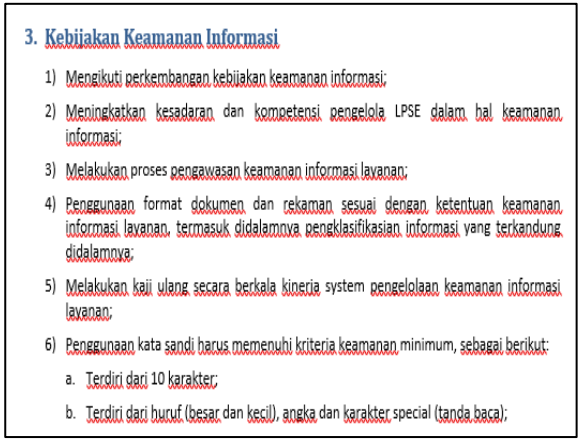
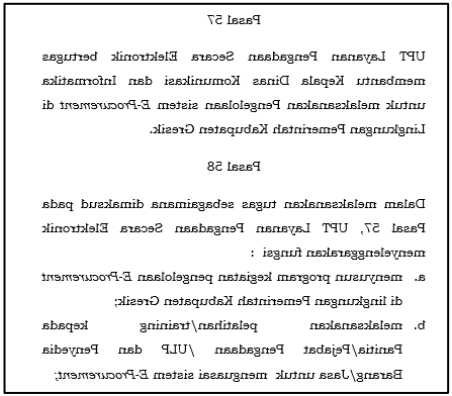
FOTO 3	FOTO 4
	
Screenshot dokumen kebijakan Keamanan Informasi UPT LPSE	Peraturan Bupati No. 72 Tentang UPT

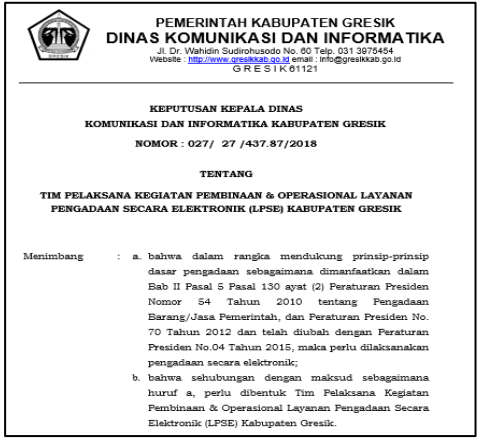
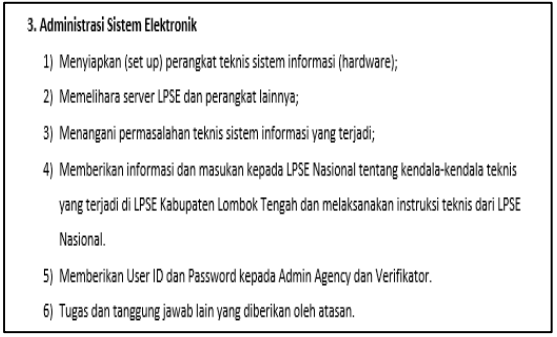
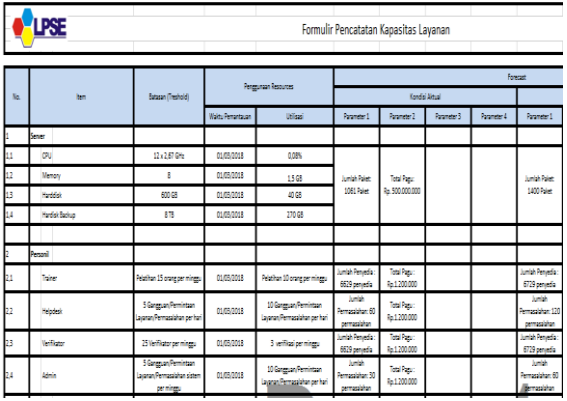
FOTO 5	FOTO 6
	
Dokumen Organisasi layanan	SK pelaksana dan Operasional LPSE

FOTO 7	FOTO 8
	
Screenshot tugas pokok dan fungsi UPT LPSE	Screenshot formulir pencatatan kapasitas

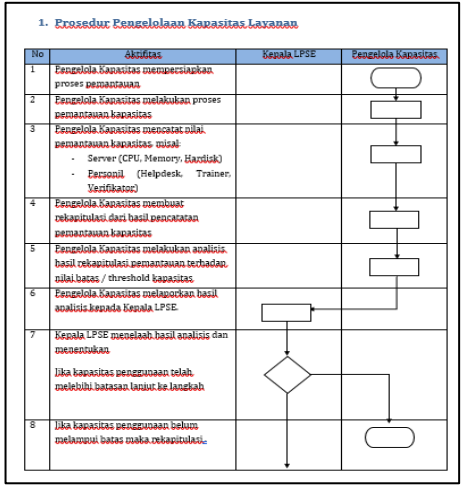
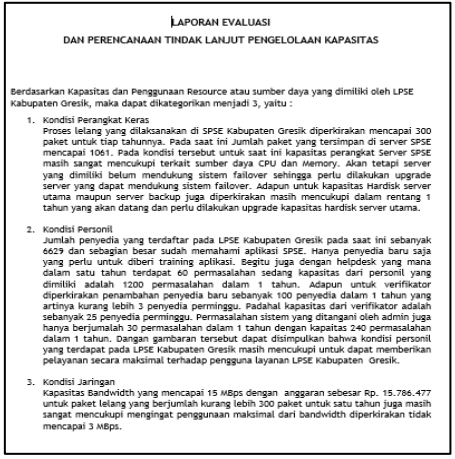
3. Administrasi Sistem Elektronik

1) Menyiapkan (set up) perangkat teknis sistem informasi (hardware);
2) Memelihara server LPSE dan perangkat lainnya;
3) Menangani permasalahan teknis sistem informasi yang terjadi;
4) Memberikan informasi dan masukan kepada LPSE Nasional tentang kendala-kendala teknis yang terjadi di LPSE Kabupaten Lombok Tengah dan melaksanakan instruksi teknis dari LPSE Nasional.
5) Memberikan User ID dan Password kepada Admin Agency dan Verifikator.
6) Tugas dan tanggung jawab lain yang diberikan oleh atasan.

LPSE

Formulir Pencatatan Kapasitas Layanan

No.	Item	Batasan (Treshold)	Penggunaan Resources		Kondisi Aktual				Forecast
			Waktu Pemantauan	Utilisasi	Parameter 1	Parameter 2	Parameter 3	Parameter 4	Parameter 1
1	Server								
1.1	CPU	12 x 2.87 Ghz	01/05/2018	0,08%					
1.2	Memory	8	01/05/2018	1.5 GB	Jumlah Paket: 1061 Paket	Total Pagu: Rp. 500.000.000			Jumlah Paket: 1400 Paket
1.3	Harddisk	600 GB	01/05/2018	40 GB					
1.4	Harddisk Backup	8 TB	01/05/2018	270 GB					
2	Personil								
2.1	Trainer	Pelatihan 15 orang per minggu	01/05/2018	Pelatihan 10 orang per minggu	Jumlah Penyedia: 6629 penyedia	Total Pagu: Rp.1.200.000			Jumlah Penyedia: 8729 penyedia
2.2	Helpdesk	5 Gangguan/Permintaan Layanan/Permasalahan per hari	01/05/2018	10 Gangguan/Permintaan Layanan/Permasalahan per hari	Jumlah Permasalahan: 60 permasalahan	Total Pagu: Rp.1.200.000			Jumlah Permasalahan: 120 permasalahan
2.3	Verifikator	15 Verifikator per minggu	01/05/2018	5 verifikasi per minggu	Jumlah Penyedia: 6629 penyedia	Total Pagu: Rp.1.200.000			Jumlah Penyedia: 8729 penyedia
2.4	Admin	5 Gangguan/Permintaan Layanan/Permasalahan sistem per minggu	01/05/2018	10 Gangguan/Permintaan Layanan/Permasalahan per hari	Jumlah Permasalahan: 30 permasalahan	Total Pagu: Rp.1.200.000			Jumlah Permasalahan: 60 permasalahan

FOTO 9	FOTO 10
	
Screenshot SOP pengelolaan kapasitas	Screenshot dokumen laporan evaluasi dan tindak lanjut pengelolaan kapasitas

1. Prosedur Pengelolaan Kapasitas Layanan

No	Aktifitas	Kepala LPSE	Pengelola Kapasitas
1	Pengelola Kapasitas mempersiapkan proses pemantauan		
2	Pengelola Kapasitas melakukan proses pemantauan kapasitas		
3	Pengelola Kapasitas mencatat nilai pemantauan kapasitas, misal: - Server (CPU, Memory, Hardisk) - Personil (Helpdesk, Trainer, Verifikator)		
4	Pengelola Kapasitas membuat rekapitulasi dari hasil pencatatan pemantauan kapasitas		
5	Pengelola Kapasitas melakukan analisis hasil rekapitulasi pemantauan terhadap nilai batas / threshold kapasitas		
6	Pengelola Kapasitas melaporkan hasil analisis kepada Kepala LPSE		
7	Kepala LPSE menelaah hasil analisis dan menentukan Jika kapasitas penggunaan telah melebihi batasan lanjut ke langkah		
8	Jika kapasitas penggunaan belum melampui batas maka rekapitulasi.		

LAPORAN EVALUASI
DAN PERENCANAAN TINDAK LANJUT PENGELOLAAN KAPASITAS

Berdasarkan Kapasitas dan Penggunaan Resource atau sumber daya yang dimiliki oleh LPSE Kabupaten Gresik, maka dapat dikategorikan menjadi 3, yaitu :

1. Kondisi Perangkat Keras
   Proses lelang yang dilaksanakan di SPSE Kabupaten Gresik diperkirakan mencapai 300 paket untuk tiap tahunnya. Pada saat ini Jumlah paket yang tersimpan di server SPSE mencapai 1061. Pada kondisi tersebut untuk saat ini kapasitas perangkat Server SPSE masih sangat mencukupi terkait sumber daya CPU dan Memory. Akan tetapi server yang dimiliki belum mendukung sistem failover sehingga perlu dilakukan upgrade server yang dapat mendukung sistem failover. Adapun untuk kapasitas Hardisk server utama maupun server backup juga diperkirakan masih mencukupi dalam rentang 1 tahun yang akan datang dan perlu dilakukan upgrade kapasitas hardisk server utama.

2. Kondisi Personil
   Jumlah penyedia yang terdaftar pada LPSE Kabupaten Gresik pada saat ini sebanyak 6629 dan sebagian besar sudah memahami aplikasi SPSE. Hanya penyedia baru saja yang perlu untuk diberi training aplikasi. Begitu juga dengan helpdesk yang mana dalam satu tahun terdapat 60 permasalahan sedang kapasitas dari personil yang dimiliki adalah 1200 permasalahan dalam 1 tahun. Adapun untuk verifikator diperkirakan penambahan penyedia baru sebanyak 100 penyedia dalam 1 tahun yang artinya kurang lebih 3 penyedia perminggu. Padahal kapasitas dari verifikator adalah sebanyak 25 penyedia perminggu. Permasalahan sistem yang ditangani oleh admin juga hanya berjumlah 30 permasalahan dalam 1 tahun dengan kapaitas 240 permasalahan dalam 1 tahun. Dangan gambaran tersebut dapat disimpulkan bahwa kondisi personil yang terdapat pada LPSE Kabupaten Gresik masih mencukupi untuk dapat memberikan pelayanan secara maksimal terhadap pengguna layanan LPSE Kabupaten Gresik.

3. Kondisi Jaringan
   Kapasitas Bandwidth yang mencapai 15 MBps dengan anggaran sebesar Rp. 15.786.477 untuk paket lelang yang berjumlah kurang lebih 300 paket untuk satu tahun juga masih sangat mencukupi mengingat penggunaan maksimal dari bandwidth diperkirakan tidak mencapai 3 MBps.

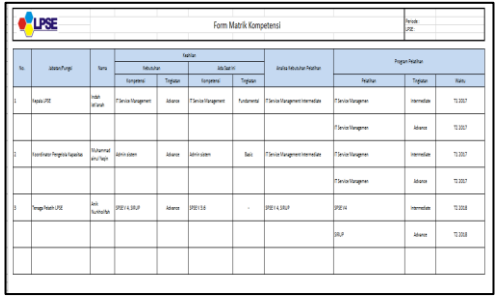
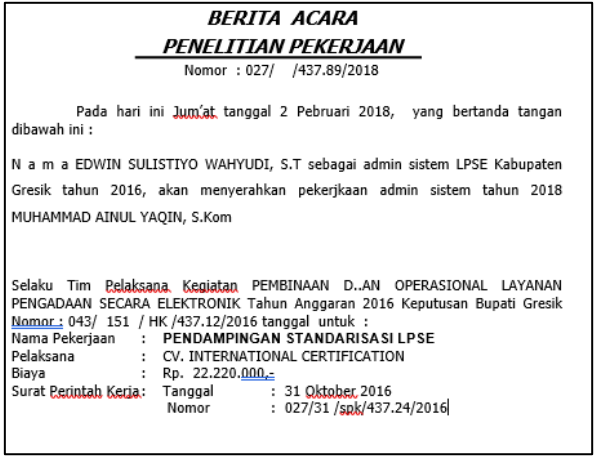
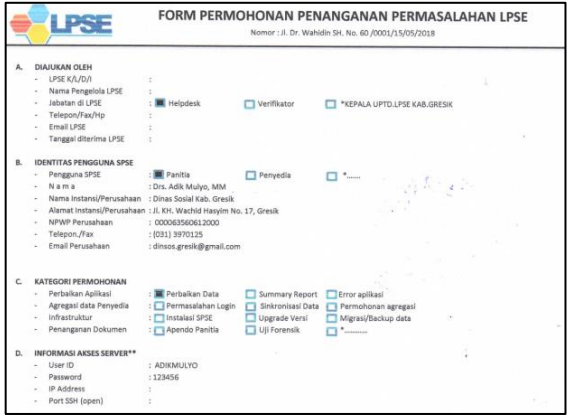
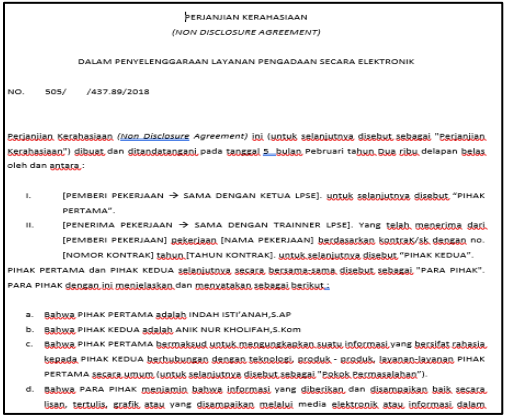
FOTO 11	FOTO 12
	
Screenshot matriks Kompetensi pada LPSE	Screenshot Berita Acara Pembinaan layanan UPT LPSE

FOTO 13	FOTO 14
	
Formulir penanganan permasalahan dengan pihak pengguna sistem LPSE	Screenshot dokumen perjanjian kerahasiaan

FORM PERMOHONAN PENANGANAN PERMASALAHAN LPSE

Nomor : Jl. Dr. Wahidin SH. No. 60 /0001/15/05/2018

A. DIAJUKAN OLEH

- LPSE K/L/D/I :
- Nama Pengelola LPSE :
- Jabatan di LPSE : ☑ Helpdesk ☐ Verifikator ☐ *KEPALA UPTD.LPSE KAB.GRESIK
- Telepon/Fax/Hp :
- Email LPSE :
- Tanggal diterima LPSE :

B. IDENTITAS PENGGUNA SPSE

- Pengguna SPSE : ☑ Panitia ☐ Penyedia ☐ *.....
- N a m a : Drs. Adik Mulyo, MM
- Nama Instansi/Perusahaan : Dinas Sosial Kab. Gresik
- Alamat Instansi/Perusahaan : Jl. KH. Wachid Hasyim No. 17, Gresik
- NPWP Perusahaan : 000063560612000
- Telepon./Fax : (031) 3970125
- Email Perusahaan : dinsos.gresik@gmail.com

C. KATEGORI PERMOHONAN

- Perbaikan Aplikasi : ☑ Perbaikan Data ☐ Summary Report ☐ Error aplikasi
- Agregasi data Penyedia : ☐ Permasalahan Login ☐ Sinkronisasi Data ☐ Permohonan agregasi
- Infrastruktur : ☐ Instalasi SPSE ☐ Upgrade Versi ☐ Migrasi/Backup data
- Penanganan Dokumen : ☐ Apendo Panitia ☐ Uji Forensik ☐ *.....

D. INFORMASI AKSES SERVER**

- User ID : ADIKMULYO
- Password : 123456
- IP Address :
- Port SSH (open) :

PERJANJIAN KERAHASIAAN

(NON DISCLOSURE AGREEMENT)

DALAM PENYELENGGARAAN LAYANAN PENGADAAN SECARA ELEKTRONIK

NO. 505/ /437.89/2018

Perjanjian Kerahasiaan *(Non Disclosure Agreement)* ini (untuk selanjutnya disebut sebagai "Perjanjian Kerahasiaan") dibuat dan ditandatangani pada tanggal 5 bulan Pebruari tahun Dua ribu delapan belas oleh dan antara :

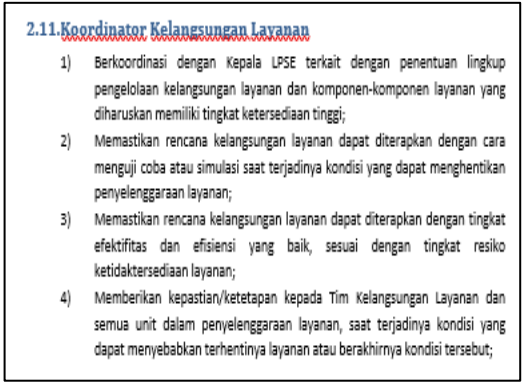
I. [PEMBERI PEKERJAAN → SAMA DENGAN KETUA LPSE]. untuk selanjutnya disebut "PIHAK PERTAMA".

II. [PENERIMA PEKERJAAN → SAMA DENGAN TRAINNER LPSE]. Yang telah menerima dari [PEMBERI PEKERJAAN] pekerjaan [NAMA PEKERJAAN] berdasarkan kontrak/sk dengan no. [NOMOR KONTRAK] tahun [TAHUN KONTRAK]. untuk selanjutnya disebut "PIHAK KEDUA".

PIHAK PERTAMA dan PIHAK KEDUA selanjutnya secara bersama-sama disebut sebagai "PARA PIHAK".

PARA PIHAK dengan ini menjelaskan dan menyatakan sebagai berikut :

a. Bahwa PIHAK PERTAMA adalah INDAH ISTI'ANAH,S.AP
b. Bahwa PIHAK KEDUA adalah ANIK NUR KHOLIFAH,S.Kom
c. Bahwa PIHAK PERTAMA bermaksud untuk mengungkapkan suatu informasi yang bersifat rahasia kepada PIHAK KEDUA berhubungan dengan teknologi, produk - produk, layanan-layanan PIHAK PERTAMA secara umum (untuk selanjutnya disebut sebagai "Pokok Permasalahan").
d. Bahwa PARA PIHAK menjamin bahwa informasi yang diberikan dan disampaikan baik secara lisan, tertulis, grafik atau yang disampaikan melalui media elektronik atau informasi dalam

FOTO 15	FOTO 16
	
Screenshot surat Keterangan LKPP	Screenshot dokumen organisasi Layanan yang menyangkut Kelangsungan Layanan

LEMBAGA KEBIJAKAN PENGADAAN BARANG/JASA PEMERINTAH
REPUBLIK INDONESIA
Gedung LKPP - Kompleks Rasuna Epicentrum, Jln. Epicentrum Tengah Lot 11B, Jakarta
www.lkpp.go.id

Nomor : 3979 /D2.3/04/2018 19 April 2018
Lampiran : 3 (tiga) berkas
Sifat : Penting
Hal : Himbauan Terhadap Penerapan Standardisasi LPSE: 2014

Kepada Yth.

1. Sekretaris Daerah Pemerintah Provinsi/Kabupaten/Kota
2. Kepala Kepolisian Daerah
3. Rektor Perguruan Tinggi Negeri
4. Direktur Utama BUMN/BUMD

di

Tempat

Dengan diterbitkannya Peraturan Presiden Nomor 16 Tahun 2018 tentang Pengadaan Barang/Jasa Pemerintah, maka penyelenggaraan Pengadaan Barang/Jasa dilakukan secara elektronik menggunakan sistem informasi yang terdiri atas Sistem Pengadaan Secara Elektronik (SPSE) dan sistem pendukung yang dikembangkan oleh Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah. Proses penyelenggaraan SPSE dilaksanakan secara menyeluruh dimulai dari perencanaan pengadaan, persiapan pengadaan, pemilihan penyedia, pelaksanaan kontrak, serah terima pekerjaan, pengelolaan penyedia, sampai dengan katalog elektronik.

Layanan Pengadaan Secara Elektronik (LPSE) merupakan unit layanan yang memiliki kontribusi penting dalam mengelola dan memfasilitasi para pemangku kepentingan selama penyelenggaraan proses Pengadaan Barang/Jasa Pemerintah secara elektronik di lingkup Kementerian/Lembaga/Perangkat Daerah sehingga prinsip-prinsip dan *value for money* pengadaan barang/jasa dapat terwujud.

2.11. Koordinator Kelangsungan Layanan

1) Berkoordinasi dengan Kepala LPSE terkait dengan penentuan lingkup pengelolaan kelangsungan layanan dan komponen-komponen layanan yang diharuskan memiliki tingkat ketersediaan tinggi;
2) Memastikan rencana kelangsungan layanan dapat diterapkan dengan cara menguji coba atau simulasi saat terjadinya kondisi yang dapat menghentikan penyelenggaraan layanan;
3) Memastikan rencana kelangsungan layanan dapat diterapkan dengan tingkat efektifitas dan efisiensi yang baik, sesuai dengan tingkat resiko ketidaktersediaan layanan;
4) Memberikan kepastian/ketetapan kepada Tim Kelangsungan Layanan dan semua unit dalam penyelenggaraan layanan, saat terjadinya kondisi yang dapat menyebabkan terhentinya layanan atau berakhirnya kondisi tersebut;

FOTO 17

PAKTA INTEGRITAS

Saya yang bertanda tangan di bawah ini:

Nama : MUHAMMAD AINUL YAQIN,S.Kom

NIP : 19850729 200901 1 001

Jabatan : Administrator Sistem LPSE Kabupaten Gresik

dengan ini menyatakan bahwa:

1. Bertanggung jawab penuh atas akses server LPSE Kabupaten Gresik baik secara fisik maupun non fisik.
2. Bersedia menjaga kerahasiaan akses server LPSE Kabupaten Gresik
3. tidak akan melakukan praktek Korupsi, Kolusi dan Nepotisme (KKN)
4. Akan melaporkan kepada LKPP apabila mengetahui ada ketidakwajaran pada server LPSE Kabupaten Gresik
5. Akan menjalankan tugas dan fungsi sesuai denan kewenangan secara bersih, transparan, bertanggung jawab dan profesional untuk memberikan hasil kerja terbaik sesuai ketentuan peraturan perundang-undangan
6. Apabila melanggar hal-hal yang dinyatakan dalam Pakta Integritas ini, bersedia menerima sanksi administratif, dan digugat secara perdata dan/atau dilaporkan secara pidana.

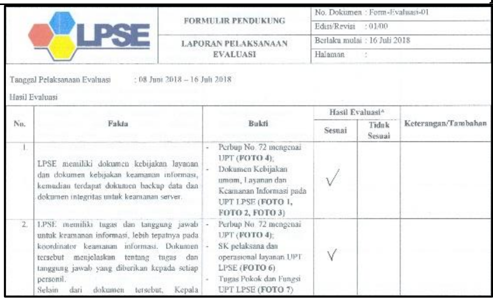
Gresik, 5 Pebruari 2018

Administrator LPSE Kabupaten Gresik

Screenshot pakta Integritas

“*Halaman ini sengaja dikosongkan”*

LAMPIRAN H
Klarifikasi penilaian fakta dan bukti

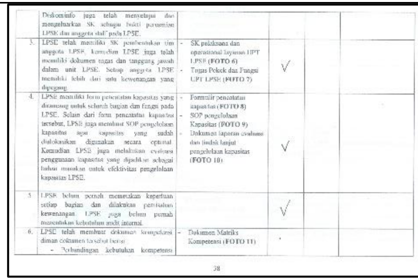


FORMULIR PENDUKUNG	No. Dokumen : Form-Evaluasi-01
	Edisi/Revisi : 01/00
LAPORAN PELAKSANAAN EVALUASI	Berlaku mulai : 16 Juli 2018
	Halaman :

Tanggal Pelaksanaan Evaluasi : 08 Juni 2018 – 16 Juli 2018

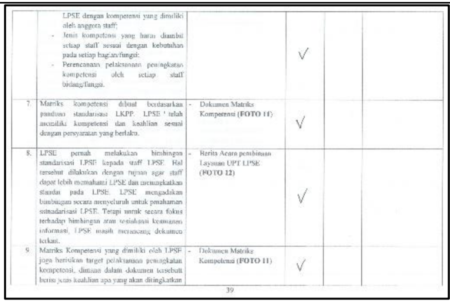
Hasil Evaluasi

No.	Fakta	Bukti	Hasil Evaluasi* Sesuai	Tidak Sesuai	Keterangan/Tambahan
1.	LPSE memiliki dokumen kebijakan layanan dan dokumen kebijakan keamanan informasi, kemudian terdapat dokumen backup data dan dokumen integritas untuk keamanan server.	- Perbup No. 72 mengenai UPT (**FOTO 4**); - Dokumen Kebijakan umum, Layanan dan Keamanan Informasi pada UPT LPSE (**FOTO 1, FOTO 2, FOTO 3**)	√		
2.	LPSE memiliki tugas dan tanggung jawab untuk keamanan informasi, lebih tepatnya pada koordinator keamanan informasi. Dokumen tersebut menjelaskan tentang tugas dan tanggung jawab yang diberikan kepada setiap personil. Selain dari dokumen tersebut, Kepala	- Perbup No. 72 mengenai UPT (**FOTO 4**); - SK pelaksana dan operasional layanan UPT LPSE (**FOTO 6**) - Tugas Pokok dan Fungsi UPT LPSE (**FOTO 7**)	√		



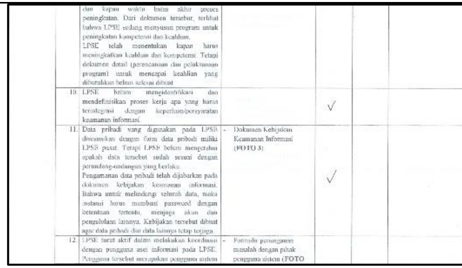
	Diskominfo juga telah menyetujui dan mengeluarkan SK sebagai bukti peresmian LPSE dan anggota staff pada LPSE.				
3.	LPSE telah memiliki SK pembentukan tim anggota LPSE, kemudian LPSE juga telah memiliki dokumen tugas dan tanggung jawab dalam unit LPSE. Setiap anggota LPSE memiliki lebih dari satu kewenangan yang dipegang.	- SK pelaksana dan operasional layanan UPT LPSE (**FOTO 6**) - Tugas Pokok dan Fungsi UPT LPSE (**FOTO 7**)	√		
4.	LPSE memiliki form pencatatan kapasitas yang dirancang untuk seluruh bagian dan fungsi pada LPSE. Selain dari form pencatatan kapasitas tersebut, LPSE juga membuat SOP pengelolaan kapasitas agar kapasitas yang sudah dialokasikan digunakan secara optimal. Kemudian LPSE juga melakukan evaluasi penggunaan kapasitas yang dijadikan sebagai bahan masukan untuk efektivitas pengelolaan kapasitas LPSE.	- Formulir pencatatan kapasitas (**FOTO 8**) - SOP pengelolaan Kapasitas (**FOTO 9**) - Dokumen laporan evaluasi dan tindak lanjut pengelolaan kapasitas (**FOTO 10**)	√		
5.	LPSE belum pernah menentukan keperluan setiap bagian dan dilakukan pemisahan kewenangan. LPSE juga belum pernah menentukan kebutuhan audit internal.		√		
6.	LPSE telah membuat dokumen kompetensi dimana dokumen tersebut berisi: - Perbandingan kebutuhan kompetensi	- Dokumen Matriks Kompetensi (**FOTO 11**)	·		

38



	LPSE dengan kompetensi yang dimiliki oleh anggota staff; - Jenis kompetensi yang harus diambil setiap staff sesuai dengan kebutuhan pada setiap bagian/fungsi; - Perencanaan pelaksanaan peningkatan kompetensi oleh setiap staff bidang/fungsi.		√		
7.	Matriks kompetensi dibuat berdasarkan panduan standarisasi LKPP. LPSE ' telah memiliki kompetensi dan keahlian sesuai dengan persyaratan yang berlaku.	- Dokumen Matriks Kompetensi (**FOTO 11**)	√		
8.	LPSE pernah melakukan bimbingan standarisasi LPSE kepada staff LPSE. Hal tersebut dilakukan dengan tujuan agar staff dapat lebih memahami LPSE dan meningkatkan standar pada LPSE. LPSE mengadakan bimbingan secara menyeluruh untuk pemahaman standarisasi LPSE. Tetapi untuk secara fokus terhadap bimbingan atau sosialisasi keamanan informasi, LPSE masih merancang dokumen terkait.	- Berita Acara pembinaan Layanan UPT LPSE (**FOTO 12**)	√		
9.	Matriks Kompetensi yang dimiliki oleh LPSE juga berisikan target pelaksanaan peningkatan kompetensi, dimana dalam dokumen tersebut berisi jenis keahlian apa yang akan ditingkatkan	- Dokumen Matriks Kompetensi (**FOTO 11**)	√		

39



	dan kapan waktu batas akhir proses peningkatan. Dari dokumen tersebut, terlihat bahwa LPSE sedang menyusun program untuk peningkatan kompetensi dan keahlian. LPSE telah menentukan kapan harus meningkatkan keahlian dan kompetensi. Tetapi dokumen detail (perencanaan dan pelaksanaan program) untuk mencapai keahlian yang dibutuhkan belum selesai dibuat				
10.	LPSE belum mengidentifikasi dan mendefinisikan proses kerja apa yang harus terintegrasi dengan keperluan/persyaratan keamanan informasi.		√		
11.	Data pribadi yang digunakan pada LPSE disesuaikan dengan form data pribadi milik LPSE pusat. Tetapi LPSE belum mengetahui apakah data tersebut sudah sesuai dengan perundang-undangan yang berlaku. Pengamanan data pribadi telah dijabarkan pada dokumen kebijakan keamanan informasi. Bahwa untuk melindungi seluruh data, maka instansi harus membuat password dengan ketentuan tertentu, menjaga akun dan pengelolaan lainnya. Kebijakan tersebut dibuat agar data pribadi dan data lainnya tetap terjaga.	- Dokumen Kebijakan Keamanan Informasi (**FOTO 3**)	√		
12.	LPSE turut aktif dalam melakukan koordinasi dengan pengguna aset informasi pada LPSE. Pengguna tersebut merupakan pengguna sistem	- Formulir penanganan masalah dengan pihak pengguna sistem (FOTO			

	LPSE. Biasanya, komunikasi yang dilakukan jika terdapat permasalahan pada LPSE. Permasalahan tersebut masuk ke dalam bagian helpdesk dan akan diselesaikan bagian administrasi sistem elektronik jika menyangkut teknis sistem. Data pengguna yang diberikan kepada LPSE valid karena dilakukan tahap verifikasi dan validasi data. Tahap validasi tersebut telah disetujui oleh LPSE pusat terlebih dahulu.	13) - Dokumen perjanjian kerahasiaan (FOTO 14)	√		
13	Menurut narasumber, LPSE selalu berkodinasi dengan LKPP terkait standarisasi LKPP, tetapi belum terdapat hasil koordinasi tersebut. LPSE hanya memiliki surat keterangan mengenai himbauan kepada LPSE untuk melakukan standarisasi. LPSE pernah melakukan perjanjian kerahasiaan dengan salah satu anggota Diskominfo untuk melakukan pertukaran informasi.	- Surat Keterangan Sndarisasi LKPP (FOTO 15) - Dokumen perjanjian kerahasiaan (FOTO 14)	√		
14	LPSE memiliki dokumen layanan yang berisikan tugas dan tanggung jawab koordinator kelangsungan layanan.	- Dokumen organisasi Layanan pada bagian kordinator kelangsungan layanan (FOTO 16)	√		
15	LPSE hanya melaporkan keadaan keamanan informasi jika ditanya oleh pimpinan instansi. LPSE belum pernah melaporkan kondisi keamanan informasi kepada pimpinan instansi secara resmi dan rutin.		√		

41

16	LPSE belum mengaitkan kondisi permasalahan keamanan informasi dengan hubungan bagian konsideran dan proses pengambilan keputusan strategis.		√		
17.	LPSE tidak memiliki program khusus untuk mematuhi tujuan kepatuhan pengamanan informasi.		√		
18.	LPSE tidak memiliki proses pengukuran kinerja, metriks beserta parameternya		√		
19	LPSE tidak menerapkan program perbaikan kinerja		√		
20	LPSE belum menetapkan target dan sasaran pengelolaan keamanan informasi		√		
21	LPSE belum mengidentifikasi kaitan dengan keamanan informasi yang harus dipatuhi		√		
22	LPSE belum mendefinisikan kebijakan dan langkah penanggulangan insiden		√		
Saran untuk perbaikan :					

*Sesuai dengan kondisi terkini pada UPT LPSE

Menyetujui,
Bagian Administrasi Sistem Informasi LPSE

Muhammad Ainul Yaqin, S.Kom

42

LEMBAR PENGESAHAN

"Setelah menimbang, membaca dan meneliti hasil yang dimaksud dalam laporan Evaluasi dan Rekomendasi Keamanan Informasi berdasarkan Indeks Keamanan Informasi (Indeks KAMI) yang telah dilaksanakan oleh peneliti dan evaluator Isnaini Nur, maka dokumen ini telah menjadi dokumen hasil evaluasi keamanan informasi UPT LPSE Gresik"

Gresik, 19 Juli 2018

Menyetujui, Kepala Dinas Komunikasi dan Informatika Gresik	Pelaksana,
Budi Raharjo, S.H NIP. 19680921 198809 1 001	Isnaini Nur Rohmawati