TUGAS AKHIR – KS 141501

EVALUASI KEPATUHAN IMPLEMENTASI MANAJEMEN KEAMANAN INFORMASI PADA PENYELENGGARA SISTEM ELEKTRONIK DENGAN TINGKAT KEMATANGAN REAKTIF TERHADAP INDEKS KEAMANAN INFORMASI SNI ISO/IEC 27001

EVALUATION OF COMPLIANCE INFORMATION SECURITY MANAGEMENT IMPLEMENTATION IN ELECTRONIC SYSTEMS IMPLEMENTERS WITH REACTIVE MATURITY LEVEL TOWARD INDEKS KEAMANAN INFORMASI SNI ISO/IEC 27001

Arymasu Godhein Ndoen
NRP 052 1144 0000 015

Dosen Pembimbing
Ir. Khakim Ghozali, M.MT

Departemen Sistem Informasi
Fakultas Teknologi Informasi dan Komunikasi
Institut Teknologi Sepuluh Nopember
Surabaya 2018

TUGAS AKHIR – KS 141501

EVALUASI KEPATUHAN IMPLEMENTASI MANAJEMEN KEAMANAN INFORMASI PADA PENYELENGGARA SISTEM ELEKTRONIK DENGAN TINGKAT KEMATANGAN REAKTIF TERHADAP INDEKS KEAMANAN INFORMASI SNI ISO/IEC 27001

Arymasu Godhein Ndoen
052 1144 0000 015

Dosen Pembimbing
Ir. Khakim Ghozali, M.MT

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

FINAL PROJECT – KS 141501

EVALUATION OF COMPLIANCE INFORMATION SECURITY MANAGEMENT IMPLEMENTATION IN ELECTRONIC SYSTEMS ORGANIZERS WITH REACTIVE MATURITY LEVEL TOWARD INDEKS KEAMANAN INFORMASI SNI ISO/IEC 27001

Arymasu Godhein Ndoen
052 1144 0000 015

Supervisor :
Ir. Khakim Ghozali, M.MT

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

LEMBAR PENGESAHAN

EVALUASI KEPATUHAN IMPLEMENTASI MANAJEMEN KEAMANAN INFORMASI PADA PENYELENGGARA SISTEM ELEKTRONIK DENGAN TINGKAT KEMATANGAN REAKTIF TERHADAP INDEKS KEAMANAN INFORMASI SNI ISO/IEC 27001

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 :

ARYMASU GODHEIN NDOEN
052 1144 0000 015

Surabaya, Juni 2018

KEPALA
DEPARTEMEN SISTEM INFORMASI

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

LEMBAR PERSETUJUAN

EVALUASI KEPATUHAN IMPLEMENTASI MANAJEMEN KEAMANAN INFORMASI PADA PENYELENGGARA SISTEM ELEKTRONIK DENGAN TINGKAT KEMATANGAN REAKTIF TERHADAP INDEKS KEAMANAN INFORMASI SNI ISO/IEC 27001

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 :

ARYMASU GODHEIN NDOEN
052 1144 0000 015

Disetujui Tim Penguji: Tanggal Ujian : 03 Juli 2018

Periode Wisuda : September 2018

Ir. Khakim Ghozali, M.MT **(Pembimbing 1)**

Hanim Maria Astuti, S.Kom., M.Sc. **(Penguji 1)**

Dr. Apol Pribadi Subriadi, S.T., MT. **(Penguji 2)**

“Halaman ini sengaja dikosongkan”

EVALUASI KEPATUHAN IMPLEMENTASI MANAJEMEN KEAMANAN INFORMASI PADA PENYELENGGARA SISTEM ELEKTRONIK DENGAN TINGKAT KEMATANGAN REAKTIF TERHADAP INDEKS KEAMANAN INFORMASI SNI ISO/IEC 27001

Nama Mahasiswa : Arymasu Godhein Ndoen

NRP : 052 1144 0000 015

Departemen : Sistem Informasi FTIK-ITS

Dosen Pembimbing 1 : Ir. Khakim Ghozali, M.MT

ABSTRAK

Perkembangan teknologi yang pesat membantu berbagai kalangan masyarakat dalam berbagai bidang kehidupan. Hal itu terbukti dari penggunaan telepon genggam di Indonesia sebesar 371,4 juta per Januari 2017 (Databooks, Katadata) dan penggunaan komputer sebesar 92% (Survei Kominfo) pada perusahaan di Indonesia untuk mendukung proses bisnisnya. Namun tidak disadari seiring perkembangan teknologi maka memungkinkan kerentanan dan ancaman yang timbul terhadap keamanan informasi. Untuk itu diperlukanlah penerapan standar keamanan informasi yaitu SNI ISO/IEC 27001 dalam mengelola sistem manajemen keamanan informasi suatu lembaga penyelenggara sistem elektronik. Sebelum menerapkan standar, penyelenggara sistem elektronik perlu melakukan penilaian terhadap kesiapannya menerapakan SNI. Untuk itu dilakukanlah evaluasi dengan Indeks KAMI untuk mengetahui kondisi terkini dari lembaganya. Namun setelah

dilakukan penilaian sering kali didapati permasalahan bahwa lembaga penyelenggara sistem elektronik belum siap dalam menerapkan SNI ISO/IEC 27001.
Berangkat dari permasalahan ketidaksiapan penyelenggara sistem elektronik maka dilakukanlah analisis kesenjangan hasil poin pertanyaan terhadap penerapan evaluasi Indeks KAMI pada lembaga penyelenggara sistem elektronik dengan tingkat kematangan reaktif..
Hasil dari analisis kesenjangan yang dilakukan diketahui bahwa ada 11 indikator pertanyaan yang memiliki kesenjangan diatas 7. Ada 7 pada area kerangka kerja, 2 pada area risiko, 1 pada area tata kelola dan 1 dari area teknologi. Hal ini berarti penyelenggara sistem elektronik memiliki masalah besar dalam proses pengelolaan proses pengamanan informasinya terkait kepatuhan pada kerangka kerja yang digunakan. Hasil analisis temuan diketahui bahwa ada 33 indikator pertanyan yang berkategori tinggi jika tidak diterapkan berdasarkan kriteria dampak dan probabilitasnya. Dari hasil itu dibuatkanlah rekomendasi berdasarkan SNI ISO/IEC 27001.
Kemudian lewat penelitian ini memberikan gambaran mengenai poin area pada Indeks KAMI yang paling rentan menjadi ancaman yang membuat penyelenggara sistem elektronik belum siap dalam penerapan SNI ISO/IEC 27001. Hasil ini dapat dijadikan evaluasi lebih awal serta memberikan rekomendasi untuk perbaikan keamanan informasi penyelenggara sistem elektronik pada umumnya.

Kata Kunci: Evaluasi, Indeks KAMI, SNI ISO/IEC 27001, Analisis Kesenjangan.

EVALUATION OF COMPLIANCE INFORMATION SECURITY MANAGEMENT IMPLEMENTATION IN ELECTRONIC SYSTEMS ORGANIZERS WITH REACTIVE MATURITY LEVEL TOWARD INDEKS KEAMANAN INFORMASI SNI ISO/IEC 27001

Name **: Arymasu Godhein Ndoen**

NRP **: 052 1144 0000 015**

Department **: Sistem Informasi FTIK-ITS**

Supervisor **: Ir. Khakim Ghozali, M.MT**

ABSTRACT

The rapid development of technology helps various societies in various fields of life. This is proven from the usage of mobile phones in Indonesia amounted to 371.4 million users in January 2017 (Databooks, Katadata) and computer usage 92% (Survey of Kominfo) by companies in Indonesia to support its business processes. However, unconsciously, as technology develops, it enables vulnerabilities and threats to information security. Therefore, it is necessary to apply the information security standard that as SNI ISO / IEC 27001 in managing the information security management system of an electronic system organizing institution. Before applying the standards ,electronic system organizing institution need to make an assessment of their readiness to apply SNI. For that purpose an evaluation is performed with Indeks KAMI to know the current condition of the institution. However, after the assessment is often found the problem that the electronic system organizing institution is not ready to apply SNI ISO / IEC 27001.

Because problem of unreadiness electronic system organizer institution, this theses will performing a gap analysis of the research result of question indicator on the implementation of Index KAMI on electronic system organizer institution with reactive maturity level.
The results of the gap analysis show that there are 11 question indikator that have gaps above 7. There are 7 in the framework area, 2 in the risk area, 1 in the governance area and 1 in technology area. This means that the electronic system organizer has a major problem in the process of managing its information security process in relation to compliance with the framework that has been used. The result of the analysis finds that there are indicators that are categorized high if not applied based on the impact and probability criteria. From that result, the recommendations were made based on SNI ISO / IEC 27001.
This theses can provide an overview of the most vulnerable areas of the Index KAMI that can be a threat that makes the electronic system organizer institution not ready in the application of SNI ISO / IEC 27001. These results can be used as an early evaluation and provide recommendations for improving the information security of electronic system organizer institution in generally.

Keyword: Evaluation, Information Security Management System, Indeks KAMI, SNI ISO/IEC 27001, Gap.

KATA PENGANTAR

Puji dan syukur dipanjatkan oleh peneliti atas segala berkat, rahmat, hikmat, pertolongan, kasih dan kekuatan yang diberikan oleh Tuhan Yang Maha Esa. Hanya karena atas seijinnya, peneliti dapat menyelesaikan laporan Tugas Akhir, dengan judul **EVALUASI KEPATUHAN IMPLEMENTASI MANAJEMEN KEAMANAN INFORMASI PADA PENYELENGGARA SISTEM ELEKTRONIK DENGAN TIINGKAT KEMATANGAN REAKTIF TERHADAP INDEKS KEAMANAN INFORMASI SNI ISO/IEC 27001**

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 :

- Ayahanda Marthyn P.M Ndoen dan Ibunda Fransica Sri Hardjani, ST serta kakak maupun adik penulis yang mendoakan dan mendukung penulis untuk segera menyelesaikan tugas akhir ini.
- Para penyeliti yang mengimplementasikan Indeks KAMI yaitu Moch. Rashid Ridho, Luthfiya Ulinnuha, Roodhin Firmana, Endi Lastyono Putra, Mustaqim Siga, Asrani Kasiran, Diah Wardani, Radhifan Hidayat, Winda Septilia, Dedi Wirasasmita yang hasil penelitiannya dijadikan sebagai bahan analisis.
- Bapak Ir. Khakim Ghozali, M.MT selaku dosen pembimbing yang telah meluangkan waktu untuk membimbing dan mendukung dalam penyelesaian tugas akhir ini.
- Bapak Dr. Apol Pribadi Subriadi, ST., MT selaku dosen wali yang senantiasi memberikan pengarahan selam penulis menempuh masa perkuliahan dan pengerjaan tugas akhir ini.

- Bapak Hermono, selaku admin Laboratorium MSI yang membantu pernulis dalam hal administrasi tugas akhir ini.
- Teman – teman Laboratorium MSI dan Osiris yang telah memberikan semangat dala menyelesaikan tugas akhir ini
- Teman – teman dari BALI terkhususnya Doran dan Juli yang memberikan semangat dan menemani penulis saat mengerjakan tugas akhir ini.
- Serta pihak lain yang telah mendukung dan membantu dalam kelancaran penyelesaian tugas akhir ini.

Surabaya, 01 Juni 2018

Penulis

DAFTAR ISI

“Halaman ini sengaja dikosongkan”

DAFTAR TABEL

“Halaman ini sengaja dikosongkan”

DAFTAR GAMBAR

BAB I
PENDAHULUAN

Pada bab pendahuluan ini akan dibahas mengenai latar belakang pengambilan tugas akhir ini, masalah yang ingin diselesaikan pada penelitian ini, batasan dari permasalahan yang diangkat, tujuan dari penelitian ini, manfaat yang didapat dari penelitian ini untuk berbagai pihak, relevansi penelitian ini dengan matakuliah yang ada pada Departemen Sistem Informasi dan sistematika penulisan tugas akhir ini.

1.1. Latar Belakang

Teknologi informasi merupakan sesuatu yang membantu manusia dalam melakukan kegiatan keseharian. Dengan adanya teknologi informasi maka pekerjaan yang dulu membutuhkan waktu yang cukup lama dalam pengerjaannya dapat diselesaikan dalam waktu yang singkat, sebagai contoh komunikasi surat antar wilayah tidak perlu lagi mengirimkan selembar surat fisik dengan adanya e-mail informasi yang ingin kita sampaikan dapat sampai dalam hitungan detik saja. Penggunaan teknologi memang membantu mempermudah kegiatan harian maupun menyederhanakan proses bisnis. Lewat pemanfaatan teknologi informasi perusahaan – perusahaan akan dengan mudah memperoleh keuntungan bisnisnya. Dari survei yang dilakukan Kementerian Komunikasi dan Informatika mengenai penggunaan teknologi informasi dan komunikasi di sektor bisnis pada tahun 2011 menunjukkan bahwa 92 % perusahaan di Indonesia menggunakan komputer sebagai pendukung keberlangsungan bisnisnya dan 86 % perusahaan telah memanfaatkan internet. Dari survei ini kita mengetahui bahwa ketergantungan terhadap penggunaan teknologi informasi sangat besar dari hasil pemanfaatan teknologi informasi yang dilakukan oleh perusahaan [1].

Ketergantungan yang besar terhadap teknologi informasi menimbulkan kesadaran akan celah keamanan yang dapat menimbulkan kehilangan data atau perusakan dari pihak luar perusahaan atau organisasi yang dapat mengganggu keberlangsungan proses bisnis. Maka dari itu diperlukan pengelolaan keamanan teknologi dan sistem informasi yang menganggap keamanan teknologi informasi sebagai aset yang harus memiliki perlindungan yang tepat yang mana memenuhi kaidah *CIA* diantaranya *Confidentiality* atau kerahasiaan yang memastikan informasi yang ada diakses oleh orang yang memiliki otoritas, *Integrity* atau integritas yang memastikan informasi yang ada sesuai dengan kenyataan dimana tidak adanya perubahan informasi untuk kepentingan perorangan kemudian *Availability* atau ketersediaan yang memastikan teknologi informasi tersedia pada waktu yang dibutuhkan [2].

Dalam memastikan keamanan informasi Kementerian Komunikasi dan Informatika mengeluarkan suatu alat yang digunakan untuk mengetahui tingkat kematangan dan tingkat penerapan ISO/IEC 27001 dimana versi terakhirnya dikeluarkan pada tahun 2015 (Versi 3.1) dengan mengacu pada ISO/IEC 27001:2013. Dengan adanya alat ini akan membantu mengetahui kondisi kesiapan kerangka kerja kemanan informasi organisasi. Untuk mengetahui kondisi kesiapan, Indeks KAMI 3.1 membagi menjadi beberapa area yang berisikan pertanyaan yang mencakup area tersebut. Adapun area yang pertama adalah Kategori Sistem Elektronik yang digunakan instasi atau organisasi, Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset Informasi dan Teknologi dan Keamanan Informasi [3].

Oleh karena manfaat yang didapatkan lewat penggunaan Indeks KAMI maka sudah banyak penerapan yang dilakukan untuk mengetahui kesiapan instansi/organisasi dalam penerapan kerangka kerja kemanan informasi dalam beberapa tahun.

Adapun penelitian yang dilakukan oleh Ridho pada tahun 2012 mengenai "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" yang mana menggunakan Indeks KAMI versi 2.3 yang mengacu pada SNI ISO/IEC 27001:2009 [8], kemudian ada penelitian yang dilakukan oleh Luhfiya pada 2012 yang melakukan penilaian Indeks KAMI pada DPTSI ITS Sub Bagian Jaringan dengan menggunakan Indeks KAMI versi 2.3 [9]. Kemudian selain di perguruan tinggi ada juga penelitian yang dilakukan oleh Rodhin (2013) yang melakukan evaluasi dengan Indeks KAMI pada BUMN PT.PLN Distribusi Jawa Timur [10].

Untuk itu pada tugas akhir ini tidak akan melakukan penerapan secara langsung Indeks KAMI melainkan melakukan evaluasi kepatuhan penelitian yang menerapkan Indeks KAMI pada tingkat kematangan reaktif untuk mengetahui kondisi instansi atau lembaga penyelenggara sistem elektronik dan melihat poin pertanyaan pada Indeks KAMI yang rata – rata tidak diterapkan oleh instansi pada penelitian yang dilakukan. Perbandingan dilakukan dengan analisis *gap* antara jawaban setiap penelitian – penelitian terhadap pertanyaan Indeks KAMI dengan hasil jawaban ideal yang diharapkan. Lewat tugas akhir ini diharapkan akan memberikan sejauh mana penerapan keamanan informasi instansi penyelenggara sistem elektronik dan dapat memberikan saran perbaikan mengenai poin – poin pernyataan yang menjadi permasalahan yang dialami instansi – instansi di Indonesia pada umumnya.

1.2. Perumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan pada bagian sebelumnya, maka rumusan masalah yang akan diselesaikan pada tugas akhir ini adalah sebagai berikut:

1. Apa poin area pada Indeks KAMI yang paling rentan menjadi masalah yang membuat lembaga penyelenggara sistem elektronik dengan tingkat kematangan reaktif belum siap dalam menerapkan SNI ISO/IEC 27001?
2. Bagaimana rekomendasi perbaikan yang diperlukan oleh lembaga penyelenggara sistem elektronik dengan tingkat kematangan reaktif untuk memperbaiki manajemen keamanan informasi?

1.3. Batasan Masalah

Dari permasalahan yang disebutkan adapun batasan masalah dalam penyelesaian tugas akhir ini adalah sebagai berikut:

- Tugas akhir ini melakukan evaluasi terhadap Penelitian yang menggunakan Indeks KAMI versi 2.3 pada tingkat kematangan reaktif.
- Evaluasi pertanyaan yang dilakukan berdasarkan area Indeks KAMI, adalah :
  a. Tata Kelola
  b. Risiko
  c. Kerangka Kerja
  d. Pengelolaan Aset
  e. Teknologi

1.4. Tujuan Tugas Akhir

Berdasarkan rumusan dan batasan masalah, adapun tujuan tugas akhir ini adalah :

1. Mengetahui poin area pada Indeks KAMI yang paling rentan menjadi masalah yang membuat lembaga penyelenggara sistem elektronik dengan tingkat kematangan reaktif belum siap dalam menerapkan SNI ISO/IEC 27001
2. Memberikan rekomendasi perbaikan yang diperlukan oleh lembaga penyelenggara sistem elektronik untuk memperbaiki manajemen keamanan informasi

1.5. Manfaat Tugas Akhir

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

1. Bagi Akademisi
   Sebagai referensi penelitian mengenai evaluasi penerapan Indeks KAMI pada lembaga penyelenggara sistem elektronik.
2. Bagi Instansi atau Penyelenggara Sistem Elektronik
   Mengetahui poin area pada Indeks KAMI yang paling rentan menjadi ancaman yang membuat instansinya belum siap dalam penerapan kerangka kerja sehingga dapat dijadikan evaluasi lebih awal untuk perbaikan.

1.6. Relevansi Tugas Akhir

Tugas akhir ini berkaitan dengan mata kuliah Keamanan Aset Informasi untuk mengetahui area mana yang menjadi titik kelemahan penerapan teknologi informasi, Tata Kelola Teknologi Informasi pada pemahaman mengenai pembuatan tata kelola dalam memahami penilaian tata kelola pada Indeks

KAMI , Manajemen Risiko dalam memahami risiko yang mungkin muncul dalam penerapan teknologi informasi, Kemudian Audit SI dalam melakukan evaluasi untuk menemukan temuan dan memberikan rekomendasi terhadap temuan tersebut. Topik pada tugas akhir ini berdasarkan ranah penelitian Laboratorium Manajemen Sistem Informasi (MSI).

1.7. Sistematika Penulisan

Dalam penulisan pada tugas akhir ini, sistematikanya dibagi menjadi 5 bab sebagai berikut :

BAB I: PENDAHULUAN

Pada bab ini akan berisikan pendahuluan mengenai latar belakang masalah yang diangkat, rumusan dari permasalahan, batasan – batasan permasalahan, tujuan tugas akhir yang menjawab permasalahan, manfaat yang didapat dari tugas akhir ini, relevansi tugas akhir ini dengan mata kuliah di Departemen Sistem Informasi beserta sistematika penulisan

BAB II: TINJAUAN PUSTAKA

Pada bab ini akan berisikan penilitian yang dilakukan sebelumnya yang berkaitan dengan tugas akhir ini dan dasar teori yang digunakan untuk mendukung tugas akhir ini.

BAB III: METODOLOGI

Pada bab ini membahas alur metodologi yang digunakan untuk mengerjakan tugas akhir ini, dimana diberikan penjelasan secara singkat mengenai metode yang digunakan.

BAB IV: PERANCANGAN

Pada bab ini dilakukan penjelasan yang lebih dalam mengenai objek yang diangkat kemudian dan metode pengumpulan data serta rancangan hasil akhir yang diharapkan.

BAB IV: IMPLEMENTASI

Pada bab ini dilakukan penjelasan mengenai data yang diambil, metode pengambilan yang digunakan dan hambatan yang dihadapi saat pengumpulan data.

BAB V: HASIL DAN PEMBAHASAN

Pada bab ini berisikan pembahasan proses evaluasi perbandingan yang dilakukan terhadap penelitian yang menerapkan Indeks KAMI pada tingkat kematangan reaktif sehingga diketahui gap yang ada antar penelitian serta pemberian rekomendasi terhadap poin area yang menjadi masalah bagi penyelenggara sistem elektronik.

BAB VI: KESIMPULAN DAN SARAN

Pada bab ini berisi kesimpulan akhir dari serangkaian proses penelitian tugas akhir dan pemberian saran untuk perbaikan ataupun penelitian lanjutan yang memiliki topik yang sama.

“Halaman ini sengaja dikosongkan”

BAB II
TINJAUAN PUSTAKA

Bagian ini akan memberikan penjelasan mengenai penelitian maupun studi literatur sebelumnya yang berkaitan dan dijadikan sebagai acuan selama pengerjaan tugas akhir, serta landasan teori yang berkaitan dengan tugas akhir yang dapat membantu pemahaman selama pengerjaan tugas akhir ini.

2.1. Penelitian Sebelumnya

Terdapat beberapa penelitian serupa yang telah dilakukan sebelumnya. Penelitian tersebut digunakan sebagai bahan kajian dalam membangun tujuan, permasalahan, metodologi, dan hasil tugas akhir. Berikut adalah tabel 2.1 yang menjelaskan penelitian terkait yang sudah dilakukan sebelumnya:

Tabel 2 1. Daftar Penelitian Sebelumnya

Evaluasi Kinerja Aplikasi Indeks Pengajaran Dosen dengan Menggunakan *Gap* Analisis [5]	
Nama Penulis	Dimas Prayogo
Tahun Penelitian	2013
Deskripsi umum penelitian	Penelitian ini memiliki tujuan untuk melihat apakah aplikasi IPD saat ini sudah benar – benar efektif dan sesuai dengan tujuan bisnisnya. Penelitian dilakukan dengan menyebarkan kuisioner kepada

	pengguna aplikasi dengan berdasarkan indikator DeLone & McLean (D&M)
Hasil penelitian	Hasil penelitian ini berupa penilaian *gap* berupa perbandingan antara keadaan yang diharapkan dengan keadaan saat ini berdasarkan indikator DeLone & McLean (D&M)
Keterkaitan peneliatian	Penelitian ini memiliki bahasan yang hampir sama yaitu perbandingan. Namun pada penelitian ini membandingkan hasil responden berdasarkan indikator DeLone & McLean (D&M) sedangkan pada tugas akhir ini akan membandingkan hasil penilaian yang dilakukan dengan 5 area Indeks KAMI
Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 Pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya [6]	
Nama Penulis	Firzah Abdullah Basyarahil
Tahun Penelitian	2017

Deskripsi umum penelitian	Penelitian ini dilakukan untuk meningkatkan kualitas penyelenggaraan keamanan informasi yang dilakukan pada DPTSI. Peningkatan kualitas dilakukan dengan cara mengukur tingkat kematangan dan kelengkapan keamanan informasi DPTSI menggunakan Indeks KAMI versi 3.1 yang merujuk pada standar ISO/IEC 27001 : 2013.
Hasil penelitian	Dari hasil penilaian yang dilakukan dengan Indeks KAMI versi 3.1 didapatkan skor sebesar 249 dari total skor 645 yang membuat DPTSI masih dikategorikan tidak layak untuk menerapkan ISO/IEC 27001.
Keterkaitan peneliatian	Penelitian ini merupakan penelitian terbaru mengenai Indeks KAMI yang dilakukan oleh peneliti ITS sehingga dijadikan acuan dalam memahami langkah pengukuran tingkat kematangan dan kelengkapan keamanan informasi.

Analisa Kesenjangan dan Dampak Perubahan Proses Bisnis Finansial Accounting Berdasarkan Best Pracice SAP (Studi Kasus: PT. Perkebunan Nusantara XI) [7]	
Nama Penulis	Rizki Fadhil Syahrial
Tahun Penelitian	2017
Deskripsi umum penelitian.	Penelitian ini bertujuan untuk mengetahui dampak perubahan yang terjadi pada proses bisnis finansial accounting dengan melakukan perbandingan kesenjangan ketika SAP itu belum diterapkan dengan kondisi harapan sesuai *best practice* SAP.
Hasil penelitian	Hasil penelitian berupa hasil analisa kesenjangan antara model proses bisnis finansial yang dibandingkan dengan model proses bisnis finansial yang berdasarkan *best practice* SAP yang berguna sebagai rekomendasi dalam penerapan SAP.
Keterkaitan peneliatian	Perbandingan ini memiliki bahasan yang sama yaiitu melakukan analisis *gap* antara *AS IS* (kondisi saat ini) dengan

	TO BE (kondisi yang diharapkan).

2.2. Dasar Teori

Bagian ini akan membahas teori dan konsep yang berkaitan dengan penelitian tugas akhir ini.

2.2.1. Evaluasi

Evaluasi merupakan suatu proses dalam dunia manajemen untuk menilai sejauh mana penerapan proses manajemen yang dilakukan sehingga dapat dilakukan perbaikan yang berkelanjutan. Menurut KBBI evaluasi merupakan proses pengumpulan dan pengamatan dari berbagai macam bukti untuk mengukur dampak dan efektivitas dari suatu objek, program, atau proses berkaitan dengan spesifikasi dan persyaratan pengguna yang telah ditetapkan sebelumnya. Evaluasi sering diartikan sebagai audit, padahal kedua hal ini merupakan dua hal yang cukup berbeda. Evaluasi merupakan satu kesatuan dalam proses manajemen sedangkan audit bersifat independen diluar proses manajemen. Pada umumnya evaluasi melakukan penilaian terhadap proses yang telah berlangsung. Sedangkan audit lebih ke pencarian temuan terhadap suatu proses kemudian memberikan rekomendasi perbaikan. Menurut Federica Calidoni ada 4 tahap dalam melakukan evaluasi [21]. Adapun tahapannya adalah :

1. Mengidentifikasi tujuan
   Pada tahapan ini dilakukan pengidentifikasikan terhadap tujuan melakukan evaluasi contohnya seperti meningkatkan efektivitas atau untuk pengukuran kinerja.

2. Mendefinisikan permasalahan
   Setelah tujuan didefinisikan dengan jelas maka ditentukan cakupan dari evaluasi permasalahan yang diangkat. Apakah masalah yang ingin diselesaikan bersekala kecil, sedang ataupun besar.
3. Menentukan model
   Pada bagian ini dilakukan perancangan terhadap evaluasi yang akan dilakukan. Hal ini dilakukan untuk memastikan setiap kegiatan yang dilakukan sudah dalam perencanaan yang matang.
4. Menentukan metode evaluasi
   Penentuan metode evaluasi dilakukan ketika rancangan evaluasi sudah dibuat berdasarkan tujuan dan permasalahan yang ingin diselesaikan. Secara garis besar ada 2 metode evaluasi yaitu kualitatif dan kuantitatif.

Pemilihan metode yang tepat untuk evaluasi sangat dibutuhkan. Hal ini akan mendukung dalam menyelesaikan permasalahan yang ada dengan cara yang tepat. Berikut dijelaskan beberapa metode evaluasi secara kualitatif [21]:

- *Analytic induction*
  Metode evaluasi yang mengacu pada pemeriksaan secara sistematis antara bebagai fenomena sosial dalam kategori tertentu untuk mengembangkan suatu konsep atau ide.
- *Focus groups*
  Bentuk evaluasi secara interaktif dimana sekelompok orang dimintai pendapatnya mengenai suatu topik tertentu. Topiknya bisa berupa produk, konsep, ide, dan hal lainnya yang ingin dievaluasi.
- *Ethnography*
  Metode evaluasi dengan melakukan pengamatan secara langsung perilaku sehari – hari, percakapan, serta wawancara yang mendalam.

- *Participant observation*
  Merupakan metode evaluasi dengan menjalin keakraban dengan objek observasi sengan keterlibatan langsung pada lingkungan sekitar.

Metode kuantitatif adalah metode yang menggunakan perangkat perhitungan untuk mengevaluasi [21]. Adapun beberapa metode evaluasi secara kuantitatif adalah :

- *Statistical surveys*
  Metode evaluasi dengan mengumpulkan informasi yang berguna di berbagai bidang
- *Content or textual analysis (Holsti)*
  Merupakan teknik evaluasi untuk membuat kesimpulan secara obyektif dan sistematis yang memungkinkan peneliti memasukkan sejumlah besar informasi tekstual dan mengidentifikasi secara sistematis sifat-sifatnya dengan mendeteksi struktur komunikasi konten yang lebih penting.
- *Statistical descriptive techniques*
  Merupakan teknik statistik yang terdiri dari deskripsi diagram, deskripsi tabular dan deskripsi parametrik..
- *Statistical inferential techniques*
  Teknik evaluasi yang melibatkan generalisasi sampel ke seluruh populasi dan melakukan pengujian hipotesis.

2.2.2. Keamanan Iinformasi

Perkembangan teknologi informasi dimulai dari era perkembangan teknologi komputer dimana mulai dilakukan pengembangan komputer untuk membantu kegiatan manusia baik komunikasi dan perang. Kemudian pada awal tahun 1960 sudah mulai ada perusahaan yang mengadopsi komputer canggih untuk kegiatan administratif yang menanadakan sudah

mulai memasuki era komputerisasi. Penggunaan komputer pada era ini ditujukan untuk efisiensi, hal ini dapat dilihat dari pekerjaan tertentu yang jauh lebih efisien dari segi waktu dan biaya daripada memperkerjakan puluhan SDM. Kemudian masuk pada awal tahun 1970 an mulai diperkenalkan Personal Computer yang menyediakan paket komputer secara ringkas yang ditaruh diatas meja sehingga dapat memudahkan pihak eksekutif untuk memperoleh informasi dengan cepat serta melakukan pengolahan data. Setelah itu dunia teknologi informasi memasuki era keempat yaitu era globalisasi informasi. Pada era ini perkembangan teknologi sangat cepat melebihi kemampuan manusia untuk memanfaatkannya. Informasi yang disalurkan dari satu negara ke negara lain dapat sampai dalam hitungan detik sehingga dapat dipastikan bahwa batas fisik antar negara tidak ada lagi dengan pemanfaatan teknologi seperti internet [19]. Hal ini pun yang membuat perlu adanya perhatian khusus pada perkembangan keamanan informasi terkait perkembangannya yang begitu cepat dan akses yang sebebas – bebasnya. Menurut ISO/IEC 27001 keamanan informasi adalah memastikan bahwa informasi itu tetap terjaga kerahasiaannya, ketersediaannya, dan integritasnya [2]. Ketiga hal yang harus dijaga itu merupakan karakteristik dari keamanan informasi, adapun penjelasan ketiganya adalah sebagai berikut :

1. Kerahasiaan, merupakan upaya yang digunakan untuk mencegah pengungkapan informasi penting baik itu milik perseorangan maupun organisasi ke individu ataupun sistem yang tidak sah.
2. Ketersediaan, berarti memastikan informasi atau teknologi yang ingin disampaikan dari suatu sistem haruslah tersedia saat dibutuhkan.
3. Integritas, merupakan istilah yang menyatakan bahwa data tidak boleh dimodifikasi tanpa persetujuan dari pihak yang memiliki otoritas [20].

Menurut Riyanarto (2009) keamanan informasi dapat dibagi menjadi 5 bagian berdasarkan fokus dan kebutuhannya [22]. Adapun macam – macam keamanan informasi adalah :

1. *Pysical Se*curity
   Keamanan informasi ini berfokus pada strategi untuk mengamanankan aset fisik berupa orang, barang fisik, dokumen fisik, dan ruang kerja dari ancaman seperti bencana alam yang memungkinkan kehilangan informasi penting perusahaan.
2. *Personal Security*
   Kemanan informasi ini berfokus pada cara pengamanan personil yang menjadi komponen informasi perusahaan.
3. *Operation Security*
   Pada bagian ini berfokus pada strategi pengamanan organisasi untuk menjaga *capability* organisasi dari gangguan yang dapat mengganggu keberlangsungan bisnisnya.
4. *Communication Security*
   Fokus pada keamanan informasi ini berpusat pada media komunikasi yang digunakan organisasi untuk mencapai tujuan bisnisnya.
5. *Network Security*
   Keamanan informasi ini berpusat pada pengamanan jaringan dari adanya ancaman pihak yang tidak bertanggungjawab untuk mensabotase atau mengganggu jaringan hingga tidak bisa dimanfaatkan sebagaimana mestinya.

Keamanan informasi sangat terkait dengan komponen teknologi informasi. Hal ini dikarenakan dengan adanya pengelolaan keamanan informasi yang baik akan membantu dalam menjaga sumber daya perusahaan (komponen teknologi informasi) maupun menjaga keberlangsungan bisnis perusahaan. Dalam

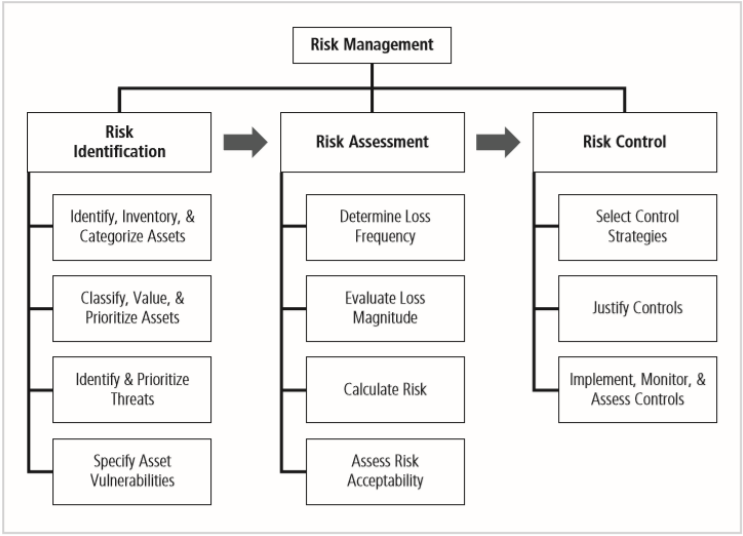
buku Sistem Manajemen Keamanan Informasi, Riyanarto mengatakan bahwa perlindungan yang dilakukan terhadap aset dan komponen informasi dilakukan untuk memenuhi aspek keamanan informasi [22]. Adapun aspek – aspek keamanan informasi dijelaskan sebagai berikut :

1. Privacy
   Informasi yang dimiliki oleh organisasi atau perusahaan bersifat rahasia dan digunakan untuk tujuan tertentu saja. Dengan adanya privacy maka akan menjaga keamanan informasi dari orang yang tidak memiliki wewenang.
2. Identification
   Dengan adanya aspek *identification* akan membantu melakukan pengenalan terhadap pihak yang ingin meminta hak akses.
3. Authentication
   Aspek ini membuktikan bahwa pengguna yang meminta hak akses adalah memang benar yang memiliki identitas.
4. Authorization
   Pada aspek ini dilakukan proses yang memberikan jaminan bahwa pengguna merupakan pengguna yang telah di autorisasi secara spesifik untuk melakukan fungsi *create, read, update* dan *delete* informasi.
5. Accountability
   Aspek ini dipenuhi ketika sistem dapat menampilkan semua kegiatan yang telah dilakukan terhadap informasi dan siapa yang bertanggung jawab terhadap kegiatan tersebut.

2.2.3. Manajemen Risiko Teknologi Informasi

Manajemen risiko teknologi informasi merupakan kesatuan proses untuk mengelola risiko yang berguna untuk melindungi aset teknologi informasi dari ancaman yang datang dari dalam maupun luar organisasi sehingga dapat memastikan proses bisnis dapat tetap berlangsung. Secara garis besar, manajemen

risiko merupakan proses yang terdiri dari pengidentifikasian risiko, penilaian tingkat risiko dan langkah penanggulangannya [23]. Oleh sebab itu dapat dikatakan bahwa komponen manajemen risiko terdiri dari 3 bagian yaitu *risk identification, risk assesment* dan *risk control* seperti pada gambar 2.1 di bawah ini.



Gambar 2 1. Komponen Risk Management [23]

Manajemen risiko yang baik dilakukan dengan melakukan pengidentifikasian aset yang dimiliki organisasi dan menspesifikasikan apa saja ancaman yang mungkin mengganggu aset. Kemudian dilanjutkan dengan perhitungan dampak terhadap ancaman yang mungkin terjadi sehingga dapat diketahui nilai dari risiko yang telah dispesifikasikan. Setelah itu dilanjutkan dengan pemilihan upaya kendali yang tepat untuk menangani risiko untuk menjadi bisnis tetap

berlangsung. Ada 5 strategi kontrol yang bisa dilakukan untuk mengendalikan risiko [23], diantranya :

1. Defense
   Strategi pengendalian risiko yang mencoba menghilangkan dan mengurangi risiko melalui penerapan pengamanan tambahan.
2. Transfer
   Strategi pengendalian risiko yang mencoba untuk melimpahkan dampak risiko ke aset, proses ataupun organisasi lainnya.
3. Mitigation
   Strategi pengendalian risiko yang mencoba untuk mengurangi dampak dari kegagalan yang terjadi lewat perencanaan yang telah disiapkan.
4. Acceptance
   Strategi pengendalian risiko yang mencoba untuk menerima risiko pada tingkatan tertentu.
5. Termination
   Strategi pengendalian risiko yang mencoba untuk menghilangkan seluruh risiko yang berhubungan dengan aset informasi.

2.2.4. Tata Kelola Keamanan Informasi

Tata kelola dalam kemananan informasi adalah hal yang memastikan bahwa tindakan kemananan yang baik dimiliki dan dikelola oleh organisasi. Dalam tata kelola dilakukan pendefinisian siapa yang melakukan apa dan kapan sehingga dengan adanya tata kelola membantu dalam mendefinisikan tanggung jawab yang jelas dalam organisasi untuk mencapai tujuan organisasi [24]. Dalam membantu untuk menata kelola keamanan informasi, berikut merupakan kerangka kerja tata kelola yang paling banyak digunakan [24] :

- *National Institute of Standards Cybersecurity Framework*

- *Control Objectives for Information and Related Technology (COBIT)*
- *Health Information Trust Alliance (HITRUST)*
- *ISO/IEC 27001*

Dengan pemilihan kerangka kerja yang tepat maka dapat membantu organisasi atau perusahaan dalam menata kelola kemanan informasinya lebih baik sesuai dengan kebutuhan organisasinya masing – masing sehingga memudahkan dalam mencapai tujuan organisasi. Tata kelola keamanan informasi secara umum memiliki tujuannya sendiri [23], adapun tujuan tata kelola keamanan informasi adalah :

1. *Strategic Alignment*
   Menyelaraskan penerapan keamanan informasi dengan strategi bisnis untuk mendukung pencapaian tujuan organisasi.
2. *Risk Management*
   Melakukan tindakan yang tepat untuk mengelola dan memitigasi ancaman terhadap sumber daya maupun aset informasi.
3. *Resource Management*
   Memanfaatkan keunggulan keamanan informasi untuk mengelola infrastruktur secara efektif dan efisien.
4. *Performance Management*
   Melakukan tindakan pengukuran, pengawasan dan pelaporan kegiatan penata kelolaan keamanan informasi untuk memastikan tujuan organisasi tercapai.
5. *Value Delivery*
   Mengoptimalkan pemanfaatan investasi pada keamanan informasi untuk mendukung tujuan organisasi.

2.2.5. Sistem Manajemen Keamanan Informasi

Menurut SNI ISO/IEC 27001 : 2009 Sistem Manajemen Keamanan Informasi (SMKI) merupakan bagian dari sistem manajemen secara keseluruhan yang akan menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan dan memelihara keamanan informasi menggunakan pendekatan risiko. Dalam penerapannya, seluruh proses SMKI mengadopsi model PDCA (Plan, Do, Check dan Act) [28]. Dengan mengadopsi PDCA memudahkan dalam melakukan prinsip asesmen risiko, desain keamanan, penerapan, manajemen keamanan dan reasesmen. Berikut merupakan model PDCA yang diterapkan untuk proses sistem manajemen keamanan informasi [22]:

- *Plan*
  Pada tahap ini dilakukan penetapan kebijakan, tujuan dan prosedur SMKI untuk menghasilkan tujuan yang ingin dicapai oleh organisasi. Adapun langkah dalam melakukannya adalah :
  1. Mendapatkan dukungan manajemen
  2. Menentukan ruang lingkup SMKI
  3. Melakukan pendataan dari informasi (*information inventory*)
  4. Melakukan pengelolaan risiko (*risk management*)
  5. Membuat rencana implementasi SMKI
- *Do*
  Pada tahap ini dilakukan implementasi dari kebijakan dan prosedur SMKI untuk mengatasi risiko dan meningkatkan keamanan informasi. Adapun langkah dalam melakukannya adalah :
  1. Membuat program implementasi SMKI
  2. Operasional atau pelaksanaan SMKI
  3. Membuat dokumen operasional SMKI
- *Check*
  Pada tahap ini dilakukan 2 hal, yang pertama melakukan pengecekan dengan mengukur kinerja dengan sasaran

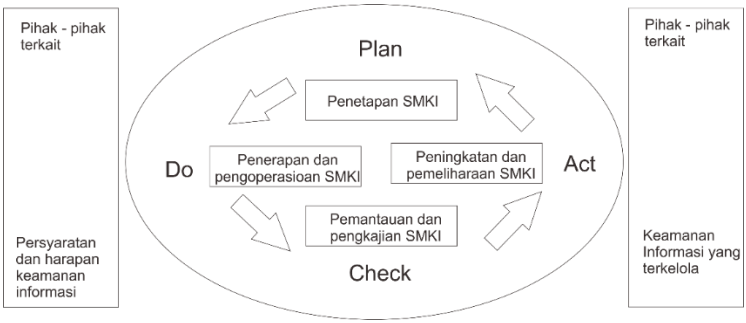
SMKI dan memberikan laporan hasil pengecekan kepada pihak manajemen untuk dikaji lebih lanjut. Adapun langkah dalam melakukannya adalah :

1. Melakukan tinjauan kesesuaian pelaksanaan SMKI (*compliance review*)

- *Act*

  Pada tahap ini dilakukan tindakan aktif untuk memperbaiki maupun mencegah kerawanan yang terjadi dari proses audit internal terhadap SMKI sehingga perbaikan dapat dilakukan terus menerus untuk mencapai keamanan yang diharapkan. Adapun langkah dalam melakukannya adalah :

  1. Melakukan perbaikan SMKI
  2. Penilaian awal sertifikasi SMKI
  3. Pelaksanaan sertifikasi SMKI



Gambar 2 2. Model PDCA dalam SMKI [28]

Dengan melakukan proses SMKI berarti instansi pemerintah maupun swasta yang menyelenggarakan sistem elektronik dapat menjamin aset teknologi informasinya dari kerentanan dan ancaman yang ditimbulkan oleh pihak yang tidak memiliki akuntabilitas. Pada tabel di bawah ini disajikan hubungan siklus PDCA dengan klausul pada ISO/IEC 27001: 2005 [22].

Tabel 2 2. Hubungan Siklus PDCA Indeks KAMI dengan ISO/IEC 27001:2005 [22]

Siklus PDCA	Klausul ISO/IEC 27001: 2005	Keterangan
Plan	4.2.1, 5.1	Pembangunan dan Perencanaan SMKI
Do	4.2.2, 5.2	Implementasi dan pengoperasian SMKI
Check	4.2.3, 6, 7	Pemantauan dan pengecekan SMKI
Act	4.2.4, 8.2, 8.3	Pemeliharaan dan peningkatan SMKI

Dalam Permen Kominfo No. 4 tahun 2016 bahwa setiap lembaga yang menyelenggarakan sistem elektronik harus melakukan sertifikasi kemanan informasi, pemerintah merekomendasikan SMKI yang mengacu pada standar nasional Indonesia yaitu SNI ISO/IEC 27001: 2013 [29]. Untuk mengetahui kesiapan lembaga penyedia sistem elektronik apakah bisa menerapkan standar SNI ISO/IEC 27001 maka dilakukan penilaian dengan Indeks KAMI untuk mengetahui kesiapan lembaga penyelenggara sistem elektronik dalam menerapkan keamanan informasi. Pada panduan penerapan SMKI berbasis Indeks KAMI yang dikeluarkan Kementerian Komunikasi dan Informasi (2017) dijabarkan 6 tahapan penerapan SMKI seperti pada gambar di bawah ini [30].

Gambar 2 3. Tahapan Penerapan SMKI [30]

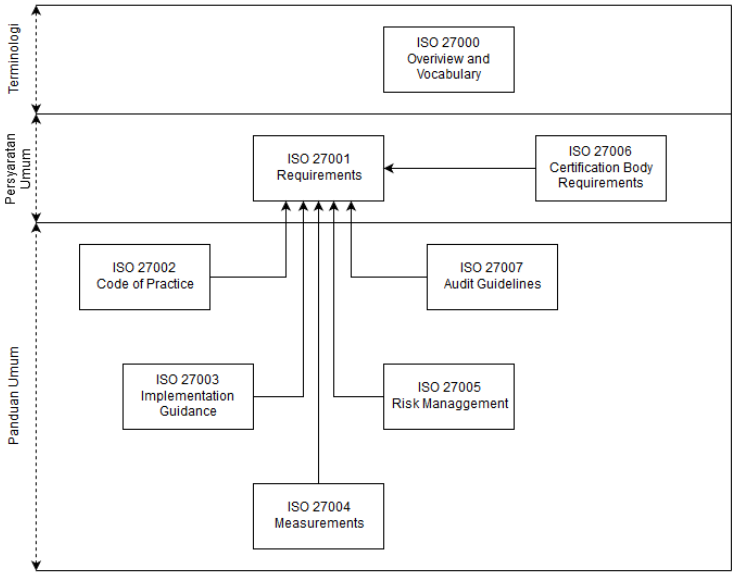
Pada tahap awal dilakukan komitmen dari manajemen tingkat atas untuk menyediakan sumber daya SDM, sistem teknologi informasi dan finansial serta menetapkan tanggung jawab yang jelas terhadap keberlangsungan penerapan SMKI. Selanjutnya dilakukan pendefinisian penerapan SMKI pada layanan ataupun satuan kerja untuk memfokuskan pengimplementasian. Selanjutnya dilakukan *gap analysis* untuk memastikan seberapa jauh penerapan persyaratan ISO/IEC 27001. Kemudian dilanjutkan dengan penilaian risiko yang meungkin terjadi dan dapat berpengaruh terhadap keamanan informasi serta menetapkkan kontrol yang tepat untuk mengatasi risiko yang diidentifikasi. Setelah penetapan kontrol dilakukan maka dilakukan penyusunan kebijakan dan prosedur SMKI yang mengacu pada kontrol yang memang diterapkan untuk penyelenggaraan layanan publik. Setelah itu tinggal dilakukan penerapan kebijakan dan prosedur SMKI yang diselaraskan dengan proses bisnis organisasi.

2.2.6. ISO/IEC 27001

ISO/IEC 27001 merupakan standar pengelolaan keamanan informasi yang dibuat oleh ISO dan IEC yang memberikan panduan praktik terbaik dalam menjaga keamanan informasi. Standar ini membantu organisasi dalam mengelola aset informasi seperti info keuangan, hak cipta, data karyawan maupun semua informasi penting perusahaan yang rentan untuk dicuri atau disalahgunakan oleh orang yang tidak memiliki otoritas [20].

Produk ini merupakan satu rangkaian dalam keluarga ISO/IEC 27000, berikut adalah produk dari keluarga ISO/IEC 27000 :

1. ISO/IEC 27001, pada bagian ini mencakup *Requirements* dari *Information Security Management Systems*.
2. ISO/IEC 27002, pada bagian ini berisikan *Code of Practices* atau atau langkah – langkah dari kontrol yang lebih detil.
3. ISO/IEC 27003, mencakup *Implementation Guidance* yang tentunya berdasarjan konsep PDCA
4. ISO/IEC 27004, berisikan *Measurements* yang memberikan panduan organisasi dalam melakukan evaluasi kinerja dan keefektifan dari kemanan informasinya.
5. ISO/IEC 27005, pada bagian ini mengenai *Risk Management* yang membantu organisasi dalam melaksanakan keamanan informasi berdasarkan pendekatan manajemen risiko
6. ISO/IEC 27006, tentang *Certification Body Requirements* yang memaparkan persyaratan formal untuk organisasi dalam mengesahkan sertifikasi ISO/IEC 27001
7. ISO/IEC 27007, berisikan *Audit Guidelines* untuk membantu organisasi memahami pelaksanaan audit .



Gambar 2 4.Keluarga ISO 27001 [20]

Pada versi ISO/IEC 27001: 2013 terdiri dari 14 klausa yang berisikan 114 kontrol sedangkan pada versi ISO/IEC 27001: 2005 terdiri dari 11 klausa yang berisikan 133 kontrol [27]. Pada tabel 2.3vdi bawah ini disajikan perbandingan klausa antara ISO/IEC 27001: 2005 dengan ISO/IEC 27001: 2015 [25] [26].

Tabel 2 3. Perbandingan ISO/IEC 27001: 2005 dengan ISO/IEC 27001: 2013 [25][26]

ISO/IEC 27001: 2005	**ISO/IEC 27001: 2013**
A.5 Security policy A.5.1 Information security policy	A.5 Information security policies A.5.1 Management direction for information security
A.6 Organization of information security A.6.1 Internal organization A.6.2 External parties	A.6 Organization of Information security A.6.1 Internal organization A.6.2 Mobile devices and teleworking
A.7 Human resource management A.7.1 Responsibility for assets A.7.2 Information classification	A.7 Human resource security A.7.1 Prior to employment A.7.2 During e,ployment A.7.3 Termination and change of employment
A.8 Human resources security A.8.1 Prior to employment A.8.2 During employment	A.8 Aset Management A.8.1 Responsibility for assets A.8.2 Information classification

A.8.3 Termination or change of employment	A.8.3 Media handling
A.9 Physical and environmental security A.9.1 Secure areas A.9.2 Equipment security	A.9 Access control A.9.1 Business requirements of access control A.9.2 User access management A.9.3 User responsibilities A.9.4 System and application access control
A.10 Communications and operations management A.10.1 Operational procedures and responsibilities A.10.2 Third party service delivery management A.10.3 System planning and acceptance A.10.4 Protection against malicious and mobile code A.10.5 Back-up	A.10 Cryptography A.10.1 Cryptographic controls

A.10.6 Network security management A.10.7 Media handling A.10.8 Exchange of information A.10.9 Electronic commerce services A.10.10 Monitoring	
A.11 Access control A.11.1 Business requirement for access control A.11.2 User access management A.11.3 User responsibilities A.11.4 Network access control A.11.5 Operating system access control A.11.6 Application and information access control A.11.7 Mobile computing and teleworking	A.11 Physical and environmental security A.11.1 Secure areas A.11.2 Equipment

A.12 Information systems acquisition, development and maintenance A.12.1 Security requirements of information systems A.12.2 Correct processing in applications A.12.3 Cryptographic controls A.12.4 Security of system files A.12.5 Security in development and support processes A.12.6 Technical Vulnerability Management	A.12 Operation Security A.12.1 Operationalprocedures and responsibilities A.12.2 Protection from malware A.12.3 Backup A.12.4 Logging and monitoring A.12.5 Control of operational software A.12.6 Technical vulnerability management A.12.7 Information systems audit considerations
A.13 Information security incident management A.13.1 Reporting information security events and weaknesses A.13.2 Management of information security	A.13 Communications security A.13.1 Network security management A.13.2 Information transfer

incidents and improvements	
A.14 Business continuity management A.14.1 Information security aspects of business continuity management	A.14 System acquisition, development and maintenance A.14.1 Security requirements of information systems A.14.2 Security in development and support processes A.14.3 Test Data
A.15 Compliance A.15.1 Compliance with legal requirements A.15.2 Compliance with security policies and standards, and technical compliance A.15.3 Information systems audit considerations	A.15 Supplier relationships A.15.1 Information security in supplier relationships A.15.2 Supplier service delivery management
	A.16 information security incident management A.16.1 Management of information security incidents and improvements

	A.17 Information security aspects of business continuity management A.17.1 Information security continuity A.17.2 Redundancies
	A.18 Compliance A.18.1 Compliance with legal and contractual requirements A.18.2 Information security reviews

Dalam penerapannya organisasi/perusahaan dapat memilih kontrol mana yang menjadi fokusnya dalam menjalankan pengelolaan keamanan informasi [27].

2.2.7. Indeks KAMI

Indeks KAMI merupakan alat yang dikeluarkan oleh Kementerian Komunikasi dan Informatika RI untuk mengetahui seberapa jauh kesiapan instansi penyelenggara sistem elektronik dalam memenuhi semua aspek keamanan dari ISO/IEC 27001. Versi terbarunya adalah Indeks KAMI 3.1 yang dikelauarkan pada april 2015 lalu. Pada versi ini mengacu pada ISO/IEC 27001: 2013 sebelumnya ada versi Indeks Kmai 2.3 yang mengacu pada ISO/IEC 27001 : 2009. Dari hasil evaluasi yang dilakukan dengan Indeks KAMI diharapkan

memerikan pandangan kesiapan suatu instansi dalam memenuhi standar keamanan informasi dan apakah sudah cukup mematuhi aspek kelengkapan dan keamatangan yang diharapkan.Indeks KAMI terdiri dari 5 area yang masing – masing area terdiri dari sejumlah pertanyaan untuk menentukan level keamanan informasi. Adapun kelima area Indeks KAMI adalah :

1. Tata Kelola
   Pada bagian ini dilakukan pengevaluasian penata kelolaan keamanan informasi pada penyelenggara sistem elektronik. Dilakukan penilaian terhadap penata kelolaan kebijakan, prosedur, peran, tanggungjawab, dan pengawasan kegiatan operasional untuk menjaga keamanan informasi.
2. Risiko
   Pada bagian ini dilakukan evaluasi terhadap pengelolaan risiko untuk memastikan strategi keamanan informasi yang diterapkan sudah memnuhi standar keamanan ISO/IEC 27001.
3. Kerangka Kerja
   Pada bagian ini dilakukan evaluasi kelengkapan dan kesiapan kerangka kerja dan strategi penerapannya terhadap upaya menjaga keamanan informasi
4. Pengelolaan Aset
   Pada bagian ini dilakukan evaluasi terhadap pengamanan aset informasi yang memastikan dalam siklus penggunaan aset tersebut dilakukan pengamanan yang tepat.
5. Teknologi
   Pada bagian ini dilakukan evaluasi tehadap efektivitas pemanfaatan teknologi dalam menerapkan strategi pengamanan informasi.

Sebelum mengisi pertanyaan untuk masing – masing area diharuskan mengisi Perak TIK atau Sistem Elektronik untuk mengetahui kondisi terkini dari penggunaan teknologi informasi oleh instansi. Setelah itu maka didapatkan kategori

dari penggunaan teknologi informasi pada instansi tersebut sehinga bisa dilanjutkan dengan menjawab kelima area. Dalam menjawab pertanyaan kelima area dilakukan dengan memberikan jawaban berdasarkan kategori pengamanan seperti tidak dilakukan, dalam perencanaan, dalam perencanaan atau diterapkan sebagian, dan ditetapkan secara menyeluruh [3].

	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 5. Kategori Pengamanan [3]

Dari hasil jawaban tiap pertanyaan maka akan dihasilkan skor, jumlah skor untuk masing – masing area akan menentukan tingkat kematangan suatu instansi. Pada Indeks KAMI tingkat kematangan atau levelnya didefinisikan dalam tingkatan seperti dibawah ini [4]:

- Tingkat 0 – Tidak Diketahui (PASIF)
  Pada tingkatan ini, status kesiapan lembaga penyedia sistem elektronik tidak diketahui atau tidak didapati dalam hasil penilaian. Hal ini bisa terjadi jika lembaga penyedia sistem elektronik tidak melakukan penilaian dengan Indeks KAMI atau tidak melakukan pelaporan peringkat Indeks KAMI.
- Tingkat I – Kondisi Awal (REAKTIF)
  Tingkatan ini ditandai dengan sudah mulai adanya pemahaman mengenai pengelolaan keamanan informasi

namun masih pada tahap awal sehingga tidak terdefinisi tanggung jawab yang jelas. Usaha pengamanan dilakukan secara reaktif untuk menangani masalah insidentil yang menyebabkan ketidakteraturan komunikasi dan pengawasan.

- Tingkat II – Penerapan Kerangka Kerja Dasar (AKTIF)
  Pada tingkatan ini pemahaman mengenai keamanan informasi sudah diterapkan namun belum ada keterkaitan antara langkah pengamanan. Manajemen pengamanan belum menjadi prioritas dan masih banyak ditemukannya kelemahan serta banyak penanganan masalah yang belum selesai sehingga keefektifan pengamanan tidak terlihat.
- Tingkat III – Terdefinisi dan Konsisten (PRO AKTIF)
  Lembaga penyelenggara sistem elektronik yang berada pada tingkatan ini sudah menerapkan pengamanan yang baku secara konsisten dan terdokumentasi. Pada tingkatan ini seluruh pihak sudah menyadari perannya sehingga pelaksanan pengelolaan keamanan sudah sesuai dengan batas minimum standar pengamanan informasi.
- Tingkat IV – Terkelola dan Terukur (TERKENDALI)
  Pada tingkatan ini strategi pengamanan sudah diterapkan secara efektif sesuai dengan strategi manajemen risiko. Dimana dilakukan evaluasi yang rutin terhadap pencapaian sasaran dan penerapan pengamanan informasi. Manajemen keamanan bersifat pro-aktif dalam melakukan pembenahan berkelanjutan yang membuat pengelolaan keamanan semakin efisien.
- Tingkat V – Optimal (OPTIMAL)
  Tingkatan ini ditandai dengan dilakukannya pengamanan secara menyeruluh, berkelanjutan dan efektif sesuai dengan strategi manajemen risiko yang didefinisikan. Adanya integrasi pengamanan dengan tugas pokok instansi yang membuat peningkatan pada efektivitas pengamanan. Kemudian dilakukan evaluasi dan perbaikan secara berkelanjutan untuk peningkatan kinerja terhadap target program pengamanan.

Dari kelima area itu ada tambahan tingkatan untuk memberikan uraian yang lebih detil berupa I+, II+, III+ dan IV+. Secara umum proses penilaian dengan Indeks KAMI dilakukan dalam 5 langkah seperti di bawah ini [4]:

1. Mendefinisikan Ruang Lingkup
   Pada bagian ini dilakukan pendefinisian ruang lingkup penilaian mulai dari cakupan lokasi kerja, sistem elektronik yang diselenggarakan, dan mitra penyedia layanan yang sangat penting untuk dijabarkan secara jelas untuk mengetahui batasan dari penilaian.
2. Menetapkan Peran atau Tingkat Kepentingan TIK di Instansi
   Pada bagian ini dilakukan pengelompokkan sejauh mana peran TIK pada instansi yang dinilai. Pengelompokkan dilakukan dalam kategori rendah, sedang, tinggi dan kritis. Dengan dilakukan proses ini, dapat mengetahui pemanfaatan TIK sehingga tahu cakupan dan evaluasinya.

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi			
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.			
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis		**Status**	Skor
#	**Karakteristik Instansi**		
1,1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Minim	0
1,2	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Minim	0
1,3	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas Pokok	Minim	0
1,4	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Minim	0
1,5	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Minim	0
1,6	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Minim	0

Gambar 2 6. Ilustrasi Penlaian Peran TIK [4]

3. Menilai Kelengkapan Pengamanan 5 Area
   Penilaian dilakukan dengan mengisi jawaban pertanyaan berdasarkan kategori pengamanan yang sesuai dengan standar ISO/IEC 27001. Pertanyaan dengan kategori 1 mengenai kerangka kerja dasar keamanan informasi, pertanyaan kategori 2 mengenai efektivitas dan konsistensi penerapan pengamanan dan pada kategori 3 pertanyaannya mengenai peningkatan kinerja pengamanan.

Bagian II: Tata Kelola Keamanan Informasi

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

[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?	Diterapkan Secara Menyeluruh	3
2,2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	Dalam Perencanaan	1
2,3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	Diterapkan Secara Menyeluruh	3
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 keahlian pelaksana pengelolaan keamanan informasi?	Tidak Dilakukan	0
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 organsiasi 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

Gambar 2 7. Ilustrasi Penilaian Pengamanan 5 area [4]

4. Mengkaji Hasil Indeks KAMI, Menetapkan Langkah Perbaikan, Penetapan Prioritas.
   Hasil penilaian Indeks KAMI disajikan dalam 2 tampilan, yang pertama dalam bentuk tabel nilai pada masing – masing area kemudian dalam bentuk *Radar Chart* yang sesuai dengan 5 area pengamanan.

Gambar 2 8. Ilustrasi Diagram Radar 5 Area [4]

Kemudian untuk tingkatan kelengkapan didefinisikan dalam 3 tingkat yang disajikan dalam *bar chart* seperti di bawah ini :

Gambar 2 9. Bar Chart Tingkat Kelengkapan [4]

- Tidak Layak (Merah)
- Memerlukan Perbaikan (Kuning)
- Baik/ Cukup (Hijau)

Dalam menentukan langkah perbaikan dan penetapan prioritas dilakukan dengan melihat hasil penilaian dari tingkat kematangan dan tingkat kelengkapan organisasi.

Gambar 2 10. Tingkat Kematangan dan Kelengkapan [4]

Dari hasil tingkat kematangan dan kelengkapan yang didapat akan dijadikan tolak ukur untuk menigkatkan kesiapan instansi melakukan sertifikasi ISO 27001.

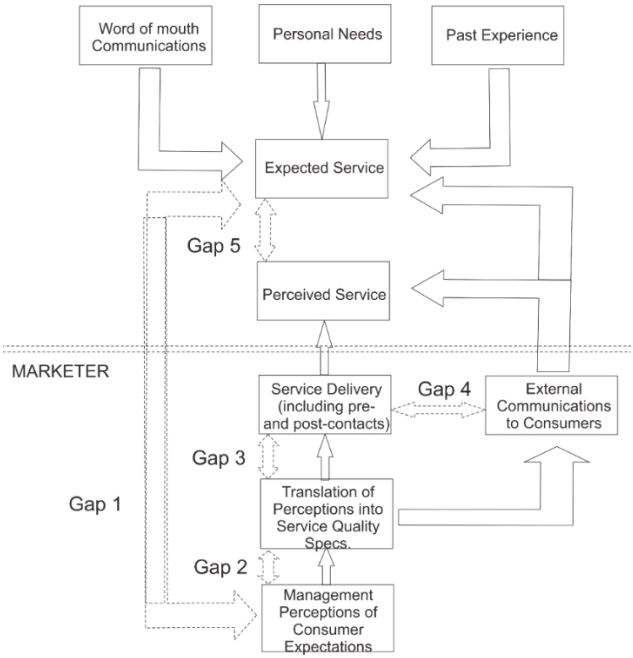
5. Mengkaji Ulang Tingkat Kelengkapan dan Kematangan dengan Indeks KAMI
   Penilaian dengan Indeks KAMI dilakukan secara berulang untuk memantau kondisi perbaikan yang dilakukan

sehingga penerapan tata kelola keamanan informasi dapat dipastikan dilakukan sesuai dengan standar ISO/IEC 27001.

2.2.8. Analisis Kesenjangan (GAP Analysis)

Analisis kesenjangan banyak digunakan di bidang manajemen untuk melakukan evaluasi dan perencanaan. Evaluasi yang biasa dilakukan biasanya mengenai pengukuran kualitas layanan (*quality of service*) [31]. Pada gambar 2.11 diperlihatkan model *gap* yang dikembangkan oleh Parasuraman (1985) yang membagi *gap* menjadi 5 bagian [32], diantaranya :

1. *Gap* 1
   Merupakan *gap* yang terjadi antara apa yang pelanggan harapkan dengan persepsi manajemen mengenai harapan pelanggan yang akan memberikan dampak pada kualitas pelayanan terhdap pelanggan.
2. *Gap* 2
   Merupakan *gap* yang terjadi antara persepsi manajemen mengenai ekspektasi pelanggan dengan spesifikasi kualitas pelayanan perusahaan yang memberikan dampak pada kualitas layanan dari sudut pandang pelanggan.
3. *Gap* 3
   Merupakan *gap* antara spesifikasi kualitas layanan dengan layanan yang disampaikan kepada pelanggan.
4. *Gap* 4
   Merupakan *gap* antara layanan yang diberikan kepada pelanggan dengan komunikasi yang dilakukan oleh perusahaan. Hal ini dapat berpengaruh pada pandangan pelanggan mengenai kualitas layanan.
5. *Gap* 5
   Merupakan *gap* antara pelayanan yang dirasakan dimana memperhatikan kesenjangan antara layanan yang diharapkan pelanggan dengan layanan yang dirasakan pelanggan.



Gambar 2 11. Service Quality Model [32]

Analisis kesenjangan (*gap)* merupakan sebuah alat yang juga digunakan untuk meningkatkan pengelolaan teknologi informasi di perusahaan dimana perlu adanya pemahaman pada bagian yang membutuhkan perubahan dengan pengidentifikasian masalah yang menghambat perbaikan kemudian menggunakan proses yang tepat untuk melakukan peningkatan [33].

Menurut John Murray analisis kesenjangna (*gap)* merupakan proses yang mengukur kesenjangan antara kondisi saat dengan kondisi yang diharapkan untuk memenuhi kebutuhan organisasi. Berikut merupakan proses untuk mengukur kesenjangan menurut John Murray [33] :

1. Mengidentifikasi tujuan analisis kesenjangan.
2. Menganalisis proses yang sedang berlangsung yang menghambat pencapaian tujuan.
3. Mengembangkan perencanaan untuk mengecilkan kesenjangan antara kondisi saat ini dan tujuan yang ingin dicapai.
4. Mereview seluruh pihak yang terlibat untuk memastikan komitmennya terhadap perencanaan analisis kesenjangan.
5. Melakukan audit saat penyelesaian proses kesenjangan untuk memastikan apakah goal yang ingin dicapai sudah terpenuhi dan pihak yang melaksanakan prosesnya mengerti dan dapat menggunakannya sebagai sarana peningkatan pengelolaan teknologi informasi yang lebih produktif lagi.

Dengan adanya analisis kesenjangan pada penerapan teknologi informasi dapat memberikan pengetahuan akan proses mana yang perlu ditingkatkan pada perusahaan. Ada dua poin yang digunakan sebagai perbandingan dalam anlisis kesenjangan untuk menengkitakan pengembangan teknologi informasi [18][34]. Adapun kedua poin tersebut adalah :

1. *TO-BE*
   Poin ini menggambarkan kondisi yang ingin dicapai oleh organisasi atau perusahaan. Contohnya adalah lembaga penyelenggara elektronik yang ingin mencapai penerapan standar SNI ISO/IEC 27001.
2. *AS-IS*
   Poin ini menggambarkan kondisi saat ini dari perusahaan atau organisasi. Contohnya adalah kondisi saat ini dari penyelenggara layanan elektronik yang belum melakukaan penata kelolaan yang baik dalam menjaga keamanan informasinya.

Kedua poin tersebutlah yang dibandingkan untuk mengetahui kesenjangan atau *gap* antara kedua poin sehingga dapat diketahui seberapa jauh kesenjangannya. Dari kedua poin *TO-*

BE dan *AS-IS* akan menghasilkan 2 macam nilai. Yang pertama adalah gap yang bernilai positif (+) yang terjadi ketika nilai *AS-IS* lebih besar dari nilai *TO-BE*. Kemudian yang kedua adalah nilai negatif (-) yang terjadi jika nilai *TO-BE* lebih besar dari nilai AS-IS. Perbandingan antara kedua poin itu dihitung dengan rumus *G (Kesenjangan) = expected service (TO-BE) – preceived service (AS-IS)*. Setelah diketahui kesenjangan antara kedua poin tersebut maka dilakukan pemberian rekomendasi untuk membantu organisasi atau perusahaan pada umumnya dalam memperkecil kesenjangan yang ada untuk mencapai tujuannya [34].

2.2.9. Lembaga Penyelenggara Sistem Elektronik

Lembaga penyelenggara sistem elektronik merupakan suatu lembaga yang mengoperasikan sistem elektronik secara mandiri maupun dengan bekerja sama dengan beberapa pihak terkait untuk memberikan layanan untuk dirinya sendiri maupun pihak diluar lembaganya. Lembaga penyelenggara sistem elektronik disini bisa berupa perorangan, penyelenggara negara, badan usaha, masyarakat, perusahaan swasta maupun instansi pendidikan. Pada penelitian ini dilakukan evaluasi terhadap implementasi manajemen keamanan informasi pada beberapa penyelenggara sistem elektronik terhadap Indeks KAMI yang mengacu pada SNI ISO/IEC 27001. Dengan penelitian ini diharapkan akan memberikan gambaran mengenai poin pertanyaan yang menjadi masalah bagi lembaga penyelenggara sistem elektronik dalam menerapkan standar keamanan informasi yang berlaku.

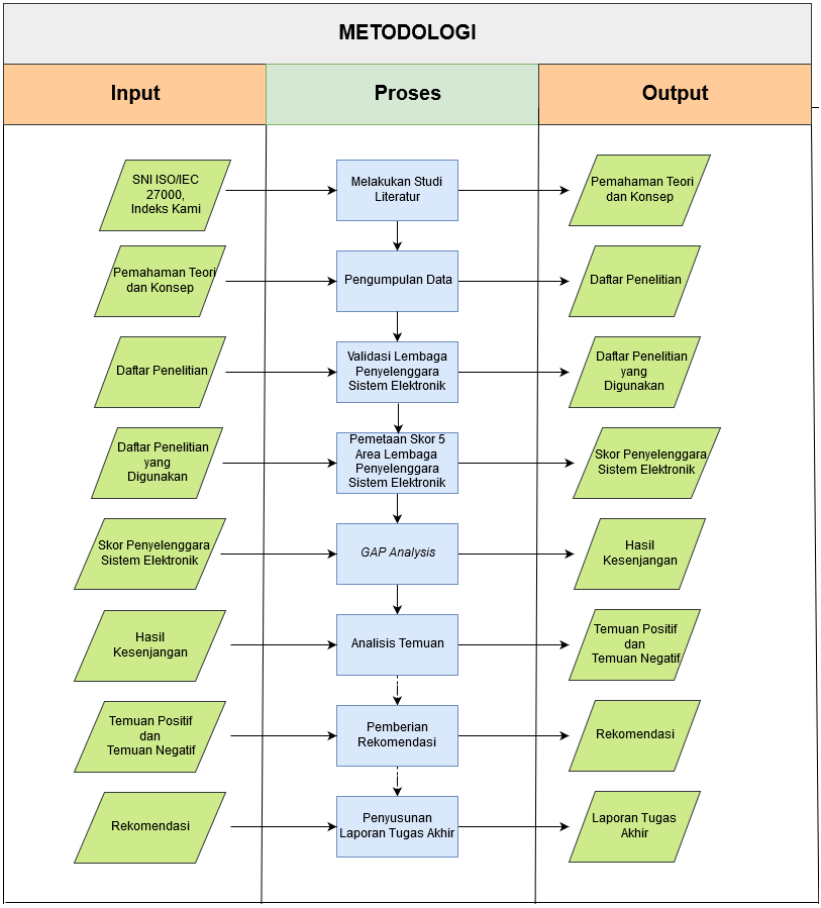
“Halaman ini sengaja dikosngkan”

BAB III
METODOLOGI PENELITIAN

Bagian ini menjelaskan metodologi yang digunakan dalam pengerjaan tugas akhir ini. Metodologi ini diperlukan sebagai panduan secara sistematis dalam pengerjaan tugas akhir.

3.1. Tahapan Pelaksanaan Tugas Akhir

Pada sub bab ini akan menjelaskan mengenai metodologi dalam pengerjaan tugas akhir. Dimana teridiri dari 8 langkah yaitu studi literatur, pengumpulan data, validasi lembaga penyelenggara sistem elektronik, pemetaan skor 5 area lembaga penyelenggara sistem elektronik, *gap analysis*, analisis temuan, pemberian rekomendasi dan penyusunan laporan tugas akhir. Metodologi dapat dilihat pada gambar 3.1 dibawah ini.



Gambar 3 1. Metodologi Pengerjaan Tugas Akhir

3.2. Uraian Metodologi

Berdasarkan metodologi penelitian di atas, berikut merupakan uraian untuk setiap tahapannya.

3.2.1. Melakukan Studi Literatur

Pada tahap ini dilakukan identifikasi masalah yang diangkat menjadi topik tugas akhir kemudian dilanjutkan dengan

pemahaman literatur dengan mengumpulkan buku, jurnal, penelitian dan dokumen lainnya yang akan menjadi dasar pemahaman dalam membentuk kerangka berpikir. Pada tahapan ini dilakukan pemahaman konsep dan metode yang nantinya akan digunakan untuk menyelesaikan permasalahan yang telah diidentifikasi pada tugas akhir ini.

3.2.2. Pengumpulan Data

Setelah dilakukan pemahaman mengenai topik yang diangkat dan konsep dasar maka dilanjutkan dengan tahapan pengumpulan data penelitian yang melakukan penilaian dengan Indeks KAMI versi 2.3. Pengumpulan data dilakukan dengan mengumpulkan penelitian – penelitian yang melakukan penilaian Indeks KAMI pada suatu lembaga penyelenggara sistem elektronik. Data yang dikumpulkan didapatkan melalui buku penelitian, internet maupun dari penelitinya langsung.

3.2.3. Validasi Lembaga Penyelenggara Sistem Elektronik

Pada tahapan ini dilakukan validasi terhadap data penilaian dari penelitian yang dilakukan. Dengan validasi ini diharapkan kesetaraan cakupan penelitian lembaga penyelenggara sistem elektronik yang akan dievaluasi. Pemilihan sistem elektronik dilakukan berdasarkan kriteria peran TIK pada penyelenggara sistem elektronik. Kemudian dilakukan validasi terhadap penelitian yang telah dikumpulkan berdasarkan kriteria yang telah dibuat. Data penelitian yang digunakan adalah data yang telah diklasifikasikan berdasarkan kriteria lembaga penyelenggara sistem elektronik yang beradapada level *medium* dan *high* yang mengisyaratkan bahwa lembaga tersebut telah menggunakan TIK sebagai satu kesatuan pada proses kerja lembaganya dan kategorisasi berdasarkan tingkat kematangannya.

3.2.4. Pemetaan Skor 5 Area Lembaga Penyelenggara Sistem Elektronik

Pada tahapan ini dilakukan pemetaan skor akhir dari masing – masing lembaga yang dibandingkan untuk mengidentifikasi kondisi lembaga yang dibandingkan kemudian menempatkan skor untuk masing – masing lembaga pada indikator pertanyaan Indeks KAMI. Lewat pemetaan yang dilakukan maka didapatkan poin *AS-IS* untuk *Gap Analysis.*

Tabel 3 1. Ilustrasi Pemetaan Skor 5 Area Lembaga Penyelenggara Sistem Elektronik

Tata Kelola	Pertanyaan	AS IS					TO - BE
		P1	P2	P3	P4	P5	

3.2.5. Analisis Kesenjangan *(Gap)*

Setelah dilakukan penempatan masing – masing skor dan jawaban untuk masing – masing lembaga pada indikator pertanyaan Indeks KAMI maka akan dilakukan analisis kesenjangan yang mana melihat perbandingan penelitian kondisi lembaga yang telah dinilai dengan kondisi yang diharapkan atau yang memenuhi kriteria yang dikatakan siap sehingga dapat memastikan bahwa keamanan yang dibangun pada sistem informasi. Kondisi yang diharapkan disini adalah ketika menerapkan secara menyeluruh pertanyaan Indeks KAMI (poin *TO-BE*) Pada bagian ini dilakukan perhitungan ksenjangan dengan metode statistik deskriptif yaitu

menggunakan rumus : Kesenjangan = *TO-BE – AS-IS.* Kesenjangan penilaian penelitian dengan kondisi yang diharapkan disajikan dalam bentuk tabel dan grafik.

Tabel 3 2. Kesenjangan Penyelenggara Sistem Eleektronik

Tata Kelola	Pertanyaan	Kesenjangan			Rataan
		P1	P2	P3	

Dari hasil perbandingan ini nantinya akan mendapatkan suatu hasil berupa suatu temuan.

3.2.6. Analisis Temuan

Setelah didapatkan kesenjangan setiap penelitian terhadap Indeks KAMI maka akan dilakukan pengurutan poin pertanyaan pada tiap area yang memiliki kesenjangan paling besar.

Tabel 3 3. Analisis Temuan

No.	Area	Poin Pertanyaan	Kesenjangan	To-Be	Masalah
1.	Tata Kelola				

Dari hasil temuan yang didapat bisa berupa temuan positif dan temuan negatif. Temuan disini berupa daftar indikator yang menjadi permasalahan bagi lembaga pemberintahan dalam menyiapkan diri untuk mencapai Standar Nasional Indonesia ISO/IEC 27001 berdasarkan perbandingan antar lembaga yang telah melakukan evaluasi kesiapan dengan Indeks KAMI sehingga bisa diantisipasi sejak dini.

3.2.7. Pemberian Rekomendasi

Dari hasil temuan tersebut maka akan diberikan rekomendasi untuk menangani permasalahan yang paling sering muncul sebagai masalah bagi lembaga penyelenggara sistem elektronik dalam menerapkan Standar Nasional Indonesia ISO/IEC 27001.

Tabel 3 4. Pemberian Rekomendasi

No.	Poin Pertanyaan	Kesenjangan	Masalah	Rekomendasi
1.				ISO 27001

Hasil rekomendasi ini akan menjadi bahan evaluasi bagi lembaga penyelenggara sistem elektronik yang lainnya untuk memperhatikan poin tertentu dalam bidang keamaman informasi yang perlu ditingkatkan serta menyiapkan diri lebih awal untuk memastikan organisasinya dapat mematuhi Standar Nasional Indonesia dalam Manajemen Keamanan Informasi.

BAB IV
PERANCANGAN

Pada bab perancangan ini akan menjelaskan perancangan dari penelitian tugas akhir ini.

4.1. Perancangan Studi Kasus

Pada bagian ini akan dijelaskan mengenai tujuan dari studi kasus penelitian dan unit of analysis yang digunakan.

4.1.1. Tujuan Studi Kasus

Tujuan dari penelitian tugas akhir ini adalah mengetahui poin pernyataan area pada Indeks KAMI yang paling rentan menjadi masalah yang membuat lembaga penyelenggara sistem elektronik belum siap dalam menerapkan SNI ISO/IEC 27001 dan untuk memberikan rekomendasi perbaikan yang diperlukan lembaga penyelenggara sistem elektronik untuk memperbaiki manajemen keamanan informasinya.

Menurut Creswell studi kasus merupakan suatu proses yang menggunakan satu atau lebih kasus yang digunakan untuk mengeksplorasi dengan menggunakan metode pengumpulan data yang bermacam – macam [35]. Ada 2 macam perancangan model penelitian yaitu perancangan *sequential* dan *concurent*. Dimana perancangan *sequential* melakukan pengumpulan dan analisis dalam fase yang berbeda untuk jenis data yang berbeda secara berututan. Sedangkan perancangan *concurent* melakukan pengumpulan data yang berbeda dalam tahap yang sama. Kemudian kedua model perancangan ini dapat dipecah menjadi enam bagian yang lebih spesifik [38], yaitu :

- *Sequential Explanatory Design*, model perancangan yang melakukan penelitian dalam dua tahap yaitu pengumpulan

dan anlisis secara kuantitatif kemudian diikuti oleh pengumpulan dan analisis secara kualitatif

- *Sequential Exploratory Design*, model perancangan yang melakukan penelitian dalam dua tahap dimana diawali dengan fase kualitatif dan dilanjutkan dengan fase kuanitatif
- *Sequential Transformative Design*, model perancangan yang melakukan penelitian dalam 2 fase yang bisa diawali dengan fase kualitatif atau kuantitatif dan dilanjutkan dengan fase kualitatif atau kuantitatif dimana dimungkinkan perspektif teoritis dari peneliti dalam melakukan penelitian dan pengumpulan data.
- *Concurent Triangulation Design*, model perancangan ini melakukan pengumpulkan jenis data yang berbeda pada waktu yang bersamaan dan menganalisisnya secara berbeda yang kemudian hasilnya digabungkan, dimana dapat memberikan konfirmasi serta menguatkan temuan.
- *Concurent Embedded Design*, model perancangan yang menggunakan metode dan pengumpulan data kuantitatif dan kualitatif secara bersamaan namun dengan pembobotan yang berbeda.
- *Concurent Transformatif Design*, model perancangan yang merupakan gabungan dari triangulation dan embedded dimana mengumpulkan berbagai data secara bersamaan dan memberikan bobot yang bisa sama maupun tidak sama.

Penelitian ini termasuk *concurent triangulation design* karena dalam pengumpulan data dilakukan secara bersamaan dan masing – masing data dianalisis untuk pada akhirnya didapatkan hasil secara keseluruhan terhadap data.Triangulasi sumber data adalah sarana untuk mencari kekonvergenan antar data yang berbeda – beda tapi pada fenomena permasalahan yang sama untuk menanggulangi kelemahan yang mungkin muncul dari satu jenis metode atau sumber data dengan cara *merging*, *connecting* dan *embedding*. Dalam melakukan penggabungan data tentunya perlu kriteria untuk menyamakan

data. Adapun kriterianya ada 4 yaitu *credibility, dependability, conformability dan transferability* [39].

Yin mendefinisikan studi kasus sebagai penyelidikan empiris yang menggunakan metode pengumpulan data seperti observasi dan wawancara [36]. Ada 3 kategori studi kasus diantaranya :

- Eksplorasi, studi kasus yang melakukan penggalian data apapun sebagai tujuan peneliti
- Deskriptif, studi kasus dengan menggambarkan fenomena ilmiah dalam data dalam bentuk narasi.
- Explanatory, studi kasus yang menjelaskan fenomena data secara mendalam.

Pada penelitian tugas akhir ini menggunakan kategori eksplorasi deskriptif dengan melakukan penggalian data pada penelitian yang menerapkan Indeks KAMI yang kemudian dijelaskan secara deskriptif apa saja fenomena yang dapat diambil dari data.

4.1.2. Unit of Analysis

Perancangan studi kasus ada 2 tipe. Yang pertama adalah single-case design yang menggunakan satu kasus yang diteliti. Kemudian ada multiple-case desain yang menggunakan lebih dari satu kasus yang diteliti. Dari 2 tipe perancangan studi kasus itu dapat dibagi menjadi 4 bagian berdasarkann unit of analysis [36]. Adapun keempat tipe perancangan tersebut adalah :

- *Single-case designs* dengan single unit of analysis
- *Single-case designs* dengan multiple units of analysis
- *Multiple-case designs* dengan single unit of analysis
- *Multiple-case desaigns* dengan multiple units of analysis

Pada penelitian tugas akhir ini menggunakan perancangan multiple-case design dengan single unit of analysis yang

digunakan untuk mencari fakta dari perbedaan antara kondisi kekinian dan harapan yang ingin dicapai dari beberapa penelitian pada penyelenggara sistem elektronik. *Unit of analysis* pada penelitian ini adalah hasil penilaian pada penelitian - penelitian yang menggunakan Indeks KAMI.

4.2. Subjek dan Objek Penelitian

Tugas akhir ini akan meneliti implementasi manajemen keamanan informasi pada penyelenggara sisatem elektronik terhadap Indeks KAMI SANI ISO/IEC 217001. Adapun penelitian dengan penyelenggasra sistem elektronik yang digunakan adalah saebagai berikut :

Tabel 4 1. Penelitian Penyelenggara Sistem Elektronik

No.	Penelitian
1	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 [8].
2	Evaluasi pengelolaan keamanan jaringan di ITS dengan menggunakan Standar Indeks Keamanan informasi (KAMI) KEMENKOMINFO RI [9].
3	Penggunaan indeks keamanan informasi (KAMI) sebagai evaluasi keamanan informasi pada PT. PLN Distribusi Jawa Timur [10].
4	Evaluasi keamanan informasi pada divisi network of broadband PT. Telekomunikasi Indonesia Tbk dengan

	menggunakan Indeks Keamanan Informasi (KAMI) [11].
5	Evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi (KAMI) pada kantor wilayah Ditjen Perbendaharaan Negara Jawa Timur [12].
6	Analisa tingkat keamanan informasi pada sistem informasi administrasi kependudukan (SIAK) di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bantaeng menggunakan indeks KAMI [13].
7	Evaluasi Keamanan Informasi pada PTI PDAM Tirta Moedal Kota Semarang Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001: 2009 [14].
8	Evaluasi keamanan informasi menggunakan metode indeks keamanan informasi (KAMI) (Studi kasus: STIE Perbanas Surabaya) [15].
9	Evaluasi tingkat kelengkapan dan kematangan sistem keamanan informasi berdasarkan Indeks KAMI pada Divisi Sampling dan Pengujian BBPOM Kota Semarang [16].
10	Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan SNI ISO/IEC 27001:2009 Studi Kasus : Pengamanan

	Informasi Pada Institusi Perguruan Tinggi Sekolah Tinggi Teknologi Duta Bangsa Bekasi [17].

Fokus dari objek yang diteliti adalah penilaian 5 area yang dilakukan terhasdap lembaga penyelenggara sistem elektronik yang menggunakan Indeks KAMI 2.3. Kemudian nanti akan dianalisis kesenjangannya sehingga dketahui poin pertanyaaan pada area yang menjadi masalah bagi penyelenggara sistem elektronik. Dengan begitu dapat dijadikan evaluasi awal untuk memberikan rekomendasi terhadap permasalahasn yang paling sering muncul pada lembaga penyelenggasra sistem elektronik.

4.3. Data yang Diperlukan

Data yang diperlukan dalam penelitian tugas akhir ini digunakan untuk mendukung proses analisis yang akan dilakukan. Adapun data yang diperlukan disajikan sebagai berikut :

1. Peran TIK
   Penilaian peran TIK pada penyelenggara sistem elektronik untuk mengkategorikan penelitian yang akan digunakan nantinya.
2. Hasil Penilaian Tata Kelola
   Penilaian Tata Kelola Keamanan informasi pada beberapa penelitian penyelenggara sistem elektronik
3. Hasil Penilaian Risiko
   Penilaian Risiko Keamanan informasi penelitian pada beberapa penelitian penyelenggara sistem elektronik.
4. Hasil Penilaian Kerangka Kerja
   Penilaian Kerangka Kerja Keamanan informasi penelitian pada beberapa studi kasus penyelenggara sistem elektronik.
5. Hasil Penilaian Pengelolaan Aset
   Penilaian Pengelolasan Aset informasi penelitian pada beberapa studi kasus penyelenggara sistem elektronik.

6. Hasil Penilaian Teknologi
   Penilaian Teknologi dan Keamanan informasi penelitian pada beberapa studi kasus penyelenggara sistem elektronik.

4.4. Persiapan Pengumpulan Data

Pada bagian ini dijelaskan mengenai metode pengumpulan data. Pada penelitian tugas akhir ini metode pengumpulan data yang digunakan adalah pengumpulan data yang bersumber dari penelitian – penelitian yang menggunakan Indeks KAMI versi 2.3. Dari dokumen penelitian tersebut maka akan didapatkan data yang dibutuhkan berupa nilai Peran TIK, Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informais, Pengelolaan Aset Informasi dan Teknologi dan Keamanan Informasi. Data didapatkan dengan mengumpulkan dokumen secara langsung kepada penulis maupun lewat perpustakaan.

4.5. Metode Pengolahan Data

Setelah didapatkan hasil dari pengumpulan data melalui dokumen – dokumen penelitian yang mengimplementasikan Indeks KAMI versi 2.3 maka akan dilakukan pengecekan validitas dan realibilitas data berdasarkan kriteria *credibility, dependability, conformability* dan *transferability* kemudian akan dilakukan penulisan ulang penilaian yang dilakukan pada software microsoft excel. Setelah data sudah disajikan dalam excel maka akan dilakukan validasi terhadap lembaga penyelenggara sistem elektroniknya berdasarkan kriteria Peran TIK (*High*, *Medium* dan *Low*) dan dikategorikan berdasarkan tingkat kematangan reaktif untuk memastikan kesetaraan untuk penilaian yang akan dibandingkan.

Tabel 4 2. Kategori Peran TIK

No.	Nilai Peran TIK	Status	Keterangan
1	0 – 16	*Low*	Penggunaan TIK pada ruang lingkup yang terbatas dan tidak berpengaruh terhadap proses kerja yang sedang berjalan.
2	17 – 32	*Medium*	Penggunaan TIK merupakan bagian dari proses kerja yang berjalan
3	33 – 48	*High*	Penggunaan TIK memberikan ketergantungan yang sangat besar untuk mendukung proses strategis

Kemudian dilakukan validasi terhadap penelitian yang telah dikumpulkan berdasarkan kriteria yang telah dibuat.

Tabel 4 3.Rancangan Validasi Peran

No.	Pertanyaan	P1	P2	P3	P4	P5
1						
2						

Total Skor					
Status					

Data penelitian yang digunakan adalah data yang telah diklasifikasikan berdasarkan kriteria lembaga penyelenggara sistem elektronik yang beradapada level *medium* dan *high* yang mengisyaratkan bahwa lembaga tersebut telah menggunakan TIK sebagai satu kesatuan pada proses kerja lembaganya. Kemudian dilakukan pengelompokkan berdasarkan tingkat kematangan reaktif dari penyelenggara sistem elektronik. Berdasarkan penilaian yang sudah divalidasi dalam kriteria selanjutnya dilakukan analisis kesenjangan yang ingin melihat mana poin pertanyaan yang memiliki kesenjangan paling besar yang dapat dinyatakan sebagai masalah bagi lembaga penyelenggara sistem elektronik. Berdasarkan daftar poin yang menjadi masalah bagi penyelenggara sistem elektronik maka akan diberikan rekomendasi berdasarkan SNI ISO/IEC 27001.

4.6. Penentuan Pendekatan Analisis

Setelah dilakukan pengeolahan terhadap data sehingga datanya bisa dijadikan bahan anlisis, selanjutnya dilakukan analisis kesenjangan dan anlisis temuan.

4.6.1. Pendekatan Analisis Kesenjangan

Analisis kesenjangan (*gap analysis*) untuk membandingkan nilai pada penelitian Indeks KAMI. Dimana membandingkan poin AS-IS dengan poin TO-BE yang merupakan penerapan secara menyeluruhnya dari Indeks KAMI. Perbandingan antara kedua poin itu dihitung dengan rumus G (Kesenjangan) = expected service (TO-BE) – preceived service (AS-IS). Setelah

didapat kesenjangan atau gap antara kedua poin tersebut maka akan diberikan rekomendasi secara umum sebagai bahan evaluasi untuk lembaga penyelenggara sistem elektronik dalam mencapai standar SNI ISO/IEC 27001. Berikut merupakan rancangan tabel kesenjangannya.

Tabel 4 4. Rancangan Analisis Kesenjangan

Tata Kelola	Pertanyaan	Kesenjangan					Rata
		P1	P2	P3	P4	P5	

4.6.2. Pendekatan Aanlisis Temuam

Pada analisis temuan ini dilakukan pengeolahan terhadap hasil kesenjangan institutsi/ lembaga penyelenggara sistem elektronik. Adapun Hal yang dilakukan adalah :

1. Visualisasi Kesenjangan
   Pada bagian ini dilakukan pengolahan terhadap hasil analisis kesenjangan dimana disajikan dalam bentuk diagram batang untuk membandingkan kesenjangan tiap poin pertanyaan area pada hasil analisis kesenjangan.
2. Pengurutan Kesenjangan
   Pada bagian ini dilakukan pengurutan terhadap nilai kesenjangan untuk mengetahui poin pertanyaan mana yang memiliki kesenjangan paling besar secara keseluruhan maupun secara area sehingga bisa disimpulkan poin pertanyaan yang menjadi masalah. Setelah itu dilanjutkan dengan pengkategorian masalah.

3. Pengkategorian Masalah
   Pada kesenjangan yang sudah diurutkan, dilakukan proses pengidentifikasian masalah yang mungkin muncul jika poin pertanyaan tidak diterapkan. Kemudian dilakukan penilaian berdasarkan kriteria untuk dapat mengetahui kategori masalahnya. Kriteria yang digunakan adalah kriteria dampak dan kriteria probabilitas [37]. Adapun kriterianya adalah sebagai berikut :

Kriteria Dampak

Tabel 4 5 Kriteria Dampak

Dampak		
Rating	Kriteria	Keterangan
1	Insignificant	Dampak dapat diabaikan dengan aman karena tidak mengganggu
2	Minor	Dampak kecil dan dapat dan dapat diatasi dengan prosedur sederhana
3	Moderate	Dampak tergolong besar, namun dapat dikelola dengan menggunakan prosedur tertentu

4	Major	Dampak besar, berpotensi pada *financial cost* dan terhambatnya kinerja organisasi
5	Catastrophic	Dampak ekstrim, berptensi pada large finansial cost dan terhentinya kinerja organisasi, serta berdampak pada reputasi organisasi

Kriteria Probabilitas

Tabel 4 6. Kriteria Probabilitas

Probabilitas		
Rating	Kriteria	Keterangan
1	Rare	Sekali dalam > 5 tahun
2	Unlikely	Sekali dalam 2 – 5 tahun
3	Possible	Sekali dalam 1 – 2 tahun
4	Likely	Beberapa kali dalam setahun
5	Almost Certain	Terjadi tiap minggu/bulan

Dari hasil kedua kriteria dampak dan probabilitas maka akan dilakukan pengkalian (DxP) keduanya sehingga didapatkan kategori masalah yang mungkin muncul. Pemetaan hubungan mendapatkan permasalahan dari poin pertanyaan yang memiliki efek besar jika tidak diimplementasikan. Berikut merupakan kategori masalah untuk kriteria dampak dan probabilitas :

Kriteria Masalah

Tabel 4 7. Kriteria Masalah

		Dampak				
		5	4	3	2	1
Probabilitas	5	H(25)	H(20)	H(15)	M(10)	M(5)
	4	H(20)	H(16)	M(12)	M(8)	L(4)
	3	H(15)	M(12)	M(9)	M(6)	L(3)
	2	M(10)	M(8)	M(6)	L(4)	L(2)
	1	M(5)	L(4)	L(3)	L(2)	L(1)
Skala Dampak : 15 – 25 = High; 5 – 14 = Medium; 1 – 4 Low						

“Halaman ini sengaja dikosongkan”

BAB V
IMPLEMENTASI

Pada bab ini akan dijelaskan hasil dari proses perancangan studi kasus dan penggalian data yang didapatkan lewat dokumen penelitian – penelitian yang menerapkan Indeks KAMI 2.3

5.1. Hasil Penggalian Data Dokumen

Pengumpulan data dokumen dilakukan dengan pencarian penelitian yang menerapkan Indeks KAMI dengan menggunakan berbagai sumber. Pencarian yang dilakukan dimulai dari internet, perpustakaan dan email secara langsung kepada peneliti. Dari pencarian yang dilakukan tersebut maka didapatkan 10 data penilaian penelitian yang menerapkan Indeks KAMI. Adapun dokumen penelitian penilaian Indeks KAMI kepada penyelenggara sistem elektronik adalah sebagai berikut :

Tabel 5 1. Dokumen Penelitian

No.	Judul	Penulis	Tahun	Temuan
1	Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan SNI ISO/IEC 27001:2009 Studi Kasus:	Ridho, Moch. Rashid	2012	Dari evaluasi 5 area yang dilakukan pada Indeks KAMI dengan studi kasus Bidang Aplikasi Dan Telematika Dinas Komunikasi Dan Informatika Surabaya,

No.	Judul	Penulis	Tahun	Temuan
	Bidang Aplikasi Dan Telematika Dinas Komunikasi Dan Informatika Surabaya [8].			diketahui mendapat skor total 498 yang dapat diartikan baik dalam mengimplement asikan standar ISO 27001
2	Evaluasi pengelolaan keamanan jaringan di ITS dengan menggunakan Standar Indeks Keamanan informasi (KAMI) KEMENKOMI NFO RI [9].	Luthfiya Ulinnuha	2013	Pada penelitian ini didapatkan temuan bahwa skor akhir sejumlah 286 satu untuk penilaian kelima area dari total 588. Kemudian untuk tingkat kematangan seluruh area berada pada level I yang artinya pemahaman keamanan informasinya dikategorkan reaktif.
3	Penggunaan indeks keamanan	Roodhin Firmana	2013	Pada penelitian yang dilakukan pada PT. PLN

No.	Judul	Penulis	Tahun	Temuan
	informasi (KAMI) sebagai evaluasi keamanan informasi pada PT. PLN Distribusi Jawa Timur [10].			Distribusi Jawa Timur ini didapatkan total skor 190 dari total skor 588 sehingga masih dikatakan bahwa masih tidak layak untuk mencapai sertifikasi SNI ISO/IEC 27001.
4	Evaluasi keamanan informasi pada divisi network of broadband PT. Telekomunikasi Indonesia Tbk dengan menggunakan Indeks Keamanan Informasi (KAMI) [11].	Endi Lastyono Putra	2014	Dari penilaian yang dilakukan pada Divisi Network Telkom ini diketahui bahwa total skor untuk kelima areanya senilai 582 dari total 588 total skor sehingga menempatkannya pada level V yang dapat dikatakan sudah optimal dalam penerapan menajemen

No.	Judul	Penulis	Tahun	Temuan
				keamanan informasinya.
5	Evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi (KAMI) pada kantor wilayah Ditjen Perbendaharaan Negara Jawa Timur [12].	Mustaqim Siga	2014	Pada penelitian yang dilakukan oleh Mustaqim diketahui bahwa kesiapan pengelolaan keamanan informasi pada pada kantor wilayah Ditjen Perbendaharaan Negara Jawa Timur mendapat skor 337 dari nilai maksimal 588.
6	Analisa tingkat keamanan informasi pada sistem informasi administrasi kependudukan (SIAK) di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bantaeng menggunakan	Kasiran, Asrani	2014	Objek dari penelitian adalah sistem informasi administrasi kependudukan (SIAK). Dari hasil penilaian diketahui bahwa total skor sebesar 244 dengan status

No.	Judul	Penulis	Tahun	Temuan
	indeks KAMI [13].			kematangan pada I+
7	Evaluasi Keamanan Informasi pada PTI PDAM Tirta Moedal Kota Semarang Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001: 2009 [14].	Diah Wardani	2015	Pada penelitian ini diketahui bahwa tingkat keamanan informasi pada PTI PDAM Tirta Moedal Kota Semarang memperoleh skor sebesar 325 dari total 588 sehingga bisa dikatakan tingkat kematangannya berada pada level I+
8	Evaluasi keamanan informasi menggunakan metode indeks keamanan informasi (KAMI) (Studi kasus: STIE	Radhifan Hidayat	2016	Penelitian yang dilakukan oleh Radhifan ini melakukan evaluasi keamanan informasi pada STIE Perbanas Surabaya yang

No.	Judul	Penulis	Tahun	Temuan
	Perbanas Surabaya) [15].			mana mendapatkan skor sebesar 252 dari 588 sehingga tingkat kematangan STIE Perbanas berada pada level I.
9	Evaluasi tingkat kelengkapan dan kematangan sistem keamanan informasi berdasarkan Indeks KAMI pada Divisi Sampling dan Pengujian BBPOM Kota Semarang [16].	Winda Septilia	2016	Penelitian ini bertujuan meningkatkan pengelolaan keamanan informasi agar daapt mendukung tujuan bisnis. Dari evaluasi yang dilakukan diketahui bahwa skor untuk tingkat kematangan Divisi Sampling dan Pengujian ini sebesar 381 yang berada pada level II+.

No.	Judul	Penulis	Tahun	Temuan
10	Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan SNI ISO/IEC 27001:2009 Studi Kasus : Pengamanan Informasi Pada Institusi Perguruan Tinggi Sekolah Tinggi Teknologi Duta Bangsa Bekasi [17].	Dedi Wirasasmita	2017	Hasil penelitian yang dilakukan di Sekolah Tinggi Teknologi Duta Bangsa Bekasi ini menyimpulkan bahwa pengamanan informasi yang dilakukan masih rendah. Hal ini dibuktikan dengan skor yang didapat berjumlah 121 dari toatl 588 sehingga dapat dikatakan tingkat kematangannya masih rendah (level I).

5.2. Validasi Lembaga Penyelenggara Sistem Elektronik

Setelah berhasil dikumpulkan 10 penelitian yang menerapkan Indeks KAMI versi 2.3 maka dilakukan validasi untuk memastikan penelitian yang digunakan cukup setara untuk disandingkan yang mana menggunakan kriteria peran TIK low medium dan high. Yang digunakan dalam penelitian ini adalah objek penelitian yang berstatus medium dan high yang mengisyaratkan bahwa penggunaan TIK sudah digunakan dalam proses kerja. **LAMPIRAN A1 – A10**

Tabel 5 2. Peran TIK Penelitian

Penelitian	1	2	3	4	5	6	7	8	9	10
Total Skor	48	29	40	44	36	22	36	30	26	10
Status	H	M	H	H	H	M	H	M	M	L

Dari hasil validasi peran TIK terhadap kesepuluh penelitian yang menerapkan Indeks KAMI maka didapatkan hasil bahwa 9 penelitian memenuhi kriteria high dan medium. Setelah itu dilakukan validasi yang dilakukan adalah sebagai berikut :

Tabel 5 3. Validasi Kriteria Penelitian

No	Credibility	Transferability	Dependability	Conformability
1	Penilaian pada peneitian ini dilakukan pada Dinas Komunikasi dan Informastika	Menerapkan Indeks KAMI versi 2.3, Melakukan Penilaian pada total	Total Kematangan 498 pada level III+ (Terdefinisi	Penilaian untuk masing – masing penelitian atau kondisi as-is dapat

	Bidang Aplikasi & Telematika Surabaya, Pengisi evaluasi adalah Emadarta Tri Wijaya, ST, MT selaku Kepala Seksi Aplikasi dan Database. Pengisian dilakukan pada tanggal 12 -30 Mei 2012.	119 poin pertanyaan area pada area Tata Kelola, Risiko, Kerangka Kerja, Pengelolaan Aset dan Teknologi.	dan Konsisten)	dilihat pada lampiran
2	Penilaian ini dilakukan pada Badan Teknologi Sistem Informasi (BTSI) ITS Surabaya, Pengisi evaluasi adalah Ardian Naftali, ST selaku Kepala sub.bagian Jaringan dan Sistem	Menerapkan Indeks KAMI versi 2.3, Melakukan Penilaian pada total 119 poin pertanyaan area pada area Tata Kelola, Risiko, Kerangka Kerja, Pengelolaan	Total kematangan 286 pada level I (Kondisi Awal)	Penilaian untuk masing – masing penelitian atau kondisi as-is dapat dilihat pada lampiran

	informasi pada tahun 2013.	Aset dan Teknologi.		
3	Penilaian dilakukan pada PT. PLN Distribusi Jatim, Sub Bidang Teknologi Informasi Bidang Perencanaan. Pengisi evaluasi adalah Anton S.B. Utomo yang menjabat sebagai SPV Aplikasi TI. Pengisian dilakukan pada tanggal 12 Desember 2012	Menerapkan Indeks KAMI versi 2.3, Melakukan Penilaian pada total 119 poin pertanyaan area pada area Tata Kelola, Risiko, Kerangka Kerja, Pengelolaan Aset dan Teknologi.	Total kematangan 190 pada level I+ (Kondisi Awal)	Penilaian untuk masing – masing penelitian atau kondisi as-is dapat dilihat pada lampiran
4	Penilaian dilakukan pada PT. Telekounikasi Indonesia Tbk divisi Network of Broadband. Pengisian dilakukan oleh Suratmin selaku Manajer	Menerapkan Indeks KAMI versi 2.3, Melakukan Penilaian pada total 119 poin pertanyaan area pada area Tata	Total kematangan 582 pada level V (Optimal)	Penilaian untuk masing – masing penelitian atau kondisi as-is dapat dilihat pada lampiran

	IP Security Network & Services. Pengisian dilakukan pada 22 Mei 2014.	Kelola, Risiko, Kerangka Kerja, Pengelolaan Aset dan Teknologi.		
5	Penilaian pada Kanwil DJPBN Prop. Jawa Timur Direktorat Jenderal Perbendaharaan Kementerian Keuangan RI. Pengisi evaluasi adalah Heri Susanto selaku pelaksana tugas. Pengisian dilakukan pada tanggal 10-24 Maret 2014	Menerapkan Indeks KAMI versi 2.3, Melakukan Penilaian pada total 119 poin pertanyaan area pada area Tata Kelola, Risiko, Kerangka Kerja, Pengelolaan Aset dan Teknologi.	Total kematangan 286 pada level II (Penerapan Kerangka Kerja Dasar)	Penilaian untuk masing – masing penelitian atau kondisi as-is dapat dilihat pada lampiran
6	Penilaian dilakukan pada Dinas Kependudukan dan Pencatatan	Menerapkan Indeks KAMI versi 2.3, Melakukan	Total kematangan 244 pada level I+	Penilaian untuk masing – masing penelitian

	Sipil Kabupaten Bantaeng. Pengisi evaluasi M. Nurhaer selaku Administrator Database pada tanggal 28 Agustus 2013.	Penilaian pada total 119 poin pertanyaan area pada area Tata Kelola, Risiko, Kerangka Kerja, Pengelolaan Aset dan Teknologi.	(Kondisi Awal)	atau kondisi as-is dapat dilihat pada lampiran
7	Penilaian pada Divisi Pengembangan Teknologi Informastika Perusahaan Daerah Air Minum Tirta Moedal Kota Semarang. Pengisi adalah Diah Wardani selaku Kepala PTI PDAM Tirta Moedal Kota Semarang pada 21 Mei 2015.	Menerapkan Indeks KAMI versi 2.3, Melakukan Penilaian pada total 119 poin pertanyaan area pada area Tata Kelola, Risiko, Kerangka Kerja, Pengelolaan Aset dan Teknologi.	Total kematangan 325 pada level I+ (Kondisi Awal)	Penilaian untuk masing – masing penelitian atau kondisi as-is dapat dilihat pada lampiran
8	Penilaia dilakukan pada STIE Perbanas	Menerapkan Indeks KAMI versi	Total kematangan 252 pada	Penilaian untuk masing –

	Surabaya yang diisi oleh Hariadi Yutanto, S.Kom, M.Kom selaku Kasie TIK yang dilakukan pada 14 April 2016	2.3, Melakukan Penilaian pada total 119 poin pertanyaan area pada area Tata Kelola, Risiko, Kerangka Kerja, Pengelolaan Aset dan Teknologi.	level I (Kondisi Awal)	masing penelitian atau kondisi as-is dapat dilihat pada lampiran
9	Penilaian dilakukan pada Divisi Sampling dan Pengujiian BBPOM kota Semarang dilakukan oleh Anggota Divisi Sampling dan Pengujian pada 2016.	Menerapkan Indeks KAMI versi 2.3, Melakukan Penilaian pada total 119 poin pertanyaan area pada area Tata Kelola, Risiko, Kerangka Kerja, Pengelolaan	Total kematangan 381 pada level II+ (Penerapan Kerangka Kerangka Kerja Dasar)	Penilaian untuk masing – masing penelitian atau kondisi as-is dapat dilihat pada lampiran

		Aset dan Teknologi.		

Dari tabel diatas diketahui masing – masing penelitian memiliki kematangan yang berbeda – beda. Untuk menyamakan objek analisis maka dilakukan pemilihan pada kematangan yang paling banyak muncul yaitu pada 5 penelitian yang sudah mencapai level I (Reaktif) dalam jangka 3 tahun. Selanjutnya untuk mempermudah penulisan, setiap penelitian diberikan inisial untuk mempermudah penulisan dan penomoran P1 – P5 pada proses selanjutnya. Adapun ke 5 penelitian tersebut adalah :

Tabel 5 4. Penelitian Yang Memenuhi Kriteria

No.	Judul	Penulis	Tahun	Inisial
1	Evaluasi pengelolaan keamanan jaringan di ITS dengan menggunakan Standar Indeks Keamanan informasi (KAMI) KEMENKOMINFO RI [9].	Luthfiya Ulinnuha	2013	P1
2	Penggunaan indeks keamanan informasi (KAMI) sebagai evaluasi keamanan informasi pada PT. PLN Distribusi Jawa Timur [10].	Roodhin Firmana	2013	P2
3	Analisa tingkat keamanan informasi pada sistem informasi administrasi kependudukan (SIAK) di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bantaeng menggunakan indeks KAMI [13].	Kasiran, Asrani	2014	P3
4	Evaluasi Keamanan Informasi pada PTI PDAM Tirta Moedal Kota Semarang Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001: 2009 [14].	Diah Wardani	2014	P4

5	Evaluasi keamanan informasi menggunakan metode indeks keamanan informasi (KAMI) (Studi kasus: STIE Perbanas Surabaya) [15].	Radhifan Hidayat	2015	P5

5.3. Pemetaan Kondisi AS-IS Penerapan Indeks KAMI

Kondisi AS-IS disinis adalah hasil penilaian yang telah dilakukan pada kesembilan penelitian yang nantinya akan diolah sengan analisis kesenjangan untuk mengetahui poin yang menjadi permasalahan bagi lembaga penyelenggara sistem elektronik. Data ini sudah dilakukan pemetaan dari dokumen – dokumen ke rancangan tabel pada *microsoft excel*.

5.3.1. Tata Kelola Keamanan informasi

Hasil dari penggalian data dokumen maka akan didapatkan penilaian tata kelola kemanan informasi dengan Indeks KAMI yang akan digunakan dalam analisis kesenjangan. **LAMPIRAN B-1**

5.3.2. Pengelolaan Risiko Keamanan informasi

Hasil dari penggalian data dokumen maka akan didapatkan penilaian pengelolaan risiko kemanan informasi dengan Indeks KAMI yang akan digunakan dalam analisis kesenjangan. **LAMPIRAN B - 2**

5.3.3. Kerangka Kerja Keamanan informasi

Hasil dari penggalian data dokumen maka akan didapatkan penilaian kerangka kerja kemanan informasi dengan Indeks KAMI yang akan digunakan dalam analisis kesenjangan. **LAMPIRAN B - 3**

5.3.4. Pengelolasan Aset informasi

Hasil dari penggalian data dokumen maka akan didapatkan penilaian tata kelola kemanan informasi dengan Indeks KAMI yang akan digunakan dalam analisis kesenjangan. **LAMPIRAN B - 4**

5.3.5. Teknologi dan Keamanan informasi

Hasil dari penggalian data dokumen maka akan didapatkan penilaian tata kelola kemanan informasi dengan Indeks KAMI yang akan digunakan dalam analisis kesenjangan. **LAMPIRAN B - 5**

5.4. Kondisi TO-BE Penerapan Indeks KAMI

Kondisi TO-BE merupakan kondisi yang akan dibandingkan dengan kondisi AS-IS dimana kondisi TO-BE akan menggunakan status pada Indeks KAMI yaitu “Diterapkan Secara Menyeluruh”. Perbandingan yang dilakukan akan mencari kesenjangan antara kedua kondisi tersebut sehingga dapat diketahui poin pertanyaan pada area Indeks KAMI yang menjadi permasalahan pagi lembaga penyelenggara sistem elektronik.

5.5. Hambatan

Dalam melakukan pengumpulan data dokumen penelitian yang menggunakan Indeks KAMI ditemukan beberapa hambatan yang perlu dilalui oleh penulis, diantaranya :

- Pencarian objek dokumen penelitian yang memiliki kriteria yang sama ataupun menyediakan data yang dibutuhkan lumayan sulit dikarenakan penilaian 5 area tidak disajikan secara lengkap.
- Untuk komunikasi lewat email kepada peneliti ada yang tidak dijawab, kalaupun dijawab membutuhkan beberapa hari untuk berkomunikasi hingga mendapatkan data yang diperlukan.

- Data yang diberikan ada yang memiliki kekurangan setelah diperiksa lebih lanjut.
- Tidak tersedianya setiap buku laporan cetak dari penelitian diperpustakaan karena sudah digudangkan atau memang tidak tersedia.

“Halaman ini sengaja dikosongkan”

BAB VI
HASIL DAN PEMBAHASAN

Pada bab ini akan disajikan hasil yang didapatkan dari penelitian ini serta pembahasan hasil yang didapat berdasarkan metode analisis yang digunakan.

6.1. Pemetaan Skor 5 Area Lembaga Penyelenggara Sistem Elekronik

Pada bagian ini dilalakukan pemetaan skor untuk masing – masing – masing penelitian Indeks KAMI pada lembaga penyelenggara sistem elektronik berdasarkan kelima area Indeks KAMI. Pemetaan disini merupakan penempatan nilai untuk setiap poin pertanyaan kesembilan penelitian pada tabel rancangan pada excel untuk di lakukan ke tahapan analisis kesenjangan. Adapun total poin pertanyaan yang ada adalah 119 poin pertanyaan. Berikut merupakan hasil pemetaan dari dokumen ke *microsoft excel*.

No	Pertanyaan	AS-IS						TO-BE
		P1	P2	P3	P4	P5	Rata-rata AS-IS	
1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan sebelumnya	3	2	3	3	2	2,6	3
2	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	3	2	0	3	1	1,8	3

Gambar 6 1. Hasil Pemetaan

Setelah dilakukan proses pemetaan ini, maka akan bisa dilanjutkan ke proses analisis kesenjangan dan analisis temuan.

Detail keseluruhan pemetaan area daapt dilihat pada **LAMPIRAN B-1 – B-5**

6.2. Analisis Kesenjangan

Setelah dilakukan pemetaan terhadap as-is dan to-be maka dilanjutkan dengan melakukan *gap analysis* antara kedua poin tersebut. Analisis yang dilakukan dengan menggabungkan seluruh poin as-is dari setiap penelitian untuk dicari kesenjangannya dengan nilai harapan sesuai dengan perangkat Indeks KAMI. Perhitungan dilakukan dengan menggunakan microsoft excel sesuai untuk masing – masing area. Dimana pada tahap awal dilakukan pengurangan dari poin to-be dengan as-is untuk tiap penelitian. Berikut contoh hasil perhitungan kesenjangan antara kelima penelitian pada area Tata Kelola.

No	Pertanyaan	Kesenjangan					Jumlah	Rata -Rata GAP	Peringkat Area	ringkat Keseluruh
		P1	P2	P3	P4	P5				
I.1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan	0	1	0	0	1	2	0,40	20	117
I.2	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	0	1	3	0	2	6	1,20	17	86

Gambar 6 2. Kesenjangan Pada 5 Penelitian

Kemudian dari seluruh hasil kesenjangan untuk tiap penelitian diratakan untuk mendapatkan kesenjangan yang mewakili seluruh penelitian. Pada kotak merah dibawah diperlihatkan hasil rataan untuk masing – masing kesenjangan tiap poin pertanyaan.

No	Pertanyaan	Kesenjangan					Jumlah	Rata -Rata GAP	Peringkat Area	ringkat Keseluruh
		P1	P2	P3	P4	P5				
I1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan	0	1	0	0	1	2	0,40	20	117
I2	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	0	1	3	0	2	6	1,20	17	86

Gambar 6 3. Hasil Kesenjangan Tiap Poin Pertanyaan

6.2.1. Hasil Nilai Kesenjangan Area Tata Kelola

Tabel 6.1 di bawah merupakan hasil analisis kesenjangan yang berkaitan dengan area tata kelola keamanan informasi pada lembaga – lembaga penyelenggara sistem elektronik.

Tabel 6 1. Hasil Nilai Kesenjangan Tata Kelola

Kode	AS-IS	TO-BE	GAP
I.1	2,6	3	0,40
I.2	1,8	3	1,20
I.3	2,4	3	0,60

I.4	2,2	3	0,80
I.5	1,2	3	1,80
I.6	1,4	3	1,60
I.7	1,2	3	1,80
I.8	1,2	3	1,80
I.9	3,6	6	2,40
I.10	4	6	2,00
I.11	3,6	6	2,40
I.12	3,2	6	2,80
I.13	3,6	6	2,40
I.14	4,4	6	1,60
I.15	2,4	9	6,60
I.16	2,4	9	6,60
I.17	2,4	9	6,60

I.18	1,8	9	7,20
I.19	3	9	6,00
I.20	3	9	6,00

Pada tabel 6.1 diketahui bahwa kesenjangan maksimal pada area tata kelola dimiliki oleh poin pertanyaan nomor I.18 dengan nilai 7,20. Poin peryanyaan ini membahas mengenai penerapan target dan sasaran pengelolaan keamanan informasi, dimana apakah lembaga penyelenggara sistem elektronik sudah menerapkan target dan sasaran dan melakukan pengevaluasian pencapaian dari target yang dibuat kemudian melaporkan kepada pemimpin instasnsi. Dari hasil ini diketahui bahwa dari kelima penelitian lembaga yang dinilai memiliki kecendrungan belum melakukkan pengelolaan pengukuran kinerja yang dilakukan pada poin pertanyaan ini. Hal itu terbukti dari P1, P3, dan P4 baru dalam tahap perencanaan sedangkan P2 dan P5 tidak melakukan apapun terkait poin ini. Kemudian kesenjangan terendah pada area tata kelola ini terletak pada poin I.1 dengan nilai 0,40 yang membahas mengenai komitmen dari pemimpin intansi secara prinsip dan resmi bertanggungjawab dalam pelaksanaan program keamanan informasi. Hal ini baik dan dapat dikatakan bahwa secara umum pemimpin intansi/lembaga penyelenggara sistem elektronik sudah sangat berkomitmen dalam pelaksanaan program keamanaan informasi secara resmi. Hal itu dibuktikan dari kelima penelitian yaitu P1, P3 dan P4 sudah menerapkan secara menyeluruh terhadap poin ini dan sisanya meenrapkan secara sebagian.

Pada tabel 6.2 disajikan kepatuhan tiap instansi terhadap penerapan secara keseluruhan poin pada area tata kelola. Dari 20 poin pertanyaan pada area tata kelola diketahui bahwa intansi/lembaga penyelenggara sistem elektronik pada P4 menerapkan secara menyeluruh 12 poin pertanyaan pada area tata kelola kemudian disusul oleh P1 dengan penerapan 6 poin, P3 dengan 2. Sedangkan P2 dan P5 tidak sama sekali menerapkan secara menyeluruh area ini. Secara keseluruhan intansi/lembaga penyelenggara sistem elektronik melaksanakan tata kelola keamanan informasi baru pada tahap perencanaan dan penerapan sebagian saja terhadap penata kelolaan keamanan informasi.

Tabel 6 2. Penerapan Secara Menyeluruh Tata Kelola

Kategori Pengamanan	P1	P2	P3	P4	P5
Tidak Dilakukan	0	8	6	0	8
Dalam Perencanaan	7	5	6	4	3
Diterapkan Sebagian	7	7	6	4	9
Diterapkan Secara Menyeluruh	6	0	2	12	0

6.2.2. Hasil Nilai Kesenjangan Area Risiko

Pada tabel 6.3 merupakan hasil analisis kesenjangan yang berkaitan dengan area risiko keamanan informasi pada lembaga – lembaga penyelenggara sistem elektronik.

Tabel 6 3. Hasil Nilai Kesenjangan Risiko

Kode	AS-IS	TO-BE	GAP
II.1	1,2	3	1,80
II.2	1,2	3	1,80
II.3	1,2	3	1,80
II.4	1,4	3	1,60
II.5	1,8	3	1,20
II.6	1,4	3	1,60
II.7	1,2	3	1,80
II.8	1,2	3	1,80
II.9	0,8	3	2,20
II.10	1,6	6	4,40

II.11	1,6	6	4,40
II.12	1,6	6	4,40
II.13	1,2	6	4,80
II.14	1,2	9	7,80
II.15	1,2	9	7,80

Dari hasil analisis kesenjangan yang dilakukan diketahui bahwa kesenjangan terbesar terletak pada poin II.15 dan II.14 dengan nilai yang sama yaitu 7,80. Poin pertanyaan II.15 mengenai proses pengelolaan risiko yang dijadikan bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan. Dari hasil ini diketahui bahwa intansi/lembaga penyelenggara sistem elektronik masih tidak menjadikan proses pengelolaan risiko menjadi kriteria penilaian kinerja pengamanan informasi di intansinya. Padahal lewat pengelolaan risiko yang baik dapat diketahui bahwa organisasi tersebut melakukan program pengamanan informasi yang baik pula. Dari intansi/lembaga pada kelima penelitian diketahui bahwa tidak ada yang menerapkan poin ini, hanya P3 dan P4 yang baru melakukan perencanaan sedangkan yang lainnya tidak melakukan sama sekali. Pada poin II.14 mengenai pengkajian kerangka kerja pengelollaan risiko secara berkala, diketahui bahwa tidak ada yang menerapkannya. Kelima penelitian tertinggi baru berada pada tahap perencanaan saja. Kemudian untuk kesenjangan terendah terletak pada poin pertanyaan II.5 dengan nilai 1,20 mengenai pendefinisian kepemilikan dan pengelola dari suatu aset informasi. Ini berarti sebagian besar instansi/organisasi sudah baik dalam melakukan pendefinisian tanggung jawab terhadap aset. Hal ini dibuktikan dari intansi pada P1 sampai P4

yang sudah menerapkannya sedangkan P5 sudah merencanakannya.

Pada tabel 6.4 di bawah disajikan kepatuhan tiap instansi terhadap penerapan secara keseluruhan poin pada area risiko. Dari 15 poin pertanyaan pada area risiko diketahui bahwa tidak ada intansi/lembaga penyelenggara sistem elektronik yang menerapkan secara menyeluruh pertanyaan pada risiko. Secara keseluruhan intansi/lembaga penyelenggara sistem elektronik baru dalam tahap perencanaan terhadap pengelolaan risiko keamanan informasi.

Tabel 6 4.Penerapan Secara Menyeluruh Risiko

Kategori Pengamanan	P1	P2	P3	P4	P5
Tidak Dilakukan	2	6	5	0	2
Dalam Perencanaan	10	1	9	11	13
Diterapkan Sebagian	3	8	1	4	0
Diterapkan Secara Menyeluruh	0	0	0	0	0

x

6.2.3. Hasil Nilai Kesenjangan Area Kerangka Kerja

Pada tabel 6.5 bawah ini merupakan hasil analisis kesenjangan yang berkaitan dengan area kerangka kerja keamanan informasi pada lembaga – lembaga penyelenggara sistem elektronik

Tabel 6 5. Hasil Nilai kesenjangan Kerangka Kerja

Kode	AS-IS	TO-BE	GAP
III.1	1,8	3	1,20
III.2	1,2	3	1,80
III.3	1,8	3	1,20
III.4	1,6	3	1,40
III.5	1,2	3	1,80
III.6	2,2	3	0,80
III.7	3,6	6	2,40
III.8	1,6	6	4,40
III.9	2	6	4,00
III.10	3,6	6	2,40
III.11	2	6	4,00
III.12	2	6	4,00

III.13	0,6	9	8,40
III.14	0,6	9	8,40
III.15	0	9	9,00
III.16	1,2	9	7,80
III.17	1,2	3	1,80
III.18	1,2	3	1,80
III.19	1,4	3	1,60
III.20	1,4	3	1,60
III.21	1,2	3	1,80
III.22	2,8	6	3,20
III.23	3,2	6	2,80
III.24	1,8	9	7,20
III.25	1,2	9	7,80

III.26	1,2	9	7,80

Pada tabel 6.5 diatas diketahui hasil kesenjangan terbesar terletak pada poin pertanyaan III.15 dengan nilai 9,00. Poin ini mengenai pengelolaan rencana pemulihan bencana (*disaster recovery plan*) apakah dievaluasi untuk memastikan keefektifannya dalam menangani bencana. Dari lima penelitian, tidak ada yang menerapkan secara menyeluruh poin area ini, semuanya tidak melakukannya sama sekali. Hal ini berarti instansi – instansi ini tidak melakukan pengevaluasian terhadap rencana pemulihan yang ada untuk mengecek apakah masih efektif dalam menyelesaikan bencana. Kemudian untuk kesenjangan terendah terletak pada poin III.6 dengan nilai 0,80 yang mengisyaratkan bahwa instansi penyelenggara sistem elektronik sangat memperhatikan aspek keamanan informasi mencakup pelaporan isiden, penjagaan kerahasiaan, penjagaan HAKI dan aturan penggunaan aset dengan pihak ketiga yang dituangkan dalam kontrak kerja. Hal ini dibuktikan dari intansi/lembaga penyelenggara elektronik P1 sudah menerapkan secara menyeluruh poin pertanyaan ini dalam kerja organisasi. Sisanya sudah menerapkan juga poin ini walaupun secara sebagian di dalam instansinya.

Pada tabel 6.6 di bawah disajikan kepatuhan tiap instansi terhadap penerapan secara keseluruhan poin pada area kerangka kerja keamanan informasi. Dari 26 poin pertanyaan pada area kerangka kerja diketahui bahwa intansi/lembaga penyelenggara sistem elektronik masih sangat sedikit dalam penerapan area ini. P4 menerapkan 1 poin secara menyeluruh pertanyaan pada area kerangka kerja kemudian P2 0 poin, P3 dengan 3 poin, P4 dengan 2 poin dan P5 dengan 1 poin. Secara keseluruhan intansi/lembaga penyelenggara sistem elektronik belum menerapkan dengan baik pengelolaan terhadap kerangka kerja keamanan informasi.

Tabel 6 6. Penerapan Secara Menyeluruh Kerangka Kerja

Kategori Pengamanan	P2	P3	P6	P7	P8
Tidak Dilakukan	7	15	9	3	16
Dalam Perencanaan	10	3	6	0	3
Diterapkan Sebagian	8	8	8	21	6
Diterapkan Secara Menyeluruh	1	0	3	2	1

6.2.4. Hasil Nilai Kesenjangan Area Pengelolaan Aset

Pada tabel 6.7 di bawah ini merupakan hasil nilai kesenjangan yang berkaitan dengan area pengelolaan aset keamanan informasi pada lembaga – lembaga penyelenggara sistem elektronik

Tabel 6 7. Nilai Kesenjangan pengelolaan Aset

Kode	AS-IS	TO-BE	GAP
IV.1	1,6	3	1,40
IV.2	1,8	3	1,20
IV.3	1,6	3	1,40
IV.4	2	3	1,00

IV.5	2	3	1,00
IV.6	1,6	3	1,40
IV.7	2	3	1,00
IV.8	1,8	3	1,20
IV.9	1,2	3	1,80
IV.10	1,8	3	1,20
IV.11	2	3	1,00
IV.12	1,6	3	1,40
IV.13	1,8	3	1,20
IV.14	2,4	3	0,60
IV.15	1,6	3	1,40
IV.16	2,4	3	0,60
IV.17	4	6	2,00
IV.18	4	6	2,00

IV.19	2	6	4,00
IV.20	2,8	6	3,20
IV.21	4,8	6	1,20
IV.22	6	9	3,00
IV.23	5,4	9	3,60
IV.24	4,2	9	4,80
IV.25	2	3	1,00
IV.26	2	3	1,00
IV.27	2,2	3	0,80
IV.28	2,6	3	0,40
IV.29	1,4	3	1,60
IV.30	4,8	6	1,20
IV.31	4	6	2,00

IV.32	4,4	6	1,60
IV.33	4	6	2,00
IV.34	4,8	9	4,20

Pada tabel 6.7 diatas diketahui bahwa nilai kesenjangan tertinggi terletak pada poin pertanyaan IV.24 yang membahas mengenai prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan. Hal ini berarti masih banyak instansi/ lembaga penyelenggara elektronik yang tidak memiliki dan menerapkan prosedur yang mengatur penggunaan perangkat pengolahan informasi pihak ketiga. Hal ini dapat dibuktikan dari lima penelitian hanya P3, P4 dan P5 yang menerapkannya secara sebagian. Sedangkan P1 baru merencanakan dan P2 tidak melakukannya. Kemudian kesenjangan terendah pada area pengelolaan aset ini terletak pada poin IV.28 yang mengatur mengenai perlindungan yang diberikan kepada infrstruktur komputasi dari gangguan kelistrikan dan dampak dari petir yang mengisyaratkan bahwa instansi/lembaga penyelenggara sistem elektronik sangat memerhatikan kerusakan yang bisa ditimbulkan dari konsleting listrik maupun dampak dari petir. Hal ini dibuktikan dari intansi pada lima penelitian ada P1, P4 dan P5 yang melakukan penerapan secara menyeluruh terhadap poin pertanyaan ini dan sisanya sudah menerapkan poin area ini pada sebagian instansinya.

Pada tabel 6.8 di bawah disajikan kepatuhan tiap instansi terhadap penerapan secara keseluruhan poin pada area pengelolaan aset. Dari 34 poin pertanyaan pada area pengelolaan aset diketahui bahwa intansi/lembaga penyelenggara sistem elektronik sudah banyak yang

menerapkan sebagian area pengelolaan aset jika dibandingkan area lainnya, kedepannya perlu ditingkatkan untuk penerapan secara keseluruhan instansi/lembaga.

Tabel 6 8. Penerapan Secara Menyeluruh Pengelolaan Aset

Kategori Pengamanan	P1	P2	P3	P4	P5
Tidak Dilakukan	0	6	9	0	5
Dalam Perencanaan	6	4	5	0	0
Diterapkan Sebagian	24	24	17	20	17
Diterapkan Secara Menyeluruh	4	0	3	14	12

6.2.5. Hasil Nilai Kesenjangan Area Teknologi

Pada tabel 6.9 di bawah ini merupakan hasil nilai kesenjangan yang berkaitan dengan area teknologi keamanan informasi pada lembaga – lembaga penyelenggara sistem elektronik

Tabel 6 9. Hasil Nilai Kesenjangan Teknologi

Kode	AS-IS	TO-BE	GAP
V.1	2,2	3	0,80
V.2	2,2	3	0,80
V.3	2	3	1,00

V.4	1,6	3	1,40
V.5	1,8	3	1,20
V.6	2,2	3	0,80
V.7	2,2	3	0,80
V.8	1,6	3	1,40
V.9	1,6	3	1,40
V.10	2	3	1,00
V.11	2,4	6	3,60
V.12	2,8	6	3,20
V.13	2,8	6	3,20
V.14	2,8	6	3,20
V.15	4	6	2,00
V.16	4,8	6	1,20
V.17	1,6	3	1,40

V.18	2,2	3	0,80
V.19	2,8	3	0,20
V.20	3,6	6	2,40
V.21	3,6	6	2,40
V.22	4	6	2,00
V.23	3,6	6	2,40
V.24	1,8	9	7,20

Pada tabel 6.9 diatas diketahui bahwa nlai kesenjangan terbesar terletak pada poin pertanyaan V.24 dengan nilai 7,20. Poin pertanyaan ini berkaitan dengan pengkajian keamanan informasi instansi secara rutin yang melibatkan pihak independen. Hal ini berarti organisasi kurang memperhatikan pengkajian keamanan informasi organisasinya yang dapat menyebabkan pengamanan informasi yang dilakukan intansi tidak layak atau tidak memenuhi standar keamanan terbaru. Untuk itu instansi perlu mendatangkan pihak independen atau tanaga ahli yang dapat mengkajinya secara berkala. Dari kelima penelitian 3 instansi tidak melakukan, 1 instansi menerapkan secara sebagian dan 1 instansi dalam perencanaan. Kemudian kesenjangan terendah terletak pada point pertanyaan V.19 dengan nilai 0,20 yang membahas mengenai perlindungna yang diberikan terhadap setiap perangkat *desktop* dan *server* dari

serangan virus. Hal ini berarti instansi/lembaga penyelenggara sistem elektronik sangat memerhatikan ancaman dari virus yang dapat merusak data dan informasi pada perangkat pengolahan informasi. Dari 5 instansi/lembaga penyelenggara sistem elektronik 4 instansi menerapkan secara keseluruhan pada instansinya dan hanya 1 instansi yang menerapkan secara sebagian.

Pada tabel 6.10 di bawah disajikan kepatuhan tiap instansi terhadap penerapan secara keseluruhan poin pada area teknologi keamanan informasi. Dari 24 poin pertanyaan pada area teknologi keamanan informasi diketahui bahwa intansi/lembaga penyelenggara sistem elektronik masih sedikit yang menerapkan secara menyeluruh area teknologi keamanan informasi. Hal ini dapat dilihat dari P5 yang sudah menerapkan 13 poin pertanyaan, kemudian P1 dengan disusul dengan 6 poin, disusul P3 dan P4 dengan masing – masing menerapkan 5 poin, terakhir P2 dengan 4. Secara keseluruhan intansi/lembaga penyelenggara sistem elektronik melaksanakan teknologi keamanan informasi pada tahap penerapan sebagian terhadap pengelolaan teknologi keamanan informasi.

Tabel 6 10. Penerapan Secara Menyeluruh Teknologi

Kategori Pengamanan	P1	P2	P3	P4	P5
Tidak Diterapkan	1	8	5	2	3
Dalam Perencanaan	4	1	0	7	4
Diterapkan Sebagian	13	11	14	10	4
Diterapkan Secara Menyeluruh	6	4	5	5	13

6.3. Analisis Temuan

Setelah dilakukan analisis kesenjangan untuk setiap point pertanyaan pada penelitian, selanjutnya dilakukan visualisasi

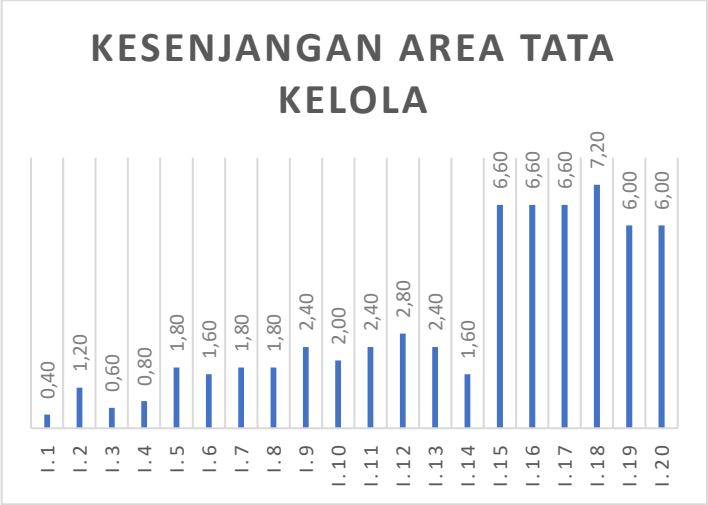
kesenjangan antara poin pertanyaan untuk tiap area. Setelah itu akan dilanjutkan dengan pengurutan poin pertanyaan yang memiliki kesenjangan paling besar dan dapat diartikan sebagai poin pertanyaaan yang menjadi permasalahan bagi instansi/lembaga penyelenggara sistem elektronik. Setelah pengurutan berdasarkan kesenjangan, dilakukan juga pengidentifikasian masalah untuk tiap area, bila poin tiap pertanyaan itu tidak diterapkan.

6.3.1. Visualisasi kesenjangan

Pembuatan visualisasi kesenjangan dilakukan dengan menggunakan data kesenjangan tiap area yang dibuat dalam bentuk diagram batang dengan menggunakan *microsoft excel*. Pembuatan visualisasi dilakukan untuk mempermudah penyampaian dan penyajian hasil kesenjangan.

6.3.1.1. Diagram Tatakelola

Diagram di bawah ini merupakan hasil kesenjangan area tata kelola yang membandingkan antara poin as-is yang merupakan hasil penilaian pada penelitian instansi/lembaga penyelenggara sistem elektronik dengan poin to-be yang merupakan penerapan secara menyeluruh area.



Gambar 6 4. Digram Tata Kelola

Pada gambar 6.4 diatas menunjukkan bahwa kesenjangan secara garis besar terbagi menjadi 2 bagian dimana ada kesenjangan yang rendah yaitu di bawah 4 pada poin pertanyaan I.1 sampai 1.14 dan tinggi yaitu diatas 4 pada poin pertanyaan I.15 sampai I.20. Sehingga dapat dikatakan poin I.15 sampai I.20 menjadi kelompok permasalahan besar yang harus dihadapi intansi/lembaga penyelenggara sistem elektronik.

Tabel 6 11. Statistik Area Tata kelola

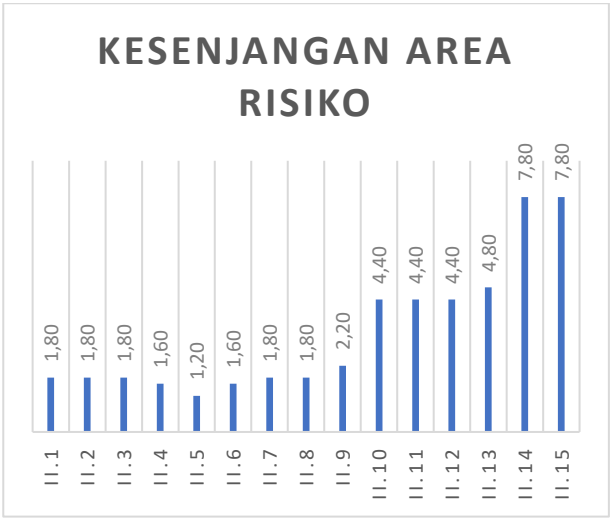
	Tata Kelola
Rata - rata	3,13
Max	7,20
Min	0,40

Pada tabel 6.11 diatas menunjukkan bahwa pada area tata kelola ini kesenjangan terbesar yang menjadi masalah bagi penyelenggara sistem elektronik berada pada poin pertanyaan nomor I.18 mengenai penetapan target dan sasaran pengelolaan keamanan informasi yang berguna dalam pengukuran kinerja

secara rutin. Kemudian untuk kesenjangan terendah berada pada poin I.1 dengan nilai 0,40 yang membahas mengenai komitmen dari pemimpin intansi untuk melaksanakan kemanaan informasi. Kemudian area tata kelola memiliki rata – rata kesenjangan bernilai 3,13 untuk keseluruhan poin pertanyaaan yang jika dibandingkan dengan area lain maka area tata kelola memiliki peringkat 3 dengan kesenjangan yang menjadi masalah terbesar.

6.3.1.2. Diagram Risiko

Diagram di bawah ini merupakan hasil kesenjangan area risiko yang membandingkan antara poin as-is yang merupakan hasil penilaian pada penelitian instansi/lembaga penyelenggara sistem elektronik dengan poin to-be yang merupakan penerapan secara menyeluruh area.



Gambar 6 5. Diagram Risiko

Pada gambar 6.5 diatas menunjukkan bahwa kesenjangan terbagi menjadi 2 bagian yaitu yang rendah berada di bawah 4 pada poin II.1 sampai II.9. Kemudian bagian yang tinggi berada pada nilai diatas 4 yaitu poin pertanyaan II.10 sampai II.15. Sehingga dapat dikatakan bahwa poin II.10 sampai II.15 menjadi permasalahan besar yang dihadapi oleh instansi/lembaga penyelenggara sistem elektronik terutama pada poin II.14 dan II.15 yang memiliki kesenjangna sangat besar.

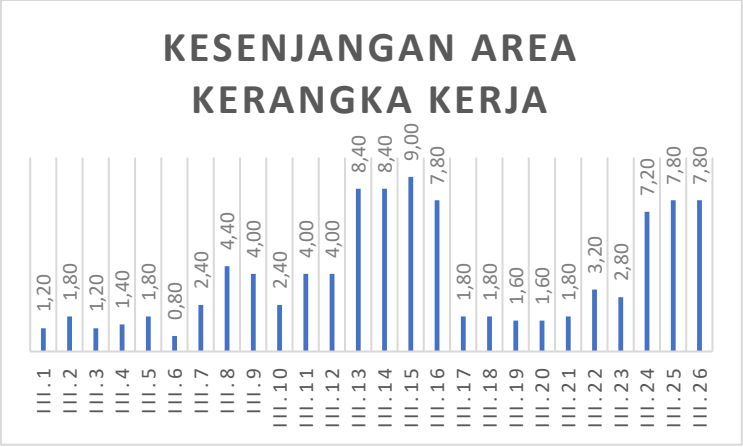
Tabel 6 12. Statistik Area Risiko

	Risiko
Rata - rata	3,28
Max	7,80
Min	1,20

Pada tabel 6.12 diatas menunjukkan bahwa pada area risiko ini kesenjangan terbesar yang menjadi masalah bagi penyelenggara sistem elektronik berada pada poin pertanyaan nomor II.15 mengenai pengelolaan risiko yang yang dijadikan kriteria penilaian efektifitas keamanaan. Berarti secara umum instansi atau lembaga belum menjadikan pengelolaan risiko menjadi kriteria keefektifan pengamanannya padahal pengelolaan risiko adalah kesatuan proses yang mengelola risiko aset hingga upaya pemulihannya.Kemudian untuk kesenjangan terendah berada pada poin II.5 dengan nilai 1,20 yang mengenai pendefinisian pengelola aset. Hal ini dapat diartikan secara umum intansi/lembaga penyelenggar elektronik sudah mendefinisikan pengelola aset pentingnya. Kemudian area tata risiko memiliki rata – rata kesenjangan bernilai 3,28 untuk keseluruhan poin pertanyaaan yang jika dibandingkan dengan area lain maka area risiko memiliki peringkat 2 dengan kesenjangan terbesar yang menjadi masalah bagi intansi/lembaga penyelenggara sistem elektronik.

6.3.1.3. Diagram Kerangka Kerja

Diagram di bawah ini merupakan hasil kesenjangan area kerangka kerja yang membandingkan antara poin as-is yang merupakan hasil penilaian pada penelitian instansi/lembaga penyelenggara sistem elektronik dengan poin to-be yang merupakan penerapan secara menyeluruh area.



Gambar 6 6. Diagram Kerangka Kerja

Pada gambar 6.6 diatas menunjukkan 2 kelompok besar yang memiliki kesenjangan saling berdekatan. Yang pertama ada kelompok dengan nilai di bawah 4 yang terdiri dari poin III.1 sampai III.7, III.9 sampai III.12 dan III.17 Sampai III.23. Kemudian kelompok kedua dengan nilai kesenjangan diatas 4 yaitu poin III.8, poin III.13 sampai III.16 dan III.24 sampai III.26. Untuk itu intansi penyelenggara sistem elektronik perlu melakukan perhatian yang serius pada poin pertanyaan yang memiliki kelompok nilai diatas 4.

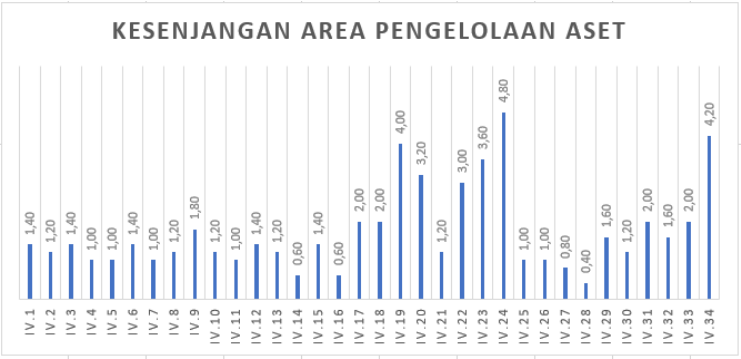
Tabel 6 13. Statistik Area Kerangka Kerja

	Kerangka Kerja
Rata - rata	3,86
Max	9,00
Min	0,80

Pada tabel 6.13 diatas menunjukkan kesenjangan terbesar terjadi pada III.15 dengan nilai 9,00 mengenai pengevaluasian secara berkala terhadap *disaster recovery plan* dan kesenjangan terendah terjadi pada poin III.6 dengan nilai 0,80 mengenai kontrak aturan keamanan informasi yang menyangkut pihak ketiga. Kemudian kerangkat kerja memiliki rata – rata kesenjangan sebesar 3,86 yang menjadikannya area dengan peringkat 1 yang menjadi masalah bagi instansi/lembaga penyelenggara sistem elektronik.

6.3.1.4. Diagram Pengelolaan Aset

Diagram di bawah ini merupakan hasil kesenjangan area pengelolaan aset yang membandingkan antara poin as-is yang merupakan hasil penilaian pada penelitian instansi/lembaga penyelenggara sistem elektronik dengan poin to-be yang merupakan penerapan secara menyeluruh area.



Gambar 6 7. Diagram Pengelolaan Aset

Pada gambar 6.7 diatas menunjukkan kesenjangan pada area pengelolaan aset. Nilai kesenjangan pada area ini hampir seluruhnya berada di bawah 4. Hanya poin IV.24 dan IV.34 dapat dikatakan tingga jika dikelompokkan berdasarkan pengelompokkan kesenjangan pada area sebelumnya dapat dikatakan kesenjangan pada area pengelolaan aset cukup rendah.

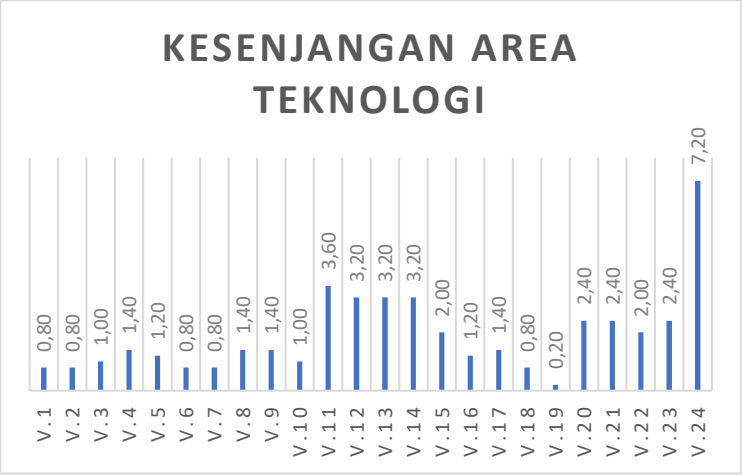
Tabel 6 14. Statistik Area Pengelolaan Aset

	Pengelolaan Aset
Rata - rata	1,72
Max	4,80
Min	0,40

Pada tabel 6.14 diatas diketahui bhwa kesenjangan tertinggi bernilai 4,80 yang dimiliki oleh poin pertanyaan IV.24 mengenai prosedur keamanan penggunaan perangkat pihak ketiga dan kesenjangan terendah bernilai 0,40 dimiliki oleh poin pertanyaan IV.28 mengenai peangamanan perangkat komputasi terkait kelistrikan dan petir. Kemudian untuk rata – rata kesenjangan pada area pengelolaan aset bernilai 1,72 yang menjadikannya peringkat terakhir dalam peringkat area dengan kesenjangan terbesar.

6.3.1.5. Diagram Teknologi

Diagram di bawah ini merupakan hasil kesenjangan area teknologi yang membandingkan antara poin as-is yang merupakan hasil penilaian pada penelitian instansi/lembaga penyelenggara sistem elektronik dengan poin to-be yang merupakan penerapan secara menyeluruh area.



Gambar 6 8. Diagram Teknologi

Pada gambar 6.8 diatas menunjukkan kesenjangan pada area teknologi dan keamanan inforamsi. Pada area ini dapat diaktegorikan bahwa poin pertanyaan dari V.1 sampai V.23 rendah karena memiliki nilai di bawah 4 sedangkan V.24 dikategorikan tinggi karena memiliki nilai diatas 4 berdasarkan pengkategorian area – area sebelumnya.

Tabel 6 15. Statistik Area Teknologi

	Teknologi
Rata - rata	1,91
Max	7,20
Min	0,20

Pada tabel 6.15 diatas disajikan nilai kesenjangan maksimal yang bernilai 7,20 yang dimiliki oleh V.24 mengenai pelibatan pihak independen dalam pengkajian keamanan informasi secara rutin. Dan kesenjangan minimal pada area teknologi ini bernilai 0,20 yang dimiliki oleh poin pertanyaan V.19 mengenai pengamanan *desktop* dan *server* dari virus. Hal ini berarti

lembaga penyelenggara elekronik sudah sangat memperhatikan ancaman dari virus sehingga sudah menerapkan perlindungan dari virus. Kemudian kesenjangan area teknologi memilki rata – rata sebesar 1,91 yang membuat area ini menjadi peringkat ke-2 dari terakhir dalam peringkat kesenjangan terbesar untuk tiap area.

6.3.2. Pengurutan Kesenjangan dan Kategori Masalah

Pengurutan kesenjangan dilakukan untuk melihat poin pada area yang memiliki kesenjangan yang sangat besar dan menjadi masalah bagi penyelenggara sistem elektronik. Pengurutan dilakukan dengan dua jenis yang pertama berdasarkan Area menghasilkan peringkat area (PA), yang kedua berdasarkan keseluruhan menghasilkan peringkat keseluruhan (PK).

Setelah itu dilakukan pengidentifikasian masalah yang didapatkan jika poin pertanyaan tidak diterapkan. Kemudian dilakukan pengkategorian masalah berdasarkan kriteria dampak dan probabilitas yang telah dibuat sebelumnya. Sehingga dapat diketahui poin pertanyaan yang berpeluang merugikan jika tidak diterapkan.

6.3.2.1. Pengurutan dan Kategori Masalah Area Tata Kelola

Pada tabel 6.16 dilakukan pengurutan poin pertanyaaan pada area tata kelola keamanan informasi dilakukan berdasarkan nilai kesenjangan area dari kesenjangan yang paling besar hingga yang terkecil. Pengidentifikasian masalah pada area tata kelola dilakukan dengan pengidentifikasian masalah jika poin pertanyaaan area tidak diterapkan. Kemudian akan dilakukan penilaian berdasarkan kriteria yang akan menentukan kategori masalah yang mungkin dihasilkan.

Tabel 6 16. Pengurutan dan Masalah Area Tata Kelola

Kode	Gap	PA	PK	Permasalahan	D	P	Kategori Masalah
I.18	7,2	1	9	Organisasi jadi tidak tahu apakah target dan sasaran yang diterapkan untuk tiap area tercapai sehingga tidak adanya perbaikan secara berkala	3	3	Medium
I.15	6,6	2	12	Kepatuhan terhadap keamaanan informasi diragukan karena tidak adanya program untuk mencapai target dan sasaran keamanan informasi sehingga pengamanan dipastikan kurang terkait tujuan dan sasaran yang tidak diberikan perhatian khusus	4	3	Medium

				oleh pemimpin instansi.			
I.16	6,6	3	13	Tidak bisa mengetahui kinerja dari pengelolaan keamanan yang dilakukan bisa dikatakan berhasil atau tidak.	3	3	Medium
I.17	6,6	4	14	Penilaian akan mengarah pada upaya pengamanan dan mengesampingkan pertan dari individu yang melakukan tindakan operasionalnya. Padahal kesalahan bisa dilakukan oleh individu yang merupakan komponen dari teknologi informasi.	2	4	Medium

I.19	6	5	15	Terjadinya pelanggaran hukum dan aturan terkait penerapan keamanan informasi yang tidak sesuai aturan yang berlaku.	2	2	Low
I.20	6	6	16	Organisasi akan kesusahan untuk menanggulangi pelanggaran hukum terkait insiden keamanan informasi sebagai akibat tidak adanya kebijakan yang mengatur.	4	3	Medium
I.12	2,8	7	36	Penangggung jawab yang tidak dipustuskan akan menyebabkan mangkraknya proses pengelolaan keberlangsungan TIK karena tidak adanya orang yang didefinisikan secara formal bertanggung jawab.	4	3	Medium
I.9	2,4	8	38	Pejabat dan petugas pelaksana	2	4	Medium

				kurang berkompetensi dalam mengikuti perkembangan teknologi informasi.			
I.11	2,4	9	39	Tak adanya koordinasi antara pengelola keamanan informasi dengan unit organisasi maupun pihak ekternal akan menghambat dalam penerapan program pengelolaan informasi dan membuat pengelolaan informasi tidak berjalan secara merata untuk setiap unit.	3	4	Medium

I.13	2,4	10	40	Pimpinan instansi tidak mengetahui perkembangan pengelolaan keamanan informasi dan keefektifan program yang telah diterapkan.	4	4	High
I.10	2	11	47	Tanggungjawab yang tidak didefinisikan dengan jelas akan membuat fungsi tidak berjalan dengan maksimal dalam melakukan pengelolaan keamanan informasi.	3	4	Medium
I.5	1,8	12	54	Adanya peran dan tanggungjawab yang tidak dipetakan dan menyebabkan tidak adanya tanggung jawab dalam menjalankan perannya.	3	3	Medium

I.7	1,8	13	55	Adanya pelaksana pengamanan informasi yang tidak memiliki kompetensi dan keahlian yang memadai seuai standar perusahaan sehingga dalam melakukan kegiatan opersionalnya tidak bisa mengimbangi peaksanan pengamanan informasi yang lainnya.	3	3	Medium

I.8	1,8	14	56	Tidak adanya pemahaman karyawan dan pihak terkait mengenai keamanan informasi dan kepatuahhnya. Hal ini menyebabkan terjadinya tidak kepatuhan karyawan maupun pihak terkait terhadap aturan keamanan informasi sebagai akibat kurangnya kurangnya sosialisasi.	2	4	Medium
I.6	1,6	15	68	Pelaksanan pengelolaan keamanan informasi memiliki spesifikasi yang berbeda setiap unit karena tidak adanya standar kompetensi dan keahlian.	2	2	Low

I.14	1,6	16	69	Penanganan masalah keamanan informasi menjadi proses independen dengan proses pengambilan keputusan sehingga keputusan yang diambil tidak menyelesaikan permasalahan keamanan informasi.	4	3	Medium
I.2	1,2	17	86	Tidak adanya fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya sehingga pengelolaan keamanan informasi pada organisasi tidak berjalan dan	4	1	Low

				informasi penting organisasi menjadi sangat rentan terhadap ancaman internal maupun eksternal.			
I.4	0,8	18	106	Pengealokasian yang tidak tepat sehingga menyebabkan kekurangan sumber daya dalam melakukan pengelolaan keamanan informasi yang berdampak pada ketidakefektifan pengelolaan keamanan informasi.	4	3	Medium
I.3	0,6	19	114	Pendefinisian tugas dan wewenang yang tidak jelas akan berdampak pada pelaksanaan pengamanan informasi yang tidak dapat berjalan secara efektif.	3	3	Medium
I.1	0,4	20	117	Kurangnya pendefinisian tanggung jawab	4	1	Low

				akan membuat kurangnya kinerja dalam pelaksanaan program keamanan informasi.			

6.3.2.2. Pengurutan dan Kategori Masalah Area Risiko

Pada tabel 6.17 dilakukan pengurutan poin pertanyaaan pada area risiko keamanan informasi dilakukan berdasarkan nilai kesenjangan area dari kesenjangan yang paling besar hingga yang terkecil. Pengidentifikasian masalah pada area risiko dilakukan dengan pengidentifikasian masalah jika poin pertanyaaan area tidak diterapkan. Kemudian akan dilakukan penilaian berdasarkan kriteria yang akan menentukan kategori masalah yang mungkin dihasilkan.

Tabel 6 17. Pengurutan dan Kategori Masalah Area RIsiko

Kode	Gap	PA	PK	Permasalahan	D	P	Kategori Dampak
II.14	7,8	1	4	Keefektifan dari kerangka kerja pengelolaan risiko tidak diketahui oleh oraganisasi apakah cukup handal dalam menangani risiko.	4	3	Medium

II.15	7,8	2	5	Pengelolaan risiko dan penilaian kinerja efektifitas penagamanan menjadi proses yang tidak saling berkaitan dan berjalan sendiri - sendiri	3	3	Medium
II.13	4,8	3	17	Akurasi dan kevaliditasan profil risiko dan mitigasinya untuk menangani permasalahan yang baru muncul diragukan terkait tidak adanya pengkajian ulang secara berkala.	4	3	Medium
II.10	4,4	4	19	Penyusunan langkah mitigasi risiko akan tidak memerhatikan tingkat prioritas, efektifitas biaya dan dampaknya.	4	3	Medium
II.11	4,4	5	20	Pihak manajemen tidak mengetahui perkembangan yang terjadi atas upaya mitigasi risiko.	3	4	Medium
II.12	4,4	6	21	Langkah mitigasi yang sudah diterapkan tidak diketahui apakah bisa menagngani risiko	4	3	Medium

				yang sama kedepannya.			
II.9	2,2	7	46	Risiko akan menjadi masalah besar yang dapat mengganggu keberlangsungan bisnis jika langkah mitigasi risiko tidak disusun.	5	3	High
II.1	1,8	8	57	Tidak adanya program kerja dari organisasi dalam pengelolaan risiko yang terdokumentasi sehingga dalam penerapannya dapat jauh dari kerangka pengelolaan risiko.	5	3	High
II.2	1,8	9	58	Tidak adanya panduan dalam pengelolaan risiko yang terdokumentasi sehingga dalam penerapannya dapat jauh dari kerangka pengelolaan risiko.	5	3	High

II.3	1,8	10	59	Pengklasifikasian aset informasi , tingkat ancaman, kemungkinan keterjadian dan dampak kerugian tidak didefinisikan sehingga dalam mengidentifikasi risiko tidak sesuai dengan masalah yang benar – benar menjadi prioritas dalam penyelesaiannya.	3	3	Medium
II.7	1,8	11	60	Dampak yang tidak ditentukan dpat mempengaruhi dalam analisis apakah risiko itu memiliki pengaruh yang besar dalam keberlangsungan bisnis organisasi/perusahaan.	4	3	Medium
II.8	1,8	12	61	Tidak adanya respon yang cepat terhadap insiden yang terjadi mengenai keamanan informasi.	3	3	Medium
II.4	1,6	13	70	Setiap risiko akan diterima oleh organisasi tanpa adanya batasan tertentu yang menyatakan bahwa	3	3	Medium

				risiko tersebut harus dihentikan.			
II.6	1,6	14	71	Ancaman terkait aset informasi membantu dalam identifikasi risiko. Ketika tidak dilakukan akan menghambat kecepatan tanggapan organisasi dalam menangani risiko yang mungkin terjadi.	3	3	Medium
II.5	1,2	15	87	Akan ada tindakan saling klaim tehadap aset informasi karena tidak adanya aturan yang jelas mendefinisikan kepemilikan dan pihak pengelola aset informasi yang ada.	4	3	Medium

6.3.2.3. Pengurutan dan Kategori Masalah Area Kerangka Kerja

Pada tabel 6.18 dilakukan pengurutan poin pertanyaaan pada area kerangka kerja keamanan informasi dilakukan berdasarkan nilai kesenjangan area dari kesenjangan yang paling besar hingga yang terkecil. Pengidentifikasian masalah pada area kerangka kerja dilakukan dengan pengidentifikasian masalah jika poin pertanyaaan area tidak diterapkan. Kemudian akan

dilakukan penilaian berdasarkan kriteria yang akan menentukan kategori masalah yang mungkin dihasilkan.

Tabel 6 18. Pengurutan dan Kategori Masalah Area Kerangka Kerja

Kode	Gap	PA	PK	Permasalahan	D	P	Kategori Masalah
III.15	9	1	1	Proses pemulihan yang dimiliki oleh oraganisasi gagal menangani permasalahan. Hal ini terkait tidak adanya pengevaluasian upaya pemulihan bencana secara berkala untuk memastikan apakah proses pemulihannya masih relevan. Akibatnya perencanaan pemulihan yang telah dibuat tidak bisa menyelesaikan permasalahan.	4	4	High

III.13	8,4	2	2	Tidak adanya pendefinisian peran dan tanggung jawab akan menghambat proses pemulihan karena belum terdefinisi peran siapa yang melakukan apa sehingga proses pemulihan dilakukan dengan lambat atau tidak sesuai dengan harapan karena peran dan wewenang yang tidak dijabarkan.	3	3	Medium
III.14	8,4	3	3	Uji coba yang tidak dilakukan terhadap upaya pemulihan akan membuat organisasi menjadi tidak sadar bahwa upaya pemulihannya tidak relevan lagi.	4	3	Medium

III.16	7,8	5	6	Kebijakan dan prosedur keamanan informasi yang tidak dievaluasi secara berkala akan menyebabkan kebijakan itu tidak dapat lagi memastikan keberlangsungan bisnis yang terus berkembang dan keefektifan dari kebijakannya akan diragukan.	3	2	Medium
III.25	7,8	6	7	Organisasi yang tidak melakukan pengujian terhadap kepatuhan dari program keamanannya tidak akan bisa memastikan bahwa keamanan yang ia rencanakan bisa menanggulangi ancaman. Dan juga menimbulkan banyak kerentanan pada bagian yang tidak menerapkan program keamanan.	4	3	Medium

III.24	7,2	7	10	Kebijakan dan prosedur harus direvisi untuk memenuhi kebutuhan bisnis organisasi. Untuk itu diperlukan analisa finansial, perubahan, dan pengelolaan perubahan. Jika tidak ada maka kebijakan baru yang direvisi tidak bisa dijamin dalam menangani kebutuhan organisasi karena setiap kebijakan yang dibuat harus menjawab permasalahan dari orgamisasi.	4	2	Medium
III.26	7,8	7	8	Organisasi yang tidak memiliki rencana upaya peningkatan keamanan informasi dapat membuat organisasinya memiliki banyak kerentanan terhadap ancaman yang mungkin terjadi dari	3	3	Medium

				internal maupun eksternal. Dan juga perencanaan tingkat keamanan informasi membntu organisasi untuk tanggap terhadap ancaman yang akan terus berkembang.			
III.8	4,4	8	22	Penerapan keamanan iniformasi dalam penerapannya akan berubah – ubah mengikuti situasi terkait tidak adanya prosedur resmi yang mengikat.	2	2	Low
III.9	4	9	24	Tidak adanya kebijakan dan prosedur yang mengatur menyebabkan pengimplementasian yang terhambat terkait peran dan tanggung jawab untuk implementasi, memonitor, dan pelaporannya tidak didefinisikan.	3	4	Medium

III.11	4	10	25	Risiko berantai baru akan muncul tekait penerapan pengamanan informasi yang dan organisasi akan kebingungan dalam menghadapi risiko yang timbul dari penerapan pengamanan informasi terkait tidak ada pengaturan terhadap cara menghadapi permasalahan ini.	4	3	Medium
III.12	4	11	26	Organisasi tidak tanggap terhadap insiden yang terjadi karena tidak memiliki perencanaan yang bisa menghadapi kemungkinan insiden agar bisnis dapat terus dijalankan.	4	4	High

III.22	3,2	12	30	Hasil audit tidak dikaji sehigga langkah pembenahan terhadap temuan audit tidak diidentifikasi sehingga keamanan informasi masih dalam keadaan yang belum berkembang dan rentan.	4	3	Medium
III.23	2,8	13	37	Hasil audit hanya menjadi syarat pengelolaan manajemen yang baik tanpa melihat hasilnya sehingga manajer tidak tahu terkait permasalaahan yang mungkin terjadi sehingga tidak bisa melanjutkan ke tahapan perbaikan.	3	3	Medium
III.7	2,4	14	41	Banyak pegawai yang tidak mengetahui kebijakan yang diterapkan sehingga terjadinya pelanggaran terkait tidak adanya aturan maupun komunikasi dengan pegawai.	5	4	High

III.10	2,4	15	42	Organisasi akan kebingungan terkait risiko yang bisa muncul ketika melakukan implementasi sistetem baru terkait tidak adanyaa pengkajian terhadap risiko yang pernah terjadi sebelumnya.	3	4	Medium
III.2	1,8	16	62	Kebijakan yang tidak diketahui oleh pihak terkait karena kurang adanya komunikasi maupun penetapan kebijakan secara formal yang mengakibatkan ketidaktahuan pihak terkait.	2	4	Medium
III.5	1,8	17	63	Kebijakan yang dibuat tidak berdasarkan pengelolaan risiko dan mitigasi yang telah dianalisis sehingga menyebabkan kebijakan tidak tepat sasran dan tidak dapat menjawab	3	1	Low

				permasalahan organisasi dan membantu dalam menyelesaikan permasalahan.			
III.17	1,8	18	64	Strategi penerapan keamanan informasi yang tidak sesuai dengna hasil analisis risiko akan mengakibatkan kemanan yang diterapkan tidak selalu akan menjawab permasalahan yang dihadapi oleh organisasi.	2	3	Medium
III.18	1,8	19	65	Strategi penerapan keamanan informasi yang tidak sesuai dengan hasil analisis risiko akan mengakibatkan kemanan yang diterapkan tidak selalu akan menjawab permasalahan yang dihadapi oleh organisasi.	3	3	Medium

III.21	1,8	20	66	Audit tidak melakukan evaluasi kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi sehingga tidak didapatkan temuan terkait hal tersebut yang bisa diberikan saran perbaikan.	4	3	Medium
III.19	1,6	21	72	Strategi penerapan keaman informasi yang tidak sesuai dengan program kerja organisasi akan menjadi strategi yang tidak tepat sasaran dan tidak menjawab kebutuhan organisasi.	3	2	Medium
III.20	1,6	22	73	Organisasi tidak dapat mengevaluasi fungsi organisasinya dan memberikan perbaikan terkait temuan permasalahan dalam unit bisnis untuk memperbaiki kinerja organisasi.	5	3	High

III.4	1,4	23	76	Tidak adanya mekanisme untuk mengkomunikasikan kebijakan keamanan informasi akan menyebabkan ketidaktahuan pihak terkait terhadap kebijakan dan berakibat pelanggaran kebijakan yang tidak disengaja.	2	4	Medium
III.1	1,2	24	88	Kebijakan yang tidak jelas mendefinisikan peran dan tanggung jawab kepada pihak yang diberikan wewenang maka akan membuat implementasi kebijakan terhambat terkait tidak adanya pihak yang mengurusi permasalahan secara spesifik.	4	4	High

III.3	1,2	25	89	Tidak adanya mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi akan menyebabkan kerusakan atau kehilangan dari dokumen karena tidak dilakukan pengelolaan dengan baik dan penempatan orang yang harus bertanggung jawab terhadap dokumen tersebut.	4	4	High
III.6	0,8	26	107	Terjadinya pelanggaran oleh pihak ketiga mengenai pelaporan insiden, penjagaan kerahasiaan, HAKI dan pengamanan aset.	4	4	High

6.3.2.4. Pengurutan dan Kategori Masalah Area Pengelolaan Aset

Pada tabel 6.19 dilakukan pengurutan poin pertanyaaan pada area pengelolaan aset keamanan informasi dilakukan berdasarkan nilai kesenjangan area dari kesenjangan yang paling besar hingga yang terkecil. Pengidentifikasian masalah pada area pengelolaan aset dilakukan dengan pengidentifikasian masalah jika poin pertanyaaan area tidak diterapkan. Kemudian akan dilakukan penilaian berdasarkan kriteria yang akan menentukan kategori masalah yang mungkin dihasilkan.

Tabel 6 19. Pengurutan dan Kategori Masalah Area Pengelolaan Aset

Kode	Gap	PA	PK	Permasalahan	D	P	Kategori Masalah
IV.24	4,8	1	18	Penggunaan perangkat pengeolah informasi milik pihak ketiga jadi semena – mena dan memungkinkan adanya akses dari orang yang tidak memilik otentikasi untuk mengakses terkait tidak adanya prosedur untuk mengaturnya.	4	4	High

IV.34	4,2	2	23	Lokasi kerja dapat diakses oleh orang yang tidak memiliki otentikasi terkait tidak adanya prosses untuk mengamankan lokasi kerja.	3	5	High
IV.19	4	3	27	Orang yang bertanggung jawab menangani insiden akan kebingungan dalam menangani insiden yang membutuhkan campur tangan pihak eksternal.	2	4	Medium
IV.23	3,6	4	28	Tidak adanya rekaman menyebabkan organisasi tidak bisa belajar dari insiden masa lalu yang telah terjadi dan upaya penagamanan yang diterapkan.	3	4	Medium
IV.20	3,2	5	31	Kebocoran data/aset kepada	4	3	Medium

				pihak luar organisasi yang dapat mengganggu keberlangsungan bisnis.			
IV.22	3	6	35	Kemugkinan adanya data/informasi yang tidak di-*backup* dan tidak adanya pelaporan terhadap kondisi data/informasi tersebut.	3	4	Medium
IV.17	2	7	48	Pengamanan akan sama untuk setiap aset, padahal ada aset yang memiliki kerentanan yang sangat besar dan harus diprioritaskan dalam pengamaanannya.	4	4	High
IV.18	2	8	49	SDM yang tidak jelas latar belakangnya dapat menjadi ancaman bagi organisasi nantinya terkait jejak kriminnal maupun ketidakpemenuhan sesuai dengan kriteria organisasi.	2	3	Medium

IV.31	2	9	50	Perangkat komputer yang digunakan untuk menyimpan informasi penting mengalami kerusakan yang tidak diketahui sehingga kerentanan terhadap informasi bisa muncul. Ketidaklayakan yang tidak diketahui akan menyebabkan permasalahan yang panjang kedepannya.	3	5	High
IV.33	2	10	51	Adanya kegiatan yang dapat menyebabkan kerusakan, kehilangan dan sabotase terkait lokasi kerja yang dapat memberikan efek buruk pada keberlangsungan bisnis terkait tidak adanya peraturan untuk meangamankan	5	5	High

				lokasi kerja penting.			
IV.9	1,8	11	67	Penyalahgunaan penggunaan aset Instansi terkait HAKI.	3	4	Medium
IV.29	1,6	12	74	Penggunaan perangkat komputasi diluar kantor tidak mementingkan keamanan perangkat informasi yang memungkinkan kerusakan maupun kehilangan data/informasi pada perangkat komputasi.	3	5	High
IV.32	1,6	13	75	Kehilangan aset informasi sebagai kelalalian dari petugas atau pengemasan yang kurang diatur oleh perusahaan untuk meminimalkan kerentanan.	4	3	Medium

IV.1	1,4	14	77	Aset yang dimiliki organisasi tidak terdokumentasi sehingga tidak tersedia informasi terkait aset yang dimiliki.	3	4	Medium
IV.3	1,4	15	78	Tingkat akses yang tidak dibedakan akan menyebabkan penyelahgunaan wewenang dan kehilangan data jika akses diberikan sama kepada seluruh pihak.	3	5	High
IV.6	1,4	16	79	Aset yang dimiliki oleh perusahaan tidak akan diketahui *update* dan kondisi terkininya karena tidak adanya penginventarisan aset baru.	2	4	Medium

IV.12	1,4	17	80	Akses yang bebas terhadap aset informasi organisasi yang memungkinkan penyalahgunaan akses oleh orang yang tidak memiliki wewenang.	3	5	High
IV.15	1,4	18	81	Insiden kegagalan informasi tidak akan memiliki upaya penyelesaian jika tidak dilakukan investigasi untuk mengetahui penyebab dan dampaknya terhadap keberlangsungan bisanis organisasi.	5	4	High
IV.2	1,2	19	90	Tidak adanya pengelolaan yang baik terhadap aset sehingga aset sangat rentan terhadap ancaman dari luar maupun dalam organisasi yang menyebabkan pada kerusakan	3	3	Medium

				maupun hilangnya aset.			
IV.8	1,2	20	91	Penggunaan sewenang – wenang oleh orang yang tidak memiliki otentikasi maupun kemungkinanan penyalahgunaan fungsi aset yang bukan untuk kepentingan organisasi.	2	5	Medium
IV.10	1,2	21	92	Ketidakadaan pengaturan mengenai pengelolaan data pribadi akan menyebabkan data rentan dan pengelolaannya tidak tersetandarisasi.	2	5	Medium
IV.13	1,2	22	93	Adanya penumpukan data yang tidak dihancurkan.	3	4	Medium
IV.21	1,2	23	94	Pengkajian terhadap hak akses tidak dilakukan	2	3	Medium

				akan menimbulkan pembiaran terhadap tindakan penyalahgunaan akses, dan akan menimbulkan pelanggaran yang dari karyawan yang dapat mengganggu proses bisnis perusahaan.			
IV.30	1,2	24	95	Pengamanan fisik informasi yang tidak sesuai dapat menyebabkan risiko – risiko yang tidak diinginkan terjadi. Baik itu dari alam, kelalalian manusia dan percobaan sabotase.	5	4	High
IV.4	1	25	98	Tidak adanya pengendalian terhadap perubahan sehingaga berdampak pada kekurang sigapan organisasi dalam menghadapi efek dari perubahan pengelolaan	2	2	Low

				keamanan informasi.			
IV.5	1	26	99	Adanya penerapan konfigurasi yang berbeda – beda untuk setiap infrstruktur informasi.	2	2	Low
IV.7	1	27	100	Tidak adanya rasa memiliki terhadap aset informasi kerena tugas tidak didefinisikan yang berakibat pada ketidakefektifan dalam pengamanan informasi.	3	4	Medium
IV.11	1	28	101	Penggunaan yang tidak sesuai standar dan dapat terjadi penyalahgunaan oleh orang yang tidak memiliki otentikasi.	3	5	High

IV.25	1	29	102	Adanya akses oleh pihak yang tidak berwenang yang mengambil data/informasi penting organisasi dan melakukan perusakan terhadap aset informasi organisasi.	5	5	High
IV.26	1	30	103	Adanya akses yang tidak diinginkan yang mengganggu keberlangsungan bisnis dan melakukan tindakan yang mengancam aset informasi.	5	5	High
IV.27	0,8	31	108	Infrstruktur komputasi mengalami kerusakan terkait tidak diterapkan perlindungan yang melindungi infrstruktur dari bahaya lingkungan serta tidak dilakukan perlindungan seperti prasyarat pabrikannya.	5	4	High

IV.14	0,6	32	115	Terjadinya penyebaran informasi rahasia organisasi karena tidak adanya aturan pembatasan pembagian informasi dan ada kemungkinan kebocoran penting organisasi.	4	4	High
IV.16	0,6	33	116	Kehilangan data sebelumnya ketika implementasi yang diterapkan gagal.	4	3	Medium
IV.28	0,4	34	118	Terjadinya kerusakan pada alat – alat elektronik dan kemungkinan terjadinya konsleting yang dapat menyebabkan kebakaran.	5	4	High

6.3.2.5. Pengurutan dan Kategori Dampak Area Teknologi

Pada tabel 6.20 dilakukan pengurutan poin pertanyaaan pada area teknologi keamanan informasi dilakukan berdasarkan nilai kesenjangan area dari kesenjangan yang paling besar hingga yang terkecil. Pengidentifikasian masalah pada area teknologi dilakukan dengan pengidentifikasian masalah jika poin pertanyaaan area tidak diterapkan. Kemudian akan dilakukan penilaian berdasarkan kriteria yang akan menentukan kategori masalah yang mungkin dihasilkan.

Tabel 6 20. Pengurutan dan Kategori Masalah Area Teknologi

Kode	Gap	PA	PK	Permasalahan	D	P	Kategori Masalah
V.24	7,2	1	11	Kehandalan keamanan informasi kurang bisa dibuktikan terkait tidak adanya perencanaan terkait pengkajian kehandalan keamanan informasi	3	3	Medium
V.11	3,6	2	29	Dalam penerapan enkripsi dapat berbeda – beda tiap unit terkait tidak adanya ukuran baku.	3	4	Medium

V.12	3,2	3	32	Kunci enkripsi akan digunakan semena – mena oleh orang yang tidak bertangung jawab. Bahkan oleh orang yang memiliki tanggung jawab tidak tahu apa yang perlu dilakukan untuk mengamankan kunci enkripsi terkait belum adanya prosedur untuk mengamankannya.	3	3	Medium
V.13	3,2	4	33	*Password* pengguna akan rentan terhadap ancaman dari pihak yang tidak bertanggung jawab terkait tidak adanya pengaturan terhadap standar *password* yang dianjurkan oleh aplikasi dan sistem maupun yang sesuai dengan standar yang	*3*	*4*	Medium

				diterapkan organisasi.			
V.14	3,2	5	34	Adanya pembobolan sistem dari pihak yang tidak berkepentingan untuk pengambilan data penting perusahaan.	4	3	Medium
V.20	2,4	6	43	Tidak adanya data rekaman akan membuat organisasi tidak bisa belajar dari masalah masa lalu untuk menghadapi masalah yang terjadi sekarang dan memiliki kriteria yang sama dengan masalah masa lalu.	3	5	High
V.21	2,4	7	44	Ketidaktahuan status pengamanan oleh anti virus yang menyebabkan orgnaisasi tidak tahu ancaman yang menggangu asetnya.	3	5	High

V.23	2,4	8	45	Tidak dilakukan verifikasi menyebabkan aplikasi yang digunakan kemungkinan tidak sesuai dengan tujuan yang diharapkan oleh organisasi.	3	4	Medium
V.15	2	9	52	Kemungkinan akses oleh pihak yang tidak diinginkan dan juga kebocoran data/informasi penting organisasi.	3	4	Medium
V.22	2	10	53	Perbedaan waktu antar perangkat yang menyebabkan kesalahan dalam kegiatan opersional dan perekaman kejadian.	2	1	Low

V.4	1,4	11	82	Organisasi tidak pernah melakukan analisis kepatuhan yang menyebabkan organisasi tidak tahu penerapan standar apakah benar – benar dilakukan.	3	3	Medium
V.8	1,4	12	83	Akses yang tidak terekam menyebabkan kemungkinan tindakan pengaksesan kembali teulang dan dapat berakibat pada kehilangan data penting organisasi.	2	4	Medium
V.9	1,4	13	84	Tidak dilakukan pemeliharaan kepada log sehingga adanya log yang hilang maupun sudah tidak valid lagi sehingga tidak bisa dijadikan acuan analisis untuk menghadapi permasalahan yang terjadi.	3	4	Medium

V.17	1,4	14	85	Adanya akses dari luar organisasi untuk melakukan kegiatan jahat seperti mencuri, merusak, dan penggunaan infrstruktur secara sewenang – wenang.	4	4	High
V.5	1,2	15	96	Adanya celah keamanan yang tidak terdeteksi dan dimanfatkan oleh pihak yang tidak bertanggung jawab untuk membobol sistem dan mengambil data/informasi penting organisasi.	3	4	Medium
V.16	1,2	16	97	Adanya akses yang tak terdeteksi pada jaringan menyebabkan hilangnya data perusahaan dan informasi penting lainnya.	4	4	High
V.3	1	17	104	Terjadinya perbedaan	3	4	Medium

				konfigurasi keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan tiap unit organisasi. Yang menyebabkan perlindungan yang diberikan ada yang kuat dan ada yang lemah.			
V.10	1	18	105	Terjadinya pencurian data dan pembobolan karena pengamanan yang buruk terhadap aset informasi.	3	3	Medium
V.1	0,8	19	109	Terjadinya upaya akses secara ilegal untuk menembus lapisan pengamanan yang mengambil data/informasi penting organisasi.	4	4	High
V.2	0,8	20	110	Tidak adanya abtasan akses untuk tiap segmen instansi yang menyebabkan kemungkinan terjadinya penyelahgunaan	2	3	Medium

				oleh segmen yang tidak memiliki kepentingan.			
V.6	0,8	21	111	Terjadinya kekurangan kapasitas infrastruktur untuk kebutuhan organisasi karena tidak adanya pengawasan infrastruktur secara berkala.	2	4	Medium
V.7	0,8	22	112	Dengan tidak dilakukan perekaman log otomatis maka perusahaan tidak memiliki data aktivitas dari pengguna, kesalahan dan kegiatan pengamanan informasi yang dapat digunakan untuk keperluan audit dan pengembangan kedepannya.	2	5	Medium

V.18	0,8	23	113	Perangkat desktop dan server kurang mutahir sehingga terdapat banyak celah keamanan yang belum diperbaiki pada sistemnya.	3	4	Medium
V.19	0,2	24	119	Data pada *desktop* dan *server* terinfeksi sehingga hilang serta rusak. Menyebabkan sistem komputer menjadi lambat dan banyak program yang *error*.	4	4	High

Dari hasil pengurutan kesenjangan diatas, didapatkan data poin pertanyaan yang memiliki gap terbesar untung masing – masing area dan secara keseluruhan. Pada tabel 6.21 disajikan 11 poin pertanyaan yang menjadi masalah terbesar bagi penyelenggara sistem elektronik berdasarkan kesenjangannya yang memiliki nilai diatas 7.

Tabel 6 21. Peringkat 11 Kesenjangan Terbesar

Kode	Keterangan	G	Peringkat Keseluruhan
III.15	Pengevaluasian hasil dari perencanaan pemulihan bencana *(disaster recovery*	9,00	1

	plan) untuk menjaga keandalannya.		
III.13	Pendefinisikan komposisi, peran, wewenang dan tanggungjawab pemulihan bencana (*disaster recovery plan*).	8,40	2
III.14	Pengujian sesuai jadwal terhadap perencanaan pemulihan bencana (*disaster recovery plan*).	8,40	3
II.14	Pengkajian kerangka kerja pengelolaan risiko secara berkala untuk memastikan/meningkatkan efektifitasnya	7,80	4
II.15	Pengelolaan risiko dijadikan bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan	7,80	5
III.16	Pengevaluasian kelayakan kebijakan dan prosedur keamanan informasi secara berkala.	7,80	6

III.25	Pengujian dan evaluasi secara periodik mengenai tingkat/status kepatuhan program keamanan informasi yang ada untuk memastikan bahwa keseluruhan inisiatif yang ada telah diterapkan secara efektif.	7,80	7
III.26	Kepemilikan rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten.	7,80	8
I.18	Penerapan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan dan mengevaluasi pencapaiannya secara rutin, termasuk pelaporannya kepada pimpinan Instansi.	7,20	9
III.24	Analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkan	7,20	10

	perevisian kebijakan dan prosedur.		
V.24	Pelibatan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin	7,20	11

Pada 11 urutan kesenjangan diatas diketahui bahwa area kerangka kerja memiliki banyak poin pertanyaan dengan kesenjangan tertinggi. Dari peringkat diatas, 7 dari area kerangka kerja, kemudian 2 dari area risiko, 1 dari area tata kelola dan 1 dari area teknologi. Peringkat diatas selaras dengan peringkat rata – rata kesenjangan pada 5 area. Dimana area kerangka kerja memiliki rata – rata 3,86 sebagai peringkat pertama, diikuti area risiko dengan rata -rata 3,28, kemudian diikuti area tata kelola dengan rata – rata 3,13, setelah itu area teknologi dengan rata – rata 1,91 dan area pengelolaan aset dengan rata – rata 1,72 diurutan ke 5. Hal ini mengisyaratkan bahwa instansi/lembaga penyelenggara elektronik memiliki masalah besar dalam proses pengelolaan proses pengamanan informasinya terkait kepatuhan pada kerangka kerja yang digunakan.

Kemudian pada gambar 6.9 disajikan kategorisasi masalah yang mungkin terjadi jika poin pertanyaan tidak diterapkan. Dari 119 poin pertanyaan ada 33 poin pertanyaan yang dikategorikan *high* bila tidak diterapkan, 77 poin pertanyaan pada kategori *medium* dan 9 poin pertanyaan pada kategori *low*.

Probabilitas	Dampak					
	5	4	3	2	1	
5	IV.33, IV.25, IV.26		IV.34, IV.31, IV.29, IV.3, IV.11, IV.12, V.20, V.21	IV.8, IV.10, V.7		
	HIGH (25)	HIGH (20)	HIGH (15)	MEDIUM (10)	MEDIUM (5)	
4	III.7, IV.30, IV.15, IV.27, IV.28	I.13, III.15, III.12, III.3, III.1, III.6, IV.24, IV.17, IV.14, V.16, V.17, V.1, V.19	I.11, I.10, II.11, III.9, III.10, IV.22, IV.23, IV.9, IV.1, IV.7, IV.13, V.11, V.13, V.23, V.15, V.5, V.9, V.18, V.3	I.17, I.9, I.8, III.2, III.4, IV.19, IV.6, V.8, V.6		
	HIGH (20)	HIGH (16)	MEDIUM (12)	MEDIUM (8)	LOW (4)	
3	II.9, II.1, II.2, III.20	I.15, I.20, I.12, I.14, I.4, II.14, II.13, II.10, II.12, II.7, II.5, III.14, III.25, III.11, III.22, III.21, IV.20, IV.32,	I.18, I.16, I.5, I.7, I.3, III.15, II.3, II.4, II.8, II.6, III.13, III.26, III.23, III.18, IV.2, V.24, V.12, V.4, V.10	III.17, IV.18, IV.21, V.2		
	HIGH (15)	MEDIUM (12)	MEDIUM (9)	MEDIUM (6)	LOW (3)	
2		III.24	III.16, III.19	I.19, I.6, III.8, IV.4, IV.5		
	MEDIUM (10)	MEDIUM (8)	MEDIUM (6)	LOW (4)	LOW (2)	
1		I.2, I.1	III.5	V.22		
	MEDIUM (5)	LOW (4)	LOW (3)	LOW (2)	LOW (1)	

Gambar 6 9. Hasil Kategori Masalah

Pada tabel 6.22 disajikan poin pertanyaan yang menjadi masalah dengan kategori tinggi jika tidak diterapkan. Area pertanyaan yang memiliki masalah terbesar disini berbanding terbalik dengan hasil kesenjangan. Hal itu dapat dilihat dari jumlah poin pertanyaan dengan kategori high pada area tata kelola ada 1, kemudian area risiko ada 3, area kerangka kerja ada 7, area pengelolaan aset ada 16 dan area teknologi ada 6 poin yang dikategorikan tinggi bila tidak dilakukan. Ini berarti poin pertanyaan dengan kesenjangan tinggi belum tentu memiliki dampak besar jika tidak diterapkan. Hal ini disebabkan pada analisis kesenjangan menggunakan menggunakan data lembaga yang bisa dikatakan sadar akan pentingnya pengelolaan aset dan teknologinya dan lemah dalam mejaga kepatuhan dan penerapan kerangka kerja . Sedangkan pada kategori masalah yang tinggi pada area pengelolaan aset sebagai akibat pengelolaan aset terkait dengan aset penting organisasi. Ketika aset itu dikatakan penting maka memiliki nilai finansial. Saat masalah terjadi yang mengganggu pengelolaan dari aset informasi maka akan memberikan dampak kerugian yang tinggi bagi organisasi.

Tabel 6 22. Hasil Kategori Masalah High

Kode	Keterangan	Gap	DxP	Kategori Masalah
IV.25	Pengamanan fasilitas fisik untuk mencegah akses ilegal	0,78	25	High
IV.26	Proses pengelolaankunci fisik dan elektronik ke fasilitas fisik	0,67	25	High
IV.33	Peraturan untuk mengamankan lokasi kerja penting	1,78	25	High

III.7	Pengelolaan konsekuensi dari pelanggaran kebijakan keamanan informasi	2	20	High
IV.15	Investigasi terhadap kegagalan kemanaan informasi	1,11	20	High
IV.27	Perlindungan infrastruktur komputasi dari dampak lingkungan dan api	0,67	20	High
IV.28	Perlindungan infrastruktur komputasi dari gangguan listrik lingkungan dan petir	0,44	20	High
IV.30	Kontruksi ruang penyimpanan perangkat pengolah informasi penting	1,33	20	High
I.13	Penerapan program kompetensi keahlian bagi pertugas	1,78	16	High
III.1	Kejelasan kebijakan dan prosedur yang mengatur peran dan tanggung jawab	0,89	16	High
III.12	Tersedia BCP yang berisikan syarat kemanan termasuk penjadwalan ujicobanya	2,67	16	High
III.15	Pengevaluasian perencanaan pemulihan bencana (DRP)	6,67	16	High
III.3	Mekanisme pengelolaan dokumen kebijakan & prosedur	1	16	High
III.6	Kontrak dengan pihak ketiga terkait aspek keamann informasi	0,67	16	High
IV.14	Ketetapan pengamanan pertukaran data dengan eksternal	0,56	16	High

IV.17	Ketentuan pengamanan fisik berdasarkan zona klasifikasi aset	2	16	High
IV.24	Prosedur penggunaan perangkat pengolah informasi milik pihak ketiga	3,33	16	High
V.1	Perlindungan lebih dari 1 lapis terhadap layanan yang menggunakan internet	0,67	16	High
V.16	Prosedur *back-up* dan *restore*	1,33	16	High
V.17	Penerapan pengamanan khusus untuk melindungi akses dari luar	0,89	16	High
V.19	Perlindungan *desktop* dan *server* dari virus	0,11	16	High
II.1	Program kerja pengelolaan risiko terdokumentasi dan digunakan	1,33	15	High
II.2	Kerangka kerja pengelolaan risiko terdokumentasi dan digunakan	1,33	15	High
II.9	Penyusunan langkah mitigasi risiko	1,44	15	High
III.20	Memiliki dan melaksanakan program audit internal	1	15	High
IV.11	Pengelolaan identitas elektronik dan proses otentikasi	1	15	High
IV.12	Prosedur pemberian, otentikasi, dan otorisasi penggunaan aset informasi	1	15	High

IV.29	Peraturan pengamanan perangkat komputasi di luar kantor	1,22	15	High
IV.3	Pendefinisian tingkat akses dan perekaman akses	1,11	15	High
IV.31	Proses inspeksi dan merawat fasilitas untuk memastikan kelayakan & keamann informasi penting	1,33	15	High
IV.34	Proses pengamanan lokasi dari pihak ketiga yang bekerja untuk instansi	3,33	15	High
V.20	Rekaman & analisa pemutakhiran antivirus secara rutin	1,78	15	High
V.21	Laporan virus yang gagal/sukses ditindaklanjuti	1,78	15	High

Pada tabel 6.22 dapat dilihat irisan yang terjadi. Dimana poin III.15 mengenai Pengevaluasian perencanaan pemulihan bencana (DRP) memiliki kategori tinggi dan merupakan kesenjangan yang tertinggi juga pada poin pertanyaan secara keseluruhan. Berarti dapat dikatakan pengevaluasian rencana pemulihan merupakan proses yang jarang dilakukan oleh lembaga penyelenggara sistem elektronik dan memiliki dampak yang besar jika tidak diterapkan.

6.4. Pemberian Rekomendasi

Setelah didapatkan pemeringkatan poin pertanyaan yang memiliki kesenjangan yang menjadi masalah bagi instansi/lembaga penyelenggara sistem elektronik. Serta dampak dari setiap poin pada area pertanyaan yang memiliki akibat yang signifikan jika tidak diterapkan maka dilanjutkan dengan pemberian rekomendasi. Pemberian rekomendasi disini diberikan untuk keeluruhan poin, namun pada kesenjangan

tertinggi diberi tanda kuning dan yang berkategori *high* berwarna merah.

6.4.1. Rekomendasi Perbaikan Area Tata Kelola

Tabel 6.23 merupakan hasil rekomendasi pada poin pertanyaan area tata kelola keamanan informasi yang paling menjadi masalah bagi instansi/lembaga penyelenggara sistem elektronik. Pemberian rekomendasi berdasarkan pada kendali dan panduan yang dimiliki oleh SNI ISO/IEC 27001.

Tabel 6 23. Rekomendasi Area Tata Kelola

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
I.18	Apakah Instansi Anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan dan mengevaluasi pencapaiannya secara rutin, termasuk pelaporannya kepada pimpinan Instansi?	7,20	**Medium**	9

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
Rekomendasi Perbaikan **Control 5.1.1 Policies for Information Security** Harus ada sekumpulan kebijakan untuk keamanan informasi yang dedefinisikan , disetujui oleh pihaka manajemen dan diterbitkan serta dikomunikasikan kepada karyawan dan pihak ketiga. Kebijakan keamanan informasi harus memenuhi kriteria berdasarkan : - Strategi bisnis - Aturan, undang – undang dan kontrak - Lingkungan yang mengancam keamanan informasi Untuk itu kebijakan informasi harus berisi tentang : - Pengertian keamanan informasi, tujuan dan prinsip untuk memandu seluruh aktivitas yang berhubungan dengan keamanan informasi - Pernyataan mengenaitanggungjawab secara umum danspesifik untuk pengelolaan keamanan informasi untuk mendefinisikan peran - Proses untuk menangani penyimpangan dan pengecualian.				
I.15	Apakah pimpinan satuan kerja di Instansi Anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang	6,60	**Medium**	12

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	menjadi tanggungjawabnya?			
Rekomendasi Perbaikan **Control 7.2.1 Management Responsibility** Manajemen harus memastikan bahwa seluruh karyawan dan kontraktor melaksanakan kebijakan dan prosedur keamanan informasi yang dibuat organisasi. Untuk itu yang harus dilakukan manajemen adalah : - Penjelasan mengenai peran dan tanggung jawab yang diberikan untuk mangakses informasi rahasia - Memberikan panduan untuk memenuhi peran dalam menjaga keamanan informasi - Memotivasi untuk memenuhi kebijakan keamanan informasi organisasi - Mencapai tingkat kesadaran mengenai keamanan informasi yang relevan dengan tanggung jawabnya - Menyesuaikan syarat dan ketentuan dalam bekerja - Memiliki keahlian dan kualifikasi dan berpendidikan - Menyediakan pelaporan terhadap tindakan pelanggaran kebijakan keamanan informasi				
I.16	Apakah Instansi Anda sudah mendefinisikan paramater, metrik dan mekanisme pengukuran kinerja pengelolaan	6,60	**Medium**	13

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	keamanan informasi?			
Rekomendasi Perbaikan **Control 6.1.5 Information Security In Project Management** Pengelolaan keamanan informasi harus dimasukkan dalam pengelolaan proyek. Hal ini dilakukan untuk memastikan proses pengidentifikasian risiko didalamnya dilakukan dan ditinjau secara berkala. Peran dan tanggung jawab mengenai keamanan informasi harus didefinisikan dalam memtode pengelolaan proyek secara berkelanjutan.				
I.17	Apakah Instansi Anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	6,60	**Medium**	14
Rekomendasi Perbaikan **Control 7.2.3 Disciplinary Process** Lemabaga penyelenggara sistem elektronik perlu melakukan tindakan formal pendisiplinan karyawannya jika diketahui bahwa karyawannya mencoba melakukan pelanggaran keamaan informasi. Proses pendisiplinan tidak akan bisa dilakukan jika tanpa adanya verifikasi terhadap pelanggaran keamanan informasi yang terjadi. Pendisiplinan harus memastikan penanganan yang adil kepada karyawan yang dicurigai melakukan tindakan pelanggaran keamanan informasi. Proses pendisiplinan juga bisa dilakukan untuk				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
mencegah karyawan lain untuk melanggar kebijakan dan prosedur keamanan informasi organisasi maupun pelanggaran lainnya.				
I.19	Apakah Instansi Anda sudah mengidentifikasi legislasi dan perangkat hukum lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	6,00	**Low**	15
Rekomendasi Perbaikan **Control 18.1.1 Identification Of Applicable Legislation And Contractual Requirements** Lembaga penyelenggara sistem elektronik perlu melakukan identifikasi terkait legislasi, peraturan perundang – undangan, dan kontrak yang harus dipatuhi dan menganisa tingkat kepatuhan organisasinya terhadap undang – undangan. Dalam penerapannya pun harus selalu didokumentasikan dan dipertahankan agar setiap proses bisnis yang ada selalu memenuhi peraturan yang berlaku. Penanggung jawab untuk melakukan identifikasi ini adalah manajer. Harus sebisa mungkin mengidentifikasi aturan yang diperlukan untuk memenuhi kebutuhan bisnisnya. Dan juga manajer bertanggung jawab dalam pemenuhan aturan yang berlaku.				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
I.20	Apakah Instansi Anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?	6,00	**Medium**	16
Rekomendasi Perbaikan **Control 7.2.3 Disciplinary Process** Lemabaga penyelenggara sistem elektronik perlu melakukan tindakan formal pendisiplinan karyawannya jika diketahui bahwa karyawannya mencoba melakukan pelanggaran keamaan informasi. Proses pendisiplinan tidak akan bisa dilakukan jika tanpa adanya verifikasi terhadap pelanggaran keamanan informasi yang terjadi. Pendisiplinan harus memastikan penanganan yang adil kepada karyawan yang dicurigai melakukan tindakan pelanggaran keamanan informasi. Proses pendisiplinan juga bisa dilakukan untuk mencegah karyawan lain untuk melanggar kebijakan dan prosedur keamanan informasi organisasi maupun pelanggaran lainnya.				
I.12	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan	2,80	**Medium**	36

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?			
Rekomendasi Perbaikan **Control 17.1.1 Planning Information Security Continuity** Lembaga penyelenggara sistem elektronik harus memastikan bahwa ketika terjadi insiden maka kegiatan operasionalnya tetap berjalan untuk itu diperlukan suatu perencanaan untuk memastikan proses bisnis organisasi tetap berlangsung. Makadari itu organisasi harus menentukan kebutuhan untuk menjaga keberlangsungan dari pengelolaan keamanan informasi pada situasi yang tidak diinginkan. Organisasi dapat melakukan BIA (*Business Impact Analysis*) untuk menentukan kebutuhan dalam menjaga keamanan informasi dari situasi yang tidak diinginkan.				
I.9	Apakah Instansi Anda menerapkan program peningkatan kompetensi dan	2,40	**Medium**	38

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?			

Rekomendasi Perbaikan

Control 7.2.2 Information Security Awareness, Education and Training

Seluruh karyawan organisasi maupun berbagai pihak terkait harus mendapatkan pelatihan terhadap aturan dan prosedur untuk pekerjaannya secara berkala. Hal ini untuk meningkatkan kesadaran akan pentingnya keamanan informasi bagi karyawan maupun pejabat terkait. Pelatihan keamanan informasi harus dilakukan berdasarkan kebijakan dan prosedur yang relevan. Dengan begitu karyawan akan sadar pentingnya keamanan informasi untuk dilindungi. Program pelatihan kesadaran informasi perlu dilakukan secara berkala untuk membuat organisasi tetap di jalur sesuai dengan kebijakan dan prosedur untuk menangani insiden yang mengganggu keamanan aset informasi. Pelatihan keamanan informasi harus berisikan aspek :

- Pernyataan sikap manajemen untuk keamanan informasi organisasi
- Kebutuhan untuk mengetahui dan mematuhi aturan keamanan informasi yang berlaku
- Akuntabilitas karyawan untuk mengamanankan informasi
- Informasi dasar prosedur keamanan informasi
- Informasi tambahan dan saran mengenai permsalahan keamanan informasi

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
I.11	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi?	2,40	**Medium**	39
Rekomendasi Perbaikan **Control 6.1.3 Contact With Authorities** Lembaga penyelenggara sistem elektronik secara proaktif berkoordinasi dengan pihak yang relevan dan memiliki otoritas dalam menjaga keamanan informasi. Untuk itu organisasi perlu memiliki prosedur yang menspesifikasikan kapan dan dan siapa yang harus dihubungi dan bagaimana				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
melakukan pengidentifikasian insiden keamanan informasi dan melakukan pelaporan dengan tepat waktu.				
I.13	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	2,40	**High**	40
Rekomendasi Perbaikan **Control 16.1.2 Reporting Information Security Events** **Control 16.1.3 Reporting Information Security Weaknesses** Dalam melaksanakan pengamanan informasi, pelaporan mengenai insiden yang terjadi harus dilaporkan secara cepat kepada pihak yang memiliki wewenang untuk memperbaiki untuk memastikan insiden dapat segera diselesaikan. Untuk itu perlu adanya kesadaran dari seluruh karyawan untuk tanggap terhadap insiden yang terjadi di wilayah tanggung jawabnya. Jika dalam pengamatannya karyawan mungkin menemukan keamanan informasi yang mungkin dicurigai sebagai kelemahan dari sistem maka karyawan harus melakukan pencatatan dan pelaporan terhadap permasalan tersebut.				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
I.10	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada?	2,00	**Medium**	47

Rekomendasi Perbaikan

Control 6.1.3 Contact With Authorities

Lembaga penyelenggara sistem elektronik secara proaktif berkoordinasi dengan pihak yang relevan dan memiliki otoritas dalam menjaga keamanan informasi. Untuk itu organisasi perlu memiliki prosedur yang menspesifikasikan kapan dan dan siapa yang harus dihubungi dan bagaimana melakukan pengidentifikasian insiden keamanan informasi dan melakukan pelaporan dengan tepat waktu.

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
I.5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	1,80	**Medium**	54
Rekomendasi Perbaikan **Control 6.1.2 Segregation Of Duties** **Control 16.1.2 Reporting Information Security Events** Pemisahan tugas dan tanggung jawab harus dilaksanakan dengan jelas untuk menghindari konflik atau penyalahgunaan yang tidak sah terhadap aset organisasi. Dalam melaksanakan pengamanan informasi, pelaporan mengenai insiden yang terjadi harus dilaporkan secara cepat kepada pihak yang memiliki wewenang untuk memperbaiki untuk memastikan insiden dapat segera diselesaikan. Untuk itu perlu adanya kesadaran dari seluruh karyawan untuk tanggap terhadap insiden yang terjadi di wilayah tanggung jawabnya.				
I.7	Apakah semua pelaksana pengamanan informasi di Instansi Anda memiliki kompetensi dan	1,80	**Medium**	55

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	keahlian yang memadai sesuai persyaratan/standar yang berlaku?			

Rekomendasi Perbaikan
Control 7.2.1 Management Responsibilities
Control 7.2.2 Information Security Awareness, Education and Training

Manajemen harus memastikan bahwa seluruh karyawan dan kontraktor melaksanakan kebijakan dan prosedur keamanan informasi yang dibuat organisasi. Untuk itu yang harus dilakukan manajemen adalah :

- Penjelasan mengenai peran dan tanggung jawab yang diberikan untuk mangakses informasi rahasia
- Memberikan panduan untuk memenuhi peran dalam menjaga keamanan informasi
- Memotivasi untuk memenuhi kebijakan keamanan informasi organisasi
- Mencapai tingkat kesadaran mengenai keamanan informasi yang relevan dengan tanggung jawabnya
- Menyesuaikan syarat dan ketentuan dalam bekerja
- Memiliki keahlian dan kualifikasi dan berpendidikan
- Menyediakan pelaporan terhadap tindakan pelanggaran kebijakan keamanan informasi

Seluruh karyawan organisasi maupun berbagai pihak terkait harus mendapatkan pelatihan terhadap aturan dan prosedur untuk pekerjaannya secara berkala. Hal ini untuk meningkatkan kesadaran akan pentingnya keamanan

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
informasi bagi karyawan maupun pejabat terkait. Pelatihan keamanan informasi harus dilakukan berdasarkan kebijakan dan prosedur yang relevan. Dengan begitu karyawan akan sadar pentingnya keamanan informasi untuk dilindungi. Program pelatihan kesadaran informasi perlu dilakukan secara berkala untuk membuat organisasi tetap di jalur sesuai dengan kebijakan dan prosedur untuk menangani insiden yang mengganggu keamanan aset informasi. Pelatihan keamanan informasi harus berisikan aspek : - Pernyataan sikap manajemen untuk keamanan informasi organisasi - Kebutuhan untuk mengetahui dan mematuhi aturan keamanan informasi yang berlaku - Akuntabilitas karyawan untuk mengamanankan informasi - Informasi dasar prosedur keamanan informasi - Informasi tambahan dan saran mengenai permsalahan keamanan informasi				
I.8	Apakah organsiasi Anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?	1,80	**Medium**	56

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
Rekomendasi Perbaikan **Control 7.2.2 Information Security Awareness, Education and Training** Seluruh karyawan organisasi maupun berbagai pihak terkait harus mendapatkan pelatihan terhadap aturan dan prosedur untuk pekerjaannya secara berkala. Hal ini untuk meningkatkan kesadaran akan pentingnya keamanan informasi bagi karyawan maupun pejabat terkait. Pelatihan keamanan informasi harus dilakukan berdasarkan kebijakan dan prosedur yang relevan. Dengan begitu karyawan akan sadar pentingnya keamanan informasi untuk dilindungi. Program pelatihan kesadaran informasi perlu dilakukan secara berkala untuk membuat organisasi tetap di jalur sesuai dengan kebijakan dan prosedur untuk menangani insiden yang mengganggu keamanan aset informasi. Pelatihan keamanan informasi harus berisikan aspek : - Pernyataan sikap manajemen untuk keamanan informasi organisasi - Kebutuhan untuk mengetahui dan mematuhi aturan keamanan informasi yang berlaku - Akuntabilitas karyawan untuk mengamanankan informasi - Informasi dasar prosedur keamanan informasi - Informasi tambahan dan saran mengenai permsalahan keamanan informasi				
I.6	Apakah Instansi Anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian	1,60	**Low**	68

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	pelaksana pengelolaan keamanan informasi?			
Rekomendasi Perbaikan **Control 7.2.1 Management Responsibilities** Manajemen harus memastikan bahwa seluruh karyawan dan kontraktor melaksanakan kebijakan dan prosedur keamanan informasi yang dibuat organisasi. Untuk itu yang harus dilakukan manajemen adalah : - Penjelasan mengenai peran dan tanggung jawab yang diberikan untuk mangakses informasi rahasia - Memberikan panduan untuk memenuhi peran dalam menjaga keamanan informasi - Memotivasi untuk memenuhi kebijakan keamanan informasi organisasi - Mencapai tingkat kesadaran mengenai keamanan informasi yang relevan dengan tanggung jawabnya - Menyesuaikan syarat dan ketentuan dalam bekerja - Memiliki keahlian dan kualifikasi dan berpendidikan - Menyediakan pelaporan terhadap tindakan pelanggaran kebijakan keamanan informasi				
I.14	Apakah kondisi dan permasalahan keamanan informasi di Instansi Anda menjadi konsideran atau bagian dari proses pengambilan	1,60	**Medium**	69

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	keputusan strategis di Instansi Anda?			
Rekomendasi Perbaikan **Control 16.1.6 Learning From Information Security Incidents** Pengkajian terhadap kerangka kerja pengelolaan insiden harus dilakukan hal ini dilakukan untuk menambahkan wawasan kepada penyelenggara sistem elektronik dari hasil analisis dan penyelesaian insiden yang pernah terjadi sebelumnya. Dengan pengkajian yang berulang maka akan mengurangi dampak maupun tingkat keterjadian dari insiden tersebut untuk perusahaan maupun organisasi.				
I.2	Apakah Instansi Anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?	1,20	**Low**	86

<table>
<tr><td>Kode</td><td>Pertanyaan</td><td>GAP</td><td>Kategori Masalah</td><td>Peringkat Keseluruhan</td></tr>
<tr><td colspan="5">Rekomendasi Perbaikan
Control 6.1.1 Information Security Roles and Responsibilities
Control 6.1.2 Segregation Of Duties
Peran dan tanggungjawab mengenai pengamanan informasi harus didefinisikan dan dialokasikan. Pengalokasiannya harus sesuai dengan kebijakan keamanan informasi. Penanggungjawab untuk melindungi aset individu dan menjaga informasi keamanan secara spesifik harus diidentifikasi. Untuk itu area dimana setiap tanggung jawab individu perlu ditetapkan. Untuk itu, adapun yang harus dilakukan adalah :
- Aset dan proses keamanan informasi harus didefinisikan
- Entitas yang bertanggungjawab terhadap tiap aset harus ditugaskan dan detil tanggung jawabnya harus dokumentasikan
- Otorisasi harus didefinisikan dan didokumentasikan
- Pemilihan individu yang diberikan tanggung jawab harus yang berkompeten
- Koordinasi dan kekeliruan yang terjadi harus diidentifikasi dan didokumentasikan
Pemisahan tugas dan tanggung jawab harus dilaksanakan dengan jelas untuk menghindari konflik atau penyalahgunaan yang tidak sah terhadap aset organisasi.</td></tr>
<tr><td>I.4</td><td>Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola</td><td>0,80</td><td>Medium</td><td>106</td></tr>
</table>

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	dan menjamin kepatuhan program keamanan informasi?			
Control 12.1.3 Capacity Management Penggunaan sunber daya harus diawasi, disesuaikan, dan diproyeksikan untuk dapat memenuhi kebutuhan dimasa yang akan datang, hal ini dilakukan untuk memastikan memastikan keberlangsungan kinerja sistem. Penyediaan kapasitas yang cukup bisa dilakukan dengan meningkatkan kapasitas maupun menguranginya. Berikut merupakan contoh pengelolaan kapasitas sumber daya : - Penghapusan data yang usang - Penghentian aplikasi, sistem dan basis data - Meningkatkan pemrosesan dan penjadwalan - Menigkatkan logika basis data (*queries*) - Menolak atau membatasi *bandwidth* terhadap sumber daya jika tidak kritikal terhadap bisnis				
I.3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan	0,60	**Medium**	114

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	program keamanan informasi?			
Rekomendasi Perbaikan **Control 6.1.2 Segregation Of Duties** Pemisahan tugas dan tanggung jawab harus dilaksanakan dengan jelas untuk menghindari konflik atau penyalahgunaan yang tidak sah terhadap aset organisasi **Control 6.1.3 Contact With Authorities** Lembaga penyelenggara sistem elektronik secara proaktif berkoordinasi dengan pihak yang relevan dan memiliki otoritas dalam menjaga keamanan informasi. Untuk itu organisasi perlu memiliki prosedur yang menspesifikasikan kapan dan dan siapa yang harus dihubungi dan bagaimana melakukan pengidentifikasian insiden keamanan informasi dan melakukan pelaporan dengan tepat waktu.				
I.1	Apakah pimpinan Instansi Anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	0,40	**Low**	117

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
Rekomendasi Perbaikan **Control 5.1.1 Policies for Information Security** Harus ada sekumpulan kebijakan untuk keamanan informasi yang dedefinisikan , disetujui oleh pihaka manajemen dan diterbitkan serta dikomunikasikan kepada karyawan dan pihak ketiga. Kebijakan keamanan informasi harus memenuhi kriteria berdasarkan : - Strategi bisnis - Aturan, undang – undang dan kontrak - Lingkungan yang mengancam keamanan informasi Untuk itu kebijakan informasi harus berisi tentang : - Pengertian keamanan informasi, tujuan dan prinsip untuk memandu seluruh aktivitas yang berhubungan dengan keamanan informasi - Pernyataan mengenaitanggungjawab secara umum danspesifik untuk pengelolaan keamanan informasi untuk mendefinisikan peran - Proses untuk menangani penyimpangan dan pengecualian.				

6.4.2. Rekomendasi Perbaikan Area Risiko

Tabel 6.24 merupakan hasil rekomendasi pada poin pertanyaan area risiko keamanan informasi yang paling menjadi masalah bagi instansi/lembaga penyelenggara sistem elektronik. Pemberian rekomendasi berdasarkan pada kendali dan panduan yang dimiliki oleh SNI ISO/IEC 27001.

Tabel 6 24. Rekomendasi Area Risiko

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
II.14	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	7,80	**Medium**	4
Rekomendasi Perbaikan **Control 16.1.6 Learning From Information Security Incidents** Pengkajian terhadap kerangka kerja pengelolaan insiden harus dilakukan hal ini dilakukan untuk menambahkan wawasan kepada penyelenggara sistem elektronik dari hasil analisis dan penyelesaian insiden yang pernah terjadi sebelumnya. Dengan pengkajian yang berulang maka akan mengurangi dampak maupun tingkat keterjadian dari insiden tersebut untuk perusahaan maupun organisasi.				
II.15	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	7,80	**Medium**	5
Rekomendasi Perbaikan **Control 16.1.1 Responsibilities and Procedures** Penyelenggara sistem elektronik harus melakukan pengelolaan yang baik terhadap pertanggungjawabannya dan prosedurnya				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
untuk memastikan keefektifan dalam menanggapi risiko yang terjadi. Untuk itu adapun pedoman dalam menanggapi risiko yang mungkin terjadi terhadap keamanan informasi sebagai berikut : - Melakukan persiapan prosedur rencana untuk menangggapi indiden - Adanya prosedur pemantauan, pendeteksian, analisis dan pelaporan insiden keamanan informasi - Melakukan pencatatan insiden - Pengaturan terhadap bukti forensik dari insiden - Melakukan penilaian terhadap insiden yang terjadi dan mencari kelemahan dari keamanan informasi - Melakukan penyelesaian insiden dengan tetap memepertahankan komunikasi antara bagian internal dan eksternal organisasi				
II.13	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau	4,80	**Medium**	17

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	keperluan penerapan bentuk pengamanan baru?			
Rekomendasi Perbaikan **Control 16.1.7 Collection Of Evidence** Penyelenggara sistem elektronik harus melakukan pengkajian terhadap risiko profil untuk memastikan akurasi dan validitas dari profil risiko apakah masih relevan dalam penggunaannya. Untuk itu organisasi perlu mendefinisikan dan menerapkan prosedur untuk pengidentifikasian, penyimpanan dan pemeliharaan informasi terkait profil dari risiko yang pernah terjadi untuk perbaikan di masa yang akan datang.Untuk itu bukti dari penanganan risiko perlu disimpan untuk menentukan penyelesaian risiko yang sama jika terjadi lagi.				
II.10	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas biaya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir	4,40	**Medium**	19

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	dampak terhadap operasional layanan TIK?			
Rekomendasi Perbaikan **Control 16.1.4 Assesment Of And Decision On Information Security Events** Langkah mitigasi dari risiko harus disusun sesuai tingkat prioritas risiko.Hal ini dilakukan untuk mengklasifikasikan skala dari kejadian yang dapat menghasilkan insiden terhadap keamanan informasi. Dari hasil pengklasifikasian akan dapat diprioritaskan dan dapat diketahui dampak dari insiden itu baik jangka panjang maupun jangka pendek sehingga bisa diminimalisir jika insiden itu memiliki dampak yang sangat besar.				
II.11	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	4,40	**Medium**	20
Rekomendasi Perbaikan **Control 17.1.3 Verify, Review And Evaluate Information Security Continuity** Penyelenggara sistem elektronik harus melakukan verifikasi langkah mitigasi risiko yang telah diterapkan pada interval tertentu untuk memastikan apakah langkah mitigasi risiko				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
tersebut masih cukup efektif untuk meangani dampak buruk dari risiko. Untuk menjaga keandalan langkah mitigasi risiko tersebut, organisasi perlu melakukan review kepada langkah pengamanannya sebagai berikut : - Melakukan pengujian terhadap fungsionalitas, prosedur dan langkah keamanan untuk memaastikan kekonsistenannya dalam mencapai keamanan informasi yang diharapkan - Menguji proses rutinitas penagamanan informasi, prosedur dan langkah pengamanan untuk memastikan kinerjanya sesuai dengan tujuan pengamanan informasi yang diharapkan. - Meninjau kevaliditasan dan keefektifan dari keberlangsungan keamanan informasi, sistem informasi, proses pengamanan informasi, prosedur dan langkah keamanan informasi.				
II.12	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi untuk memastikan konsistensi dan efektifitasnya?	4,40	**Medium**	21
Rekomendasi Perbaikan **Control 17.1.3 Verify, Review And Evaluate Information Security Continuity** Penyelenggara sistem elektronik harus melakukan verifikasi langkah mitigasi risiko yang telah diterapkan pada interval tertentu untuk memastikan apakah langkah mitigasi risiko tersebut masih cukup efektif untuk meangani dampak buruk dari risiko. Untuk menjaga keandalan langkah mitigasi risiko tersebut, organisasi perlu melakukan review kepada langkah pengamanannya sebagai berikut :				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Melakukan pengujian terhadap fungsionalitas, prosedur dan langkah keamanan untuk memaastikan kekonsistenannya dalam mencapai keamanan informasi yang diharapkan - Menguji proses rutinitas penagamanan informasi, prosedur dan langkah pengamanan untuk memastikan kinerjanya sesuai dengan tujuan pengamanan informasi yang diharapkan. - Meninjau kevaliditasan dan keefektifan dari keberlangsungan keamanan informasi, sistem informasi, proses pengamanan informasi, prosedur dan langkah keamanan informasi.				
II.9	Apakah Instansi Anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	2,20	**High**	46
Rekomendasi Perbaikan **Control 17.1.1 Planning Information Security Continuity** **Control 17.1.2 Implementing Information Security Continuity** Lembaga penyelenggara sistem elektronik harus memastikan bahwa ketika terjadi insiden maka kegiatan operasionalnya tetap berjalan untuk itu diperlukan suatu perencanaan untuk memastikan proses bisnis organisasi tetap berlangsung. Makadari itu organisasi harus menentukan kebutuhan untuk menjaga keberlangsungan dari pengelolaan keamanan informasi pada situasi yang tidak diinginkan. Organisasi dapat melakukan BIA (*Business Impact Analysis*) untuk menentukan kebutuhan				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
dalam menjaga keamanan informasi dari situasi yang tidak diinginkan. Setelah mengetahui kebutuhan dan langkah yang perlu dilakukan untuk menjaga keberlangsungan bisnis organisasi harus memiliki dokumen yang digunakan untuk menerapkan proses, prosedur dan langkah keamanan untuk memastikan keberlangsungan bisnis terhadap keamanan informasi dapat berjalan dengan baik pada situasi yang tidak diharapkan. Untuk itu organisasi perlu memastikan beberapa hal : - Struktur manajemen yang memadai untuk menghadapi upaya mitigasi dan menanggapi insiden dengan pihak yang memiliki otoritas dan berpengalaman dibidangnya - Pihak yang merespon insiden dan tanggunjawabnya, pihak yang dapat mengelola insiden dan mempertahankan keamanan informasi - Dokumen perencanaan, prosedur respon dan pemulihan yang dikembangkan dan disetujui. Hal ini berisikan detil mengenai bagaimana organisasi akan mengelola insiden yang terjadi dan dapat mempertahankan keamanan informasi.				
II.1	Apakah Instansi Anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	1,80	**High**	57

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan

Rekomendasi Perbaikan
Control 16.1.1 Responsibilities And Procedures
Control 16.1.2 Reporting Information Security Events
Control 16.1.3 Reporting Information Security Weaknesses
Control 16.1.4 Assesment Of And Decision On Information Security Events

Penyelenggara sistem elektronik harus melakukan pengelolaan yang baik terhadap pertanggungjawabannya dan prosedurnya untuk memastikan keefektifan dalam menanggapi risiko yang terjadi. Untuk itu adapun pedoman dalam menanggapi risiko yang mungkin terjadi terhadap keamanan informasi sebagai berikut :

- Melakukan persiapan prosedur rencana untuk menangggapi indiden
- Adanya prosedur pemantauan, pendeteksian, analisis dan pelaporan insiden keamanan informasi
- Melakukan pencatatan insiden
- Pengaturan terhadap bukti forensik dari insiden
- Melakukan penilaian terhadap insiden yang terjadi dan mencari kelemahan dari keamanan informasi
- Melakukan penyelesaian insiden dengan tetap memepertahankan komunikasi antara bagian internal dan eksternal organisasi

Dalam melaksanakan pengamanan informasi, pelaporan mengenai insiden yang terjadi harus dilaporkan secara cepat kepada pihak yang memiliki wewenang untuk memperbaiki untuk memastikan insiden dapat segera diselesaikan. Untuk itu perlu adanya kesadaran dari seluruh karyawan untuk tanggap terhadap insiden yang terjadi di wilayah tanggung jawabnya.

Jika dalam pengamatannya karyawan mungkin menemukan keamanan informasi yang mungkin dicurigai sebagai kelemahan

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
dari sistem maka karyawan harus melakukan pencatatan dan pelaporan terhadap permasalan tersebut. Kemudian penilaian terhadap kejadian yang dilaporkan harus dilakukan untuk memastikan bahwa kejadian tersebut bisa diklasifikasikan sebagai insiden yang besar. Dari hasil pengklasifikasian akan dapat diprioritaskan dan dapat diketahui dampak dari insiden itu baik jangka panjang maupun jangka pendek.				
II.2	Apakah Instansi Anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	1,80	**High**	58
Rekomendasi Perbaikan **Control 16.1.1 Responsibilities And Procedures** **Control 16.1.2 Reporting Information Security Events** **Control 16.1.3 Reporting Information Security Weaknesses** **Control 16.1.4 Assesment Of And Decision On Information Security Events** Penyelenggara sistem elektronik harus melakukan pengelolaan yang baik terhadap pertanggungjawabannya dan prosedurnya untuk memastikan keefektifan dalam menanggapi risiko yang terjadi. Untuk itu adapun pedoman dalam menanggapi risiko yang mungkin terjadi terhadap keamanan informasi sebagai berikut : - Melakukan persiapan prosedur rencana untuk menangggapi indiden - Adanya prosedur pemantauan, pendeteksian, analisis dan pelaporan insiden keamanan informasi				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Melakukan pencatatan insiden - Pengaturan terhadap bukti forensik dari insiden - Melakukan penilaian terhadap insiden yang terjadi dan mencari kelemahan dari keamanan informasi - Melakukan penyelesaian insiden dengan tetap memepertahankan komunikasi antara bagian internal dan eksternal organisasi Dalam melaksanakan pengamanan informasi, pelaporan mengenai insiden yang terjadi harus dilaporkan secara cepat kepada pihak yang memiliki wewenang untuk memperbaiki untuk memastikan insiden dapat segera diselesaikan. Untuk itu perlu adanya kesadaran dari seluruh karyawan untuk tanggap terhadap insiden yang terjadi di wilayah tanggung jawabnya. Jika dalam pengamatannya karyawan mungkin menemukan keamanan informasi yang mungkin dicurigai sebagai kelemahan dari sistem maka karyawan harus melakukan pencatatan dan pelaporan terhadap permasalan tersebut. Kemudian penilaian terhadap kejadian yang dilaporkan harus dilakukan untuk memastikan bahwa kejadian tersebut bisa diklasifikasikan sebagai insiden yang besar. Dari hasil pengklasifikasian akan dapat diprioritaskan dan dapat diketahui dampak dari insiden itu baik jangka panjang maupun jangka pendek.				
II.3	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat	1,80	**Medium**	59

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi Anda?			
Rekomendasi Perbaikan **Control 8.2.1 Classification Of Information** Lembaga penyelenggara elektronik yang menerapkan SNI ISO/IEC 27001 perlu melakukan pengklasifikasian informasi berdasarkan aturan pengklasifikasian informasi untuk mempermudah pemahamanan dalam menjalankan kerangka kerja pengelolaan risiko. Klasifikasi informasi yang dilakukan akan menunjukkan tingkat sensitivitas dan kekritisan nilai aset dari organisasi. Berikut merupakan contoh klasifikasi informasi berdasarkan 4 lebel : - Tidak membahayakan - Menyebabkan ketidaknyamanan - Memiliki efek jangka pendek pada tujuan operasional tasktis - Memiliki dampak yang serius pada perencanaan jangka panjang (strategis)				
II.7	Apakah dampak kerugian yang terkait dengan hilangnya/tergan ggunya fungsi aset utama sudah ditetapkan	1,80	**Medium**	60

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	sesuai dengan definisi yang ada?			
Rekomendasi Perbaikan **Control 8.1.4 Handling Of Assets** Prosedur untuk penanganan aset harus dibuat dan diimplementasikan berdasarkan pengklasifikasian informasi yang digunakan oleh organisasi. Prosedur yang tepat harus dilakukan untuk menangani, memproses, menyimpan dan menyimpan informasi yang sesuai dengan pengklasifikasian yang diterapkan organisasi. Adapun hal – hal yang perlu diperhatikan adalah : - Pembatasan akses dilakukan berdasarkan pengklasifikasian dampak terhadap aset - Pemeliharaan yang tercatat terhadap aset - Perlindungan secara sementara maupun tetap terhadap inforamsi aset - Penyimpanan aset TI berdasarkan spesifikasi pabrikan - Memberikan penanda pada seluruh media untuk penerima yang diotorisasi.				
II.8	Apakah Instansi Anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk	1,80	**Medium**	61

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?			

Rekomendasi Perbaikan

Control 16.1.1 Responsibilities And Procedures

Penyelenggara sistem elektronik harus melakukan pengelolaan yang baik terhadap pertanggungjawabannya dan prosedurnya untuk memastikan keefektifan dalam menanggapi risiko yang terjadi. Untuk itu adapun pedoman dalam menanggapi risiko yang mungkin terjadi terhadap keamanan informasi sebagai berikut :

- Melakukan persiapan prosedur rencana untuk menangggapi indiden
- Adanya prosedur pemantauan, pendeteksian, analisis dan pelaporan insiden keamanan informasi
- Melakukan pencatatan insiden
- Pengaturan terhadap bukti forensik dari insiden
- Melakukan penilaian terhadap insiden yang terjadi dan mencari kelemahan dari keamanan informasi
- Melakukan penyelesaian insiden dengan tetap memepertahankan komunikasi antara bagian internal dan eksternal organisasi

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
II.4	Apakah Instansi Anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	1,60	**Medium**	70
Rekomendasi Perbaikan **Control 8.1.3 Acceptable Use Of Assets** Lembaga penyelenggara sistem elektronik perlu menerapkan ambang batas terkait tingkat risiko terhadap aset yang dapat diterima. Perlu adanya aturan batas ambang penerimaan risiko yang berhubungan dengan informasi aset. Untuk itu perlu adanya pengidentifikasian, pendokumenan dan pengimplementasian terhadap batas – batas yang telah ditentukan. Jadi karyawan dan pemegang kepentingan yang memiliki akses langsung dengan aset organisasi harus sadar akan pentingnya penagamanan informasi yang terkait dengan aset informasi. Mereka harus siap mempertanggungjawabkan informasi yang diproses dibawah tanggung jawab mereka.				
II.6	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	1,60	**Medium**	71

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
Rekomendasi Perbaikan **Control 8.2.1 Classification Of Information** Pengklasifikasian informasi berdasarkan aturan, nilai, tingkat kekritisan dan kesensitifan terhadap tindakan yang tidak diijinkan atau tindakan memodifikasi aset informasi sebagai upaya terhadap ancaman aset informasi. Pengklasifikasian informasi untuk mempermudah pemahamanan dalam menjalankan kerangka kerja pengelolaan risiko. Klasifikasi informasi yang dilakukan akan menunjukkan tingkat sensitivitas dan kekritisan nilai aset dari organisasi. Berikut merupakan contoh klasifikasi informasi berdasarkan 4 lebel : - Tidak membahayakan - Menyebabkan ketidaknyamanan - Memiliki efek jangka pendek pada tujuan operasional tasktis - Memiliki dampak yang serius pada perencanaan jangka panjang (strategis)				
II.5	Apakah Instansi Anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	1,20	**Medium**	87
Rekomendasi Perbaikan **Control 8.1.2 Ownership Of Assets** Aset yang dipertahankan oleh organisasi harus dipellihara. Makadari itu perlu adanya pihak yang ditugaskan untuk				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
mengelola siklus dari aset tersebut. Adapun tanggung jawab yang harus diemban pengelola aset adalah : - Memastikan aset diinventarisasi - Memastikan aset diklasifikasikan sesuai jenis dan dilindungi - Mendefinisikan dan secara periodik meninjau batasan akses dan pengklasifikasiannya berdasarkan aturan yang telah diterapkan.				

6.4.3. Rekomendasi Perbaikan Area Kerangka Kerja

Tabel 6.25 merupakan hasil rekomendasi pada poin pertanyaan area kerangka kerja keamanan informasi yang paling menjadi masalah bagi instansi/lembaga penyelenggara sistem elektronik. Pemberian rekomendasi berdasarkan pada kendali dan panduan yang dimiliki oleh SNI ISO/IEC 27001.

Tabel 6 25. Rekomendasi Area Kerangka Kerja

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
III.15	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan	9,00	**High**	1

	langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?			

Rekomendasi Perbaikan

Control 17.1.3 Verify, Review And Evaluate Information Security Continuity

Penyelenggara sistem elektronik harus melakukan verifikasi langkah pemulihan bencana yang telah diterapkan pada interval tertentu untuk memastikan apakah langkah pemulihan bencana tersebut masih cukup efektif untuk menangani dampak buruk dari bencana. Untuk menjaga keandalan langkah pemulihan bencana tersebut, organisasi perlu melakukan review kepada langkah pengamanannya sebagai berikut :

- Melakukan pengujian terhadap fungsionalitas, prosedur dan langkah keamanan untuk memaastikan kekonsistenannya dalam mencapai keamanan informasi yang diharapkan
- Menguji proses rutinitas penagamanan informasi, prosedur dan langkah pengamanan untuk memastikan kinerjanya sesuai dengan tujuan pengamanan informasi yang diharapkan.
- Meninjau kevaliditasan dan keefektifan dari keberlangsungan keamanan informasi, sistem informasi, proses pengamanan informasi, prosedur dan langkah keamanan informasi.

III.13	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?	8,40	**Medium**	2

Rekomendasi Perbaikan

Control 17.1.2 Implementing Information Security Continuity

Setelah melakukan perencanaan untuk menjaga keberlangsungan bisnis organisasi harus memiliki dokumen yang digunakan untuk menerapkan proses, prosedur dan langkah keamanan untuk memastikan keberlangsungan bisnis terhadap keamanan informasi dapat berjalan dengan baik pada situasi yang tidak diharapkan. Untuk itu organisasi perlu memastikan beberapa hal :

- Struktur manajemen yang memadai untuk menghadapi upaya mitigasi dan menanggapi insiden dengan pihak yang memiliki otoritas dan berpengalaman dibidangnya
- Pihak yang merespon insiden dan tanggunjawabnya, pihak yang dapat mengelola insiden dan mempertahankan keamanan informasi
- Dokumen perencanaan, prosedur respon dan pemulihan yang dikembangkan dan disetujui. Hal ini berisikan detil mengenai bagaimana organisasi akan mengelola insiden

	yang terjadi dan dapat mempertahankan keamanan informasi.			
III.14	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?	8,40	**Medium**	3
Rekomendasi Perbaikan **Control 17.1.2 Implementing Information Security Continuity** Setelah melakukan perencanaan untuk menjaga keberlangsungan bisnis organisasi harus memiliki dokumen yang digunakan untuk menerapkan proses, prosedur dan langkah keamanan untuk memastikan keberlangsungan bisnis terhadap keamanan informasi dapat berjalan dengan baik pada situasi yang tidak diharapkan. Untuk itu organisasi perlu memastikan beberapa hal : - Struktur manajemen yang memadai untuk menghadapi upaya mitigasi dan menanggapi insiden dengan pihak yang memiliki otoritas dan berpengalaman dibidangnya - Pihak yang merespon insiden dan tanggunjawabnya, pihak yang dapat mengelola insiden dan mempertahankan keamanan informasi - Dokumen perencanaan, prosedur respon dan pemulihan yang dikembangkan dan disetujui. Hal ini berisikan detil mengenai bagaimana organisasi akan mengelola insiden yang terjadi dan dapat mempertahankan keamanan informasi.				
III.16	Apakah seluruh kebijakan dan prosedur keamanan informasi	7,80	**Medium**	6

	dievaluasi kelayakannya secara berkala?			
Rekomendasi Perbaikan **Control 5.1.2 Review Of The Policies For Information Security** Kebijakan dan prosedur penagamanan informasi harus ditinjau pada interval tertentu atau berdasarkan perubahan yang dilakukan untuk memastikan keberlangsungan kesesuaiannya, ketepatannya dan keefektifannya. Setiap kebijakan dan prosedur harus memiliki penanggung jawab yang mengembangkan, meninjau dan mengevaluasinya. Dengan begitu dapat menghasilkan pengembangan dari kebijakan organisasi yang menjaga keamanan informasi yang merespon pada perubahan lingkungan organisasi, lingkungan bisnis serta aturan hukum dan perundanga – undangan yang berlaku.				
III.25	Apakah organisasi Anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada untuk memastikan bahwa keseluruhan inisiatif tersebut telah diterapkan secara efektif?	7,80	**Medium**	7

Rekomendasi Perbaikan **Control 17.2.1 Availability Of Information Processing Facilities** Lembaga penyelenggara sistem elektronik harus merencanakan peningkatan keamanan informasi dengan redudansi yang cukup untuk memenuhi kebutuhan dalam menjaga keamanan informasi. Untuk itu organisasi perlu melakukan pengidentifikasian kebutuhan bisnis untuk memberikan ketersediaan terhadap keamanan inforamsi yang diharapkan.				
III.24	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya ?	7,20	**Medium**	10
Rekomendasi Perbaikan **Control 5.1.2 Review Of The Policies For Information Security** Kebijakan dan prosedur penagamanan informasi harus ditinjau pada interval tertentu atau berdasarkan perubahan yang dilakukan untuk memastikan keberlangsungan kesesuaiannya,				

ketepatannya dan keefektifannya. Setiap kebijakan dan prosedur harus memiliki penanggung jawab yang mengembangkan, meninjau dan mengevaluasinya. Dengan begitu dapat menghasilkan pengembangan dari kebijakan organisasi yang menjaga keamanan informasi yang merespon pada perubahan lingkungan organisasi, lingkungan bisnis serta aturan hukum dan perundanga – undangan yang berlaku.				
III.26	Apakah organisasi Anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	7,80	**Medium**	8
Rekomendasi Perbaikan **Control 17.2.1 Availability Of Information Processing Facilities** Lembaga penyelenggara sistem elektronik harus merencanakan peningkatan keamanan informasi dengan redudansi yang cukup untuk memenuhi kebutuhan dalam menjaga keamanan informasi. Untuk itu organisasi perlu melakukan pengidentifikasian kebutuhan bisnis untuk memberikan ketersediaan terhadap keamanan inforamsi yang diharapkan.				

III.8	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi?	4,40	**Low**	22
Rekomendasi Perbaikan **Control 18.2.3 Technical Compliance Review** Lembaga penyelenggara sistem elektronik harus menyelenggarakan prosedur resmi untuk meninjau kepatuhan teknis dengankebijakan pengamanan informasi dan standar yang diterapkan oleh organisasi. Peninjauan kepatuhan teknis dilakukan oleh teknisi sistem yang berpengalaman dengan menggunakan alat peninjau otomatis.				
III.9	Apakah organisasi Anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya	4,00	**Medium**	24

	dan melaporkannya?			
Rekomendasi Perbaikan **Control 14.1.1 Information Security Requirements Analysis And Specification** Lembaga penyelenggara sistem elektronik harus menerapkan prosedur opersional implementasi, pengalokasian tanggung jawab, memantau serta melakukan pelaporan yang berguna untuk meningkatkan keamanan sistem informasi yang ada. Kebutuhan pengamanan itu harus mempertimbangkan beberapa hal, diantaranya : - Tingkat kepercayaan pengguna yang diklaim untuk mendapatkan persyaratan otentikasi pengguna - Penyediaan akses dan proses autorisasi terhadap pengguna yang berhak - Menginformasikan pengguna dan operator akan tugas dan tanggung jawabnya - Perlindungan terhadap aset yang terlibat berdasarkan kaidah *CIA.* - Kebutuhan proses bisnis seperti pencatatan transaksi dan pemantauan - Persyaratan kendali keamanan termasuk pencatatan dan pemantauan serta pendeteksian kebocoran data.				
III.11	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang	4,00	**Medium**	25

	ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya ?			
Rekomendasi Perbaikan **Control 14.2.1 Secure Development Policy** Penerapan suatu sistem hendaknya menerapkan aturan untuk perangkat lunak yang telah dibuat oleh organisasi. Untuk memastikan keamanan penerapan perlu diciptakannya kondisi layanan, arsitektur, software dan sistem yang memenuhi kriteria yang dikatakan aman. Berikut merupakan aspek – aspek yang perlu diperhatikan untuk mempertahankan pengamanan informasi : - Keamanan lingkungan pengembangan - Panduan pengamanan pada siklus pengembangan sistem - Kebutuhan pengamanan pada fase desain - Mengadakan pengamanan bertahap pada proyek - Mengamankan repositori - Pengamanan versi kendali - Pemahaman tentang keamanan aplikasi - Kemampuan pengembang dalam menghindari, menemukan dan memperbaiki kelemahan.				
III.12	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business*	4,00	**High**	26

	continuity planning) yang mendefinisikan persyaratan/kon sideran keamanan informasi, termasuk penjadwalan uji-cobanya?			
Rekomendasi Perbaikan **Control 17.1.1 Planning Information Security Continuity** Lembaga penyelenggara sistem elektronik harus memastikan bahwa ketika terjadi insiden maka kegiatan operasionalnya tetap berjalan untuk itu diperlukan suatu perencanaan untuk memastikan proses bisnis organisasi tetap berlangsung. Makadari itu organisasi harus menentukan kebutuhan untuk menjaga keberlangsungan dari pengelolaan keamanan informasi pada situasi yang tidak diinginkan. Organisasi dapat melakukan BIA (*Business Impact Analysis*) untuk menentukan kebutuhan dalam menjaga keamanan informasi dari situasi yang tidak diinginkan.				
III.22	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja	3,20	**Medium**	30

	keamanan informasi?			
Rekomendasi Perbaikan **Control 12.7.1 Information Systems Audit Controls** Kegiatan audit yang dilakukan harus dilakukan dengan verifikasi sistem opersional secara hati – hati dan terencana untuk menghindari gangguan terhadap proses bisnis yang sedang berjalan. Berikut merupakan panduan yang harus diperhatikan : - Sistem dan data yang diaudit harus disetujui oleh pihak manajemen - Cakupan pengujian audit harus disetujui dan dikontrol. - Pengujian audit harus terbatas pada akses *read-only* terhadap perangkat lunak dan data. - Akses terhadap data *non read-only* dapat dilakukan pada sistem yang terisolasi dan harus segera dihapus ketika audit selesai. - Kebutuhan akan proses khusus harus diidentifikasi - Audit yang dapat mengganggu ketersediaan sistem harus dilakukan diluar jam bisnis - Setiap proses pengaksesan harus di pantau dan dicatat.				
III.23	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	2,80	**Medium**	37

Rekomendasi Perbaikan

Control 12.7.1 Information Systems Audit Controls

Kegiatan audit yang dilakukan harus dilakukan dengan verifikasi sistem opersional secara hati – hati dan terencana untuk menghindari gangguan terhadap proses bisnis yang sedang berjalan. Berikut merupakan panduan yang harus diperhatikan :

- Sistem dan data yang diaudit harus disetujui oleh pihak manajemen
- Cakupan pengujian audit harus disetujui dan dikontrol.
- Pengujian audit harus terbatas pada akses *read-only* terhadap perangkat lunak dan data.
- Akses terhadap data *non read-only* dapat dilakukan pada sistem yang terisolasi dan harus segera dihapus ketika audit selesai.
- Kebutuhan akan proses khusus harus diidentifikasi
- Audit yang dapat mengganggu ketersediaan sistem harus dilakukan diluar jam bisnis

Setiap proses pengaksesan harus di pantau dan dicatat.

III.7	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	2,40	**High**	41

Rekomendasi Perbaikan **Control 7.2.3 Disciplinary Process** Lemabaga penyelenggara sistem elektronik perlu melakukan tindakan formal pendisiplinan karyawannya jika diketahui bahwa karyawannya mencoba melakukan pelanggaran keamaan informasi. Proses pendisiplinan tidak akan bisa dilakukan jika tanpa adanya verifikasi terhadap pelanggaran keamanan informasi yang terjadi. Pendisiplinan harus memastikan penanganan yang adil kepada karyawan yang dicurigai melakukan tindakan pelanggaran keamanan informasi. Proses pendisiplinan juga bisa dilakukan untuk mencegah karyawan lain untuk melanggar kebijakan dan prosedur keamanan informasi organisasi maupun pelanggaran lainnya.				
III.10	Apakah organisasi Anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?	2,40	**Medium**	42
Rekomendasi Perbaikan **Control 14.1.1 Information Security Requirements Analysis And Spesification** Lembaga penyelenggara sistem elektronik harus menerapkan prosedur opersional implementasi, pengalokasian tanggung jawab, memantau serta melakukan pelaporan yang berguna untuk meningkatkan keamanan sistem informasi yang ada. Kebutuhan pengamanan itu harus mempertimbangkan beberapa hal, diantaranya :				

- Tingkat kepercayaan pengguna yang diklaim untuk mendapatkan persyaratan otentikasi pengguna - Penyediaan akses dan proses autorisasi terhadap pengguna yang berhak - Menginformasikan pengguna dan operator akan tugas dan tanggung jawabnya - Perlindungan terhadap aset yang terlibat berdasarkan kaidah *CIA.* - Kebutuhan proses bisnis seperti pencatatan transaksi dan pemantauan - Persyaratan kendali keamanan termasuk pencatatan dan pemantauan serta pendeteksian kebocoran data.				
III.2	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	1,80	**Medium**	62
Rekomendasi Perbaikan **Control 5.1.1 Policies For Information Security** Harus ada sekumpulan kebijakan untuk keamanan informasi yang dedefinisikan , disetujui oleh pihak manajemen dan diterbitkan serta dikomunikasikan kepada karyawan dan pihak ketiga. Kebijakan keamanan informasi harus memenuhi kriteria berdasarkan : - Strategi bisnis				

- Aturan, undang – undang dan kontrak - Lingkungan yang mengancam keamanan informasi Untuk itu kebijakan informasi harus berisi tentang : - Pengertian keamanan informasi, tujuan dan prinsip untuk memandu seluruh aktivitas yang berhubungan dengan keamanan informasi - Pernyataan mengenaitanggungjawab secara umum danspesifik untuk pengelolaan keamanan informasi untuk mendefinisikan peran - Proses untuk menangani penyimpangan dan pengecualian.				
III.5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi?	1,80	**Low**	63
Rekomendasi Perbaikan **Control 16.1.5 Response To Information Security Incidents** Keseluruhan kebijakan dan prosedur keamanan informasi yang dibuat merespon terhadap insiden keamanan informasi yang terjadi. Bagian penanganan insiden harus bertanggungjawab menjaga keberlangsungan bisnis dari insiden yang terjadi. Untuk itu bagian penanganan insiden perlu melakukan : - Pengumpulan bukti kejadian secepat mungkin - Melakukan analisis forensik - Eskalasi jika diperlukan - Memastikansetiap respon terhadap masalah dicatat dengan baik untuk analisis nantinya - Mengkomunikasikan insiden kepada pihak internal maupun eksternal organisasi.				

- Menemukan kelemahan keamanan informasi yang menjadi penyebab insiden - Ketika insiden terselesaikan secara formal menutup dan merekamnya.				
III.17	Apakah organisasi Anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	1,80	**Medium**	64
Rekomendasi Perbaikan **Control 16.1.6 Learning From Information Security Incidents** Pengkajian terhadap kerangka kerja pengelolaan risiko harus dilakukan hal ini dilakukan untuk menambahkan wawasan kepada penyelenggara sistem elektronik dari hasil analisis dan penyelesaian risiko yang pernah terjadi sebelumnya. Dengan pengkajian yang berulang maka akan mengurangi dampak maupun tingkat keterjadian dari insiden tersebut untuk perusahaan maupun organisasi.				
III.18	Apakah organisasi Anda mempunyai strategi penggunaan teknologi	1,80	**Medium**	65

	keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?			
Rekomendasi Perbaikan **Control 17.1.2 Implementing Information Security Continuity** Setelah mengetahui kebutuhan dan langkah yang perlu dilakukan untuk menjaga keberlangsungan bisnis organisasi lewat analisis risiko. Organisasi harus memiliki dokumen yang digunakan untuk menerapkan proses, prosedur dan langkah keamanan untuk memastikan keberlangsungan bisnis terhadap keamanan informasi dapat berjalan dengan baik pada situasi yang tidak diharapkan. Untuk itu organisasi perlu memastikan beberapa hal : - Struktur manajemen yang memadai untuk menghadapi upaya mitigasi dan menanggapi insiden dengan pihak yang memiliki otoritas dan berpengalaman dibidangnya - Pihak yang merespon insiden dan tanggunjawabnya, pihak yang dapat mengelola insiden dan mempertahankan keamanan informasi - Dokumen perencanaan, prosedur respon dan pemulihan yang dikembangkan dan disetujui. Hal ini berisikan detil mengenai bagaimana organisasi akan mengelola insiden yang terjadi dan dapat mempertahankan keamanan informasi.				
III.21	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan	1,80	**Medium**	66

	efektifitas penerapan keamanan informasi?			
Rekomendasi Perbaikan **Control 12.7.1 Information Systems Audit Controls** Kegiatan audit yang dilakukan harus dilakukan dengan verifikasi sistem opersional secara hati – hati dan terencana untuk menghindari gangguan terhadap proses bisnis yang sedang berjalan. Berikut merupakan panduan yang harus diperhatikan : - Sistem dan data yang diaudit harus disetujui oleh pihak manajemen - Cakupan pengujian audit harus disetujui dan dikontrol. - Pengujian audit harus terbatas pada akses *read-only* terhadap perangkat lunak dan data. - Akses terhadap data *non read-only* dapat dilakukan pada sistem yang terisolasi dan harus segera dihapus ketika audit selesai. - Kebutuhan akan proses khusus harus diidentifikasi - Audit yang dapat mengganggu ketersediaan sistem harus dilakukan diluar jam bisnis - Setiap proses pengaksesan harus di pantau dan dicatat.				
III.19	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi Anda?	1,60	**Medium**	72

Rekomendasi Perbaikan **Control 17.1.1 Planning Information Security Continuity** Lembaga penyelenggara sistem elektronik harus memastikan bahwa ketika terjadi insiden maka kegiatan operasionalnya tetap berjalan untuk itu diperlukan suatu perencanaan untuk memastikan proses bisnis organisasi tetap berlangsung. Makadari itu organisasi harus menentukan kebutuhan untuk menjaga keberlangsungan dari pengelolaan keamanan informasi pada situasi yang tidak diinginkan. Organisasi dapat melakukan BIA (*Business Impact Analysis*) untuk menentukan kebutuhan dalam menjaga keamanan informasi dari situasi yang tidak diinginkan yang dapat dituangkan dalam dokumen BCP.				
III.20	Apakah organisasi Anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	1,60	**High**	73
Rekomendasi Perbaikan **Control 12.7.1 Information Systems Audit Controls** Kegiatan audit yang dilakukan harus dilakukan dengan verifikasi sistem opersional secara hati – hati dan terencana untuk menghindari gangguan terhadap proses bisnis yang sedang berjalan. Berikut merupakan panduan yang harus diperhatikan :				

- Sistem dan data yang diaudit harus disetujui oleh pihak manajemen - Cakupan pengujian audit harus disetujui dan dikontrol. - Pengujian audit harus terbatas pada akses *read-only* terhadap perangkat lunak dan data. - Akses terhadap data *non read-only* dapat dilakukan pada sistem yang terisolasi dan harus segera dihapus ketika audit selesai. - Kebutuhan akan proses khusus harus diidentifikasi - Audit yang dapat mengganggu ketersediaan sistem harus dilakukan diluar jam bisnis - Setiap proses pengaksesan harus di pantau dan dicatat.				
III.4	Apakah tersedia mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	1,40	**Medium**	76
Rekomendasi Perbaikan **Control 5.1.1 Policies For Information Security** Harus ada sekumpulan kebijakan untuk keamanan informasi yang dedefinisikan , disetujui oleh pihaka manajemen dan diterbitkan serta dikomunikasikan kepada karyawan dan pihak ketiga. Kebijakan keamanan informasi harus memenuhi kriteria berdasarkan : - Strategi bisnis - Aturan, undang – undang dan kontrak - Lingkungan yang mengancam keamanan informasi				

Untuk itu kebijakan informasi harus berisi tentang : - Pengertian keamanan informasi, tujuan dan prinsip untuk memandu seluruh aktivitas yang berhubungan dengan keamanan informasi - Pernyataan mengenaitanggungjawab secara umum danspesifik untuk pengelolaan keamanan informasi untuk mendefinisikan peran - Proses untuk menangani penyimpangan dan pengecualian.				
III.1	Apakah kebijakan dan prosedur keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya ?	1,20	**High**	88
Rekomendasi Perbaikan **Control 5.1.1 Policies For Information Security** Harus ada seumpulan kebijakan untuk keamanan informasi yang dedefinisikan , disetujui oleh pihaka manajemen dan diterbitkan serta dikomunikasikan kepada karyawan dan pihak ketiga. Kebijakan keamanan informasi harus memenuhi kriteria berdasarkan : - Strategi bisnis - Aturan, undang – undang dan kontrak - Lingkungan yang mengancam keamanan informasi Untuk itu kebijakan informasi harus berisi tentang :				

- Pengertian keamanan informasi, tujuan dan prinsip untuk memandu seluruh aktivitas yang berhubungan dengan keamanan informasi - Pernyataan mengenaitanggungjawab secara umum danspesifik untuk pengelolaan keamanan informasi untuk mendefinisikan peran - Proses untuk menangani penyimpangan dan pengecualian.				
III.3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	1,20	**High**	89
Rekomendasi Perbaikan **Control 18.2.1 Independent Review Of Information Security** **Control 18.2.2 Compliance With Security Policies And Standards** Lembaga penyelenggara sistem elektronik perlu melakukan mekanisme untuk meninjau kebijakan dan prosedur keamanan informasi. Yang ditinjau tidak hanya dokumennya namun dalam penerapannya juga. Peninjauan dilakukan secara indipenden dan terencana dalam jangka waktu tertentu atau jika terjadi perubahan yang signifikan. Peninjauan yang dilakukan untuk memastikan kesesuaian antara pemrosesan informasi pada				

setiap area dengan kebijakan dan standar keamanan informasi yang diterapkan oleh organisasi. Tentunya peninjauan ini dilakukan oleh – masing – masing manajer tiap area. Jika manajer menemukan ketidaksesuaian dari hasil peninjauannnya maka manajer dapat melakukan : - Mengidentifikasi penyebab ketidaksesuian - Mengevaluasi aksi yang dibutuhkan untuk mencapai kesesuaian - Mengimplementasikan tindakan korektif yang tepat - Mewninjau tindakan korektif yang diambil untuk memverifikasi keefektifannya dan menemukan kelemahannya.				
III.6	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset tercantum dalam kontrak dengan pihak ketiga?	0,80	**High**	107
Rekomendasi Perbaikan **Control 15.1.1 Information Security Policy For Supplier Relationships** Segala aspek keamamanan informasi yang terkait dengan pihak ketiga haruslah disetujui dan terdokumentasi. Hal ini berkaitan dengan upaya mitigasi risiko yang terkait dengan pihak ketiga. Untuk itu lembaga penyelenggara sistem elektronik perlu mengidentifikasi kendali pengamanan informasi yang berkaitan dengan pihak ketiga dalam kebijakannya. Pengamanan tersebut merupakan proses dan prosedur yang perlu diterapkan oleh pihak ketiga. Adapun contoh proses dan prosedurnya adalah :				

- Mengidentifikasi dan mendokumentasikan tipe pihak ketiga baik layanan, keuangan, infrastrukturnya.
- Proses terstandarisasi dan siklus hidup untuk membina hubungan dengan pihak ketiga
- Mendefinisikan informasi yang boleh diakses pihak ketiga dan memantau serta mengendalikan aksesnya
- Penanganan insiden termasuk pertanggungjawaban kepada kedua belah pihak.
- Pelatihan kesadaran kepada personel organisasi.
- Kewajiban pihak ketiga untuk menjaga informasi organisasi
- Proses pemantauan untuk mencapai pengamanan informasi kedua belah pihak.

6.4.4. Rekomendasi Perbaikan Area Pengelolaan Aset

Tabel 6.26 merupakan hasil rekomendasi pada poin pertanyaan area pengelolaan aset keamanan informasi yang paling menjadi masalah bagi instansi/lembaga penyelenggara sistem elektronik. Pemberian rekomendasi berdasarkan pada kendali dan panduan yang dimiliki oleh SNI ISO/IEC 27001.

Tabel 6 26. Rekomendasi Area Pengelolaan Aset

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
IV.24	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga	4,80	**High**	18

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	(termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?			

Rekomendasi Perbaikan

Control 18.1.2 Intellectual Property Rights

Perlu adanya prosedur yang menjamin penggunaan perangkat pengoleh informasi milik pihak ketiga dan memastikan aspek HAKI untuk menjaga keamanan informasi bersama. Prosedur yang tepat harus diimplementasikan yang memastikan kesesuaian dengan peraturan dan kontrak yang berlaku. Berikut merupakan beberapa panduan yang melindungi aspek HAKI yang digunakan :

- Penerbitan kebijakan HAKI yang mendefinisikan penggunaan perangkat lunak dan informasi dari produk
- Memperoleh perangkat lunak hanya dari sumber yang terpercaya
- Mempertahankan kesadaran akan kebijakan mengenai HAKI
- Mempertahankan daftar aset yang tepat untuk melindungi HAKI
- Mempertahankan bukti kepemilikan lisensi, cd master dan panduan.
- Mengimplementasikan pengendalian yang memastikan jumlah maksimum pengguna yang diijinkan pada lisensi
- Melakukan ulasan hanya perangkat lunak yang terotorisasi dan produk berlisensi

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Membuat kebijakan untuk mempertahankan kondisi lisensi yang tepat.				
IV.34	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi Anda?	4,20	**High**	23

Rekomendasi Perbaikan

Control 11.1.2 Physical Entry Controls

Area kerja harus dilindungi dengan kendali yang tepat untuk memastikan hanya orang yang memiliki wewenang yang boleh mengaksesnya. Untuk itu dilakukan beberapa hal sebagai berikut :

- Pencatatan tanggal dan waktu masuk dan keluarnya pengunjung
- Akses ke area yang memiliki informasi penting dibatasi hanya kepada orang yang berwenang dengan kartus akses atau perlindungan pin.
- Buku log fisik dan digital harus dijaga dan ditinjau
- Seluruh karyawan, pihak ketiga dan kontraktor harus menggunakan kartu pengenal yang terlihat untuk memudahkan pengenalan
- Pihak ketiga layanan harus diberikan batasan pada area yang memiliki informasi rahasia.
- Hak akses area harus ditinjau secara berkala

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
IV.19	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	4,00	**Medium**	27
Rekomendasi Perbaikan **Control 16.1.2 Reporting Information Security Events** Dalam melaksanakan pengamanan informasi, pelaporan mengenai insiden yang terjadi harus dilaporkan secara cepat kepada pihak yang memiliki wewenang untuk memperbaiki untuk memastikan insiden dapat segera diselesaikan. Untuk itu perlu adanya kesadaran dari seluruh karyawan untuk tanggap terhadap insiden yang terjadi di wilayah tanggung jawabnya. Serta diperlukan pengetahuan akan prosedur pelaporan oleh setiap karyawan dan kontraktor terkait.				
IV.23	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	3,60	**Medium**	28
Rekomendasi Perbaikan **Control 12.4.1 Event Logging** Perlu adanya daftar rekaman pelaksanaan keamanan informasi. Hal ini dikarenakan perekaman akan merekam aktivitas dari pengguna, kesalahan dan kegiatan pengamanan informasi.				

<table>
<tr><th>Kode</th><th>Pertanyaan</th><th>GAP</th><th>Kategori Masalah</th><th>Peringkat Keseluruhan</th></tr>
<tr><td colspan="5">Rekaman tersebut harus selalu dibuat dan disimpan serta secara berkala ditinjau ulang. Untuk jenis informasi yang direkam bisa berupa :
- ID Pengguna
- Aktivitas sistem
- Tanggal, waktu dan detail kejadian log-on dan log-off
- Identitas perangkat
- Rekaman sukses dan gagalnya percobaan akses sistem
- Perubahan konfigurasi
- Hak akses
- Alamat jaringan
- Rekaman transaksi</td></tr>
<tr><td>IV.20</td><td>Prosedur penghancuran data/aset yang sudah tidak diperlukan</td><td>3,30</td><td>Medium</td><td>31</td></tr>
<tr><td colspan="5">Rekomendasi Perbaikan
Control 8.3.1 Management Of Removable Media
Control 8.3.2 Disposal Of Media
Lembaga penyelenggara sistem elektronik memerlukan prosedur untuk mengelolaan media penyimpanan data berdasarkan skema yang diadopsi oleh organisasi.
Untuk penghasncuran media dilakukan ketika data oada media sudah tidak diperlukan lagi yang tentunya dilakukan dalam prosedur yang telah dibuat organisasi. Adapun hal – hal yang perlu diperhatikan dalam penghancuran atau pembuangan data adalah :
- Media yang berisi data rahasia harus disimpan dan dibuang secara aman</td></tr>
</table>

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Prosedur diperlukan untuk mengidentifikasi hal memerlukan pembuangan secara aman - Melakukan pengaturan dahulu kemudian dibuang secara aman - Pemilihan pihak ketiga yang tepat untuk pembuangan data - Pembuangan data yang sensitif harus dicatat untuk menjaga jejak audit				
IV.22	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	3,00	**Medium**	35
Rekomendasi Perbaikan **Control 12.3.1 Information Backup** Backup merupakan hal yang harus dilakukan secara berkala berdasarkan kebijakan *backup* yang telah disetujui. Ketika merancang *backup* beberapa hal yang harus diperhatikan adalaj : - Prosedur penyalinan yang akurat dan lengkap harus dibuat. - Perpanjangan dan frekuensi *backup* berdasarkan kebutuhan bisnis - Lokasi backup harus berada pada daerah yang berbeda dengan daerah utama untuk menghindari masalah yang sama dari daerah utama - Informasi yang diberikan harus tepat berdasarkan standar yang diacu - Media backup harus diuji untuk memastikan dapat digunakan pada keadaan darurat - *Backup* harus dilindungi dengan enkripsi				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
IV.17	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya	2,00	**High**	48

Rekomendasi Perbaikan

Control 11.1.1 Physical Security Perimeter

Ketentuan pengamanan harus didefinikan dan digunakan untuk melindungi area yang memiliki informasi sensitif perusahaan. Adapun panduan yang perlu dilakukan untuk pengamanan fisik adalah :

- Ketentuan pengamanan yang didefinisikan harus sesuai dengan hasil penilaian risiko
- Bangunan harus berada pada area yang tidak sepi, memiliki kontruksi yang kuat, memiliki mekanisme penguncian dan *alarm*, dan harus terkunci untuk menghindari hal yang tidak diinginkan
- Pengendalian akses lewat *front office* harus dilakukan, untuk menghindari akses yang tidak diinginkan
- Menerpkan pelindung fisik
- Ketentuan dalam prosedur insiden kebakaran diatru dalam standar internasional.
- Pendeteksi penyusup harus diterapkan berdasarkan standar internasional
- Pengelolaan fasilitas pengelolaan informasi organisasi harus terpisah dengan pengelolaan yang dilakukan pihak ketiga.

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
IV.18	Proses pengecekan latar belakang SDM	2,00	**Medium**	49
Rekomendasi Perbaikan **Control 7.1.1 Screening** Lembaga penyelenggara sistem elektronik perlu melakukan proses pengecekan latar belakang seluruh kandidat karyawan berdasarjan hukum dan etika yang berlaku. Hal ini dilakukan untuk memnuhi keamanan informasi terhadap setiap karyawan yang masuk perusahaan supaya benar – benar memenuhi kebutuhan bisnis dan menghindari risiko kejahatan oleh karyawan yang tidak diinginkan. Adapun verifikasi yang dapat dilakukan dengan : - Karakter yang memuaskan keperluan bisnis - Verifikasi CV pemohon - Konfirmasi untuk klaim akadamic dan kualifikasi profesional - Verifikasi identitas diri - Verifikasi detail terhadap jejak kriminal				
IV.31	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	2,00	**High**	50

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
Rekomendasi Perbaikan **Control 11.2.4 Equipment Maintenance** Perlu adanya proses pemeriksaan dan perawatan fasilitas pendukung secara berkala. Hal ini dilakukan untuk memastikan ketersediaan yang terus terjaga dan dan tidak adanya perubahan yang dapat berdampak pada proses bisnis organisasi. Adapun panduan untuk perwatan fasilitas pendukung adalah : - Fasilitas harus dirawat berdasarkan waktu layanan yang ditentukan - Hasnya karyawan yang terotorisasi yang dapt melakukan perbaikan - Rekaman tindakan terhadap fasilitas harus dijaga - Kendali yang tepat harus diterapkan ketika pemeliharaan dijadwalkan - Asuransi pemeliharaan harus dipenuhi - Sebelum fasilitas dikembalikan setelah pemeliharaan perlu dilakukan pengecekan.				
IV.33	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas	2,00	**High**	51

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)			
Rekomendasi Perbaikan **Control 11.1.5 Working In Secure Areas** Lembaga penyelenggara sistem elektronik harus memiliki peraturan untuk mengamankan lokasi kerja yang dianggap penting. Prosedur untuk bekerja pada suatu area tertentu harus didesain dan di terapkan untuk menjaga keamanan lokasi kerja tertentu. Adapun panduan yang harus diperhatikan adalah : - Pegawai harus sadar terhadap keberadaan aktivitas pada area khusus - Pekerjaan yang tidak diawasi di area khusus harus dihindari untuk mencegah kesempatan untuk terjadinya aktivitas yang membahayakan - Area yang kosong harus dikunci dan di kunjungi secara berkala - Perlengkapan Foto, video, dan audio tidak diijinkan pada area khusus kecuali mendapatkan persetujuan.				
IV.9	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	1,80	**Medium**	67

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
Rekomendasi Perbaikan **Control 8.1.3 Acceptable Use Of Assets** Lembaga penyelenggara sistem elektronik perlu menerapkan ambang batas terkait tingkat risiko terhadap aset yang dapat diterima. Perlu adanya aturan batas ambang penerimaan risiko yang berhubungan dengan informasi aset. Untuk itu perlu adanya pengidentifikasian, pendokumenan dan pengimplementasian terhadap batas – batas yang telah ditentukan. Jadi karyawan dan pemegang kepentingan yang memiliki akses langsung dengan aset organisasi harus sadar akan pentingnya penagamanan informasi yang terkait dengan aset informasi. Mereka harus siap mempertanggungjawabkan informasi yang diproses dibawah tanggung jawab mereka.				
IV.29	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi Anda apabila digunakan di luar lokasi kerja resmi (kantor)?	1,60	**High**	74
Rekomendasi Perbaikan **Control 11.1.4 Protecting Against External And Enviromental Threats** Lembaga penyelenggara sistem elektronik harus membuat aturan untuk melindungi perangkat komputasi instansi jika digunakan di luar lokasi kerja remi. Perlu adanya perlindungan fisik untuk menghadapi bencana alam, serangan atau insieden. Untuk itu perlu didesain model perlindungan yang tepat untuk				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
menghadapi masalah yang mungkin terjadi itu dan menerapkannya dalam proses kerja organisasi.				
IV.32	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	1,60	**Medium**	75
Rekomendasi Perbaikan **Control 13.2.2 Agreements On Information Transfer** Mekanisme pengamanan dalam pengirimaan aset informasi yang melibatkan pihak ketiga harus diamankan agar informasi dikirimkan dapat diterima pada tujuannya. Untuk itu adapun persetujuan transfer yang dilakukan adalah : - Manajemen bertanggungjawab untuk mengendalikan dan memberitahukan pengiriman dan penerimaan - Prosedur untuk memastikan pelacakan - Standar teknis pengemasan danpengiriman - Surat pengiriman - Standar kurir - Pertanggungjawaban insiden keamanan				
IV.1	Apakah tersedia daftar inventaris aset informasi yang lengkap dan akurat?	1,40	**Medium**	77
Rekomendasi Perbaikan **Control 8.1.1 Inventory Of Assets** **Control 8.1.2 Ownership Of Assets**				

<table>
<tr><th>Kode</th><th>Pertanyaan</th><th>GAP</th><th>Kategori Masalah</th><th>Peringkat Keseluruhan</th></tr>
<tr><td colspan="5">Aset yang berkaitan dengan informasi dan fasilitas pmerosesan informasi harus diidentifikasi dan penginventarisan aset tersebut harus dibuat dan dijaga. Organisasi perlu mengidentifikasi aset yang berhubungan dengan siklus hidup informasi. Hal ini penting karena didalamnya mengatur dari permbuatan, pmerosesan, penyimpanan pemindahan, pembuangan dan penghancuran. Untuk itu diperlukan dokumentasi untuk setiap aset yang dimiliki oleh organisasi.
Aset yang dipertahankan oleh organisasi harus dipellihara. Makadari itu perlu adanya pihak yang ditugaskan untuk mengelola siklus dari aset tersebut. Adapun tanggung jawab yang harus diemban pengelola aset adalah :
- Memastikan aset diinventarisasi
- Memastikan aset diklasifikasikan sesuai jenis dan dilindungi
- Mendefinisikan dan secara periodik meninjau batasan akses dan pengklasifikasiannya berdasarkan aturan yang telah diterapkan.</td></tr>
<tr><td>IV.3</td><td>Apakah tersedia definisi tingkatan akses yang berbeda dan matrix yang merekam alokasi akses tersebut</td><td>1,40</td><td>High</td><td>78</td></tr>
<tr><td colspan="5">Rekomendasi Perbaikan
Control 9.2.3 Management Of Privileged Access Rights
Perlu adanya pengkajian prosedur penggunaan hak akses untuk mengendalikan akses dari pihak yang ingin mengakses tanpa memiliki otorisasi. Pengalokasian hak akses harus terbatas dan dikendalikan oleh pihak manajemen yang bertanggung jawab. Adapun langkah dalam melakukan pengendaliannya adalah :</td></tr>
</table>

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Hak akses pengguna harus tersasosiasi dengan sistem dan proses - Hak akses dialokasikan kepada pengguna yang memenuhi persyaratan aturan divisinya - Proses otorisasi harus dijaga - Kebutuhan untuk hak akses yang kadaluarsa harus didefinisikan - Kompetensi pengguna hak akses harus ditinjau secara berkala untuk memverifikasi pengguna melakukan tugasnya - Prosedur yang spesifik harus dibuat dan dijaga untuk menghindari penggunaan yang tidak diijinkan				
IV.6	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?Apakah Instansi Anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?	1,40	**Medium**	79

<table>
<tr><th>Kode</th><th>Pertanyaan</th><th>GAP</th><th>Kategori Masalah</th><th>Peringkat Keseluruhan</th></tr>
<tr><td colspan="5">Rekomendasi Perbaikan
Control 8.1.1 Inventory Of Assets
Control 8.1.2 Ownership Of Assets
Aset yang berkaitan dengan informasi dan fasilitas pmerosesan informasi harus diidentifikasi dan penginventarisan aset tersebut harus dibuat dan dijaga. Organisasi perlu mengidentifikasi aset yang berhubungan dengan siklus hidup informasi. Hal ini penting karena didalamnya mengatur dari permbuatan, pmerosesan, penyimpanan pemindahan, pembuangan dan penghancuran. Untuk itu diperlukan dokumentasi untuk setiap aset yang dimiliki oleh organisasi.
Aset yang dipertahankan oleh organisasi harus dipellihara. Makadari itu perlu adanya pihak yang ditugaskan untuk mengelola siklus dari aset tersebut. Adapun tanggung jawab yang harus diemban pengelola aset adalah :
- Memastikan aset diinventarisasi
- Memastikan aset diklasifikasikan sesuai jenis dan dilindungi
- Mendefinisikan dan secara periodik meninjau batasan akses dan pengklasifikasiannya berdasarkan aturan yang telah diterapkan.</td></tr>
<tr><td>IV.12</td><td>Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi</td><td>1,40</td><td>High</td><td>80</td></tr>
<tr><td colspan="5">Rekomendasi Perbaikan
Control 9.1.1 Access Control Policy</td></tr>
</table>

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
Kebijakan kendali akses harus dibuat dan didokumentasikan serta dilakukan peninjauan berdasarkan kebutuhan bisnis dan kebutuhan pengamanan informasi. Untuk itu pemilik kendali akses harus menentukan aturan akses yang tepat, hak akses dan pembatasan untuk pengguna tertentu terhadap asetnya. Adapun kebijakan akses yang perlu diperhatikan adalah : - Pengamanan dbituhkan untuk aplikasi bisnis - Kebijakan diseminasi dan otorisasi informasi - Konsistensi antara hak akses dan kebijakan pengklasifikasian informasi - Batasan akses data dan layanan - Hak akses manajemen - Pemisahan peran kendali akses - Kebutuhan formal otorisasi - Kebutuhan peninjauan hak akses - Penghilangan hak akses - Pengarsipan rekaman kejadian - Peran dengan akses diizinkan				
IV.15	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	1,40	**High**	81
Rekomendasi Perbaikan **Control 13.2.4 Confidentiality Or Non-disclosure Aggreements** Proses investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi perlu dilakukan untuk melindungi informasi rahsia dengan ketentuan yang legal. Hal ini harus dilakukan identifikasi, peninjauan secara berkala dan didokumentasikan.				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
Adapun hal – hal yang perlu diperhatikan adalah : - Definisi informasi yang dilindungi - Durasi persetujuan, termasuk kasus dimana kerajasiaan yang ingin dilindungi - Aksi yang dibutuhkan ketika persetujuan dibatalkan - Petanggungjawaban dan penandatanganan untuk menghindari penyingkapan informasi - Kepemilikan terhadap informasi - Hak penggunaan informasi - Hak untuk mengaudit dan memantau aktivitas pada informasi rahasia - Proses pelaporan kebocoran informasi				
IV.2	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya ?	1,20	**Medium**	90
Rekomendasi Perbaikan **Control 8.2.1 Classification Of Information** Lembaga penyelenggara elektronik yang menerapkan SNI ISO/IEC 27001 perlu melakukan pengklasifikasian informasi berdasarkan aturan pengklasifikasian informasi untuk mempermudah pemahamanan dalam menjalankan kerangka kerja pengelolaan risiko. Klasifikasi informasi yang dilakukan				

<table>
<tr><th>Kode</th><th>Pertanyaan</th><th>GAP</th><th>Kategori Masalah</th><th>Peringkat Keseluruhan</th></tr>
<tr><td colspan="5">akan menunjukkan tingkat sensitivitas dan kekritisan nilai aset dari organisasi. Berikut merupakan contoh klasifikasi informasi berdasarkan 4 lebel :
- Tidak membahayakan
- Menyebabkan ketidaknyamanan
- Memiliki efek jangka pendek pada tujuan operasional tasktis
- Memiliki dampak yang serius pada perencanaan jangka panjang (strategis)</td></tr>
<tr><td>IV.8</td><td>Tata tertib penggunaan komputer, email, internet dan intranet</td><td>1,20</td><td>Medium</td><td>91</td></tr>
<tr><td colspan="5">Rekomendasi Perbaikan
Control 13.1.1 Network Controls
Penggunaan jaringan harus dikelola dan dikendalikan untuk melindungi informasi yang berada pada sistem dan aplikasi.Penerapan pengamanan dilakukan untuk memastikan keamanan jaringan informasi dan perlindungan terhadap layanan yang terhubung pada akses yang menghindari akses yang tidak diijinkan. Untuk itu adapun hal yang harus diperhatikan untuk menjaga keamanan jaringan adalah :
- Tanggung jawab dan prosedur pengelolaan fasilitas jaringan harus dibuat
- Pemisahan tanggung jawab antara jaringan dan opersional komputer
- Kontrol khusus harus dilakukan terhadap data yang melintas melalui jaringan
- Pencatatan dan pemantauan harus diterapkan untuk mendeteksi tindakan yang berefek pada keamanan informasi
- Sistem dan jaringan harus terautentikasi
- Koneksi sistem ke jaringan harus dibatasi</td></tr>
</table>

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
IV.10	Peraturan pengamanan data pribadi	1,20	**Medium**	92
Rekomendasi Perbaikan **Control 18.1.4 Privacy And Protection Of Personally Identifiable Information** Pengamanan data pribadi harus dipastikan sesuai dengan peraturan dan perundang – undangan yang berlaku. Oraganisasi harus memiliki kebijakan untuk pengamankan informasi pribadi. Kebijakan ini harus dikomunikasikan kepada seluruh orang yang terlibat dalam pemrosesan pengidentifikasian informasi diri.				
IV.13	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	1,20	**Medium**	93
Rekomendasi Perbaikan **Control 8.3.1 Management Of Removable Media** **Control 8.3.2 Disposal Of Media** Lembaga penyelenggara sistem elektronik memerlukan prosedur untuk mengelolaan media penyimpanan data berdasarkan skema yang diadopsi oleh organisasi. Untuk penghasncuran media dilakukan ketika data oada media sudah tidak diperlukan lagi yang tentunya dilakukan dalam prosedur yang telah dibuat organisasi. Adapun hal – hal yang perlu diperhatikan dalam penghancuran atau pembuangan data adalah :				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Media yang berisi data rahasia harus disimpan dan dibuang secara aman - Prosedur diperlukan untuk mengidentifikasi hal memerlukan pembuangan secara aman - Melakukan pengaturan dahulu kemudian dibuang secara aman - Pemilihan pihak ketiga yang tepat untuk pembuangan data - Pembuangan data yang sensitif harus dicatat untuk menjaga jejak audit				
IV.21	Prosedur kajian penggunaan akses (*user access review*) dan langkah pembenahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku.	1,20	**Medium**	94
Rekomendasi Perbaikan **Control 9.2.3 Management Of Privileged Access Rights** Perlu adanya pengkajian prosedur penggunaan hak akses untuk mengendalikan akses dari pihak yang ingin mengakses tanpa memiliki otorisasi. Pengalokasian hak akses harus terbatas dan dikendalikan oleh pihak manajemen yang bertanggung jawab. Adapun langkah dalam melakukan pengendaliannya adalah : - Hak akses pengguna harus tersasosiasi dengan sistem dan proses - Hak akses dialokasikan kepada pengguna yang memenuhi persyaratan aturan divisinya - Proses otorisasi harus dijaga				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Kebutuhan untuk hak akses yang kadaluarsa harus didefinisikan - Kompetensi pengguna hak akses harus ditinjau secara berkala untuk memverifikasi pengguna melakukan tugasnya - Prosedur yang spesifik harus dibuat dan dijaga untuk menghindari penggunaan yang tidak diijinkan				
IV.30	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	1,20	**High**	95

<table>
<tr><th>Kode</th><th>Pertanyaan</th><th>GAP</th><th>Kategori Masalah</th><th>Peringkat Keseluruhan</th></tr>
<tr><td colspan="5">Rekomendasi Perbaikan
Control 11.1.1 Physical Security Perimeter
Ketentuan pengamanan harus didefinikan dan digunakan untuk melindungi area yang memiliki informasi sensitif perusahaan. Adapun panduan yang perlu dilakukan untuk pengamanan fisik adalah :
- Ketentuan pengamanan yang didefinisikan harus sesuai dengan hasil penilaian risiko
- Bangunan harus berada pada area yang tidak sepi, memiliki kontruksi yang kuat, memiliki mekanisme penguncian dan alarm, dan harus terkunci untuk menghindari hal yang tidak diinginkan
- Pengendalian akses lewat front office harus dilakukan, untuk menghindari akses yang tidak diinginkan
- Menerpkan pelindung fisik
- Ketentuan dalam prosedur insiden kebakaran diatru dalam standar internasional.
- Pendeteksi penyusup harus diterapkan berdasarkan standar internasional
- Pengelolaan fasilitas pengelolaan informasi organisasi harus terpisah dengan pengelolaan yang dilakukan pihak ketiga.</td></tr>
<tr><td>IV.4</td><td>Apakah tersedia proses pengelolaan perubahan terhadap sistem (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?</td><td>1,00</td><td>Low</td><td>98</td></tr>
<tr><td colspan="5">Rekomendasi Perbaikan
Control 12.1.2 Change Management</td></tr>
</table>

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
Lembaga penyelenggara sistem elektronik perlu menyediakan suatu proses untuk menangani perubahan yang terjadi di organisasi. Untuk itu perlu adanya kendali yang dilakukan jika perubahan terjadi terhadap organisasi, proses bisnis, dan sistem. Adapun hal yang perlu dilakukan organisasi adalah : - Mengidentifikasi dan merekam setiap perubahan - Melakukan perencanaan dan pengujian terhadap perubahan - Melakukan penilaian dampak yang mungkin terjadi terkait keamanan informasi - Adanya prosedur perstujuan terkait pengajuan perubahan - Verifikasi terhadap kebutuhan keamanan inforamsi yang terpenuhi - Melakukan komunikasi dari perubahan kepada seluruh pihak terkait - Adanya prosedur *fall-back* untuk menangani jika perubahan yang dilakukan gagal. - Adanya ketentuan terkait pengendalian perubahan secara darurat untuk menyelesaikan insiden yang mungkin terjadi.				
IV.5	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	1,00	**Low**	99
Rekomendasi Perbaikan **Control 12.1.1 Documented Operating Procedures** Segala proses mengenai pengelolaan keamanan informasi harus ada dan didokumentasikan untuk memungkinkan bagian organisasi yang bertanggung jawab menjalankan upaya penyelesaian yang sesuai dengan standar organisasi. Proses				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
yang didokumentasikan harus dipersiapkan untuk kegiatan operasional yang sesuai dengan proses pengamanan informasi. Adapun prosedur operasional yang harus dispesifikasikan dalam dokumen adalah : - Penginstalan dan konfigurasi sistem - Pemrosesan dan penanganan informasi baik secara otomatis dan manual - *Backup* - Penjadwalan yang terkait dengan sistem lainnya seperti kapan memulai pekerjaan dan penyelesaiannya - Instruksi penanganan eror dan pembatasan penggunaan sistem - Kontak untuk dukungan dan eskalasi terhadap kegiatan yang tidak terduga - Instruksi terhadap penanganan media - Prosedur *restart* dan *recovery* bila terjadi kegagalan sistem - Pengelolaan jejak audit dan pencatatan informasi sistem Prosedur pengawasan				
IV.7	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi Anda	1,00	**Medium**	100
Rekomendasi Perbaikan **Control 6.1.1 Information Security Roles And Responsibilities** Peran dan tanggungjawab mengenai pengamanan informasi harus didefinisikan dan dialokasikan. Pengalokasiannya harus sesuai dengan kebijakan keamanan informasi. Penanggungjawab untuk melindungi aset individu dan menjaga informasi keamanan secara spesifik harus diidentifikasi. Untuk				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
itu area dimana setiap tanggung jawab individu perlu ditetapkan. Untuk itu, adapun yang harus dilakukan adalah : - Aset dan proses keamanan informasi harus didefinisikan - Entitas yang bertanggungjawab terhadap tiap aset harus ditugaskan dan detil tanggung jawabnya harus dokumentasikan - Otorisasi harus didefinisikan dan didokumentasikan - Pemilihan individu yang diberikan tanggung jawab harus yang berkompeten - Koordinasi dan kekeliruan yang terjadi harus diidentifikasi dan didokumentasikan				
IV.11	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	1,00	**High**	101
Rekomendasi Perbaikan **Control 9.4.1 Information Access Restriction** **Control 9.3.1 Use Of Secret Authentication Information** Lembaga penyelenggara sistem elektronik perlu membatasi akses terhadap informasi pribadi pengguna. Diperlukan otentikasi untuk memastikan bahwa pihak yang mengakses adalah memang benar pihak yang memiliki wewenang penggunaan informasi. Pembatasan hak akses harus dilakukan berdasarkan kebijakan pengendalian akses yang dimiliki				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
organisasi. Berikut merupakan hal yang perlu diperhatikan dalam pembatasan hak akses : - Penyediaan menu untuk mengendalikan akses ke aplikasi - Pengendalian dimana data tertentu hanya bisa diakses oleh pengguna tertentu - Pengendalian hak akses pengguna berdasarkan *read, write, delete* dan *execute* - Pengendalian hak akses terhadap aplikasi - Pembatasan informasi yanng ditampilkan - Pengendalian akses terhadap aplikasi, data aplikasi dan sistem yang sensitif Pengguna juga harus mengikuti penggunaan untuk otentikasi terhadap informasi rahasia, yaitu : - Menjaga informasi otentikasi rahasia - Mengindari perekaman informasi otentikasi rahasia - Mengubah otentikasi rahasia jika diduga ada hal membahayakan - Membuat *password* berdasarkan kualitas *password* yang disarankan - Tidan membagi otentikasi rahasia - Memastikan perlindungan *password* pada proedur *log-on* otomatis - Tidak menggunakan otentikasi yang sama untuk untuk kebutuhan bisnis dan non bisnis.				
IV.25	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi,	1,00	**High**	102

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?			

Rekomendasi Perbaikan
Control 11.1.2 Physical Entry Controls
Control 11.1.3 Securing Offices, Rooms And Facilties
Control 11.1.4 Protecting Against External And Enviromental Threats

Area kerja harus dilindungi dengan kendali yang tepat untuk memastikan hanya orang yang memiliki wewenang yang boleh mengaksesnya. Untuk itu dilakukan beberapa hal sebagai berikut :

- Pencatatan tanggal dan waktu masuk dan keluarnya pengunjung
- Akses ke area yang memiliki informasi penting dibatasi hanya kepada orang yang berwenang dengan kartus akses atau perlindungan pin.
- Buku log fisik dan digital harus dijaga dan ditinjau
- Seluruh karyawan, pihak ketiga dan kontraktor harus menggunakan kartu pengenal yang terlihat untuk memudahkan pengenalan
- Pihak ketiga layanan harus diberikan batasan pada area yang memiliki informasi rahasia.
- Hak akses area harus ditinjau secara berkala

Lembaga penyelenggara sistem elektronik harus membuat aturan untuk melindungi perangkat komputasi instansi jika digunakan di luar lokasi kerja remi. Perlu adanya perlindungan

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
fisik untuk menghadapi bencana alam, serangan atau insieden. Untuk itu perlu didesain model perlindungan yang tepat untuk menghadapi masalah yang mungkin terjadi itu dan menerapkannya dalam proses kerja organisasi.				
IV.26	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	1,00	**High**	103
Rekomendasi Perbaikan **Control 11.1.2 Physical Entry Controls** Area kerja harus dilindungi dengan kendali yang tepat untuk memastikan hanya orang yang memiliki wewenang yang boleh mengaksesnya. Untuk itu dilakukan beberapa hal sebagai berikut : - Pencatatan tanggal dan waktu masuk dan keluarnya pengunjung - Akses ke area yang memiliki informasi penting dibatasi hanya kepada orang yang berwenang dengan kartus akses atau perlindungan pin. - Buku log fisik dan digital harus dijaga dan ditinjau - Seluruh karyawan, pihak ketiga dan kontraktor harus menggunakan kartu pengenal yang terlihat untuk memudahkan pengenalan - Pihak ketiga layanan harus diberikan batasan pada area yang memiliki informasi rahasia. - Hak akses area harus ditinjau secara berkala				
IV.27	Apakah infrastruktur komputasi terlindungi dari dampak	0,80	**High**	108

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?			

Rekomendasi Perbaikan

Control 11.2.1 Equipment Siting And Protection

Setiap infrastruktur komputasi yang dimiliki oleh lembaga penyelenggara sistem elektronik harus ditempatkan dan dilindungi dari ancaman dan bahaya terkait lingkungan serta kemungkinan adanya akses yang tidak diijinkan. Adapun hal – hal yang perlu dilakukan adalah :

- Menempatkan infrastruktur pada area tertentu untuk meminimalkan akses yang tidak diinginkan
- Penanganan terhadap data sensitif harus dilakukan secara hati – hati
- Fasilitas penyimpanan harus diamankan
- Perangkat yang membutuhkan pengamanan khusus harus dipastikan keamanannya
- Kendali terkait risiko fisik dan lingkungan harus diadopsi untuk melindungi dari pencuri, kebakaran, ledakan, asap, kegagalan supali air, debu, getaran, efek kimia, gangguan kelistrikan, gangguan komunikasi, radiasi elektromagnetik dan perusakan
- Pembuatan himbauan makan, minum dan merokok di fasilitas pengelolaan informasi
- Pengawasan terkait kondisi lingkungan terkait suhu dan kelembapan

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Perlindungan terhadap petir pada gedung, saluran listrik dan komunikasi - Penggunaan perlindungan fisik tertentu untuk infrastruktur industri - Perlindungan infrastruktur terkait kebocoran informasi				
IV.14	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya	0,60	**High**	115
Rekomendasi Perbaikan **Control 15.2.1 Monitoring And Review Of Supplier Services** Lembaga penyelenggara sistem elektronik harus secara berkala memantau, meninjau dan mengaudit layanan yang disampaikan oleh pihak eksternal atau pihak ketiga. Dengan bitu akan memastikan persetujuan syarat dan ketentuan keamanan informasi dipatuhi sehingga insiden dan masalah keamanan informasi dikelola dengan baik. Untuk itu diperlukan tindakan : - Pengawasan tingkat kinerja layanan untuk memastikan kepatuhan terhadap persetujuan - Meninjau pelaporan layanan oleh pihak ketiga dan melasanakan rapat rutin - Melaksanakan audit pihak eksternal - Meninjau jejak audit pihak eksternal - Menyelesaikan dan mengelola permasalhan yang diidentifikasi - Memastikan pihak eksternal menjaga keefektifan layanan				
IV.16	Prosedur *back-up* ujicoba pengembalian data (*restore*)	0,60	**Medium**	116

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
Rekomendasi Perbaikan **Control 12.3.1 Information Backup** Backup merupakan hal yang harus dilakukan secara berkala berdasarkan kebijakan *backup* yang telah disetujui. Ketika merancang *backup* beberapa hal yang harus diperhatikan adalaj : - Prosedur penyalinan yang akurat dan lengkap harus dibuat. - Perpanjangan dan frekuensi *backup* berdasarkan kebutuhan bisnis - Lokasi backup harus berada pada daerah yang berbeda dengan daerah utama untuk menghindari masalah yang sama dari daerah utama - Informasi yang diberikan harus tepat berdasarkan standar yang diacu - Media backup harus diuji untuk memastikan dapat digunakan pada keadaan darurat - *Backup* harus dilindungi dengan enkripsi				
IV.28	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?	0,40	**High**	118
Rekomendasi Perbaikan **Control 11.2.2 Supporting Utilities** Lembaga penyelenggara sistem elektronik perlu memasang perlindungan infrastruktur terkait gangguan pasokan listrik dan gangguan lainnya. Untuk itu organisasi harus melakukan :				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Mengkonfirmasi kepada pabrikan infrastruktur terkait spesifikasi dan kebutuhan infrastruktur - Menilai secara berkala kapasitas infrastruktur apakah memenuhi kebutuhan bisnis - Menginspeksi dan menguji secara berkala untuk memastikan infrastruktur berfungsi dengan baik - Waspada untuk mendeteksi malfungsi - Memiliki berbagai informasi mengenai perutean fisik				

6.4.5. Rekomendasi Perbaikan Area Teknologi

Tabel 6.27 merupakan hasil rekomendasi pada poin pertanyaan area teknologi keamanan informasi yang paling menjadi masalah bagi instansi/lembaga penyelenggara sistem elektronik. Pemberian rekomendasi berdasarkan pada kendali dan panduan yang dimiliki oleh SNI ISO/IEC 27001.

Tabel 6 27. Rekomendasi Area Teknologi

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
V.24	Apakah Instansi Anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	7,20	**Medium**	11

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
Rekomendasi Perbaikan **Control 18.2.1 Independent Review Of Information Security** Lembaga penyelenggara sistem elektronik perlu melakukan mekanisme untuk meninjau kebijakan dan prosedur keamanan informasi. Yang ditinjau tidak hanya dokumennya namun dalam penerapannya juga. Peninjauan dilakukan secara indipenden dan terencana dalam jangka waktu tertentu atau jika terjadi perubahan yang signifikan.				
V.11	Apakah Instansi Anda mempunyai standar dalam menggunakan enkripsi?	3,60	**Medium**	29
Rekomendasi Perbaikan **Control 10.1.1 Policy On The Use Of Cryptographic Controls** Lembaga penyelenggara elektronik harus memiliki kebijakan yang mengatur penggunaan enkripsi untuk perlindungan informasi. Jika belum ada maka harus dibuat dan diimplementasikan terkait pentingnya enkripsi bagi keamanan data organisasi. Hal – hal yang harus diperhatikan dalam pembuatan kebijakan enkripsi adalah : - Perlu adanya pendekatan oleh pihak manajemen untuk penggunaan enkripsi lintas organisasi - Berdasarkan penilaian risiko, pengamanan berdasarkan tipe, kekuatan dan kualitas algoritma enkripsi - Penggunaan enkripsi pada seluruh jalur komunikasi data - Peran dan tanggung jawab - Penerapan standar enkripsi				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Dampak penggunaan enkripsi bergantung pada konten				
V.12	Apakah Instansi Anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?	3,20	**Medium**	32

Rekomendasi Perbaikan

Control 10.1.2 Key Management

Lembaga elektronik yang menerapkan perlindungan enkripsi harus melaksanakan pengelolaan penggunaan kunci enkripsi dan siklus penggunaanya. Untuk itu diperlukan pembuatan dan penerapan kebijakan untuk perlindungan siklus penggunaan kunci enkripsi. Kunci enkripssi perlu perlindungan selama proses pembuatan, penyimpanan, pengarsipan, pengambilan, pendistribusian, penghentian penggunaan dan penghancuran. Untuk itu diperlukan perlindungan yang melindungi dari modifikasi, pencurian dan akses yang tidak diijinkan. Adapun hal – hal yang perlu diperhatikan dalam pengelolaan kunci enkripsi adalah :

- Pembuatan kunci untuk yang berbda untuk setiap aplikasi dan sistem
- Menerbitkan dan memperloleh sertifikast kunci publik
- Pendistribusian kunci
- Penyimpanan kunci
- Aturan perubahan dan pembaruan kunci
- Pengurusan dengan *compromised keys*
- Pencabutan kunci dan bagaimana menonaktifkannya

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Pemulihan kunci yang hirang dan rusak - Pembuatan cadangan dan pengarsipan kunci - Penghancuran - Pencatatan dan dan pengauditan aktivitas pengelolaan kunci				
V.13	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	3,20	**Medium**	33
Rekomendasi Perbaikan **Control 9.4.3 Password Management System** Pengelolaan *password* harus interaktif dan memastikan kualitas dari *password* sesuai dengan standar yang diterapkan. Untuk itu sistem pengelolaan *password* harus : - Memaksakan penggunaan *ID* dan *password* untuk menjaga akuntabilitas - Mengijinkan pengguna untuk memilih dan mengubah *password* nya.				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Memaksakan penggunaan *password* yang berkualitas - Menyarankan pengguna untuk mengganti *password* saat pertma kali *log-on* - Melaksanakan perubahan *password* secara berkala - Menjaga rekaman *password* lama untuk menghindari penggunaan ulang - Tidak menampilkan *password* pada layar ketika dimasukkan - Menyimpan *password* secara terpisah dengan sistem data aplikasi - Menyimpan *password* dalam bentuk perlindungan				
V.14	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	3,20	**Medium**	34
Rekomendasi Perbaikan **Control 9.4.2 Secure Log-on Procedures** Untuk menggunakan sistem aplikasi diperlukan bentuk pengamanan untuk memastikan bahwa yang mengakses adalah orang yang memiliki wewenang. Untuk itu diperlukan kebijakan yang memastikan akses kepada sistem aplikasi dilakukan berdasarkan prosedur ottentikasi yang tepat sehingga dapat dipastikan bahwa orang yang mengakses adalah orang yang memiliki wewnang. Otentikasi disini bisa berupa *password*, enkripsi, *smart cards*, *token* maupun dengan *biometric*. Berikut merupakan prosedur *log-on* yang baik : - Tidak menampilkan informasi sampai *log-on* berhasil				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Memberikan peringatan pada komputer, bahwa hanya yang otorisasi yang boleh menggunakan - Tidak menyediakan pesan bantuan - Validasi *log-on* jika data yang dimasukkan benar - Adanya perlindungan terhadap percobaan *brute force* - Mencatat percobaan gagal dan berhasil - Meningkatkan keamanan jika terdeteksi pelanggaran akses - Menampilkan tanggal dan waktu *log-on* yang berhasil dan *log-on* yang tidak berhasil - Tidak menampilkan *password* yang dimasukkan - Tidak mengirimkan *password* lewat jaringan - Menghentikan sesi yang tidak aktif - Membatasi waktu koneksi				
V.20	Apakah ada rekaman dan hasil analisa (jejak audit – *audit trail*) yang mengkonfirmasi bahwa antivirus telah dimutakhirkan secara rutin dan sistematis?	2,40	**High**	43
Rekomendasi Perbaikan **Control 12.2.1 Controls Against Malware** Lembaga penyelenggara sistem elektronik harus melakukan pencatatan pendeteksian *malware* dan melakukan pemutahiran secara rutin terhadap antivirus. Dengan begitu antivirus dapat melakukan fungsinya untuk mendeteksi, mencegah dan				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
memulihkan keamanan informasi dalam melawan serangan *malware*.				
V.21	Apakah adanya laporan penyerangan virus yang gagal/sukses ditindaklanjuti dan diselesaikan?	2,40	**High**	44
Rekomendasi Perbaikan **Control 12.4.1 Event Logging** Lembaga penyelenggara sistem elektronik perlu membuat daftar rekaman pelaksanaan keamanan informasi. Hal ini dikarenakan perekaman akan merekam aktivitas dari pengguna, kesalahan dan kegiatan pengamanan informasi. Rekaman tersebut harus selalu dibuat dan disimpan serta secara berkala ditinjau ulang. Untuk jenis informasi yang direkam bisa berupa : - *ID* Pengguna - Aktivitas sistem - Tanggal, waktu dan detail kejadian *log-on* dan *log-off* - Identitas perangkat - Rekaman sukses dan gagalnya percobaan akses sistem - Perubahan konfigurasi - Hak akses - Alamat jaringan				
V.23	Apakah setiap aplikasi yang ada memiliki spesifikasi keamanan yang diverifikasi/validasi pada saat	2,40	**Medium**	45

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	pengembangan dan uji-coba?			
Rekomendasi Perbaikan **Control 14.2.8 System Security Testing** **Control 14.2.9 System Acceptance Testing** Setiap aplikasi yang dimiliki oleh lembaga penyelenggara sistem elektronik harus memiliki spesifikasi keamanan tertentu. Untuk itu selamq proses pengembangan maka perlu adanya pengujian dan verifikasi keamanan fungsionalitsanya. Pengujian disini harus dilakukan oleh tim pengembang untuk memastikan aplikasi bisa diterima sesuai dengan kriteria yang direncanakan untuk aplikasi yang dibuat maupun diperbarui.				
V.15	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?	2,00	**Medium**	52

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
Rekomendasi Perbaikan **Control 9.2.3 Management Of Privileged Access Rights** Perlu adanya pengkajian prosedur penggunaan hak akses untuk mengendalikan akses dari pihak yang ingin mengakses tanpa memiliki otorisasi. Pengalokasian hak akses harus terbatas dan dikendalikan oleh pihak manajemen yang bertanggung jawab. Adapun langkah dalam melakukan pengendaliannya adalah : - Hak akses pengguna harus tersasosiasi dengan sistem dan proses - Hak akses dialokasikan kepada pengguna yang memenuhi persyaratan aturan divisinya - Proses otorisasi harus dijaga - Kebutuhan untuk hak akses yang kadaluarsa harus didefinisikan - Kompetensi pengguna hak akses harus ditinjau secara berkala untuk memverifikasi pengguna melakukan tugasnya Prosedur yang spesifik harus dibuat dan dijaga untuk menghindari penggunaan yang tidak diijinkan				
V.22	Apakah keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?	2,00	**Low**	53

<table>
<tr><th>Kode</th><th>Pertanyaan</th><th>GAP</th><th>Kategori Masalah</th><th>Peringkat Keseluruhan</th></tr>
<tr><td colspan="5">Rekomendasi Perbaikan
Control 12.4.4 Clock Synchronisation
Lembaga penyelenggara sistem elektronik harus melakukan sinkronisasi waktu sesuai dengan standar untuk keseluruhan sistem dari organisasi. Penyesuaian untuk waktu harus didokumentasikan kebutuhannya baik itu internal maupun eksternal. Untuk itu organisasi perlu mendefinisikan standar yang digunakan serta mendokumentasikannya.</td></tr>
<tr><td>V.4</td><td>Apakah Instansi Anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?</td><td>1,40</td><td>Medium</td><td>82</td></tr>
<tr><td colspan="5">Rekomendasi Perbaikan
Control 18.2.2 Compliance With Security Policies And Standards
Lembaga penyelenggara elektronik perlu menganalisa kepatuhan terhadap standar dan kebijakan yang mereka terapkan secara berkala. Tugas ini erlu dilakukan oleh manajer. Manajer harus melakukan peninjauan terhadap setiap proses pengamanan informasi apakah sudah sesuai dengan prosedur dan standar. Jika manajer menemukan ketidakpatuhan maka manajer perlu melakukan :
- Mengidentifikasi penyebab dari ketidakpatuhan
- Mengevaluasi aksi yang diperlukan untuk mencapai kepatuhan
- Menerapkkan aksi yang tepat terhadap ketidakpatuhan</td></tr>
</table>

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Meninjau keefektifan aksi perbaikan dan mengidentifikasi kelemahannya				
V.8	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	1,40	**Medium**	83
Rekomendasi Perbaikan **Control 12.4.1 Event Logging** Lembaga penyelenggara sistem elektronik perlu membuat daftar rekaman pelaksanaan keamanan informasi. Hal ini dikarenakan perekaman akan merekam aktivitas dari pengguna, kesalahan dan kegiatan pengamanan informasi. Rekaman tersebut harus selalu dibuat dan disimpan serta secara berkala ditinjau ulang. Untuk jenis informasi yang direkam bisa berupa : - *ID* Pengguna - Aktivitas sistem - Tanggal, waktu dan detail kejadian *log-on* dan *log-off* - Identitas perangkat - Rekaman sukses dan gagalnya percobaan akses sistem - Perubahan konfigurasi - Hak akses - Alamat jaringan				
V.9	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan	1,40	**Medium**	84

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	jejak audit dan forensik)?			
Rekomendasi Perbaikan **Control 12.4.1 Event Logging** Lembaga penyelenggara sistem elektronik perlu membuat daftar rekaman pelaksanaan keamanan informasi. Hal ini dikarenakan perekaman akan merekam aktivitas dari pengguna, kesalahan dan kegiatan pengamanan informasi. Rekaman tersebut harus selalu dibuat dan disimpan serta secara berkala ditinjau ulang. Untuk jenis informasi yang direkam bisa berupa : - *ID* Pengguna - Aktivitas sistem - Tanggal, waktu dan detail kejadian *log-on* dan *log-off* - Identitas perangkat - Rekaman sukses dan gagalnya percobaan akses sistem - Perubahan konfigurasi - Hak akses - Alamat jaringan				
V.17	Apakah Instansi Anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?	1,40	**High**	85
Rekomendasi Perbaikan **Control 9.2.6 Removal Of Adjustment Of Access Rights** Lembaga pengyelenggara sistem elektronik harus melakukan pengamanan untuk melindungi akses dari luar organisasi. Hak				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
akses untuk karyawan maupun pihak ketiga harus dihilangkan bila karyawan sudah berhenti atau kontrak dan persetujuan dengan pihak ketiga telah dihentikan.				
V.5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	1,20	**Medium**	96
Rekomendasi Perbaikan **Control 14.1.2 Securing Application Services On Public Networks** Jaringan dan sistem aplikasi harus secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah keamanan. Hal ini sangat penting karena dalam jaringan data akan melintas antar jaringan sehingga jika ada kelemahan bisa menimbulkan kerentanan yang berakibat pada pencurian sampai kehilangan data. Berikut hal yang perlu diperhatikan dalam menagamankan jaringan dan sistem aplikasi : - Perlunya kepercayaan yang tinggi lewat otentikasi - Proses otorisasi untuk transaksi dokumen - Perlindungan diperlukan untuk informasi rahasia				
V.16	Apakah Instansi Anda menerapkan pengamanan untuk mendeteksi dan	1,20	**High**	97

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?			

Rekomendasi Perbaikan
Control 13.1.1 Network Controls
Penggunaan jaringan harus dikelola dan dikendalikan untuk mendeteksi dan mencegah kebocoran inforamsi yang berada pada sistem dan aplikasi.Penerapan pengamanan dilakukan untuk memastikan keamanan jaringan informasi dan perlindungan terhadap layanan yang terhubung pada akses yang menghindari akses yang tidak diijinkan. Untuk itu adapun hal yang harus diperhatikan untuk menjaga keamanan jaringan adalah :

- Tanggung jawab dan prosedur pengelolaan fasilitas jaringan harus dibuat
- Pemisahan tanggung jawab antara jaringan dan opersional komputer
- Kontrol khusus harus dilakukan terhadap data yang melintas melalui jaringan
- Pencatatan dan pemantauan harus diterapkan untuk mendeteksi tindakan yang berefek pada keamanan informasi
- Sistem dan jaringan harus terautentikasi
- Koneksi sistem ke jaringan harus dibatasi

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
V.3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan, yang dimutakhirkan sesuai perkembangan dan kebutuhan?	1,00	**Medium**	104

Rekomendasi Perbaikan

Control 5.1.1 Policies For Information Security

Control 5.1.2 Review Of The Policies For Information Security

Harus ada sekumpulan kebijakan untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan yang disesuaikan dengan kebutuhan organisasi dan disetujui oleh pihaka manajemen dan diterbitkan serta dikomunikasikan kepada karyawan dan pihak ketiga. Kebijakan keamanan informasi harus memenuhi kriteria berdasarkan :

- Strategi bisnis
- Aturan, undang – undang dan kontrak
- Lingkungan yang mengancam keamanan informasi

Untuk itu kebijakan informasi harus berisi tentang :

- Pengertian keamanan informasi, tujuan dan prinsip untuk memandu seluruh aktivitas yang berhubungan dengan keamanan informasi
- Pernyataan mengenaitanggungjawab secara umum danspesifik untuk pengelolaan keamanan informasi untuk mendefinisikan peran
- Proses untuk menangani penyimpangan dan pengecualian.

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
Kebijakan dan prosedur penagamanan informasi harus ditinjau pada interval tertentu atau berdasarkan perubahan yang dilakukan untuk memastikan keberlangsungan kesesuaiannya, ketepatannya dan keefektifannya. Setiap kebijakan dan prosedur harus memiliki penanggung jawab yang mengembangkan, meninjau dan mengevaluasinya. Dengan begitu dapat menghasilkan pengembangan dari kebijakan organisasi yang menjaga keamanan informasi yang merespon pada perubahan lingkungan organisasi, lingkungan bisnis serta aturan hukum dan perundanga – undangan yang berlaku.				
V.10	Apakah Instansi Anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?	1,00	**Medium**	105
Rekomendasi Perbaikan **Control 10.1.1 Policy On The Use Of Cryptographic Controls** Lembaga penyelenggara elektronik harus memiliki kebijakan yang mengatur penggunaan enkripsi untuk perlindungan informasi. Jika belum ada maka harus dibuat dan diimplementasikan terkait pentingnya enkripsi bagi keamanan data organisasi. Hal – hal yang harus diperhatikan dalam pembuatan kebijakan enkripsi adalah :				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Perlu adanya pendekatan oleh pihak manajemen untuk penggunaan enkripsi lintas organisasi - Berdasarkan penilaian risiko, pengamanan berdasarkan tipe, kekuatan dan kualitas algoritma enkripsi - Penggunaan enkripsi pada seluruh jalur komunikasi data - Peran dan tanggung jawab - Penerapan standar enkripsi - Dampak penggunaan enkripsi bergantung pada konten				
V.1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	0,80	**High**	109
Rekomendasi Perbaikan **Control 13.1.1 Network Controls** Layanan TIK yang menggunakan internet harus dilindungi dengan perlindungan berlapis untuk menjaga keamanan data dari pihak yang tidak memiliki otentikasi. Penggunaan jaringan harus dikelola dan dikendalikan untuk melindungi informasi yang berada pada sistem dan aplikasi.Penerapan pengamanan dilakukan untuk memastikan keamanan jaringan informasi dan perlindungan terhadap layanan yang terhubung pada akses yang menghindari akses yang tidak diijinkan. Untuk itu adapun hal yang harus diperhatikan untuk menjaga keamanan jaringan adalah : - Tanggung jawab dan prosedur pengelolaan fasilitas jaringan harus dibuat - Pemisahan tanggung jawab antara jaringan dan opersional komputer				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Kontrol khusus harus dilakukan terhadap data yang melintas melalui jaringan - Pencatatan dan pemantauan harus diterapkan untuk mendeteksi tindakan yang berefek pada keamanan informasi - Sistem dan jaringan harus terautentikasi - Koneksi sistem ke jaringan harus dibatasi				
V.2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	0,80	**Medium**	110
Rekomendasi Perbaikan **Control 13.1.3 Seregation In Network** Lembaga penyelenggara sistem elektronik perlu melakukan pemisahan jaringan komunikasi berdasarkan kepentingan yang ada dalam organisasi, baik itu berdasarkan layanan informasi, pengguna dan sistem informasi. Pemisahan bisa dengan pembagian domain jaringan berdasarkan tingkat kerpercayaan, berdasarkan unit dalam organisasi maupun berdasarkan jaringan fisik. Pengamanan juga perlu diterapkan untuk setiap jaringan bisa dengan *firewall* dan f*iltering*.				
V.6	Apakah keseluruhan infrastruktur dimonitor untuk	0,80	**Medium**	111

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
	memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?			
Rekomendasi Perbaikan **Control 12.1.3 Capacity Management** Penggunaan sunber daya harus diawasi, disesuaikan, dan diproyeksikan untuk dapat memenuhi kebutuhan dimasa yang akan datang, hal ini dilakukan untuk memastikan memastikan keberlangsungan kinerja sistem. Penyediaan kapasitas yang cukup bisa dilakukan dengan meningkatkan kapasitas maupun menguranginya. Berikut merupakan contoh pengelolaan kapasitas sumber daya : - Penghapusan data yang usang - Penghentian aplikasi, sistem dan basis data - Meningkatkan pemrosesan dan penjadwalan - Menigkatkan logika basis data (*queries*) - Menolak atau membatasi *bandwidth* terhadap sumber daya jika tidak kritikal terhadap bisnis				
V.7	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	0,80	**Medium**	112
Rekomendasi Perbaikan **Control 12.4.1 Event Logging** Lembaga penyelenggara sistem elektronik perlu membuat daftar rekaman pelaksanaan keamanan informasi. Hal ini dikarenakan perekaman akan merekam aktivitas dari pengguna, kesalahan dan kegiatan pengamanan informasi. Rekaman tersebut harus				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
selalu dibuat dan disimpan serta secara berkala ditinjau ulang. Untuk jenis informasi yang direkam bisa berupa : - *ID* Pengguna - Aktivitas sistem - Tanggal, waktu dan detail kejadian *log-on* dan *log-off* - Identitas perangkat - Rekaman sukses dan gagalnya percobaan akses sistem - Perubahan konfigurasi - Hak akses - Alamat jaringan				
V.18	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	0,80	**Medium**	113
Rekomendasi Perbaikan **Control 12.5.1 Control Of Operastional Software** Lembaga penyelenggara sistem elektronik perlu menerapkan prosedur untuk mengendalikan proses instalasi perangkat lunak dan sistem operasi. Adapun hal yang perlu diperhatikan adalah : - Pembaruan perangkat lunak harus dilakukan oleh admin yang terlatih dan memiliki otorisasi - Sistem operasional harus menggunakan kode yang dapat dieksekusi saja - Aplikasi dan sistem operasi yang diterapkan harus melalui pengujian yang berhasil				

Kode	Pertanyaan	GAP	Kategori Masalah	Peringkat Keseluruhan
- Sistem kontrol kendali (dokumentasi) harus digunakan untuk mengendalikan perangkat lunak yang telah diterapkan - Strategi *rollback* harus ada sebelum perubahan diterapkan - Pencatatan audit harus disimpan - Versi lawas dari aplikasi harus dipertahankan sebagai tindakan kontingensi - Versi lawas dari perangkat lunak harus diarsipkan dengan seluruh informasi, parameter, prosedur dan konfigurtasi.				
V.19	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	0,20	**High**	119
Rekomendasi Perbaikan **Control 12.2.1 Controls Against Malware** Lembaga penyelenggara sistem elektronik harus melakukan pencatatan pendeteksian *malware* dan melakukan pemutahiran secara rutin terhadap antivirus. Dengan begitu antivirus dapat melakukan fungsinya untuk mendeteksi, mencegah dan memulihkan keamanan informasi dalam melawan serangan *malware*.				

BAB VII
KESIMPULAN DAN SARAN

Pada bab in akan menjelaskan kesimpulan dari penelitian, beserta saran yang dapat bermanfaat untuk perbaikan di penelitian selanjutnya

7.1. Kesimpulan

Berdasarkan rumusan masalah yang telah dibuat sebelumnya dan hasil penelitian yang telah dilakukan dengan menggunakan beberapa hasil penilaian terhadap penyelenggara sistem elektronik maka dapat diperoleh kesimpulan akhir sebagai berikut :

- Hasil dari analisis kesenjangan pada penilaian penyelenggara sistem elektronik pada tingkat kematangan reaktif menunjukkan bahwa ada 11 poin pertanyaan tertinggi yang memiliki kesenjangan diatas 7. Adapun poin pertanyaannya secara berurutan adalah III.15, III.13, III.14, II.14, II.15, III.16, III.25, III.26, I.18, III.24 dan V.24 yang membahas mengenai pengelolaan *disaster recovery plan*, program kerja, pengevaluasian dan pengujian terkait keamanan informasi. Sebagian besar kesenjangan tertinggi berada pada area III atau area kerangka kerja yang mengisyaratkan bahwa instansi/lembaga penyelenggara elektronik memiliki masalah besar dalam proses pengelolaan proses pengamanan informasinya terkait evaluasi kepatuhan pada kerangka kerja yang digunakan.
- Kesenjangan tiap area berbeda – beda. Pada area tata kelola memiliki kesenjangan tertinggi dengan nilai 7,20 pada poin I.18, area risiko memiliki kesenjangan tertinggi dengan nilai 7,80 pada poin II.14 dan II.15, area kerangka kerja memiliki kesenjangan tertinggi pada nilai 9,00 pada

poin III.15, area pengelolaan aset memiliki kesenjangan tertinggi pada nilai 4,80 pada poin IV.24 dan area teknologi memiliki kesenjangan tertinggi pada nilai 7,20 pada poin V.24

- Area Indeks KAMI yang paling besar menjadi masalah bagi penyelenggara sistem elekttronik adalah kerangka kerja dengan rata – rata kesenjangan 3,86, diikuti area risiko dengan 3,28, kemudian area tata kelola dengan 3,13, diikuti area teknologi dengan 1,91 dan terakhir area pengelolaan aset dengan 1,72.
- Hasil dari analisis temuan berdasarkan dampak dan probabilitas bila poin pertanyaan tidak dilakukan menunjukkan dari 119 poin pertanyaan ada 33 poin pertanyaan yang memiliki kategori masalah *high*, 77 poin pertanyaan berkategori *medium* dan 9 poin pertanyaan berada pada kategori *low* jika tidak diterapkan. Dari 33 poin pertanyaan yang berkategori *high* ada 1 dari area tata kelola, 3 dari area risiko, 7 dari area kerangka kerja, 16 dari pengelolaan aset dan 6 dari area teknologi. Area pengelolaan terkait dengan aset penting organisasi. Aset penting tersebut memiliki nilai finansial bagi organisasi yang jika terganggu akan memberikan dampak besar bagi organisasi. Hal ini berarti poin pertanyaan dengan kesenjangan tinggi belum tentu memiliki dampak masalah besar jika tidak diterapkan.

7.2. Saran

Berdasarkan hasil dari penelitian ini adapun saran yang diberikan adalah :

- Pada penelitian ini, penggunaan penelitian yang menilai keamanan informasi dengan Indeks KAMI berjumlah lima dan terdiri dari penyelenggara sistem elektronik dengan tingkat kematangan reaktif. Selanjutnya, sebaiknya diperhatikan mengenai penyelenggara sistem elektronik yang bergerak di bidang yang sama dengan jumlah yang lebih banyak untuk memberikan penyelesaian yang lebih

khusus pada bidang tertentu. Kemudian untuk pengambilan data sebaiknya menggunakan beberapa metode lain untuk memungkinkan temuan lain yang tidak didapatkan dari metode yang digunakan.

- Bagi instnasi/lembaga penyelenggara sistem elektronik untuk mengikuti bimbingan teknis dari pihak kominfo jika ingin melakukan penilaian dengan Indeks KAMI agar memahami proses penilaian yang tepat serta melakukan evaluasi secara rutin terhadap kerangka kerja keamanan informasinya dan penerapannya untuk mengetahui kondisi penerapan keamanan informasinya berdasarkan SNI ISO/IEC 27001.

“Halaman ini sengaja dikosongkan”

DAFTAR PUSTAKA

[1] P. D. D. S. Informatika, "HASIL SURVEI PENGGUNAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI (TIK) DI SEKTOR BISNIS INDONESIA 2011," 2011.

[2] "INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Overview and vocabulary," vol. 2016, 2016.

[3] Kementerian Komunikasi dan Informatika RI, "Indeks KAMI Versi 2.3." 2012.

[4] Direktorat Keamanan Informasi dan Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informasi, "Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik," 2011.

[5] Dimas Prayogo, Evaluasi Kinerja Aplikasi Indeks Pengajaran Dosen dengan Menggunakan Gap Analisis, Surabaya : Sistem Informasi ITS, 2013.

[6] Firzah Abdullah, Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 Pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya, Surabaya : Sistem Informasi ITS, 2017.

[7] Rizki Fadhil, Analisa Kesenjangan dan Dampak Perubahan Proses Bisnis Finansial Accounting Berdasarkan Best Practice SAP (Studi Kasus : PT. Perkebunan Nusantara XI), Surabaya : Sistem Informasi ITS. 2017.

[8] Ridho, Moch. Rashid, 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 : Sistem informasi ITS, 2012.

[9] Luthfiya Ulinnuha, Evaluasi pengelolaan keamanan jaringan di ITS dengan menggunakan Standar Indeks, Surabaya : Sistem informasi ITS, 2013

[10] Roodhin Firmana, Penggunaan indeks keamanan informasi (KAMI) sebagai evaluasi keamanan informasi pada PT. PLN Distribusi Jawa Timur, Surabaya : Sistem informasi ITS, 2013

[11] Endi Lastyono Putra, Evaluasi keamanan informasi pada divisi network of broadband PT.Telekomunikasi Indonesia. Tbk dengan menggunakan Indeks Keamanan Informasi (KAMI), Surabaya : Sistem informasi ITS, 2014

[12] Mustaqim Siga, Evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi (KAMI) pada kantor wilayah Ditjen Perbendaharaan Negara Jawa Timur, Surabaya : Sistem informasi ITS, 2014

[13] Kasiran, Asrani, Analisa tingkat keamanan informasi pada sistem informasi administrasi kependudukan (SIAK) di Dinas Kependudukan dan Pencatatan Sipil Kabupaten Bantaeng menggunakan ideks KAMI, Surabaya : Teknik Elekktro ITS, 2014

[14] Diah Restu, Evaluasi Keamanan Informasi Pada PTI PDAM Tirta Moedal Kota Semarang Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001: 2009, Semarang : Sistem Informasi Udinus, 2015.

[15] Radhifan Hidayat, Evaluasi keamanan informasi menggunakan metode indeks keamanan informasi (KAMI) (Studi kasus: STIE Perbanas Surabaya), Surabaya : Sistem informasi ITS, 2016.

[16] Winda Septilia, Evaluasi tingkat kelengkapan dan kematangan sistem keamanan informasi berdasarkan indeks KAMI pada Divisi Sampling dan Pengujian BBPOM Kota Semarang, Semarang : Sistem informasi Udinus, 2016.

[17] Dedi Wirasasmita, Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan SNI ISO/IEC 27001:2009 Studi Kasus: Pengamanan Informasi Pada Institusi Perguruan Tinggi Sekolah Tinggi Teknologi Duta Bangsa Bekasi, Bekasi : Teknik Informatika Sekolah Tinggi Teknologi Duta Bangsa, 2017.

[18] Indrajit. R.E, Manajamen Sistem Informasi dan Teknologi Informasi, 2007

[19] F. Sattarova, K. Tao-hoon, "IT Security Review: Privacy, Protection, Access Control, Assurance and System Security," International Journal of Multimedia and Ubiquitous Engineering, vol.2, No.2, hal 3, April, 2007

[20] "ISO/IEC 27001- Information Security Management," ISO , 2013. [Online]. Available: http://www.iso.org/iso/home/standards/managemen t-standards/iso27001.htm. [Diakses 20 02 2018].

[21] Federica Calidoni-Lundberg , "Evaluation: definitions, methods and models ," ITPS, Swedish Institute For

Growth Policy Studies , Sweden., R2006:002 , pp. 7-39.

[22] R. Sarno, Sistem Manajemen Keamanan Informasi. Surabaya : ITS Press, 2009.

[23] Whitman, Michael E. and Mattord, Herbert J., "Principles of Information Security", 5th Edition.United State of America : Cengage Learning, 2015.

[24] Pompon, Raymond., "IT Security Risk Control Management - An Audit Preparation Plan", 1st Edition.United State of America : Apress, 2016.

[25] Internasional Organization for Standardization ISO, “Information technology - Security techniques - Information security management systems - Reuirements,” Iso 270012005, vol. 2005, 2005.

[26] Internasional Organization for Standardization ISO, “Information technology - Security techniques - Information security management systems - Reuirements,” Iso 270012013, vol. 2013, 2013.

[27] " ISO 27001 adalah Ikon Standarisasi Manajemen Keamanan Informasi, ", 2017. [Online]. Available : https://itgid.org/iso-27001-adalah/ [Diakses 20 02 2018]

[28] Badan Standarisasi Nasional, SNI ISO/IEC 27001 : 2009, Teknologi informasi - Teknik keamanan - Sistem manajemen keamanan informasi - persyaratan (ISO/IEC 27001:2005).

[29] PERMENKOMINFO NO. 4 TAHUN 2016, BN. No. (551), LL KEMKOMINFO : 18 HLM.

[30] Direktorat Keamanan Informasi dan Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informasi, “Panduan Penerapan Sistem Manajemen

Keamanan Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI),” 2017.

[31] Y. Muchsam, Falahah, G. Irianto, "Penerapan Gap Analysis Pada Pengembangan Sistem Pendukung Keputusan Penilaian Kinerja Karyawan (Studi Kasus PT.XYZ)", Seminar Nasional Aplikasi Teknologi Informasi 2011 (SNATI 2011), hal 94-100 , 17-18 Juni, 2011.

[32] A. Parasuraman, V.A. Zeithaml, L.L. Berry, “A Conceptual Model of Service Quality and Its Implications for Future Research,” The Journal of Marketing, vol. 49, No. 4, pp. 41-50, 1985.

[33] J. Murray, "A Gap Analysis Process To Improve IT Management," 2000.

[34] Indrajit. R.E, "Teknik Analisa Gap Pengembangan Teknologi Informasi, " Renaissance Research Center, 1999.

[35] J. Creswell, “Qualitative Inquiry and Research Design: Choosing Among Five Approaches (2nd ed),” Thousand Oaks, Sage, 2007, pp. 35-41.

[36] C. Schell, “The Value of the Case Study as a Research Strategy,” 1992.

[37] Husein, Gilang M. dan Imbar, Radiant Victor, “Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada Document Management System di PT. Jabar Telematika (JATEL)”, e-ISSN: 2443-2229. vol.1, no. 2, Agustus. 2015.

[38] Creswell, John.W, RESEARCH DESIGN Qualitative,

Quantitative, and Mixed Methods Approaches, 3rd ed. United States of America : SAGE Publications, 2009.

[39] Pandey. Satyendra C, Patnaik Srilata, "ESTABLISHING RELIABILITY AND VALIDITY IN QUALITATIVE INQUIRY: A CRITICAL EXAMINATION," Jharkhand Journal of Development and Management Studies XISS, Ranchi, Vol. 12, No.1, March 2014, pp. 5743-5753.

BIODATA PENULIS

ARYMASU GODHEIN NDOEN, lahir 19 Januari 1996 di kota Singaraja. Penulis merupakan anak kelima dari enam bersaudara. Penulis pernah menempuh pendidikan formal di SDN 3 Banjar Tegal, SMPN 1 Singaraja, SMAN 1 Singaraja, dan akhirnya masuk menjadi mahasiswa program sarjana Departemen Sistem Informasi Institut Teknologi Sepuluh Nopember (ITS) angkatan 2014 dan terdaftar dengan NRP 052 1144 0000 015. Pada akhir masa perkuliahan di Departemen Sistem Informasi ITS, penulis memilih untuk mengerjakan tugas akhirdi Laboratorium Manajemen Sistem Informasi (MSI). Penulis mengambil topik mengenai evaluasi keamanan informasi dibawah bimbingan Ir. Khakim Ghozali, M.MT. Selama menjadi mahasiswa di Departemen Sistem Informasi, penulis aktif dalam orgaisasi departemen yaitu HMSI dan pernah menjabat sebagai sekretaris departemen kesejahteraan mahasiswa. Pada tahun 2016 pernah menjadi finalis GEMASTIK 9 pada kategori lomba Design UX. Penulis juga aktif dalam berbagai kegiatan kepanitiaan yang ada di kampus. Salah satunya pernah menjadi staf keamanan perijinan dan staf ahli konsumsi pada acara ISE 2015 dan ISE 2016. Untuk kepentingan penelitian penulis dapat dihubungi melalui e-mail arymasundoen@gmail.com.

“Halaman ini sengaja dikosongkan”

LAMPIRAN A

Nilai Peran TIK 10 Penelitian

A-1 Nilai Peran TIK Penelitian 1

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi			
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.			
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis		**Status**	Skor
#	**Karakteristik Instansi**		
1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Kritis	4
1	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Kritis	4
1	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas	Kritis	4
1	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Kritis	4
2	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Kritis	4
2	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Kritis	4
2	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi	Kritis	4
2	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Kritis	4
2	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Kritis	4
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Kritis	4
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Kritis	4
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Kritis	4
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	**48**	

A-2 Nilai Peran TIK Penelitian 2

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi			
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.			
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis		**Status**	Skor
#	**Karakteristik Instansi**		
1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Sedang	2
1	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Kritis	4
1	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas	Sedang	2
1	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Sedang	2
2	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Tinggi	3
2	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Sedang	2
2	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi	Sedang	2
2	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Tinggi	3
2	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Tinggi	3
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Sedang	2
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Rendah	1
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Tinggi	3
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	**29**	

A-3 Nilai Peran TIK Penelitian 3

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi			
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.			
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis		**Status**	Skor
#	**Karakteristik Instansi**		
1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Kritis	4
1	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Tinggi	3
1	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas	Kritis	4
1	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Tinggi	3
2	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Kritis	4
2	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Kritis	4
2	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi	Tinggi	3
2	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Tinggi	3
2	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Tinggi	3
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Tinggi	3
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Tinggi	3
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Tinggi	3
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	**40**	

A-4 Nilai Peran TIK Penelitian 4

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi			
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.			
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis		**Status**	Skor
#	**Karakteristik Instansi**		
1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Kritis	4
1	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Kritis	4
1	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas	Kritis	4
1	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Tinggi	3
2	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Kritis	4
2	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Kritis	4
2	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi	Kritis	4
2	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Kritis	4
2	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Kritis	4
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Kritis	4
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Rendah	1
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Kritis	4
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	**44**	

A-5 Nilai Peran TIK Penelitian 5

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi			
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.			
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis		**Status**	Skor
#	**Karakteristik Instansi**		
1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Minim	0
1	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Rendah	1
1	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas	Tinggi	3
1	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Tinggi	3
2	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Kritis	4
2	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Kritis	4
2	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi	Tinggi	3
2	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Tinggi	3
2	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Kritis	4
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Kritis	4
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Tinggi	3
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Kritis	4
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	**36**	

A-6 Nilai Peran TIK Penelitian 6

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi			
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.			
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis		**Status**	Skor
#	**Karakteristik Instansi**		
1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Minim	0
1	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Rendah	1
1	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas	Sedang	2
1	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Rendah	1
2	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Sedang	2
2	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Minim	0
2	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi	Sedang	2
2	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Sedang	2
2	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Tinggi	3
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Tinggi	3
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Sedang	2
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Kritis	4
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	**22**	

A-7 Nilai Peran TIK Penelitian 7

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi			
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.			
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis		**Status**	Skor
#	**Karakteristik Instansi**		
1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Tinggi	3
1	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Tinggi	3
1	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas	Tinggi	3
1	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Sedang	2
2	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Tinggi	3
2	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Kritis	4
2	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi	Tinggi	3
2	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Kritis	4
2	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Kritis	4
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Tinggi	3
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Rendah	1
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Tinggi	3
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	**36**	

A-8 Nilai Peran TIK Penelitian 8

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi			
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.			
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis		**Status**	Skor
#	**Karakteristik Instansi**		
1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Rendah	1
1	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Sedang	2
1	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas	Kritis	4
1	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Sedang	2
2	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Tinggi	3
2	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Tinggi	3
2	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi	Tinggi	3
2	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Kritis	4
2	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Rendah	1
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Tinggi	3
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Sedang	2
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Sedang	2
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	**30**	

A-9 Nilai Peran TIK Penelitian 9

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi			
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.			
[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis		**Status**	Skor
#	**Karakteristik Instansi**		
1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Minim	0
1	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi 600 atau lebih = Kritis	Tinggi	3
1	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas	Tinggi	3
1	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Sedang	2
2	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Tinggi	3
2	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Sedang	2
2	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja Instansi	Sedang	2
2	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Sedang	2
2	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Sedang	2
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Sedang	2
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Sedang	2
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Tinggi	3
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	**26**	

A-10 Nilai Peran TIK Penelitian 10

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi			
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.			
	[Tingkat Kepentingan] Minim; Rendah; Sedang; Tinggi; Kritis	Status	Skor
#	Karakteristik Instansi		
1	Total anggaran tahunan yang dialokasikan untuk TIK Kurang dari Rp. 1 Milyard = Minim Rp. 1 Milyard sampai dengan Rp. 3 Milyard = Rendah Rp. 3 Milyard sampai dengan Rp 8 Milyard = Sedang Rp. 8 Milyard sampai dengan Rp. 20 Milyard = Tinggi Rp. 20 Milyard atau lebih = Kritis	Minim	0
1	Jumlah staff/pengguna dalam Instansi yang menggunakan infrastruktur TIK Kurang dari 60= Minim 60 sampai dengan 120 = Rendah 120 sampai dengan 240 = Sedang 240 sampai dengan 600 = Tinggi	Minim	0
1	Tingkat ketergantungan terhadap layanan TIK untuk menjalankan Tugas	Sedang	2
1	Nilai kekayaan intelektual yang dimiliki dan dihasilkan oleh Instansi anda	Rendah	1
2	Dampak dari kegagalan sistem TIK utama yang digunakan Instansi anda	Sedang	2
2	Tingkat ketergantungan ketersediaan sistem TIK untuk menghubungkan lokasi kerja Instansi anda	Rendah	1
2	Dampak dari kegagalan sistem TIK Instansi anda terhadap kinerja	Rendah	1
2	Tingkat sensitifitas pengguna sistem TIK di Instansi anda	Rendah	1
2	Tingkat kepatuhan terhadap UU dan perangkat hukum lainnya	Minim	0
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi sistem TIK Instansi anda	Rendah	1
1.11	Tingkat ketergantungan terhadap pihak ketiga dalam menjalankan/mengoperasikan sistem TIK	Rendah	1
1.12	Tingkat klasifikasi/kekritisan sistem TIK di Instansi anda, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	Minim	0
	Skor Peran dan Tingkat Kepentingan TIK di Instansi	**10**	

,

LAMPIRAN B

Data *AS-IS* Area Indeks KAMI pada Kesembilan Penelitian

B-1 Data *AS-IS* Area Tata Kelola

Kode	AS IS					Rata AS-IS	TO-BE
	P1	P2	P3	P4	P5		
I.1	3	2	3	3	2	2,6	3
I.2	3	2	0	3	1	1,8	3
I.3	3	2	2	3	2	2,4	3
I.4	3	1	2	3	2	2,2	3

I.5	1	2	0	2	1	1,2	3
I.6	3	1	0	3	0	1,4	3
I.7	2	1	0	3	0	1,2	3
I.8	2	0	1	1	2	1,2	3
I.9	4	2	4	4	4	3,6	6
I.10	4	2	4	6	4	4	6
I.11	4	0	4	6	4	3,6	6
I.12	2	4	6	2	2	3,2	6
I.13	4	4	0	6	4	3,6	6
I.14	6	4	2	6	4	4,4	6
I.15	3	0	3	6	0	2,4	9

I.16	3	0	0	9	0	2,4	9
I.17	6	0	3	3	0	2,4	9
I.18	3	0	3	3	0	1,8	9
I.19	3	0	3	9	0	3	9
I.20	3	0	6	6	0	3	9

B-2 Data *AS-IS* Area Risiko

Kode	AS IS					Rata AS-IS	TO-BE
	P1	P2	P3	P4	P5		

II.1	1	2	1	1	1	1,2	3
II.2	1	2	1	1	1	1,2	3
II.3	1	2	1	1	1	1,2	3
II.4	1	2	1	2	1	1,4	3
II.5	2	2	2	2	1	1,8	3
II.6	1	2	1	2	1	1,4	3
II.7	1	2	1	1	1	1,2	3
II.8	1	2	0	2	1	1,2	3
II.9	1	1	0	1	1	0,8	3
II.10	2	0	2	2	2	1,6	6
II.11	4	0	0	2	2	1,6	6

II.12	4	0	0	2	2	1,6	6
II.13	2	0	0	2	2	1,2	6
II.14	0	0	3	3	0	1,2	9
II.15	0	0	3	3	0	1,2	9

B-3 Data *AS-IS* Area Kerangka Kerja

Kode	AS IS					Rata AS-IS	TO-BE
	P1	P2	P3	P4	P5		
III.1	2	2	2	2	1	1,8	3

III.2	2	2	0	2	0	1,2	3
III.3	2	2	3	2	0	1,8	3
III.4	2	2	2	2	0	1,6	3
III.5	1	1	1	2	1	1,2	3
III.6	3	2	2	2	2	2,2	3
III.7	2	4	4	4	4	3,6	6
III.8	2	0	2	4	0	1,6	6
III.9	2	4	0	4	0	2	6
III.10	2	4	4	4	4	3,6	6
III.11	2	0	0	4	4	2	6
III.12	2	0	2	4	2	2	6

III.13	0	0	3	0	0	0,6	9
III.14	0	0	3	0	0	0,6	9
III.15	0	0	0	0	0	0	9
III.16	0	0	0	6	0	1,2	9
III.17	1	0	1	2	2	1,2	3
III.18	1	1	0	2	2	1,2	3
III.19	1	0	2	2	2	1,4	3
III.20	2	1	2	2	0	1,4	3
III.21	2	0	2	2	0	1,2	3
III.22	4	0	6	4	0	2,8	6

III.23	4	0	6	6	0	3,2	6
III.24	0	0	0	9	0	1,8	9
III.25	0	0	0	6	0	1,2	9
III.26	0	0	0	6	0	1,2	9

B-4 Data *AS-IS* Area Pengelolaan Aset

Kode	AS IS					Rata AS-IS	TO-BE
	P1	P2	P3	P4	P5		
IV.1	2	0	2	2	2	1,6	3
IV.2	1	2	2	2	2	1,8	3

IV.3	2	1	1	2	2	1,6	3
IV.4	2	2	2	2	2	2	3
IV.5	2	2	1	2	3	2	3
IV.6	1	1	1	2	3	1,6	3
IV.7	2	2	2	2	2	2	3
IV.8	2	1	2	2	2	1,8	3
IV.9	2	0	2	2	0	1,2	3
IV.10	2	1	2	2	2	1,8	3
IV.11	2	2	2	2	2	2	3
IV.12	2	2	2	2	0	1,6	3

IV.13	2	2	1	2	2	1,8	3
IV.14	3	2	2	3	2	2,4	3
IV.15	2	2	0	2	2	1,6	3
IV.16	2	2	3	2	3	2,4	3
IV.17	4	4	0	6	6	4	6
IV.18	4	4	4	4	4	4	6
IV.19	2	4	0	4	0	2	6
IV.20	6	4	0	4	0	2,8	6
IV.21	4	4	6	6	4	4,8	6
IV.22	6	0	9	9	6	6	9
IV.23	6	0	6	9	6	5,4	9

IV.24	3	0	6	6	6	4,2	9
IV.25	2	2	0	3	3	2	3
IV.26	2	2	0	3	3	2	3
IV.27	3	2	0	3	3	2,2	3
IV.28	3	2	2	3	3	2,6	3
IV.29	1	2	2	2	0	1,4	3
IV.30	4	4	4	6	6	4,8	6
IV.31	4	4	0	6	6	4	6
IV.32	4	4	4	6	4	4,4	6
IV.33	4	4	0	6	6	4	6

IV.34	3	0	3	9	9	4,8	9

B-5 Data *AS-IS* Area Teknologi

Kode	AS IS					Rata AS-IS	TO-BE
	P1	P2	P3	P4	P5		
V.1	3	3	0	2	3	2,2	3
V.2	3	2	0	3	3	2,2	3
V.3	2	2	2	2	2	2	3
V.4	2	0	2	2	2	1,6	3
V.5	3	0	2	3	1	1,8	3

V.6	2	1	2	3	3	2,2	3
V.7	3	2	3	1	2	2,2	3
V.8	3	0	3	1	1	1,6	3
V.9	2	0	2	1	3	1,6	3
V.10	2	2	2	1	3	2	3
V.11	2	4	4	2	0	2,4	6
V.12	2	0	4	2	6	2,8	6
V.13	2	4	4	0	4	2,8	6
V.14	4	0	0	4	6	2,8	6
V.15	2	4	4	4	6	4	6

V.16	4	4	4	6	6	4,8	6
V.17	2	2	0	3	1	1,6	3
V.18	2	2	3	1	3	2,2	3
V.19	3	3	3	2	3	2,8	3
V.20	4	0	4	4	6	3,6	6
V.21	4	6	4	4	0	3,6	6
V.22	4	6	4	0	6	4	6
V.23	4	4	6	4	0	3,6	6
V.24	0	0	0	6	3	1,8	9

LAMPIRAN C

Hasil Analisis Kesenjangan Area Indeks KAMI Pada 9 Penelitian

C-1 Hasil Kesenjangan Area Tata kelola

Kode	Kesenjangan					Jumlah	Rata - Rata GAP	Peringkat Area	Peringkat Keseluruhan
	P1	P2	P3	P4	P5				
I.1	0	1	0	0	1	2	0,40	20	117
I.2	0	1	3	0	2	6	1,20	17	86
I.3	0	1	1	0	1	3	0,60	19	114
I.4	0	2	1	0	1	4	0,80	18	106
I.5	2	1	3	1	2	9	1,80	12	54
I.6	0	2	3	0	3	8	1,60	15	68
I.7	1	2	3	0	3	9	1,80	13	55
I.8	1	3	2	2	1	9	1,80	14	56
I.9	2	4	2	2	2	12	2,40	8	38
I.10	2	4	2	0	2	10	2,00	11	47

I.11	2	6	2	0	2	12	2,40	9	39
I.12	4	2	0	4	4	14	2,80	7	36
I.13	2	2	6	0	2	12	2,40	10	40
I.14	0	2	4	0	2	8	1,60	16	69
I.15	6	9	6	3	9	33	6,60	2	12
I.16	6	9	9	0	9	33	6,60	3	13
I.17	3	9	6	6	9	33	6,60	4	14
I.18	6	9	6	6	9	36	7,20	1	9
I.19	6	9	6	0	9	30	6,00	5	15
I.20	6	9	3	3	9	30	6,00	6	16

C-2 Hasil Kesenjangan Area Risiko

Kode	Kesenjangan					Jumlah	Rata - Rata GAP	Peringkat Area	Peringkat Keseluruhan
	P1	P2	P3	P4	P5				
II.1	2	1	2	2	2	9	1,80	8	57
II.2	2	1	2	2	2	9	1,80	9	58
II.3	2	1	2	2	2	9	1,80	10	59
II.4	2	1	2	1	2	8	1,60	13	70
II.5	1	1	1	1	2	6	1,20	15	87

II.6	2	1	2	1	2	8	1,60	14	71
II.7	2	1	2	2	2	9	1,80	11	60
II.8	2	1	3	1	2	9	1,80	12	61
II.9	2	2	3	2	2	11	2,20	7	46
II.10	4	6	4	4	4	22	4,40	6	19
II.11	2	6	6	4	4	22	4,40	6	20
II.12	2	6	6	4	4	22	4,40	6	21
II.13	4	6	6	4	4	24	4,80	4	17
II.14	9	9	6	6	9	39	7,80	3	4
II.15	9	9	6	6	9	39	7,80	3	5

C-3 Hasil Kesenjangan Area Kerangka Kerja

Kode	Kesenjangan					Jumlah	Rata - Rata GAP	Peringkat Area	Peringkat Keseluruhan
	P1	P2	P3	P4	P5				
III.1	1	1	1	1	2	6	1,20	24	88
III.2	1	1	3	1	3	9	1,80	16	62
III.3	1	1	0	1	3	6	1,20	25	89

III.4	1	1	1	1	3	7	1,40	23	76
III.5	2	2	2	1	2	9	1,80	17	63
III.6	0	1	1	1	1	4	0,80	26	107
III.7	4	2	2	2	2	12	2,40	14	41
III.8	4	6	4	2	6	22	4,40	12	22
III.9	4	2	6	2	6	20	4,00	12	24
III.10	4	2	2	2	2	12	2,40	15	42
III.11	4	6	6	2	2	20	4,00	12	25
III.12	4	6	4	2	4	20	4,00	12	26
III.13	9	9	6	9	9	42	8,40	4	2
III.14	9	9	6	9	9	42	8,40	4	3
III.15	9	9	9	9	9	45	9,00	2	1
III.16	9	9	9	3	9	39	7,80	9	6
III.17	2	3	2	1	1	9	1,80	18	64
III.18	2	2	3	1	1	9	1,80	19	65
III.19	2	3	1	1	1	8	1,60	21	72
III.20	1	2	1	1	3	8	1,60	22	73
III.21	1	3	1	1	3	9	1,80	20	66
III.22	2	6	0	2	6	16	3,20	13	30
III.23	2	6	0	0	6	14	2,80	13	37
III.24	9	9	9	0	9	36	7,20	9	10
III.25	9	9	9	3	9	39	7,80	9	7
III.26	9	9	9	3	9	39	7,80	9	8

C-4 Hasil Kesenjangan Area Pengelolaan Aset

Kode	Kesenjangan					Jumlah	Rata - Rata GAP	Peringkat Area	Peringkat Keseluruhan
	P1	P2	P3	P4	P5				
IV.1	1	3	1	1	1	7	1,40	14	77
IV.2	2	1	1	1	1	6	1,20	19	90
IV.3	1	2	2	1	1	7	1,40	15	78
IV.4	1	1	1	1	1	5	1,00	25	98
IV.5	1	1	2	1	0	5	1,00	26	99
IV.6	2	2	2	1	0	7	1,40	16	79
IV.7	1	1	1	1	1	5	1,00	27	100
IV.8	1	2	1	1	1	6	1,20	20	91
IV.9	1	3	1	1	3	9	1,80	11	67
IV.10	1	2	1	1	1	6	1,20	21	92
IV.11	1	1	1	1	1	5	1,00	28	101
IV.12	1	1	1	1	3	7	1,40	17	80
IV.13	1	1	2	1	1	6	1,20	22	93
IV.14	0	1	1	0	1	3	0,60	32	115
IV.15	1	1	3	1	1	7	1,40	18	81

IV.16	1	1	0	1	0	3	0,60	33	116
IV.17	2	2	6	0	0	10	2,00	9	48
IV.18	2	2	2	2	2	10	2,00	9	49
IV.19	4	2	6	2	6	20	4,00	7	27
IV.20	0	2	6	2	6	16	3,20	10	31
IV.21	2	2	0	0	2	6	1,20	23	94
IV.22	3	9	0	0	3	15	3,00	7	35
IV.23	3	9	3	0	3	18	3,60	6	28
IV.24	6	9	3	3	3	24	4,80	3	18
IV.25	1	1	3	0	0	5	1,00	29	102
IV.26	1	1	3	0	0	5	1,00	30	103
IV.27	0	1	3	0	0	4	0,80	31	108
IV.28	0	1	1	0	0	2	0,40	34	118
IV.29	2	1	1	1	3	8	1,60	12	74
IV.30	2	2	2	0	0	6	1,20	24	95
IV.31	2	2	6	0	0	10	2,00	11	50
IV.32	2	2	2	0	2	8	1,60	13	75
IV.33	2	2	6	0	0	10	2,00	11	51
IV.34	6	9	6	0	0	21	4,20	3	23

C-5 Hasil Kesenjangan Area Teknologi

Kode	Kesenjangan					Jumlah	Rata - Rata GAP	Peringkat Area	Peringkat Keseluruhan
	P1	P2	P3	P4	P5				
V.1	0	0	3	1	0	4	0,80	19	109
V.2	0	1	3	0	0	4	0,80	20	110
V.3	1	1	1	1	1	5	1,00	17	104
V.4	1	3	1	1	1	7	1,40	15	82
V.5	0	3	1	0	2	6	1,20	15	96
V.6	1	2	1	0	0	4	0,80	21	111
V.7	0	1	0	2	1	4	0,80	22	112
V.8	0	3	0	2	2	7	1,40	15	83
V.9	1	3	1	2	0	7	1,40	15	84
V.10	1	1	1	2	0	5	1,00	18	105
V.11	4	2	2	4	6	18	3,60	4	29
V.12	4	6	2	4	0	16	3,20	8	32
V.13	4	2	2	6	2	16	3,20	8	33
V.14	2	6	6	2	0	16	3,20	8	34
V.15	4	2	2	2	0	10	2,00	15	52

V.16	2	2	2	0	0	6	1,20	16	97
V.17	1	1	3	0	2	7	1,40	15	85
V.18	1	1	0	2	0	4	0,80	23	113
V.19	0	0	0	1	0	1	0,20	24	119
V.20	2	6	2	2	0	12	2,40	11	43
V.21	2	0	2	2	6	12	2,40	10	44
V.22	2	0	2	6	0	10	2,00	15	53
V.23	2	2	0	2	6	12	2,40	10	45
V.24	9	9	9	3	6	36	7,20	4	11

LAMPIRAN D

Justifikasi Pengkategorian Risiko Pada Kelima Area Indeks KAMI

D-1 Justifikasi Pengkategorian Masalah Area Tatat Kelola

Kode	Pertanyaan	G	Permasalahan	D	Justifikasi	P	Justifikasi	DxP	Kategori Masalah
I.18	Apakah Instansi Anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan dan mengevaluasi	7,20	Organisasi jadi tidak tahu apakah target dan sasaran yang diterapkan untuk tiap area tercapai sehingga tidak adanya perbaikan secara berkala	3	Masuk besar, perlu prosedur khusus yang mengaturnya	3	Keterjadian 1 kali dalam 1 - 2 tahun, penentuan target dan ssasaran dalam periode tertentu	9	Medium

	pencapaiannya secara rutin, termasuk pelaporannya kepada pimpinan Instansi?								
I.15	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?	6,60	Kepatuhan terhadap keamaanan informasi diragukan karena tidak adanya program untuk mencapai target dan sasaran keamanan informasi sehingga pengamanan dipastikan kurang terkait tujuan dan sasaran yang tidak diberikan perhatian khusus oleh pemimpin instansi.	4	Besar, perlu adanya perhatian khusus pemimpin satuan kerja terhadap pemenuhan pengamanan informasi	3	Pembuatan progaram dalam kurun waktu tertentu	12	Medium

I.16	Apakah Instansi Anda sudah mendefinisikan paramater, metrik dan mekanisme pengukuran kinerja pengelolaan keamanan informasi?	6,60	Tidak bisa mengetahui kinerja dari pengelolaan keamanan yang dilakukan bisa dikatakan berhasil atau tidak.	3	Masuk besar, perlu prosedur khusus yang mengatur pengukuran kinerja	3	Pengukuran kinerja dilakukan dalam periode tertentu misal sekali dalam 1 -2 tahun	9	Medium
I.17	Apakah Instansi Anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?	6,60	Penilaian akan mengarah pada upaya pengamanan dan mengesampingkan pertan dari individu yang melakukan tindakan operasionalnya. Padahal kesalahan bisa dilakukan oleh individu yang	2	Kecil, perlu dilakukan pengukuran kinerja	4	Pengukuran kinerja dilakukan dalam periode tertentu misal sekali dalam 1 -2 tahun	8	Medium

			merupakan komponen dari teknologi informasi.						
I.19	Apakah Instansi Anda sudah mengidentifikasi legislasi dan perangkat hukum lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	6,00	Terjadinya pelanggaran hukum dan aturan terkait penerapan keamanan informasi yang tidak sesuai aturan yang berlaku.	2	Perlu prosedur untuk mengidentifikasi legilasi dan hukum terkait	2	Dilakukan dalam periode tertentu bisa 1 dalam kurun 2 - 5 tahun	4	Low
I.20	Apakah Instansi Anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut	6,00	Organisasi akan kesusahan untuk menanggulangi pelanggaran hukum terkait insiden keamanan informasi sebagai akibat tidak	4	Besar perlu adanya proses yang mendefinisikan pengaturan terhadap	3	Pendefinisian kebijakan dalam kurun waktu tertentu misal sekali dalam 1 - 2 tahun	12	Medium

	pelanggaran hukum (pidana dan perdata)?		adanya kebijakan yang mengatur.		pelanggaran hukum				
I.12	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?	2,80	Penangggung jawab yang tidak dipustuskan akan menyebabkan mangkraknya proses pengelolaan keberlangsungan TIK karena tidak adanya orang yang didefinisikan secara formal bertanggung jawab.	4	Besar, jika tidak dilakukan akan kebingungan saat menghadapi bencana	3	Pendefinisian tanggung jawab dan pelaksanaannya dalam kurun waktu tertentu misal sekali dalam 1 - 2 tahun	12	Medium
I.9	Apakah Instansi Anda menerapkan program peningkatan	2,40	Pejabat dan petugas pelaksana kurang berkompetensi dalam	2	Kecil, perlu prosedur yang memastikan	4	Beberapa kali dalam setahun terkait	8	Medium

	kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?		mengikuti perkembangan teknologi informasi.		kompetensi petugas pelaksana		perkembangan teknologi yang cepat		
I.11	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi?	2,40	Tak adanya koordinasi antara pengelola keamanan informasi dengan unit organisasi maupun pihak ekternal akan menghambat dalam penerapan program pengelolaan informasi dan membuat pengelolaan informasi tidak berjalan secara merata untuk setiap unit.	3	Masuk besar, perlu ada prosedur khusus yang mengatur koordinasi	4	Beberapa kali dalam setahun dalam koordinasi terhadap kepatuhan pengamanan	12	Medium

I.13	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?	2,40	Pimpinan instansi tidak mengetahui perkembangan pengelolaan keamanan informasi dan keefektifan program yang telah diterapkan.	4	Besar, pelaporan kondisi yang tidak rutin akan menimbulkan ketidaktahuan terhadap ancaman yang bisa datang	4	Beberapa kali dalam setahun dalam melaporkan kepatuhan program pengamanan	16	High
I.10	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna	2,00	Tanggungjawab yang tidak didefinisikan dengan jelas akan membuat fungsi tidak berjalan dengan maksimal dalam melakukan	3	Masuk besar, koordinasi dengan seluruh pihak terkait akan membantu dalam	4	Koordinasi dengan pihak terkait dilakukan beberapa kali dalam setahun	12	Medium

	aset informasi internal maupun eksternal untuk mengidentifikasikan persyaratan/kebutuhan pengamanan dan menyelesaikan permasalahan yang ada?		pengelolaan keamanan informasi.		pengmanan informasi				
I.5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?	1,80	Adanya peran dan tanggungjawab yang tidak dipetakan dan menyebabkan tidak adanya tanggung jawab dalam menjalankan perannya.	3	Masuk besar, peran yang tidak jelas akan mengganggu penangganan bencana terhadap aset	3	Penentuan peran dan tanggung jawab dalam periode tertentu	9	Medium

I.7	Apakah semua pelaksana pengamanan informasi di Instansi Anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?	1,80	Adanya pelaksana pengamanan informasi yang tidak memiliki kompetensi dan keahlian yang memadai seuai standar perusahaan sehingga dalam melakukan kegiatan opersionalnya tidak bisa mengimbangi peaksanan pengamanan informasi yang lainnya.	3	Masuk besar, prosedur standar yang memastikan pelaksana berkompeten	3	Pembuatan prosedur dalam kurun waktu tertentu	9	Medium
I.8	Apakah organsiasi Anda sudah menerapkan program	1,80	Tidak adanya pemahaman karyawan dan pihak	2	Kecil, perlu prosedur sosialisasi dan	4	Beberapa kali dalam setahun	8	Medium

	sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?		terkait mengenai keamanan informasi dan kepatuahhnya. Hal ini menyebabkan terjadinya tidak kepatuhan karyawan maupun pihak terkait terhadap aturan keamanan informasi sebagai akibat kurangnya kurangnya sosialisasi.		peningkatan pemahaman				
I.6	Apakah Instansi Anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?	1,60	Pelaksanan pengelolaan keamanan informasi memiliki spesifikasi yang berbeda setiap unit karena tidak adanya standar	2	Kecil, pembuatan prosedur peryaratan pelaksana pengamanan informasi	2	Dilakukan penentuan standar kompetensi dalam periode tertentu bisa 1 dalam kurun 2 - 5 tahun	4	Low

			kompetensi dan keahlian.						
I.14	Apakah kondisi dan permasalahan keamanan informasi di Instansi Anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi Anda?	1,60	Penanganan masalah keamanan informasi menjadi proses independen dengan proses pengambilan keputusan sehingga keputusan yang diambil tidak menyelesaikan permasalahan keamanan informasi.	4	Besar, jikapelaksanaann keamanan informasi tidak menjadi penentu keputusan strategis organisasi	3	Keputusna strategis dilakukan dalam periode tertentu misal sekali dalam 1 sampai 2 tahun	12	Medium
I.2	Apakah Instansi Anda memiliki fungsi atau bagian yang secara spesifik mempunyai	1,20	Tidak adanya fungsi atau bagian yang secara spesifik mempunyai tugas dan	4	Besar, risiko terhadap aset informasi akan	1	Keterjadian 1 kali dalam >5 tahun terkait setiap	4	Low

	tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?		tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya sehingga pengelolaan keamanan informasi pada organisasi tidak berjalan dan informasi penting organisasi menjadi sangat rentan terhadap ancaman internal maupun eksternal.		menimbulkan kerugian finansial		organisasi sudah terkomputerisasi		
I.4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya	0,80	Pengealokasian yang tidak tepat sehingga menyebabkan kekurangan sumber daya dalam melakukan	4	Besar, dapat menghambat proses bisnis	3	Perencanaan pengalokasian dilakukan sekali dalam kurun 1 -2 tahun	12	Medium

	yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?		pengelolaan keamanan informasi yang berdampak pada ketidakefektifan pengelolaan keamanan informasi.						
I.3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?	0,60	Pendefinisian tugas dan wewenang yang tidak jelas akan berdampak pada pelaksanaan pengamanan informasi yang tidak dapat berjalan secara efektif.	3	Masuk besar, perlu prosedur untuk mengaturnya	3	Pendefinisian peran dilakukan dalam periode tertentu misal sekali dalam 1 sampai 2 tahun	9	Medium

I.1	Apakah pimpinan Instansi Anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?	0,40	Kurangnya pendefinisian tanggung jawab akan membuat kurangnya kinerja dalam pelaksanaan program keamanan informasi.	4	Besar, peran pimpinan dalam pengamanan informasi sangat sentral terhadap kebijakan kemanana inforamsi	1	Keterjadian 1 kali dalam >5 tahun terkait setiap organisasi sudah terkomputerisasi jadi pengamanan teknologi merupakan hal yang sangat penting	4	Low

D-2 Justifikasi Pengkategorian Masalah Area Risiko

Kode	Pertanyaan	G	Permasalahan	D	Justifikasi	P	Justifikasi	DxP	Kategori Masalah

II.14	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?	7,80	Keefektifan dari kerangka kerja pengelolaan risiko tidak diketahui oleh oraganisasi apakah cukup handal dalam menangani risiko.	4	Besar, terkait tidak handalnya dalam menangani risiko yang mungkin terjadi	3	Pengkajian dilakukan dalam periode waktu tertentu bisa sekali dalam setahun	12	Medium
II.15	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?	7,80	Pengelolaan risiko dan penilaian kinerja efektifitas penagamanan menjadi proses yang tidak saling berkaitan dan berjalan sendiri - sendiri	3	Masuk besar , jika penilaian dari risiko tidak digunakan sebagai kriteria efektifitas pengamanan	3	Keterjadian sedang karena penilaian dilakukan dalam periode tertentu	9	Medium

II.13	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?	4,80	Akurasi dan kevaliditasan profil risiko dan mitigasinya untuk menangani permasalahan yang baru muncul diragukan terkait tidak adanya pengkajian ulang secara berkala.	4	Dampak besar terkait ketidakhandalan mitigasi risiko dalam menghadapi risiko	3	Pengkajian dilakukan dalam periode waktu tertentu bisa sekali dalam setahun	12	Medium
II.10	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya,	4,40	Penyusunan langkah mitigasi risiko akan tidak memerhatikan tingkat prioritas,	4	Besar, tidak tepat dalam menyelesaikan masalah terkait	3	Penyusunan langkah mitigasi dilakukan saat analisis risiko yang	12	Medium

	dengan memastikan efektifitas biaya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?		efektifitas biaya dan dampaknya.				berlangsung dalam periode tertentu		
II.11	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?	4,40	Pihak manajemen tidak mengetahui perkembangan yang terjadi atas upaya mitigasi risiko.	3	Masuk besar , perlunya prosedur yang mengatur pemantauan mitigasi risiko yang dilakukan	4	Beberapa kali dalam setahun dpat terjadi insiden, sehingga upaya mitigasi juga sering dilakukan	12	Medium

II.12	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi untuk memastikan konsistensi dan efektifitasnya?	4,40	Langkah mitigasi yang sudah diterapkan tidak diketahui apakah bisa menagngani risiko yang sama kedepannya.	4	Besar, memastikan langkah mitigasi handal dalam menaangani risiko	3	Pengevaluasian dilakukan dalam periode tertentu, bisa sekali setahun	12	Medium
II.9	Apakah Instansi Anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?	2,20	Risiko akan menjadi masalah besar yang dapat mengganggu keberlangsungan bisnis jika langkah mitigasi risiko tidak disusun.	5	Ekstrim, risiko yang tidak ada langkah mitigasinya akan menghentikan proses bisnis	3	Penyusunan langkah mitigasi dilakukan dalam periode waktu tertentu	15	High
II.1	Apakah Instansi Anda mempunyai program kerja pengelolaan risiko keamanan	1,80	Tidak adanya program kerja dari organisasi dalam pengelolaan risiko	5	Ekstrim jika tidak memiliki langkah mitigasi risiko	3	Program kerja dibuat dalam periode tertentu	15	High

	informasi yang terdokumentasi dan secara resmi digunakan?		yang terdokumentasi sehingga dalam penerapannya dapat jauh dari kerangka pengelolaan risiko.		baik yang didokumentasikan		misal sekali dalam setahun		
II.2	Apakah Instansi Anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	1,80	Tidak adanya panduan dalam pengelolaan risiko yang terdokumentasi sehingga dalam penerapannya dapat jauh dari kerangka pengelolaan risiko.	5	Ekstrim, jika organisasi tidak menerapkan kerangka kerja yang mengelola risiko	3	Penentuan kerangka kerja pengelolaan risiko keamanan informasi dilakukan sekali dalam 1 - 2 tahun	15	High
II.3	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan	1,80	Pengklasifikasian aset informasi , tingkat ancaman, kemungkinan	3	Masuk besar jika kerangka kerja tidak mendefinisikan	3	Pendefinisian merupakan kesatuan proses yang dilakukan	9	Medium

	tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi Anda?		keterjadian dan dampak kerugian tidak didefinisikan sehingga dalam mengidentifikasi risiko tidak sesuai dengan masalah yang benar – benar menjadi prioritas dalam penyelesaiannya.		risiko asetdengan jelas		dalam kurun waktu tertentu		
II.7	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?	1,80	Dampak yang tidak ditentukan dpat mempengaruhi dalam analisis apakah risiko itu memiliki pengaruh yang besar dalam keberlangsungan bisnis organisasi/perusahaan.	4	Besar, jika kerugian tidak didefinisikan akan berdampak pada finansial perusahaan	3	Pendefinisian dampak merupakan kesatuan proses yang dilakukan dalam kurun waktu tertentu	12	Medium

II.8	Apakah Instansi Anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?	1,80	Tidak adanya respon yang cepat terhadap insiden yang terjadi mengenai keamanan informasi.	3	Perlunya prosedur tertentu yang mengatur inisiatif kejian risiko	3	Pengkajian dilakukan dalam periode waktu tertentu bisa sekali dalam setahun	9	Medium

II.4	Apakah Instansi Anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?	1,60	Setiap risiko akan diterima oleh organisasi tanpa adanya batasan tertentu yang menyatakan bahwa risiko tersebut harus dihentikan.	3	Ambang batas tidak jelas harus didefinisikan	3	Penentuanambang batas merupakan kesatuan proses yang dilakukan dalam kurun waktu tertentu	9	Medium
II.6	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?	1,60	Ancaman terkait aset informasi membantu dalam identifikasi risiko. Ketika tidak dilakukan akan menghambat kecepatan tanggapan organisasi dalam menangani risiko yang mungkin terjadi.	3	Masuk besar, perlu prosedur indentifikasi ancaman pada aset	3	Pengkajian dilakukan dalam periode waktu tertentu bisa sekali dalam setahun	9	Medium

II.5	Apakah Instansi Anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?	1,20	Akan ada tindakan saling klaim tehadap aset informasi karena tidak adanya aturan yang jelas mendefinisikan kepemilikan dan pihak pengelola aset informasi yang ada.	4	Besar, pendefinisian peran dan tanggung jawab harus jelas dalam mengelola aset yang berisi informasi penting organisasi	3	Pengkajian dilakukan dalam periode waktu tertentu bisa sekali dalam setahun	12	Medium

D-3 Justifikasi Pengkategorian Masalah Area Kerangka Kerja

Kode	Pertanyaan	G	Permasalahan	D	Justifikasi	P	Justifikasi	DxP	Kategori Masalah

III.15	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?	9,00	Proses pemulihan yang dimiliki oleh oraganisasi gagal menangani permasalahan. Hal ini terkait tidak adanya pengevaluasian upaya pemulihan bencana secara berkala untuk memastikan apakah proses pemulihannya masih relevan. Akibatnya perencanaan pemulihan yang telah dibuat tidak bisa menyelesaikan permasalahan.	4	Besar, langkah pemulihan yang gagal dapat menghambat kinerja organisasi, perlu dilakukan pengevaluasian	4	Ketika langkah pemulihan tidak pernah dievaluasi, maka langkah tersebut menjadi kurang handal dan masalah akan sering terjadi	16	High
III.13	Apakah perencanaan pemulihan bencana terhadap layanan TIK	8,40	Tidak adanya pendefinisian peran dan tanggung jawab	3	Masuk besar, pendefinisian tanggung jawab harus jelas	3	Pendefinisian dilakukan dalam kurun waktu	9	Medium

	(*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?		akan menghambat proses pemulihan karena belum terdefinisi peran siapa yang melakukan apa sehingga proses pemulihan dilakukan dengan lambat atau tidak sesuai dengan harapan karena peran dan wewenang yang tidak dijabarkan..		supaya proses pemulihan dpat dipertanggungjawabkan		tertentu, bisa saat perencanaan upaya pemulihan		
III.14	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery*	8,40	Uji coba yang tidak dilakukan terhadap upaya pemulihan akan membuat organisasi menjadi tidak sadar bahwa	4	Besar, pemulihan yang tidak diuji sesuai jadwal akan memeungkinkan ketidakefektifannya terkait perkembangan yang terus berlanjut	3	keterjadian sedang jika upaya pemulihan tidak diuji sesuai	12	Medium

	plan) sudah dilakukan sesuai jadwal?		upaya pemulihannya tidak relevan lagi.				jadwal yang dibuat		
III.16	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?	7,80	Kebijakan dan prosedur keamanan informasi yang tidak dievaluasi secara berkala akan menyebabkan kebijakan itu tidak dapat lagi memastikan keberlangsungan bisnis yang terus berkembang dan keefektifan dari kebijakannya akan diragukan.	3	Masuk besar, karena kebijakan bisa jadi tidak relevan terkait perkembangan teknologi yang sangat cepat	2	Pengevaluasian kebijakan dalam periode waktu 2 - 5 tahun sekali	6	Medium
III.25	Apakah organisasi Anda secara periodik menguji dan mengevaluasi	7,80	Organisasi yang tidak melakukan pengujian terhadap kepatuhan dari	4	Besar, akan berdampak pada terhambatnya proses bisnis jika	3	Keterjadiannya sedang, pengujian dilakukan dalam	12	Medium

	tingkat/status kepatuhan program keamanan informasi yang ada untuk memastikan bahwa keseluruhan inisiatif tersebut telah diterapkan secara efektif?		program keamanannya tidak akan bisa memastikan bahwa keamanan yang ia rencanakan bisa menanggulangi ancaman. Dan juga menimbulkan banyak kerentanan pada bagian yang tidak menerapkan program keamanan.		program keamanan ada tetapi tidak dilakukan		periode tertentu dalam setahun		
III.24	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun	7,20	Kebijakan dan prosedur harus direvisi untuk memenuhi kebutuhan bisnis organisasi. Untuk itu diperlukan analisa finansial, perubahan, dan pengelolaan	4	Besar, lewat perubahan yang dilakukan akan mungkin timbul biaya - biaya yang tidak terduga	2	Perevisian kebijakan dilakukan insidentil maupun dalam kurun waktu 2 - 5 tahun	8	Medium

	perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?		perubahan. Jika tidak ada maka kebijakan baru yang direvisi tidak bisa dijamin dalam menangani kebutuhan organisasi karena setiap kebijakan yang dibuat harus menjawab permasalahan dari orgamisasi.						
III.26	Apakah organisasi Anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?	7,80	Organisasi yang tidak memiliki rencana upaya peningkatan keamanan informasi dapat membuat organisasinya memiliki banyak kerentanan terhadap ancaman yang mungkin terjadi dari	3	Masuk besar, perlu dibuatkan prosedur kemanaan informasi	3	Keterjadian 1 dalam 1 - 2 tahun terkait rencana yang dibuat berdasarkan periode waktu tertentu	9	Medium

			internal maupun eksternal. Dan juga perencanaan tingkat keamanan informasi membntu organisasi untuk tanggap terhadap ancaman yang akan terus berkembang.						
III.8	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi?	4,40	Penerapan keamanan iniformasi dalam penerapannya akan berubah – ubah mengikuti situasi terkait tidak adanya prosedur resmi yang mengikat.	2	Kecilm dapat diatur pengecualiannya dengan prosedur	2	Keterjadiannya rendah karena prosedur dibuat dalam kurun waktu tertetntu	4	Low
III.9	Apakah organisasi Anda sudah	4,00	Tidak adanya kebijakan dan	3	Masuk besar , perlu adanya pengelolaan	4	Patch dilakukan bebrapa kali	12	Medium

	menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?		prosedur yang mengatur menyebabkan pengimplementasian yang terhambat terkait peran dan tanggung jawab untuk implementasi, memonitor, dan pelaporannya tidak didefinisikan.		patch keamanan untuk memastikan bisnis terus berlangsung		dalam setahun, jika tidak diterapkan pengelolaan, maka masalah akan terjadi beberapa kali juga dalam setahun		
III.11	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru	4,00	Risiko berantai baru akan muncul tekait penerapan pengamanan informasi yang dan organisasi akan kebingungan dalam menghadapi risiko yang timbul dari penerapan pengamanan informasi terkait	4	Besar, dampak dari penerapan sistem baru yang diidentifikasi akan mengeluarkan biaya secara mendadak	3	Keterjadiannnya sedang, penerapan sistem baru harus melalui proses yang panjang	12	Medium

	(*compensating control*) dan jadwal penyelesaiannya?		tidak ada pengaturan terhadap cara menghadapi permasalahan ini.						
III.12	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?	4,00	Organisasi tidak tanggap terhadap insiden yang terjadi karena tidak memiliki perencanaan yang bisa menghadapi kemungkinan insiden agar bisnis dapat terus dijalankan.	4	Besar, BCP digunakan untuk menjaga keberlangsungan bisnis	4	Keterjadian insiden akan menjadi masalah yang akan sering dihadapi jika organisasi tidak memiliki kerangka kerja untuk menjaga keberlangsungan bisnis	16	High
III.22	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi	3,20	Hasil audit tidak dikaji sehigga langkah pembenahan	4	Besar, hasil audit dapat dijadikan pembelajaran organisasi, untuk itu	3	Pengevaluasian audit dilakukan dalam kurun waktu 1 dalam 1	12	Medium

	langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?		terhadap temuan audit tidak diidentifikasi sehingga keamanan informasi masih dalam keadaan yang belum berkembang dan rentan.		pengevaluasiannya sangat penting		-2 tahun untuk memastikan perkembangan keamanan informasi		
III.23	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?	2,80	Hasil audit hanya menjadi syarat pengelolaan manajemen yang baik tanpa melihat hasilnya sehingga manajer tidak tahu terkait permasalaahan yang mungkin terjadi sehingga tidak bisa melanjutkan ke tahapan perbaikan.	3	Masuk besar, perlu adanya prosedur khusus yang mengatur pelaporan	3	1 kali dalam 1 - 2 tahun terkait periode audit yang dilakukan	9	Medium

III.7	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	2,40	Banyak pegawai yang tidak mengetahui kebijakan yang diterapkan sehingga terjadinya pelanggaran terkait tidak adanya aturan maupun komunikasi dengan pegawai.	5	Pelanggaran kemanan memiliki efek yang besar terhadap keberlangsungan bisnis organisasi	4	Jika kebijakan ekamanan tidak diterapkan dan tidak diatur konsekuensi yang jelas maka akan menimbulkan pelanggaran yang sering	20	High
III.10	Apakah organisasi Anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi	2,40	Organisasi akan kebingungan terkait risiko yang bisa muncul ketika melakukan implementasi sistetem baru terkait tidak adanyaa pengkajian terhadap	3	Masuk besar, setiap proses harus diidentifikasi risikonya	4	Keterjadian bisa beberapa kali dalam setahun jika risiko tidak diidentifikasi	12	Medium

	permasalahan yang muncul?		risiko yang pernah terjadi sebelumnya.						
III.2	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?	1,80	Kebijakan yang tidak diketahui oleh pihak terkait karena kurang adanya komunikasi maupun penetapan kebijakan secara formal yang mengakibatkan ketidaktahuan pihak terkait.	2	Kecil, perlu adanya prosedur dalam mengkomunikasikan informasi	4	Beberapa pelanggaran kebijakan dapat terjadi dalam setahun	8	Medium
III.5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi?	1,80	Kebijakan yang dibuat tidak berdasarkan pengelolaan risiko dan mitigasi yang telah dianalisis sehingga menyebabkan kebijakan tidak tepat sasran dan tidak	3	Masuk besar , tidak tepatnya sassaran kemanan informasi	1	Pembuatan kebijakan dan prosedur dalam kurun waktu tertentu	3	Low

			dapat menjawab permasalahan organisasi dan membantu dalam menyelesaikan permasalahan.						
III.17	Apakah organisasi Anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?	1,80	Strategi penerapan keamanan informasi yang tidak sesuai dengna hasil analisis risiko akan mengakibatkan kemanan yang diterapkan tidak selalu akan menjawab permasalahan yang dihadapi oleh organisasi.	2	Kecil, perlu prosedur tertentu untuk menyelaraskan keseluruhan proses	3	Sedang, pembuatan rencana kerja dalam kurun waktu tertentu	6	Medium

III.18	Apakah organisasi Anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?	1,80	Strategi penerapan keamanan informasi yang tidak sesuai dengan hasil analisis risiko akan mengakibatkan kemanan yang diterapkan tidak selalu akan menjawab permasalahan yang dihadapi oleh organisasi.	3	Dampak masuk besar jika strategi penggunaan teknologi keamanan informasi tidak sesuai dengna kebutuhan	3	Penyusunana strategi dilakukan dalam periode tertentu	9	Medium
III.21	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?	1,80	Audit tidak melakukan evaluasi kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi sehingga tidak didapatkan temuan terkait hal tersebut	4	Besar jika pengevaluasian tingkat kepatuhan tidak pernah dilakukan	3	Periode audit dalam kurun waktru tertentu	12	Medium

			yang bisa diberikan saran perbaikan.						
III.19	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi Anda?	1,60	Strategi penerapan keaman informasi yang tidak sesuai dengan program kerja organisasi akan menjadi strategi yang tidak tepat sasaran dan tidak menjawab kebutuhan organisasi.	3	Masuk besar jika organisasi tidak memerhatikan program kemanan informasi	2	Pembuatan program dana sasaran dalam kurun waktu tertentu	6	Medium
III.20	Apakah organisasi Anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan	1,60	Organisasi tidak dapat mengevaluasi fungsi organisasinya dan memberikan perbaikan terkait temuan permasalahan dalam	5	Dampak besar jika tidak dilakukan karena tidak ada evaluasi kerentanan sehingga tdak bisa melakukan	3	Audit dilakukan dalam periode tertetntu misal setahun sekali	15	High

	aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?		unit bisnis untuk memperbaiki kinerja organisasi.		perkembangan yang berkelanjutan				
III.4	Apakah tersedia mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?	1,40	Tidak adanya mekanisme untuk mengkomunikasikan kebijakan keamanan informasi akan menyebabkan ketidaktahuan pihak terkait terhadap kebijakan dan berakibat pelanggaran kebijakan yang tidak disengaja.	2	Kecil, pembuatan prosedur pengkomunkasian setiap kebijakan	4	Beberapa kali dalam setahun bila ada kebijakan yang perlu direvisi	8	Medium
III.1	Apakah kebijakan dan prosedur keamanan informasi sudah disusun dan dituliskan	1,20	Kebijakan yang tidak jelas mendefinisikan peran dan tanggung	4	Terhambatnya proses pengamanan informasi	4	Pengamanan akan sring terhambat dan terjadi beberapa	16	High

	dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?		jawab kepada pihak yang diberikan wewenang maka akan membuat implementasi kebijakan terhambat terkait tidak adanya pihak yang mengurusi permasalahan secara spesifik.		jika tidak dilakukan penjabaran yang jelas		kali dalam setahun		
III.3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	1,20	Tidak adanya mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi akan menyebabkan kerusakan atau kehilangan dari dokumen karena tidak dilakukan	4	Besar karena data merupakan aset penting yang bisa berisikan info penting organisasi	4	Tidak adanya prosedur pengelolaan dapat membuat permasalahan akan sering terjadi	16	High

			pengelolaan dengan baik dan penempatan orang yang harus bertanggung jawab terhadap dokumen tersebut.						
III.6	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset tercantum dalam kontrak dengan pihak ketiga?	0,80	Terjadinya pelanggaran oleh pihak ketiga mengenai pelaporan insiden, penjagaan kerahasiaan, HAKI dan pengamanan aset.	4	Dampak besar, jika kontrak dengan pihak ketifa tidak jelas menjelaskan hal - hal penting	4	Jika bebrapa kriteria tidak dicantunkan dalam kontrak maka pelanggaran bisa sering terjadi	16	High

D-4 Justifikasi Pengkategorian Masalah Area Pengelolaan Aset

Kode	Pertanyaan	G	Permasalahan	D	Justifikasi	P	Justifikasi	DxP	Kategori Masalah
IV.24	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?	4,80	Penggunaan perangkat pengeolah informasi milik pihak ketiga jadi semena – mena dan memungkinkan adanya akses dari orang yang tidak memilik otentikasi untuk mengakses terkait tidak adanya prosedur	4	Besar, karena berhubungan dengan HAKI maka bisa dilakukan penuntutan dan berdampak pada kerugian finansial	4	Penggunaan perangkat pengolahan informasi merupakan aktivitas rutin yang jika terjadi permasalahahan dapat terjadi beberapa kali	16	High

			untuk mengaturnya.						
IV.34	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi Anda?	4,20	Lokasi kerja dapat diakses oleh orang yang tidak memiliki otentikasi terkait tidak adanya prosses untuk mengamankan lokasi kerja.	3	Masuk besar perlua adanya pengamanan walaupun memili kepentingan terhadap instansi	5	Hubungan dengan pihak ketiga yang bekerja untuk instansi akan sering dilakukan, jika pengaman tidak diterapkan maka kemungkinan masalah akan terjadi sangat sering	15	High
IV.19	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.	4,00	Orang yang bertanggung jawab menangani insiden akan kebingungan dalam menangani insiden yang membutuhkan	2	Kecil, perlu penerapan adanya prosedur menganani insiden yang memerlukan pihak eksternal	4	Dalam setahun dapat terjadi beberapa kali insiden. Untuk itu pelaporan dengan pihak eksternal jika tidak dilakukan dengan prosedur yang baik akan dapat terjadi	8	Medium

			campur tangan pihak eksternal.				beberapa kali daalam setahun		
IV.23	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?	3,60	Tidak adanya rekaman menyebabkan organisasi tidak bisa belajar dari insiden masa lalu yang telah terjadi dan upaya penagamanan yang diterapkan.	3	Masuk besar karena organisasi tidak bisa belajar dari masa lalu rekaman, perlu ada prosedur khusus yang mengatur	4	Terjadi beberapa kali dalam setahun, mengingat pelaksanaan pengamanan dpat dilakukan beberapa kali dalam setahun	12	Medium
IV.20	Prosedur penghancuran data/aset yang sudah tidak diperlukan	3,20	Kebocoran data/aset kepada pihak luar organisasi yang	4	Besar, aset maupun data yang tidak digunakan dapat	3	Dapat terjadi sekali dalam 1 - 2 tahun jika tidak diatur prosedur	12	Medium

			dapat mengganggu keberlangsungan bisnis.		mengandung informasi penting organisasi, sehingga dapat berdampak pada kehilangan dan kerugian finansial		penghancuran yang benar		
IV.22	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?	3,00	Kemugkinan adanya data/informasi yang tidak di-*backup* dan tidak adanya pelaporan terhadap kondisi data/informasi tersebut.	3	Masuk besar karena tidak adanya prosedur akan menganggu pengelolaan data yang akan dibackup	4	Ada data yang tidak dibackup dalam periode backup beberapa kali dalam setahun	12	Medium
IV.17	Ketentuan pengamanan fisik yang disesuaikan dengan	2,00	Pengamanan akan sama untuk setiap aset, padahal ada	4	besar, karena bisa terjadi tidak tepatan	4	Beberapa kali dapat terjadi setahun, terkait	16	High

	definisi zona dan klasifikasi aset yang ada di dalamnya		aset yang memiliki kerentanan yang sangat besar dan harus diprioritaskan dalam pengamaanannya.		pengamanan pada aset dimanan pengamanan dapat lemah pada aset penting		tidak adanya ketentuan yang mengatur		
IV.18	Proses pengecekan latar belakang SDM	2,00	SDM yang tidak jelas latar belakangnya dapat menjadi ancaman bagi organisasi nantinya terkait jejak kriminnal maupun ketidakpemenuhan sesuai dengan kriteria organisasi.	2	Kecil, dapat dilakukan dengan prosedur pengecekan selama waawancara kerja	3	SM kurang sesuai standar perusahaan dapat ada 1 kali dalam 1 - 2 tahun	6	Medium

IV.31	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?	2,00	Perangkat komputer yang digunakan untuk menyimpan informasi penting mengalami kerusakan yang tidak diketahui sehingga kerentanan terhadap informasi bisa muncul. Ketidaklayakan yang tidak diketahui akan menyebabkan permasalahan yang panjang kedepannya.	3	Masuk besar, perawatan perangkat pendukung yang rusak karena tidak dilakukan pereawatan rutin	5	Perawatanseperti pembersihan dapat dilakukan dalam waktu mingguan atau bulanan	15	High

IV.33	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)	2,00	Adanya kegiatan yang dapat menyebabkan kerusakan, kehilangan dan sabotase terkait lokasi kerja yang dapat memberikan efek buruk pada keberlangsungan bisnis terkait tidak adanya peraturan untuk meangamankan lokasi kerja penting.	5	Ekstrem karena pengamanan yang kurang memadai pada aset penting organisasi dan areanya akan menimbulkan risiko - risiko yang dapat menimbulkan kerugian finansial	5	Jika tidak dilakukan penentuan peraturan maka aset informasi yang digunakan sehari - hari akan rusak dan menimbulkan kerugian finansial	25	High

IV.9	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI	1,80	Penyalahgunaan penggunaan aset Instansi terkait HAKI.	3	Masuk besar, penggunaan aset HAKI harus dikelola dengan baik karena merupakan penggunaan hak intelektual	4	Penggunaan aset yang tergolong aset pengolahan informasi dilakukan secara sering jika terjadi pelanggaran HAAKI terhadap aset maka dapat terjadi beberapa kali pula dalam setahun	12	Medium
IV.29	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi Anda apabila digunakan di luar lokasi kerja resmi (kantor)?	1,60	Penggunaan perangkat komputasi diluar kantor tidak mementingkan keamanan perangkat informasi yang memungkinkan kerusakan maupun kehilangan	3	Perlu adanya prosedur pengamanan perangkat komputasi untuk menghindari kerusakan di luar kantor	5	Perangkat komputasi merupakan perangkat pengolahan informasi yang digunakan sering sehigga bila terjadi permasalahan terkait maka kemungkinan keterjadiannya juga sering	15	High

			data/informasi pada perangkat komputasi.						
IV.32	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?	1,60	Kehilangan aset informasi sebagai kelalalian dari petugas atau pengemasan yang kurang diatur oleh perusahaan untuk meminimalkan kerentanan.	4	Besar, aset informasi yang hilang bisa berisi informasi penting organiasasi	3	1 dalam 1- 2 tahun karena pihak ketiga yang bekerja sama dengan perusahaan biasanya sudah menangani kontrak dalam menjaga barang yang dikirim	12	Medium
IV.1	Apakah tersedia daftar inventaris aset informasi yang lengkap dan akurat?	1,40	Aset yang dimiliki organisasi tidak terdokumentasi sehingga tidak tersedia informasi	3	Masuk besar, menyebabkan pemimpin organisasi tidak	4	Beberapa kali dalam setahun terkait aset yang terjadinya perpindahan dalam organisasi bisa banyak	12	Medium

			terkait aset yang dimiliki.		mengetahui aset yang dimilikinya		terkait adanya pemutahiran.		
IV.3	Apakah tersedia definisi tingkatan akses yang berbeda dan matrix yang merekam alokasi akses tersebut	1,40	Tingkat akses yang tidak dibedakan akan menyebabkan penyelahgunaan wewenang dan kehilangan data jika akses diberikan sama kepada seluruh pihak.	3	penyelahgunaan wewenang akses	5	Akses merupaka nkegiatan yang dilakukan secara rutin, jika belum didefinisikan tingkatan akses, maka akses yang bebas akan terjadi juga secara rutin	15	High
IV.6	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset	1,40	Aset yang dimiliki oleh perusahaan tidak akan diketahui *update* dan kondisi terkininya karena	2	Kecil, aset baru yang tidak terdata dapat dilakukan pembuatan prosedur dalam	4	Beberapa kali dalam setahun terkait aset yang dimiliki organisasi selalu	8	Medium

	informasi?Apakah Instansi Anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?		tidak adanya penginventarisan aset baru.		penanganan aset baru		berubah - ubah dan tidak tetap		
IV.12	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi	1,40	Akses yang bebas terhadap aset informasi organisasi yang memungkinkan penyalahgunaan akses oleh orang yang tidak memiliki wewenang.	3	Masuk besar, penyalahgunaan akses akan berdampak pada pencurian data	5	Dapat sering terjadi permasalahan jika prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi belum dimiliki	15	High

IV.15	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi	1,40	Insiden kegagalan informasi tidak akan memiliki upaya penyelesaian jika tidak dilakukan investigasi untuk mengetahui penyebab dan dampaknya terhadap keberlangsungan bisanis organisasi.	5	Ekstrim, kegagalan informasi yang tidak dilakukan investigasi akan menghentikan proses bisnis yang berdampak pada keugian finansial	4	Insiden dapat terjadibeberapa kali dalam setahun untuk itu organisasi perlu upaya pencegahan terhadap risiko yang mungkin muncul	20	High
IV.2	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan	1,20	Tidak adanya pengelolaan yang baik terhadap aset sehingga aset sangat rentan terhadap ancaman dari luar maupun	3	Masuk besar, karena aset sangat rentan terhadap ancaman dari luar maupun dalam organisasi yang	3	Keterjadiannya sedang perlu pengevaluaasian seklai dala m1 - 2 tahun	9	Medium

	keperluan pengamanannya?		dalam organisasi yang menyebabkan pada kerusakan maupun hilangnya aset.		menyebabkan pada kerusakan				
IV.8	Tata tertib penggunaan komputer, email, internet dan intranet	1,20	Penggunaan sewenang – wenang oleh orang yang tidak memiliki otentikasi maupun kemungkinanan penyalahgunaan fungsi aset yang bukan untuk kepentingan organisasi.	2	Kecil, penyalahgunaan fasilitas dapat ditangani dengan prosedur sederhana	5	Penyalahgunaan aset sehari - hari dapat terjadi sangat sering terkait penggunaan aset yang sering juga	10	Medium

IV.10	Peraturan pengamanan data pribadi	1,20	Ketidakadaan pengaturan mengenai pengelolaan data pribadi akan menyebabkan data rentan dan pengelolaannya tidak tersetandarisasi.	2	Kecil, pengamnan data pribadi karyawan perusahaan perlu distandarkan dalam prosedur yang mudah dipahami	5	Data pribadi sangat rentan terkait Ketidakadaan pengaturan mengenai pengelolaan data pribadi	10	Medium
IV.13	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data	1,20	Adanya penumpukan data yang tidak dihancurkan.	3	Masuk besar, karena data tersebut bisa mengandung informasi penting organisasi sehingga perlu dilakukan	4	Keterjadian masalah dpat beberapa kali dalam setahun terkait tidak adanya ketetapan dalam penyimpanan dan penghancuran data	12	Medium

					pengelolaan yang baik				
IV.21	Prosedur kajian penggunaan akses (*user access review*) dan langkah pembenahan apabila terjadi ketidaksesuaian sesuaian (*non-conformity*) terhadap kebijakan yang berlaku.	1,20	Pengkajian terhadap hak akses tidak dilakukan akan menimbulkan pembiaran terhadap tindakan penyalahgunaan akses, dan akan menimbulkan pelanggaran yang dari karyawan yang dapat mengganggu proses bisnis perusahaan.	2	hanya perlu dilakukan prosedur pengkajian akses secara rutin untuk membenahi ketidaksesuaian yang terjadi	3	Pembuatan prosedur diperlukan dalam periode tertentu.	6	Medium

IV.30	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?	1,20	Pengamanan fisik informasi yang tidak sesuai dapat menyebabkan risiko – risiko yang tidak diinginkan terjadi. Baik itu dari alam, kelalalian manusia dan percobaan sabotase.	5	Ekstrem rusaknya perngkat informasi terhadap bencana alam, kebakaran maupun kehilangan	4	Dpat terjadi beberapa kali jika tidak dilakukan bentuk pengamanan untuk mencegah dan mendeteksi risiko	20	High
IV.4	Apakah tersedia proses pengelolaan perubahan terhadap sistem (termasuk perubahan	1,00	Tidak adanya pengendalian terhadap perubahan	2	Kecil, perlu proses pengelolaan	2	Perubahan terjadi dalam jang ka waktu	4	Low

	konfigurasi) yang diterapkan secara konsisten?		sehingaga berdampak pada kekurang sigapan organisasi dalam menghadapi efek dari perubahan pengelolaan keamanan informasi.		perubahan terhadap sistem		panjang bisa dalam 2 - 5 tahunan		
IV.5	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	1,00	Adanya penerapan konfigurasi yang berbeda – beda untuk setiap infrstruktur informasi.	2	kecil, perlu prosedur standar untuk penerapan konfigurasi	2	Perubahan standar dilakukan dalam jangka waktu yang lama bisa dalam 2- 5 tahun	4	Low
IV.7	Definisi tanggungjawab	1,00	Tidak adanya rasa memiliki terhadap	3	Masuk besar, perlu adanya	4	Keterjadiannya akan sering dalam setahun	12	Medium

	pengamanan informasi secara individual untuk semua personil di Instansi Anda		aset informasi kerena tugas tidak didefinisikan yang berakibat pada ketidakefektifan dalam pengamanan informasi.		prosedur yang mengatur tanggjung jawab personil secara jelas		terkait belum didefinisikannya tanggung jawab yang jeals		
IV.11	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya	1,00	Penggunaan yang tidak sesuai standar dan dapat terjadi penyalahgunaan oleh orang yang tidak memiliki otentikasi.	3	Termasuk besar, diatasi dengan prosedur pengelolaan idnetitas elektronik yang baik	5	Pengelolaan terhadap identitas elektronik tidak dilakukan akan menyebabkan penyalahgunaan yang dapat sangat sering tekait otentikasi merupakan hal -yang diperlukan setiap memulai aktivitas	15	High

IV.25	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?	1,00	Adanya akses oleh pihak yang tidak berwenang yang mengambil data/informasi penting organisasi dan melakukan perusakan terhadap aset informasi organisasi.	5	Ekstrim terkait adanya akses oleh pihak yang tidak berwenang dapat merusakaset informasi	5	Jika tidak diterapkan pengamann fisik yang memadai akses yang tidak diinginkan dapat sangat sering terjadi	25	High
IV.26	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?	1,00	Adanya akses yang tidak diinginkan yang mengganggu keberlangsungan bisnis dan melakukan	5	Pengelolaan kunci masuk fasilitas fisik harus dilakukan untuk menghindari akses ilegal untuk pencurian aset	5	Jika tidak ada prose untuk mengelola alokasi kunci dengan baik akses ilegal akan sering terjadi karena tidak adanya perhatian	25	High

			tindakan yang mengancam aset informasi.		dan data informasi		khusus dari pemimpin organisasi		
IV.27	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?	0,80	Infrstruktur komputasi mengalami kerusakan terkait tidak diterapkan perlindungan yang melindungi infrstruktur dari bahaya lingkungan serta tidak dilakukan perlindungan seperti prasyarat pabrikannya.	5	Ekstrim, jika pengelolaan infrastruktur tidak dilakukan secara prasyarat keseharusannya akan menyebabkan kerusakan dan kerugian finansial	4	Jika tidak dilakukan pengelolaan yang sesuai syarat pabrikannya akan membuat seringnya terjadi masalah yang tidak diharapkan	20	High
IV.14	Ketetapan terkait pertukaran data dengan	0,60	Terjadinya penyebaran	4	Besar, data yang ditukar dpat berisi	4	Jika tidak adanya ketetapan , maka	16	High

	pihak eksternal dan pengamanannya		informasi rahasia organisasi karena tidak adanya aturan pembatasan pembagian informasi dan ada kemungkinan kebocoran penting organisasi.		informasi penting organisasi		pengamanan kurang, jadi masalah akan semakin sering terjadi berhubung juga aktivitas terkait merupakan aktivitas harian		
IV.16	Prosedur *back-up* ujicoba pengembalian data (*restore*)	0,60	Kehilangan data sebelumnya ketika implementasi yang diterapkan gagal.	4	Besar karena data dapat hilang jika tidak menerapkan prosedur yang tepat	3	Keterjadian sekali dalam 1 sampai 2 tahun	12	Medium
IV.28	Apakah infrastruktur komputasi yang terpasang terlindungi	0,40	Terjadinya kerusakan pada alat – alat	5	Besar memberikan kerugian finansial	4	Keterjadiannya dpat terjadi beberapa kali dalam setahun jika	20	High

	dari gangguan pasokan listrik atau dampak dari petir?		elektronik dan kemungkinan terjadinya konsleting yang dapat menyebabkan kebakaran.		terkait konsleting pada alat		tidak menerapkan pengkabelan yang benar dan pencegahan terhadap sambaran petir		

D-5 Justifikasi Pengkategorian Masalah Area Teknologi

Kode	Pertanyaan	G	Permasalahan	D	Justifikasi	P	Justifikasi	DxP	Kategori Masalah
V.24	Apakah Instansi Anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?	7,20	Kehandalan keamanan informasi kurang bisa dibuktikan terkait tidak adanya perencanaan terkait pengkajian	3	Masuk besar karena kehandalan kemananan harus dicek secara rutin untuk	3	Pengkajian dilakukan dalam kurun waktu setahun sekali	9	Medium

			kehandalan keamanan informasi		memastikan keamanaan				
V.11	Apakah Instansi Anda mempunyai standar dalam menggunakan enkripsi?	3,60	Dalam penerapan enkripsi dapat berbeda – beda tiap unit terkait tidak adanya ukuran baku.	3	Masuk besa rkarena merupakan metode peangamanan yang dapat diatur dalam prosedur khusus	4	Penggunaan enkripsi merupakan hal menjadi kebuthan yang biasa dilakukan	12	Medium
V.12	Apakah Instansi Anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan,	3,20	Kunci enkripsi akan digunakan semena – mena oleh orang yang tidak bertangung jawab. Bahkan oleh orang yang memiliki tanggung	3	Pengelolaan kunci enkripsi masuk besar dan dapat diselesaikan dengan	3	Penentuan ppengelola dapat dilakukan dalam jangka 1 - 2 tahun	9	Medium

	termasuk siklus penggunaannya?		jawab tidak tahu apa yang perlu dilakukan untuk mengamankan kunci enkripsi terkait belum adanya prosedur untuk mengamankannya.		prosedur khusus				
V.13	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?	3,20	*Password* pengguna akan rentan terhadap ancaman dari pihak yang tidak bertanggung jawab terkait tidak adanya pengaturan terhadap standar *password* yang dianjurkan oleh aplikasi dan sistem maupun yang sesuai dengan standar yang	*3*	Penggunaan dan pengelolaan password dapat diatur dalam prosedur tertentu	*4*	Pergantian password dapat dilakukan secara rutin dalam waktu bulanan	12	Medium

			diterapkan organisasi.						
V.14	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?	3,20	Adanya pembobolan sistem dari pihak yang tidak berkepentingan untuk pengambilan data penting perusahaan.	4	Pengamanan yang buruk dapat menyebabkan kehilangan data dan kerugian finansial	3	Pembobolan terhadap sistem yang internal yang lemah bisa terjadi paling tidak dalam setahun	12	Medium
V.20	Apakah ada rekaman dan hasil analisa (jejak audit – *audit trail*) yang mengkonfirmasi bahwa antivirus telah dimutakhirkan secara rutin dan sistematis?	2,40	Tidak adanya data rekaman akan membuat organisasi tidak bisa belajar dari masalah masa lalu untuk menghadapi masalah yang	3	Termasuk besar dan dapat ditangani dengan penggunaan prosedur khusus	5	Data rekamanan dalam bentuk harian maupun bulanan jadi sangat sering terjadi jika tidak diterapkan	15	High

			terjadi sekarang dan memiliki kriteria yang sama dengan masalah masa lalu.						
V.21	Apakah adanya laporan penyerangan virus yang gagal/sukses ditindaklanjuti dan diselesaikan?	2,40	Ketidaktahuan status pengamanan oleh anti virus yang menyebabkan orgnaisasi tidak tahu ancaman yang menggangu asetnya.	3	Termasuk besar karena organisasi bisa tidak mengetahui anacaman yang mungkin menyerang, perlu dibuatkan prosedur tertentu	5	Ketika tidak diterapkan, maka kemungkinan keterjadiannya dalam hitungan mingguan sampai bulanan	15	High
V.23	Apakah setiap aplikasi yang ada memiliki spesifikasi keamanan yang diverifikasi/validasi	2,40	Tidak dilakukan verifikasi menyebabkan aplikasi yang digunakan kemungkinan tidak	3	Kehandalan aplikasi diragukan, dibuatkan prosedur	4	Dapat terjadi beberapa kali dalam setahun, terutama pada organisasi yang	12	Medium

	pada saat pengembangan dan uji-coba?		sesuai dengan tujuan yang diharapkan oleh organisasi.		verifikasi dan validasi		bergerak di sistem elektronik		
V.15	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?	2,00	Kemungkinan akses oleh pihak yang tidak diinginkan dan juga kebocoran data/informasi penting organisasi.	3	Masuk besar sehingga perlu prosedur khusus untuk mengatur pengelolaan login	4	Jika tidak diterapkan kemungkinan maka akan terjadi permasalahan beberapa kali dalam setahun	12	Medium
V.22	Apakah keseluruhan sistem (aplikasi, perangkat komputer dan jaringan) sudah menggunakan mekanisme sinkronisasi	2,00	Perbedaan waktu antar perangkat yang menyebabkan kesalahan dalam kegiatan opersional dan	2	Dampak tidak besar dan dapat diselesaikan dengan prosedur standar	1	Biasanya waktu jika terhubung dengan internte akan tersinkronisasi	2	Low

	waktu yang akurat, sesuai dengan standar yang ada?		perekaman kejadian.						
V.4	Apakah Instansi Anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?	1,40	Organisasi tidak pernah melakukan analisis kepatuhan yang menyebabkan organisasi tidak tahu penerapan standar apakah benar – benar dilakukan.	3	Masuk besar perlu dilakukan penegakan prosedur dan pengecekan	3	Analisis kepatuhan dilakukan sekali dalam setahun	9	Medium
V.8	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?	1,40	Akses yang tidak terekam menyebabkan kemungkinan tindakan pengaksesan kembali teulang dan dapat berakibat pada	2	Kecil, perlu dilakukan prosedur untuk memungkinkan pencatatan	4	Jika akses tidak terekam(terdeteksi) kemungkinana mengulang kegiatan yang sama beberapa kali	8	Medium

			kehilangan data penting organisasi.						
V.9	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	1,40	Tidak dilakukan pemeliharaan kepada log sehingga adanya log yang hilang maupun sudah tidak valid lagi sehingga tidak bisa dijadikan acuan analisis untuk menghadapi permasalahan yang terjadi.	3	Masuk besar, organisasi tidak bisa belajar dari data masa lalu	4	Jika tidak dilakukan penganalisaan rutin dari log akan menyebabkan tidak valid lagi sehingga tidak bisa dijadikan acuan analisis	12	Medium
V.17	Apakah Instansi Anda menerapkan bentuk pengamanan khusus	1,40	Adanya akses dari luar organisasi untuk melakukan kegiatan jahat seperti mencuri,	4	Akses dari luar dapat memungkinkan kerusakan maupun	4	Akan terjadi beberpa kali dala msetahun bila tidak dilakukan	16	High

	untuk melindungi akses dari luar Instansi?		merusak, dan penggunaan infrstruktur secara sewenang – wenang.		kehilangan aset organisasi yang berdampak pada finansial organisasi		pengamanan sesegera mungkin		
V.5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?	1,20	Adanya celah keamanan yang tidak terdeteksi dan dimanfatkan oleh pihak yang tidak bertanggung jawab untuk membobol sistem dan mengambil data/informasi penting organisasi.	3	Masuk besar, perlu diatasi dengan prosedur khusus	4	Jika celah kemanan tidak dipindai rutin , dalam jangka waktu tertentu maka dapat terjadi beberapa kali dalam setahun	12	Medium
V.16	Apakah Instansi Anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk	1,20	Adanya akses yang tak terdeteksi pada jaringan menyebabkan hilangnya data perusahaan dan	4	Pengamanan yang kurang akan menyebabkan pencurian data	4	Jika pengamanan tidak diterapkan maka akses yang bebas dapat terjadi sangat sering	16	High

	jaringan nirkabel) yang tidak resmi?		informasi penting lainnya.		penting organisasi				
V.3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan, yang dimutakhirkan sesuai perkembangan dan kebutuhan?	1,00	Terjadinya perbedaan konfigurasi keamanan sistem bagi keseluruhan aset komputer dan perangkat jaringan tiap unit organisasi. Yang menyebabkan perlindungan yang diberikan ada yang kuat dan ada yang lemah.	3	Termasuk besar, karena bisa adaketidak setaraan dalam penerapan perlindungan	4	Jika tidak adanya standar, penerapan akan seringa terjadi dalam setahun	12	Medium
V.10	Apakah Instansi Anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai	1,00	Terjadinya pencurian data dan pembobolan karena	3	Masuk besar karena enkripsi merupakan salah satu	3	Pencurian data akan dapat terjadi, namun dalam	9	Medium

	kebijakan pengelolaan yang ada?		pengamanan yang buruk terhadap aset informasi.		perlindungan terhadap data penting organisasi		kemungkinana yang sedang		
V.1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	0,80	Terjadinya upaya akses secara ilegal untuk menembus lapisan pengamanan yang mengambil data/informasi penting organisasi.	4	Berdampak besar karena akses lewat jaringan dapat melakukan tindakan berbahaya terhadap data dan informasi organisasi	4	Jika menggunakan pengamanan yang lemah, terjadinya akses secara ilegal dapat terjadi beberapa dala msetahun	16	High
V.2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?	0,80	Tidak adanya abtasan akses untuk tiap segmen instansi yang menyebabkan kemungkinan terjadinya penyelahgunaan	2	Adanya penggunaan yang tidak semestinya, perlu adanya prosedur yang membagi akses	3	Pensegmenasian dilakukan dalam periode tertentu	6	Medium

			oleh segmen yang tidak memiliki kepentingan.						
V.6	Apakah keseluruhan infrastruktur dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	0,80	Terjadinya kekurangan kapasitas infrastruktur untuk kebutuhan organisasi karena tidak adanya pengawasan infrastruktur secara berkala.	2	Kecil, perlu adanya prosedur pengelolaan dan pengawasan infrastruktur	4	Jika tidak dilakukan pengelolaan yang baik, dapat terjadi beberapa kali dalam setahun	8	Medium
V.7	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?	0,80	Dengan tidak dilakukan perekaman log otomatis maka perusahaan tidak memiliki data aktivitas dari	2	Kecil, perlu adanya prosedur yang memastikan pencatatan	5	Log disini berupa data pengguna yang bersifat harian dan mingguan sehingga kemungkinan keterjadian	10	Medium

			pengguna, kesalahan dan kegiatan pengamanan informasi yang dapat digunakan untuk keperluan audit dan pengembangan kedepannya.		dalam setiap pengelolaan		masalah sangat besar		
V.18	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?	0,80	Perangkat desktop dan server kurang mutahir sehingga terdapat banyak celah keamanan yang belum diperbaiki pada sistemnya.	3	Masuk besar karena memberikan masalah pada perangkat terkait adanya celah keamanan	4	Pemutahiran adalah proses yang biasa dilakukan untuk memperbaiki celah keamanan yang dapat dilakukan bebrapa kali dalam setahun	12	Medium

V.19	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?	0,20	Data pada *desktop* dan *server* terinfeksi sehingga hilang serta rusak. Menyebabkan sistem komputer menjadi lambat dan banyak program yang *error*.	4	Besar, karena virus dapat merusak data penting organisasi yang berdampak pada kerugian finansial	4	Jika tidak dilakukan penerapan pengamanan terhadap virus, penyerangan virus baru dalam setahun dapat terjadi beberapa kali	16	High